PREGÃO ELETRÔNICO

20/2023

CONTRATANTE (UASG)

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (113214)

OBJETO

Aquisição de licenças de uso perpétuas da Option Oracle Advanced Security – Processor Perpetual para segurança de banco de dados Oracle e implementação de criptografia de dados em repouso.

VALOR TOTAL DA CONTRATAÇÃO

R$ 540.620,50

DATA DA SESSÃO PÚBLICA

Dia 25/09/2023 às 09h (horário de Brasília)

CRITÉRIO DE JULGAMENTO:

menor preço por item

MODO DE DISPUTA:

fechado e aberto

PREFERÊNCIA ME/EPP/EQUIPARADAS

Sim

Baixe o APP Compras.gov.br
e apresente sua proposta!

Sumário

1. DO OBJETO 3
2. DA PARTICIPAÇÃO NA LICITAÇÃO 3
3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO 5
4. DO PREENCHIMENTO DA PROPOSTA 6
5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES . 7
6. DA FASE DE JULGAMENTO 11
7. DA FASE DE HABILITAÇÃO 13
8. DOS RECURSOS 15
9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES 16
10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO 18
11. DAS DISPOSIÇÕES GERAIS 18

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL

PREGÃO ELETRÔNICO Nº 20/2023

(Processo Administrativo n° 00058.008005/2022-39)

Torna-se público que A Agência Nacional de Aviação Civil, por meio da Gerência Técnica de Licitações e Contratos, sediado no SCS, Quadra 09, Lote C, Torre A - 3º Andar, Edifício Parque Cidade Corporate - Bairro Setor Comercial Sul, Brasília/DF, CEP 70308-200, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 2021, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é a contratação de solução de tecnologia da informação e comunicação visando à aquisição de licenças de uso perpétuas da Option Oracle Advanced Security – Processor Perpetual para segurança de banco de dados Oracle e implementação de criptografia de dados em repouso, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em único item.

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.1.2. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

2.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015, bem como para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.

2.6. Não poderão disputar esta licitação:

2.6.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

2.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.6.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.6.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.6.8. agente público do órgão ou entidade licitante;

2.6.9. pessoas jurídicas reunidas em consórcio;

2.6.10. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.6.11. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

2.7. O impedimento de que trata o item 2.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.6.2 e 2.6.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.9. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.10. O disposto nos itens 2.6.2 e 2.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.11. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

2.12. A vedação de que trata o item 2.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

3.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

3.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço, observado o disposto nos itens 7.1.1 e 7.11.1 deste Edital.

3.4. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

3.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.4.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

3.4.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

3.4.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

3.5. O fornecedor enquadrado como microempresa ou empresa de pequeno porte deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

3.5.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

3.5.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa ou empresa de pequeno porte.

3.6. A falsidade da declaração de que trata os itens 3.4 ou 3.5 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.7. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

3.8. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.9. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

3.10. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.10.1. a aplicação do 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; e

3.10.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.11. O valor final mínimo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

3.11.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

3.12. O valor final mínimo parametrizado na forma do item 3.10 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

3.13. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

3.14. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

4.1.1. valores unitário e total do item;

4.1.2. Marca;

4.1.3. Fabricante*;*

4.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

4.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

4.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

4.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

4.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

4.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional.

4.8. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

4.9. O prazo de validade da proposta não será inferior a **60 (sessenta)** dias**,** a contar da data de sua apresentação.

4.10. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

4.11. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

5.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

5.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

5.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.5. O lance deverá ser ofertado pelo valor unitário do item.

5.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

5.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

5.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 0,1% (um décimo por cento).

5.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.10. O procedimento seguirá de acordo com o modo de disputa adotado.

5.11. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

5.11.1. A etapa de lances da sessão pública terá duração de 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.

5.11.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.11.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.11.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

5.11.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

5.12. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.12.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

5.12.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.12.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.12.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.12.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.13. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “fechado e aberto”, poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço e os das propostas até 10% (dez por cento) superiores àquela, em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

5.13.1. Não havendo pelo menos 3 (três) propostas nas condições definidas no item 5.13, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

5.13.2. A etapa de lances da sessão pública terá duração de 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.

5.13.3. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.13.4. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.13.5. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

5.13.6. Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.

5.14. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.15. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.16. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.17. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

5.18. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

5.19. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.20. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

5.20.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

5.20.2. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.20.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

5.20.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

5.21. Será assegurado o direito de preferência previsto no artigo 3º da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010, nos seguintes termos:

5.21.1. Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:

5.21.1.1. bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

5.21.1.2. bens e serviços com tecnologia desenvolvida no País; e

5.21.1.3. bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Lei nº 8.248, de 1991.

5.21.2. Os licitantes classificados que estejam enquadrados no item 5.21.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

5.21.3. Caso a preferência não seja exercida na forma do item 5.21.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 5.21.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 5.21.1.3 caso esse direito não seja exercido.

5.21.4. As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

5.22. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

5.22.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

5.22.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

5.22.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

5.22.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

5.22.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

5.22.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

5.22.2.1. empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

5.22.2.2. empresas brasileiras;

5.22.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

5.22.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

5.23. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.23.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

5.23.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

5.23.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

5.23.4. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.23.5. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

5.24. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.6 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

6.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, *caput*)

6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

6.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os item 3.5 deste edital.

6.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

6.7. Será desclassificada a proposta vencedora que:

6.7.1. contiver vícios insanáveis;

6.7.2. não obedecer às especificações técnicas contidas no Termo de Referência;

6.7.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.7.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.8. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.8.1. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

6.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e

6.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.9. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

6.10. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação;

6.11. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

6.12. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

6.13. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

6.14. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

6.15. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

6.16. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

6.17. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

6.18. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

6.19. Caso o Termo de Referência exija prova de conceito, o licitante classificado em primeiro lugar será convocado pelo pregoeiro, com antecedência mínima de 10 (dez) dias úteis da data estabelecia para sua realização, para executá-la, visando aferir o atendimento dos requisitos e funcionalidades mínimas da solução de tecnologia da informação e comunicação, conforme disciplinado no Termo de Referência.

6.20. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a realização da prova de conceito.

6.21. A prova de conceito será realizada por equipe técnica designada, responsável pela aferição do atendimento dos itens estabelecidos, e poderá ser acompanhada pelos demais licitantes, mediante registro formal junto ao pregoeiro.

6.22. Todas as despesas decorrentes de participação ou acompanhamento da prova de conceito são de responsabilidade de cada um dos licitantes.

6.23. A equipe técnica elaborará relatório com o resultado da prova de conceito, informando se a solução apresentada pelo licitante provisoriamente classificado em primeiro lugar está ou não de acordo com os requisitos e funcionalidades estabelecidas.

6.24. Caso o relatório indique que a solução tecnológica está em conformidade com as especificações exigidas, o licitante será declarado vencedor do processo licitatório e, caso indique a não conformidade, o licitante será desclassificado do processo licitatório.

6.25. Caso o relatório indique que a solução foi aprovada com ressalvas, as não conformidades serão listadas e o licitante terá prazo de 3 (três) dias úteis, não prorrogáveis, a contar da data de ciência do respectivo relatório, para proceder aos ajustes necessários na solução e disponibilizá-la, para a realização de testes complementares, para aferição da correção ou não das inconformidades indicada.

6.26. Poderá ser considerada aprovada com ressalva a solução que, embora possua todas as funcionalidades previstas na Prova de Conceito (PoC), venha a apresentar falha durante o teste.

6.27. Caso o novo relatório indique a não conformidade da solução ajustada às especificações técnicas exigidas, a licitante será desclassificada do processo licitatório.

6.28. Não será aceita a proposta da licitante que tiver a prova de conceito rejeitada, que não a realizar ou que não a realizar nas condições estabelecidas no Termo de Referência.

6.29. No caso de desclassificação do licitante, o pregoeiro convocará o próximo licitante, obedecida a ordem de classificação, sucessivamente, até que um licitante cumpra os requisitos e funcionalidades previstas na PoC.

6.30. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

7. DA FASE DE HABILITAÇÃO

7.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

7.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

7.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

7.4. Os documentos exigidos para fins de habilitação poderão ser apresentados em original ou por cópia.

7.5. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

7.6. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

7.7. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

7.8. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.9. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.9.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

7.10. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, *caput*).

7.10.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (IN nº 3/2018, art. 7º, parágrafo único).

7.11. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.11.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 2h (duas horas), prorrogável por igual período, contado da solicitação do pregoeiro.

7.11.2. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço, observado o disposto no § 1º do art. 36 e no § 1º do art. 39 da *Instrução Normativa SEGES nº 73, de 30 de setembro de 2022.*

7.12. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

7.12.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.12.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

7.13. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

7.13.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.13.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

7.14. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.15. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 7.11.1.

7.16. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

7.17. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

7.18. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

8.3.1.1. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

8.3.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.3.3. na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

8.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6. Os recursos interpostos fora do prazo não serão conhecidos.

8.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

8.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico https://www.gov.br/anac/pt-br/acesso-a-informacao/licitacoes-e-contratos/licitacoes.

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

9.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

9.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo pregoeiro durante o certame;

9.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

9.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

9.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

9.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

9.1.2.4. deixar de apresentar amostra;

9.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

9.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

9.1.3.1. recusar-se, sem justificativa, a assinar o contrato, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

9.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

9.1.5. fraudar a licitação;

9.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

9.1.6.1. agir em conluio ou em desconformidade com a lei;

9.1.6.2. induzir deliberadamente a erro no julgamento;

9.1.6.3. apresentar amostra falsificada ou deteriorada;

9.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

9.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

9.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

9.2.1. advertência;

9.2.2. multa;

9.2.3. impedimento de licitar e contratar e

9.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

9.3. Na aplicação das sanções serão considerados:

9.3.1. a natureza e a gravidade da infração cometida.

9.3.2. as peculiaridades do caso concreto

9.3.3. as circunstâncias agravantes ou atenuantes

9.3.4. os danos que dela provierem para a Administração Pública

9.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de **20 (vinte) dias** úteis, a contar da comunicação oficial.

9.4.1. Para as infrações previstas nos itens 9.1.1, 9.1.2 e 9.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

9.4.2. Para as infrações previstas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, a multa será de 15% a 30% do valor do contrato licitado.

9.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

9.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.1, 9.1.2 e 9.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

9.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, bem como pelas infrações administrativas previstas nos itens 9.1.1, 9.1.2 e 9.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

9.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 9.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

9.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

9.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

9.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

9.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

9.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

10.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

10.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, exclusivamente, pelo e-mail: licitacao@anac.gov.br

10.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

10.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

10.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

11. DAS DISPOSIÇÕES GERAIS

11.1. Será divulgada ata da sessão pública no sistema eletrônico.

11.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

11.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

11.4. A homologação do resultado desta licitação não implicará direito à contratação.

11.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

11.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

11.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

11.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

11.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

11.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico www.gov.br/compras.

11.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

11.12. ANEXO I - Termo de Referência TR DIGITAL nº 9/2023 (9038649)

11.12.1.1. Anexos do Termo de Referência:

11.12.1.2. Anexo I - MODELO DE PROPOSTA COMERCIAL (8077254);

11.12.1.3. Anexo II - ORDEM DE FORNECIMENTO DE BENS (8071343);

11.12.1.4. Anexo III - TERMO DE RECEBIMENTO PROVISÓRIO (8071211);

11.12.1.5. Anexo IV - TERMO DE RECEBIMENTO DEFINITIVO (8077012);

11.12.1.6. Anexo V - TERMO DE COMPROMISSO (8071135);

11.12.1.7. Anexo VI - TERMO DE CIÊNCIA (8071157);

11.12.1.8. Apêndice do Anexo I – Estudo Técnico Preliminar

11.13. Anexo II - Minuta do termo de Contrato (9077365)

Brasília, 13 de setembro de 2023

Aderson de Lima Calazans

Pregoeiro Oficial

Aderson de Lima Calazans

Assinado de forma digital por Aderson de Lima Calazans
Dados: 2023.09.11 13:36:09 -03'00'

Termo de Referência 9/2023

Informações Básicas

Número do TR	UASG	Editado por	Atualizado em
9/2023	113214-AGENCIA NACIONAL DE AVIACAO CIVIL - ANAC	FELIPE SANTOS SARMANHO	01/09/2023 17:01 (v 5.2)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação.	46/2023	00058.008005/2022-39

1. Definição do objeto

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de licenças de uso perpétuas da Option Oracle Advanced Security - Processor Perpetual para segurança de banco de dados Oracle e implementação de criptografia de dados em repouso, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

Tabela 1 - Bens e serviços que compõem a solução.

ITEM	ESPECIFICAÇÃO	CATMAT	UNIDADE DE MEDIDA	CÓD. PMC-TIC	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Licença de Software - Oracle Advanced Security	27464	Unidade	OR-007	7	R$ 77.231,50	R$ 540.620,50

1.2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.3. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

1.4. O prazo de vigência da contratação é de 12 (doze) meses contados da assinatura do contrato, na forma do artigo 105 da Lei n° 14.133, de 2021.

1.5. As vedações elencadas no art. 5º, bem como os dispositivos contidos no anexo I, da IN SGD nº 94, de 2022, foram observados durante o processo de elaboração do Termo de Referência.

1.6. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. Fundamentação da contratação

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

2.2. A presente contratação justifica-se pela necessidade de aplicação de medidas de controle de segurança da informação quanto ao armazenamento de dados em repouso em banco de dados na tecnologia Oracle, utilizado na ANAC.

2.3. É fato amplamente conhecido que a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), em vigor desde meados de 2020, prevê uma série de regras e práticas que buscam promover a proteção aos dados pessoais de todo cidadão em território brasileiro.

2.4. Neste contexto, todas as organizações, públicas ou privadas, devem adotar medidas diversas em relação à coleta, uso e compartilhamento dos dados pessoais por ela manipulados, seja em meio físico ou digital.

2.4. Especificamente, o artigo 46 da LGPD determina que os agentes de tratamento (coordenador e/ou operador) devem implementar controles internos para 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.

2.6. A Gerência Técnica de Gestão da Informação (GTGI) iniciou esforços para adequação da ANAC à LGPD. Dentre as principais iniciativas, destaca-se a produção de Relatórios de Inventário de Dados Pessoais que descrevem os procedimentos e resultados obtidos a partir de análise de bases que armazenam os dados da Agência.

2.7. Até o momento, as seguintes bases de dados foram analisadas:

Tabela 1- Inventário de Dados Pessoais realizado pela GTGI/SAF.

Base de dados/Sistema	**Relatório de Diagnóstico e Recomendações**	**Tecnologia**
AERONAUTA	Processo SEI nº 00058.011646/2021-90	Oracle
HABILITAÇÃO	Processo SEI nº 00058.021617/2021-36	Oracle
SISHAB	Processo SEI nº 00058.021766/2021-03	Oracle
CMA	Processo SEI nº 00058.021894/2021-49	SQL Server
SISMEDCRED	Processo SEI nº 00058.039351/2021-88	Oracle
Moodle	Processo SEI nº 00058.051198/2021-67	PostgreSQL
SIGRH	Processo SEI nº 00058.053008/2021-46	PostgreSQL

2.8. Observou-se que todos os relatórios presentes na Tabela 1 contêm uma seção intitulada "Recomendações" a qual apresenta orientações em relação à procedimentos e ações para cada dado pessoal ou conjunto de dados analisado. Tais orientações podem ser a eliminação do tratamento (coleta, processamento, armazenamento etc.) de dados sem fundamentação legal ou desnecessários, existência do prazo de guarda, ou até mesmo pseudonimização, anonimização ou criptografia.

2.9. Quanto a recomendação de criptografia, verifica-se que há sempre a mesma motivação, divergindo apenas quanto ao nome da base de dados e a quantidade de tabelas a serem criptografadas. O trecho abaixo foi retirado do documento SEI nº 5411816 que discorre sobre a base de dados do sistema Aeronauta:

> ***"A criptografia consiste em um processo por meio do qual um dado perde sua legibilidade. Desta forma, caso seja vazado, seu conteúdo não será lido com clareza, nitidez. Não se trata de uma medida de mitigação, mas de contingência. Em outras palavras, não impede que um vazamento ocorra, mas que caso ocorra os respectivos dados sejam inúteis. Esta técnica é totalmente pertinente e recomendada para a base de dados AERONAUTA, em função da grande quantidade de dados pessoais que ela armazena, alguns deles inclusive qualificados como sensíveis de acordo com a LGPD. Mais especificamente para as 30 tabelas que foram identificadas e sinalizadas por conterem dados sensíveis ou dados pessoais diretos, em um total de 100 existentes na base de dados.***
>
> ***Importante salientar que há diversos controles de segurança implementados na ANAC como um todo (firewalls, antivírus, monitoramento e análise de rede, backup, ações de conscientização de servidores e colaboradores, dentre outras) que resultam em um elevado nível de segurança para as bases de dados como um todo.***
>
> ***Mas apesar de todos os aspectos positivos acima descritos face ao elevado nível de adequação à LGPD, visando aumentar ainda mais a proteção aos direitos e liberdades fundamentais dos titulares dos dados, bem como diminuir riscos de violação de privacidade, recomenda-se criptografar as informações destas tabelas com dados sensíveis e dados pessoais diretos. Para as tabelas com dados pessoais indiretos, em função do esforço adicional de correlação de informações que seria necessário para identificar o titular à que pertencem, optou-se por não recomendar criptografá-las.***
>
> ***Conclui-se, assim, por recomendar que as tabelas com dados pessoais sensíveis e dados pessoais diretos sejam criptografadas. Importante salientar que se trata de uma recomendação e não uma medida imprescindível."***

2.10. Diante do Cenário apresentado, a STI elaborou Documento Oficial de Demanda SEI nº 6805759 com a seguinte necessidade de contratação:

> *"Aquisição de licenças de uso perpétuas da Option Oracle Advanced Security - Processor Perpetual para segurança de banco de dados Oracle e implementação de criptografia de dados em repouso."*

2.11. Apesar do assunto ser analisado em maior profundidade em seções futuras deste Estudo Técnico, destacam-se dois pontos importantes. O primeiro é relacionado ao nível de aplicação de criptografia, especificamente, dados em repouso.
O segundo diz respeito a plataforma tecnológica na qual os dados sensíveis estão armazenados, em exclusivo, o Sistema Gerenciador de Banco de Dados (SGBD) Oracle Database Enterprise (designado como "SGBD Oracle" neste Estudo para fins de simplificação).

2.12. A criptografia de dados em repouso consiste em cifrar dados diretamente no sistema de arquivos (storage ou disco) no qual são armazenados. Este recurso representa uma importante medida de segurança para dificultar acesso não autorizado a dados sensíveis caso ocorra furto de arquivos do SGBD (datafiles) ou arquivos de backup nos quais estão armazenados. Entretanto, destaca-se que este tipo de criptografia não possui atuação sobre os dados em trânsito na rede ou dados manipulados em memória por servidores e/ou clientes (aplicações, sistemas, usuários e outros).

2.13. No que tange a plataforma tecnológica, aponta-se que, em resumo, um SGBD é um software responsável por prover acesso, armazenamento, persistência, manipulação e organização dos dados. a diversos clientes (aplicações, sistemas, usuários e outros) de forma a garantir segurança, desempenho e consistência.

2.14. A ANAC utiliza quatro SGBDs diferentes: SQL Server, Oracle, PostGres e Mysql. Levantamento realizado em fevereiro de 2022 constatou a seguinte distribuição de dados em SGBDs na Agência (em termos de armazenamento):

Tabela 2 -Levantamento sobre SGBDs da ANAC.

SGBD	**Servidores**	**Armazenamento (TB)[1,2]**	**Parcela Armazenamento (%)**
Oracle	9	10	13,89
SQL Server	51	60	83,33
PostGres	14	2	2,78
Mysql	1	0,02	0,03
Total	**75**	**72**	-

> *[1]Os valores presentes representam totais brutos de armazenamento dos servidores virtuais (VMs) de bancos de dados e incluem o sistema operacional, arquivos temporários e demais presentes em discos dos ambientes de produção, validação e homologação da Agência.*

> [2]*Ademais, aponta-se que houve erro de digitação no item 4.2 do Documento de Oficialização de Demanda (DOD) 6805759 no qual as quantidades de servidores e total de armazenamento constam como 75, mas deveriam ser 75 e 72 TB, respectivamente.*

2.15. Com base em critérios de importância e criticidade, a STI/ANAC priorizou esforços para endereçar criptografia de dados em repouso em SGDBs através dos seguintes projetos previstos no PDTIC 2022-2023 (SEI nº 7410475):

Tabela 3 - Projetos relacionados a implementação de criptografia de dados em repouso presentes no PDTIC 2022-2023

#	Plano Interno	Nome Projeto	Objetivo estratégico atrelado	Início planejado	Término Planejado
Contratações Infraestrutura					
4	2ATDTI22070	Contratação de Criptografia de dados pessoais em repouso	E11: Aprimorar a gestão da informação para a tomada de decisão	jul/22	mar/23
Estruturantes Infraestrutura (GEIT)					
1	2XTDTI22037	Atualizar a infraestrutura do serviço de banco de dados SQL Server	E11: Aprimorar a gestão da informação para a tomada de decisão	fev/22	mai/22
15	2XTDTI22051	Criptografia de dados pessoais em repouso para SGBD SQL Server, PostgreSQL, MySQL	OE11: Aprimorar a gestão da informação para a tomada de decisão	out/22	dez/22
22	2XTDTI22041	Implantação da Criptografia em repouso	E13: Promover a alocação de recursos de forma estratégica e efetiva	nov/23	abr/24

2.16. Verifica-se que a previsão de projetos citados na Tabela 3 foi baseada na premissa presente no item 4.5 do Documento Oficial de Demanda SEI nº 6805759:

> *"4.5. Para os SGBD com tecnologias Microsoft SQL Server, PostgreSQL e MySQL, a STI já identificou a possibilidade de implementação da criptografia de dados em repouso com os recursos existentes. Também já iniciou as ações e projetos necessários para realizar a criptografia dos dados nessas tecnologias. Contudo, para o SGBD na tecnologia Oracle, a solução atualmente contratada na ANAC não dispõe do mecanismo apropriado para criptografia de dados em repouso. Sendo assim, faz-se necessária a aquisição de licenciamento de software de componente adicional, também chamado "option", para implementar o referido mecanismo de segurança."*

2.17. Portanto, enfatiza-se que o projeto 2ATDTI22070 ("Contratação de Criptografia de dados pessoais em repouso"), o qual deu origem ao DOD SEI nº 6805759 e a este Estudo Técnico, possui escopo de análise limitado ao SGBD Oracle, uma vez que a implementação de criptografia de dados em repouso nos demais SGBDs (SQL Server, PostgreSQL e MySQL) foi ou será endereçada em projetos diferentes, tais como: 2XTDTI22037 ("Atualizar a infraestrutura do serviço de banco de dados SQL Server") e 2XTDTI22051 ("Criptografia de dados pessoais em repouso para SGBD SQL Server, PostgreSQL, MySQL").

2.18. Para fins de completude, o projeto 2XTDTI22041 ("Implantação da Criptografia em repouso") tem como objeto a implementação da solução indicada ao fim deste Estudo Técnico. Sob tal ponto de vista, reforça-se que a criptografia de dados em repouso não é citada pela LGPD e não previne todos os tipos de ataques. No entanto, caso as barreiras de segurança de sistemas operacionais de servidores ou dispositivos de armazenamento nos quais dados sensíveis residam sejam violadas, a tal recuso irá impedir a visualização dos mesmos em formato legível por pessoas não autorizadas.

2.19. Logo, a STI/ANAC entende que, além de criptografia de dados em repouso em SGBDs, várias outras medidas técnicas e gerenciais, que não estão no escopo de Estudo Técnico, precisam ser adotadas para garantir atendimento aos requisitos provenientes da LGPD no que tange aos sistemas de informação da Agência.

2.20. O objeto da contratação está previsto no Plano de Contratações Anual 2023, conforme detalhamento a seguir:

I) ID PCA no PNCP: 07947821000189-0-000001/2023

II) Data de publicação no PNCP: 13/02/2023

III) Id do item no PCA: 97

IV) Classe/Grupo: 165 - SERVICOS PARA A INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃOE COMUNICAÇÃO (TIC), NAO CLASSIFICADOS EM OUTROS TÓPICOS

V) Identificador da Futura Contratação: 113214-46/2023

2.21. O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2023 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2022-2023 da Agência Nacional de Aviação Civil, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
Plano	**Objetivos Estratégicos**
Plano Estratégico da ANAC - 2020-2026	OE11: Aprimorar a gestão da informação para a tomada de decisão
	OE2: Garantir a segurança da aviação civil
	OE6: Fortalecer a gestão de riscos no sistema de aviação civil e a cultura de segurança
	OE13: Promover a alocação de recursos de forma estratégica e efetiva
Estratégia de Governo Digital - 2020 a 2022	Objetivo 10: Implementação da Lei Geral de Proteção de Dados - LGPD no Governo
	Objetivo 1: Oferta de serviços públicos digitais
	Objetivo 11: Garantia da segurança das plataformas de governo digital e de missão crítica

ALINHAMENTO AO PDTIC 2022-2023	
ID	**Ação do PDTIC**
2ATDTI22070	Contratação de Criptografia de dados pessoais em repouso

ALINHAMENTO AO PAC 2022	
Item	**Descrição**

144	Contratação de Criptografia de dados pessoais em repouso

2.22. Por tratar de solução de TI de suporte a sistemas de informação que contemplam a oferta de serviços públicos digitais, é importante ressaltar que estes sistemas de informação já se encontram integrados à Plataforma Gov.br, ou que tem planejamento de integração, conforme PDTI-ANAC 2022-2023, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, e suas atualizações.

2.23. Termo de Referência elaborado tendo como base o modelo da AGU para "Compras TIC" aderente à Lei nº14.133/2021, disponível em: https://www.gov.br/agu/pt-br/composicao/cgu/cgu/modelos/licitacoesecontratos/14133/modelos-da-lei-14-133-21-para-bens-e-servicos-de-tic, versão de 19/04/2023.

3. Descrição da solução

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

3.1. A descrição da solução como um todo encontra-se pormenorizada no Estudo Técnico Preliminar, apêndice deste Termo de Referência.

3.2. A solução de TIC consiste na aquisição de licenças de uso software denominado Oracle Advanced Security para atender às necessidades de criptografia de dados em repouso instalados em servidores de banco de dados da tecnologia Oracle para reduzir o risco de exposição de dados sensíveis, inclusive dados pessoais, conforme orientações da LGPD.

3.3. O quantitativo necessários de licenças é de 7 (sete), e para chegar a este quantitativo a equipe de planejamento da contratação fez o levantamento da infraestrutura de servidores de banco de dados na tecnologia Oracle instaladas na ANAC que precisam dessa proteção de criptografia.

3.4. A equipe de planejamento da contratação orienta pela contratação da solução Oracle Advanced Security, pois, conforme demonstrado ao longo dos itens 8, 9 e 10 deste Estudo Técnico Preliminar, é a única opção que atende aos requisitos propostos e é compatível com o ambiente tecnológico da ANAC.

3.5. Cumpre assinalar que todos os servidores de SGBD Oracle estão hospedados em salas seguras localizadas dentro da ANAC. Neste contexto, a única forma de contratação da solução Oracle Advanced Security é a aquisição de licenças de direito de uso perpétuo.

3.6. O serviço de suporte técnico por parte da fabricante e direito de atualização são essenciais para atendimento das requisitos levantados, especialmente no que diz respeito ao correção de eventuais falhas, erros ou bugs de código, assim como, apoio técnico do fabricante para solução de problemas avançados que podem comprometer a integridade e disponibilidade dos dados.

3.7. Além disso, como o OAS faz parte do software Oracle Database Enterprise, a não contratação do direito de atualização para o primeiro impedira atualização do SGBD nos servidores que compõe o escopo deste Estudo Técnico. Vale lembrar que há previsão de projeto identificado como 2XTDTI22056 no PDTI 2022-2023 cuja descrição é "Atualizar infraestrutura de Oracle para versão mais recente".

3.8. A licença Oracle Advanced Security foi precificada juntamente com serviço de suporte e direito de atualização por 12 meses como item único no Acordo Corporativo N. 10/2021 firmado entre SGD/ME e Oracle (SEI nº 7379867). Dessa forma, não se vislumbra possibilidade de parcelamento da solução.

3.9. De acordo com o Requisitos de Negócio 2 (descrito no Estudo Técnico Preliminar), a solução deve ser contratada para os bancos de dados que possuem dados pessoais armazenados.

3.10. Como pode ser visto no email SEI nº 7375362, em pesquisa realizada em março de 2022, a Gerência de Sistemas de Informação (GESI/ANAC), área responsável pela governança da dados da Agência, listou os servidores que se encontram na situação descrita no item anterior:

Tabela 4: Servidores de SGBDs Oracle que possuem dados pessoais na ANAC

						Quantidade de Núcleos	**Quantidade de**

ID	Servidor	TCP/IP	Versão	Instância	Banco	de Processamento	Memória (GB)
1	SPBDF1034	10.161.50.206	12.2.0.1.0	PRODUCAO1	PRODUCAO	4	20
2	SPBDF1035	10.161.50.208	12.2.0.1.0	PRODUCAO2		4	20
3	SPBDF1087	10.161.50.202	11.2.0.4.0	PRODDW	PRODDW	2	16
4	SHBDF1014	10.161.50.29	12.2.0.1.0	VALIDACAO	VALIDACAO	4	16
				HOMOLOG	HOMOLOG		
				OPHOMOLG	OPHOMOLG		
				TREINA	TREINA		

3.11. O resumo de cada banco de dados segue abaixo:

1. **PRODUCAO:** O banco PRODUCAO está hospedado no Oracle Database Enterprise 12c e é utilizado pelas aplicações desenvolvidas através do Oracle APEX, tais como: ANAC+, Santos Dumond e outras. É o único da que utiliza tecnologia RAC (Real Application Clusters) para suportar funcionamento de mais de um servidor (SPBDF1034 e SPBDF1035) de forma paralela com objetivo de prover alta disponibilidade e desempenho.
2. **PRODW:** O banco PRODDW está hospedado no Oracle Database Enterprise 11c (servidor SPBDF1087) e é utilizado para armazenar dados negociais gerados por rotinas de ETL (Extract, transform and load) de ferramentas tal como o Power Center.
3. **VALIDAÇÃO:** O servidor SHBDF1014 contém 4 bancos de dados, VALIDACAO, HOMOLOG, OPHOMOLOG e TREINA, hospedados no Oracle Database Enterprise 12c.. O VALIDACAO representa uma cópia reduzida da base PROD (SPBDF1088) enquanto o HOMOLOG é uma cópia integral da base da base PRODUCAO (SPBDF1034 e SPBDF1035). Ambos são utilizados para realização de testes de recursos e atualizações das aplicações e sistemas antes que sejam submetido(a)s para o ambiente de produção.
4. Quanto ao OPHOMOLOG e ao TREINA, cabe ressaltar que o primeiro representa o banco de homologação do sistema IBM Open Pages (sistema de Fiscalização Integrada) e o segundo acomoda dados necessários para um ambiente de treinamento de aplicações.

4. Requisitos da contratação

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio

4.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

4.2. A solução deve ser contratada para todos os bancos de dados do fabricante Oracle que possuem dados pessoais elegíveis de tratamento pela LGPD.

4.3. Dados pessoais sensíveis não podem ser acessados fora do banco de dados e/ou por usuários sem privilégios adequados.

4.4. A solução deve permitir implementação de criptografia em repouso sem necessidade de alteração nas aplicações ou sistemas.

4.5. A solução não deve impactar de forma significativa a performance do acesso aos dados pelos sistemas e demais componentes do ponto de vista do usuário.

4.6. Não poderá haver perda ou corrompimento de dados criptografados.

4.7. A solução deve ter suporte e garantia do fabricante.

Requisitos Técnicos

4.8. A solução deve ter integração e compatibilidade com as seguintes ferramentas Oracle utilizados pela ANAC:

4.8.1. Oracle Database Enterprise - Versão 12c ou superior;

4.8.2. Oracle Recovery manager (RMAN) - Versão 12c ou superior;

4.8.3. Oracle RAC (Real Application Clusters) - Versão 12c ou superior;

4.8.4. Tuning Pack - Versão 12c ou superior;

4.8.5. Diagnostic Pack - Versão 12c ou superior;

4.8.6. APEX (Oracle Application Express) - Versão 19.1 ou superior.

4.9. A solução deve ser capaz de encriptar/decriptar qualquer tipo de dado suportado pelo SGBD Oracle, tais como: números, datas, texto e outros.

4.10. A solução deve oferecer segurança contra tentativas de leitura de dados sensíveis a partir do sistema operacional de servidores Oracle, arquivos de backup (físicos e exports) ou furto de dispositivos físicos de armazenamento.

4.11. A solução deve utilizar de algoritmos de criptografia padrão de mercado e compatíveis com ePING ("Tabela 6 - Criptografa" do item 2.2 "Especificações Técnicas" do Documento SEI-ANAC nº 7380334).

4.12. A solução não pode exigir nenhum tipo de alteração ou modificação no sistemas ou aplicações que utilizam o SGBD Oracle.

4.13. A solução deve possuir processos de criptografia e descriptografia automatizados (sem necessidade de interferência dos sistemas ou aplicações).

4.14. A solução deve possuir mecanismo de armazenamento de chaves criptográficas históricas de forma a permitir rotação das mesmas.

4.15. A solução deve ser capaz de criptografar dados históricos forma online, ou seja, sem necessidade de desligamento do SGBD Oracle.

Requisitos de Capacitação

4.16. Não foi identificado nenhum requisito adicional de capacitação dado que os produtos da Oracle já são utilizados na Agência há pelo menos 10 anos.

4.17. A solução de banco de Oracle na ANAC é administrar e operada principalmente por colaboradores terceirizados que prestam serviço especializado e que, portanto, já comprovam a qualificação técnica e capacitações em razão daquele contrato.

4.18. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação.

Requisitos Legais

4.19. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

4.20. Lei nº 8.248, de 23 de outubro de 1991 – Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências;

4.21. Decreto nº 3.505, de 13 de junho de 2000 – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

4.22. Decreto nº 3.555, de 08 de agosto de 2000 – Aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns;

4.23. Lei nº 12.846, de 1º de agosto de 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;

4.24. Lei Complementar nº 123, de 2006 – Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte; altera dispositivos das Leis no 8.212 e 8.213, ambas de 24 de julho de 1991, da Consolidação das Leis do Trabalho - CLT, aprovada pelo Decreto-Lei no 5.452, de 1o de maio de 1943, da Lei no 10.189, de 14 de fevereiro de 2001, da Lei Complementar no 63, de 11 de janeiro de 1990; e revoga as Leis no 9.317, de 5 de dezembro de 1996, e 9.841, de 5 de outubro de 1999;

4.25. Lei nº 11.077, de 30 de dezembro de 2004 – Altera a Lei nº 8.248, de 23 de outubro de 1991, a Lei nº 8.387, de 30 de dezembro de 1991, e a Lei nº 10.176, de 11 de janeiro de 2001, dispondo sobre a capacitação e competitividade do setor de informática e automação e dá outras providências;

4.26. Decreto nº 10.818, de 27 de setembro de 2021 – Regulamenta o disposto no art. 20 da Lei nº 14.133, de 1º de abril de 2021, para estabelecer o enquadramento dos bens de consumo adquiridos para suprir as demandas das estruturas da administração pública federal nas categorias de qualidade comum e de luxo;

4.27. Decreto nº 11.246, de 27 de outubro de 2022 – Regulamenta o disposto no § 3º do art. 8º da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre as regras para a atuação do agente de contratação e da equipe de apoio, o funcionamento da comissão de contratação e a atuação dos gestores e fiscais de contratos, no âmbito da administração pública federal direta, autárquica e fundacional;

4.28. Decreto nº 10.024, de 20 de setembro de 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;

4.29. Decreto nº 7.174, de 12 de maio de 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;

4.30. Decreto nº 7.845, de 14 de novembro de 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;

4.31. Instrução Normativa ANAC nº 128, de 6 de novembro de 2018 – Institui a Política de Segurança da Informação no âmbito da Agência Nacional de Aviação Civil - ANAC;

4.32. Instrução Normativa ANAC nº 172, de 2 de agosto de 2021 – Aprova a Política de Proteção de Dados Pessoais - PoPD no âmbito da Agência Nacional de Aviação Civil - ANAC.

Requisitos de Manutenção

4.33. Devido às características da solução, há necessidade de realização de manutenções corretivas e evolutiva pela Contratada ou Fabricante, visando à manutenção da disponibilidade da solução.

4.34. A fabricante deverá fornecer correções, patches, atualizações e novas versões tão logo estas se tornem disponíveis.

4.35. Caberá a CONTRATANTE a decisão por migrar ou permanecer em determinada versão de software, bem como aplicar ou não as atualizações de software, no caso em que estas novas versões/atualizações não forem obrigatórias para continuidade do suporte.

Requisitos Temporais

4.36. A Entrega das licenças adquiridas deverá ser efetivada no prazo máximo de 20 dias corridos, a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

4.37. Os prazos para o início da prestação dos serviços e demais atividades necessárias para execução contratual estão previstas nos itens 6 - MODELO DE EXECUÇÃO DO CONTRATO e 7 - MODELO DE GESTÃO DO CONTRATO.

4.38. Não há outros requisitos temporais relevantes.

Requisitos de Segurança da Informação e Privacidade

4.39. A CONTRATADA deverá atender às normas acerca de conformidade técnica e de integridade de dados na Administração Pública Federal, assim como atender às normas e aos procedimentos de que trata a Instrução Normativa/ANAC nº 128, de 6 de novembro de 2018, relativos à Política de Segurança da Informação e Comunicações - PoSIC - no âmbito da Agência Nacional de Aviação Civil – ANAC, sem prejuízo dos demais atos, documentos e normativos expedidos e publicados pela Administração Pública Federal, bem como pela própria ANAC relativos ao sigilo, à segurança e à privacidade das informações e comunicações, além dos respectivos Termos de Compromisso e de Ciência previstos nas alíneas “a” e “b” do inciso V do art. 18 da Instrução Normativa nº 1, de 4 de abril de 2019, da Secretaria de Governo Digital do Ministério da Economia.

4.40. A CONTRATADA deverá atender a, no mínimo, os seguintes requisitos previstos na Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709 de 14 de agosto de 2018:

1. **Recursos em Versões Comprovadamente Seguras e Atualizadas**: Utilizar recursos de segurança da informação e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e em versões comprovadamente seguras e atualizadas, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a CONTRATANTE está exposta, considerando os critérios de aceitabilidade de riscos definidos pela CONTRATANTE.
2. **Reportar Incidentes**: Reportar de imediato à CONTRATANTE incidentes que envolvam vazamento de dados, indisponibilidade ou comprometimento da informação relacionados à Solução de TIC adquirida.
3. **Termo de Compromisso e Ciência**: Implementar e manter controles e procedimentos específicos para assegurar completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da contratada venham a tomar conhecimento em razão da execução do contrato, de forma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem o uso dos dados somente para as finalidades previstas em contrato e as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da Solução de TIC, cumprindo e fazendo cumprir o disposto nos Termo de Compromisso e Termo(s) de Ciência firmados respectivamente, pelo representante legal e pelo(s) empregado(s) da contratada.
4. **Descarte Seguro**: Definir e executar procedimento de descarte seguro dos dados pessoais ou sigilosos da CONTRATANTE ao encerrar a execução do contrato.
5. **Revogação de Privilégios**: Comunicar à CONTRATANTE, de imediato, a ocorrência de transferência, remanejamento ou demissão de funcionário, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da CONTRATANTE, porventura colocados à disposição para realização dos serviços contratados.
6. **Utilização de Serviços de Terceiros**: Informar e obter a anuência do órgão CONTRATANTE sobre a utilização de serviços de terceiros (como suporte técnico etc.) para sustentar ou viabilizar o funcionamento da Solução de TIC contratada.
7. **Tratamento de incidentes de segurança da informação e privacidade**: Realizar em conjunto com a CONTRATANTE, ou com outros órgãos por ela indicados, ações de tratamento de incidentes de segurança da informação e privacidade relacionados ao objeto do contrato, bem como apoiar essas ações com o monitoramento e o envio de informações tempestivos.
8. Toda informação confidencial disponibilizada em razão da contratação, seja ela armazenada em meios físico, magnético ou eletrônico, deverá ser devolvida nas seguintes hipóteses:
    8.1. Término ou rompimento do Contrato;
    8.2. Solicitação da ANAC.
9. A CONTRATADA deverá manter a ANAC informada, formal e tempestivamente, sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados;
10. A CONTRATADA deverá credenciar seus profissionais junto à ANAC, caso seja necessário acesso às instalações e infraestrutura de TI da ANAC para prestação de serviços de suporte.

Requisitos Sociais, Ambientais e Culturais

4.41. Toda a documentação fornecida pela CONTRATADA deverá ser fornecido em mídia eletrônica (digital) e preferencialmente na língua portuguesa do Brasil, sendo aceito, em caráter excepcional, documentos na língua inglesa.

4.42. Qualquer atendimento presencial, quando necessário, realizado pela CONTRATADA deverá ser feito por técnicos que possuem domínio da língua portuguesa ou acompanhados de intérprete para essa língua.

4.43. As comunicações realizadas (e-mails, conferências, entre outros) entre CONTRATANTE e CONTRATADA deverão ocorrer na língua portuguesa.

Requisitos de Arquitetura Tecnológica

4.44. Não há requisitos de arquitetura tecnológica a ser relacionado, uma vez que a solução consiste em componente padronizado que faz parte do software Oracle Database Enterprise e já está instalada na ANAC.

Requisitos de Projeto e de Implementação

4.45. Não se aplica a esta contratação, uma vez que a solução consiste em componente padronizado que faz parte do software Oracle Database Enterprise e já está instalada na ANAC.

Requisitos de Implantação

4.46. A implantação da solução está prevista como projeto 2XTDTI22041 no PDTIC 2022-2023 com o título "Implantação da Criptografia em repouso" e será executado no escopo do Contrato nº 21/ANAC/2021 (Global Web) com execução prevista no primeiro semestre de 2023, após a conclusão deste processo de contratação.

Requisitos de Garantia, Manutenção e Assistência Técnica

4.47. O prazo de garantia contratual dos bens, complementar à garantia legal, será de, no mínimo, 12 (doze) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

4.48. Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o fornecedor deverá complementar a garantia do bem ofertado pelo período restante.

4.49. A manutenção deverá garantir a atualização de versões dos softwares.

4.50. O serviço de suporte técnico deverá ser via telefone, e-mail ou ferramenta fornecida pela CONTRATADA, pelo período contratado, disponibilizando o atendimento no regime 24/7/365 (24 horas por dia, 7 dias por semana,365 dias no ano) ininterruptamente.

4.51. O serviço de suporte técnico deverá garantir o funcionamento, manutenção e fornecimento de novas versões e modificações (updates e upgrades) para os produtos contratados.

4.52. Deverá, ainda, ser informada a CONTRATANTE página na Internet, do fabricante do(s) software(s), onde estejam disponíveis, últimas versões do(s) software(s) e informações sobre correções e reporte de problemas, sem restrições de acesso público ou via cadastramento de pessoas autorizadas para o acesso. A página deverá conter, ainda, documentação técnica detalhada do(s) software(s) contratado(s).

4.53. A garantia técnica deverá ser realizada pelo próprio fabricante com capacidade de atendimento remoto.

4.54. Todo software utilizado para o perfeito desempenho das funções dos produtos deverá ser assegurado durante todo o período de garantia, com correção de todas as possíveis falhas apresentadas e atualizações nas versões dos softwares, ocorridas no período, sem acarretar ônus para a Agência Nacional de Aviação Civil.

4.55. Fazem parte da garantia e terão seus custos cobertos pelo contrato as reprogramações dos sistemas que não estejam em funcionamento adequado, correções de falhas de software (bugs), bem como o acesso a versões atualizadas de módulos de software (updates, firmware, etc.) disponibilizadas pelo fabricante da solução durante o prazo contratado.

4.56. O serviço de garantia deverá contemplar as manutenções corretivas e o saneamento de todos os vícios e defeitos que a solução porventura venha apresentar.

Requisitos de Experiência Profissional

4.57. Não serão exigidos requisitos de experiência profissional para a presente a contratação.

Requisitos de Formação da Equipe

4.58. Não serão exigidos requisitos de formação da equipe para a presente a contratação.

4.59. A equipe responsável pela operação da solução está atualmente vinculada ao Contrato nº 21/ANAC/21 (Global Web) e já possui requisitos de formação devidamente estabelecidos e validados.

Requisitos de Metodologia de Trabalho

4.60. O fornecimento das licenças de software está condicionado ao recebimento pelo Contratado de Ordem de fornecimento de Bens (OFB) emitida pela Contratante.

4.61. A OFB indicará o tipo de licença de software, a quantidade e a localidade na qual as licenças deverão ser entregues.

4.62. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica e por via telefônica.

4.63. O andamento do fornecimento das licenças de software dever ser acompanhado pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

Requisitos de Segurança da Informação e Privacidade

4.64. A CONTRATADA deverá atender às normas acerca de conformidade técnica e de integridade de dados na Administração Pública Federal, assim como atender às normas e aos procedimentos de que trata a Instrução Normativa/ANAC nº 128, de 6 de novembro de 2018, relativos à Política de Segurança da Informação e Comunicações - PoSIC - no âmbito da Agência Nacional de Aviação Civil – ANAC, sem prejuízo dos demais atos, documentos e normativos expedidos e publicados pela Administração

Pública Federal, bem como pela própria ANAC relativos ao sigilo, à segurança e à privacidade das informações e comunicações, além dos respectivos Termos de Compromisso e de Ciência previstos nas alíneas “a” e “b” do inciso V do art. 18 da Instrução Normativa nº 94, de 23 de dezembro de 2022, da Secretaria de Governo Digital do Ministério da Economia.

4.65. A CONTRATADA deverá atender a, no mínimo, os seguintes requisitos previstos na Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709 de 14 de agosto de 2018:

1. **Recursos em Versões Comprovadamente Seguras e Atualizadas**: Utilizar recursos de segurança da informação e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e em versões comprovadamente seguras e atualizadas, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a CONTRATANTE está exposta, considerando os critérios de aceitabilidade de riscos definidos pela CONTRATANTE.
2. **Reportar Incidentes**: Reportar de imediato à CONTRATANTE incidentes que envolvam vazamento de dados, indisponibilidade ou comprometimento da informação relacionados à Solução de TIC adquirida.
3. **Termo de Compromisso e Ciência**: Implementar e manter controles e procedimentos específicos para assegurar completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da contratada venham a tomar conhecimento em razão da execução do contrato, de forma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem o uso dos dados somente para as finalidades previstas em contrato e as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da Solução de TIC, cumprindo e fazendo cumprir o disposto nos Termo de Compromisso e Termo(s) de Ciência firmados respectivamente, pelo representante legal e pelo(s) empregado(s) da contratada.
4. **Descarte Seguro**: Definir e executar procedimento de descarte seguro dos dados pessoais ou sigilosos da CONTRATANTE ao encerrar a execução do contrato.
5. **Revogação de Privilégios**: Comunicar à CONTRATANTE, de imediato, a ocorrência de transferência, remanejamento ou demissão de funcionário, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da CONTRATANTE, porventura colocados à disposição para realização dos serviços contratados.
6. **Utilização de Serviços de Terceiros**: Informar e obter a anuência do órgão CONTRATANTE sobre a utilização de serviços de terceiros (como suporte técnico etc.) para sustentar ou viabilizar o funcionamento da Solução de TIC contratada.
7. **Tratamento de incidentes de segurança da informação e privacidade**: Realizar em conjunto com a CONTRATANTE, ou com outros órgãos por ela indicados, ações de tratamento de incidentes de segurança da informação e privacidade relacionados ao objeto do contrato, bem como apoiar essas ações com o monitoramento e o envio de informações tempestivos.
8. Toda informação confidencial disponibilizada em razão da contratação, seja ela armazenada em meios físico, magnético ou eletrônico, deverá ser devolvida nas seguintes hipóteses:
    8.1. Término ou rompimento do Contrato;
    8.2. Solicitação da ANAC.
9. A CONTRATADA deverá manter a ANAC informada, formal e tempestivamente, sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados;
10. A CONTRATADA deverá credenciar seus profissionais junto à ANAC, caso seja necessário acesso às instalações e infraestrutura de TI da ANAC para prestação de serviços de suporte.

Sustentabilidade

4.66. Não se verifica requisitos de sustentabilidade elencados no Guia Nacional de Contratações Sustentáveis. 4ª ed. 2021, da AGU (Advocacia-Geral da União), que estejam diretamente relacionados ao objeto desta contratação, qual seja aquisição de bens de licença de software. Os softwares adquiridos serão executados em parque computacional já adquiridos pela ANAC e que naquela situação já tiveram os requisitos de sustentabilidade devidamente considerados.

Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133, de 2021):

4.67. Na presente contratação será adotada a indicação da seguinte marca, característica ou modelo, de acordo com as justificativas contidas nos Estudos Técnicos Preliminares.

4.68. A aquisição será de produto de software denominado Oracle Advanced Security produzido pela empresa de tecnologia da informação Oracle.

Subcontratação

4.69. Não é admitida a subcontratação do objeto contratual.

Garantia da contratação

4.70. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% (cinco) do valor contratual, conforme regras previstas no contrato.

1. A garantia nas modalidades caução e fiança bancária deverá ser prestada em até 10 (dez) dias após assinatura do contrato.
2. No caso de seguro-garantia sua apresentação deverá ocorrer, no máximo, até a data de assinatura do contrato.
3. A inobservância do prazo fixado para apresentação da garantia poderá acarretar a aplicação das sanções previstas neste Termo de Referência.
4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

Outros Requisitos Aplicáveis

4.71. Não foram identificados requisitos adicionais.

5. Modelo de execução do objeto

5. MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de Execução: ***Do Encaminhamento Formal de Demandas***

5.1. O gestor do contrato emitirá a Ordem de fornecimento de bens (OFB) para a entrega dos bens desejados.

5.2. O Contratado deverá fornecer equipamentos com as mesmas configurações e quantidades definidas na OFB.

5.3. Os bens serão recebidos provisoriamente, quando da entrega integral do objeto (incluindo todas as parcelas), pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

5.4. Os bens serão recebidos definitivamente no prazo de 5 (cinco) dias úteis, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado, desde que estejam de acordo com os critérios de aceitação constante da seção 7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO deste Termo de Referência.

Forma de execução e acompanhamento dos serviços: ***Condições de Entrega***

5.5. O prazo de entrega dos bens é de 20 (vinte) dias, contados do(a) da formalização da ordem de fornecimento de bens (OFB), em remessa única.

5.6. A CONTRATADA tem um prazo máximo de 20 (vinte) dias contados do início da vigência do contrato para:

1. Operacionalizar o suporte técnico;
2. Disponibilizar o acesso ao sistema onde será possível baixar patches e atualizações do software; e
3. Disponibilizar o acesso para abertura de chamados técnicos.

5.7. Novas versões de software, quando disponíveis, deverão ser disponibilizadas tão logo ocorra o lançamento oficial da nova versão.

5.8. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 5 (cinco) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

5.9. As licenças de software e demais informações para acesso aos serviços relacionados deverão ser entregues por meio de mensagem eletrônica (e-mail) para a equipe de fiscalização do contrato, ou conforme orientação expressa por ocasião da reunião inicial do contrato.

Garantia, manutenção e assistência técnica

5.10. O prazo de garantia contratual dos bens, produto de software, será de, no mínimo, 12 (doze) meses, contado a partir da disponibilização das licenças de software.

5.11. Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o fornecedor deverá complementar a garantia do bem ofertado pelo período restante.

Rotinas de Execução

5.12. Em até 15 dias a contar do início da vigência do contrato, será convocada reunião inicial em conformidade com a IN SGD /ME Nº 94, de 2022, com presença obrigatória do representante legal da CONTRATADA, que apresentará o preposto da mesma.

5.13. Caso seja necessário, a reunião inicial poderá ser realizada virtualmente através de ferramenta colaborativa a ser indicada pela CONTRATANTE.

5.14. O preposto indicado pela CONTRATADA deve responder pela fiel execução dos serviços contratados, orientar os técnicos de manutenção que prestarão os serviços, bem como comparecer à CONTRATANTE sempre que convocado. Para evitar que a CONTRATANTE fique eventualmente sem acesso ao preposto, deverá ser indicado um substituto.

5.15. O preposto e demais profissionais da CONTRATADA envolvidos em atividades relativas à execução do Contrato resultante da presente licitação deverão providenciar seu cadastramento no Sistema Eletrônico de Informações (SEI!) da ANAC, para que dessa forma possam acessar e assinar quaisquer documentos formais relativos à execução contratual;

5.16. Diante de situações de irregularidades de caráter urgente, o Preposto deverá comunicar-se por escrito com a CONTRATANTE para apresentar os esclarecimentos julgados necessários, as informações sobre possíveis paralisações de serviços, a apresentação de relatório técnico, ou as razões justificadoras a serem apreciadas e decididas pelo agente designado.

5.17. As decisões e providências sugeridas pela CONTRATADA que forem julgadas imprescindíveis, mas que ultrapassarem a competência dos Fiscais designados pela ANAC, deverão ser encaminhadas à Gerência Técnica de Licitações e Contratos, para a adoção das medidas cabíveis.

5.18. Deverá ser disponibilizado pela CONTRATADA sistema Web para registro e acompanhamento de chamados técnicos, ou mecanismo similar tais como telefone ou endereço de e-mail.

5.19. A CONTRATADA será encarregada de realizar os atendimentos de suporte técnico através da avaliação e resolução dos chamados de incidentes ou problemas encaminhados pela CONTRATANTE via sistema ou telefone.

5.20. O suporte técnico será realizado remotamente e deverá ser fornecido durante a vigência contratual.

5.21. Os contatos de suporte técnico deverão estar disponíveis 24 horas por dia, 7 dias por semana, via web ou telefone.

5.22. É responsabilidade da CONTRATADA o correto cadastramento dos dados da CONTRATANTE junto à fabricante do software para efeito de vigência contratual e benefícios inerentes a forma de licenciamento.

Prazos de execução

5.23. A CONTRATADA tem um prazo máximo de 20 (vinte dias) contados do início da vigência do contrato para:

5.24. Operacionalizar o suporte técnico;

5.25. Disponibilizar o acesso ao sistema onde será possível baixar *patches* e atualizações do *software*; e

5.26. Disponibilizar o acesso para abertura de chamados técnicos.

5.27. Novas versões de software, quando disponíveis, deverão ser disponibilizadas tão logo ocorra o lançamento oficial da nova versão.

Mecanismos formais de comunicação

5.28. A comunicação entre CONTRATANTE e CONTRATADA poderá ocorrer por e-mail ou telefone, exceto nos casos onde se exija outro documento formal que poderá ser através de: Atas de Reunião; Termos de Aceite; Notas Técnicas; Relatórios; Ordens de Serviço ou de Fornecimento de Bens; E-mails: da alta gestão da ANAC, da equipe de fiscalização do contrato, das Superintendências de Tecnologia da Informação (STI) e de Administração e Finanças (SAF) da ANAC; Correspondências oficiais, tais como Ofícios ou Memorandos.;

5.29. O Preposto deverá estar disponível para contato em dias úteis, das 8h às 12h e das 14h às 18h.

5.30. A reunião poderá ser realizada de forma presencial, ou de forma virtual através de plataforma disponibilizada pela CONTRATANTE. Poderá ser utilizada plataforma indicada pela CONTRATADA, caso se mostre razoável.

5.31. Os atendimentos técnicos serão solicitados através da abertura de chamados via sistema disponibilizado pela CONTRATADA ou aberto através de telefone 0800.

Formas de Pagamento

5.32. Os critérios de medição e pagamento serão tratados no item 7 e seguintes deste Termo de Referência.

Manutenção de Sigilo e Normas de Segurança

5.33. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

5.34. O **Termo de Compromisso e Manutenção de Sigilo**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e **Termo de Ciência**, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se no Anexo V - Termo de Compromisso e no Anexo VI - Termo de Ciência.

Quantidade mínima de bens ou serviços para comparação e controle

5.35. A quantidade mínima de bens e serviços está especificada na Tabela 1 - Bens e serviços que compõem a solução.

Formas de transferência de conhecimento

5.36. Não será necessária transferência de conhecimento devido às características do objeto.

Procedimentos de transição e finalização do contrato

5.37. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

6. Modelo de gestão do contrato

6. MODELO DE GESTÃO DO CONTRATO

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução do contrato.

6.6. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 15 (quinze) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

6.7. A pauta desta reunião observará, pelo menos:

1. Presença do representante legal da contratada, que apresentará o seu preposto;
2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;
3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;
4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;
5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

6.8. A execução do contrato será acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput) e conforme orientações da Instrução Normativa SGD/ME Nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

6.8.1. O **fiscal técnico** do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

6.8.2. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

6.8.3. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

6.8.4. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

6.8.5. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

6.8.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

6.8.7. O **fiscal administrativo** do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

6.8.8. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

6.8.9. O **gestor do contrato**, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

6.8.10. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

6.8.11. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

6.8.12. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

6.8.13. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

6.8.14. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual. (Decreto nº 11.246, de 2022, art. 22, VII).

6.8.15. O gestor do contrato deverá elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

6.9. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

6.9.1. O fornecimento dos produtos e serviços objetos da presente licitação ocorrerá mediante prévia emissão de Ordem de Serviço ou Fornecimento de Bens pelo gestor do contrato indicando os itens e quantidades.

6.9.2. A fiscalização se dará de forma complementar com observação aos ditames do Manual de Fiscalização de Contratos da ANAC.

6.9.3. Devem ser cumpridos os prazos e condições descritos no item 7.20 - Níveis Mínimos de Serviço Exigidos deste Termo de Referência, que estabelecem requisitos para o suporte da solução contratada.

6.9.4. Sempre que houver quebra dos Níveis Mínimos de Serviço Exigidos, a CONTRATANTE poderá notificar a CONTRATADA, que terá prazo máximo de 5 (cinco) dias úteis para apresentar as justificativas para as falhas verificadas. Caso não haja manifestação da CONTRATADA dentro desse prazo ou caso a CONTRATANTE entenda serem improcedentes as justificativas, poderá ser iniciado processo de aplicação das sanções previstas.

6.10. A fiscalização não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em co-responsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 120 da Lei nº 14.133, de 2021.

Níveis Mínimos de Serviço Exigidos

6.11. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAE – INDICADOR DE ATRASO NO FORNECIMENTO DO EQUIPAMENTO		
Tópico	***Descrição***	
Finalidade	*Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens.*	
Meta a cumprir	***IAE <= 0***	*A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento de Bens dentro do prazo previsto.*
Instrumento de medição	*OFB, Termo de Recebimento Provisório (TRP)*	
	A avaliação será feita conforme linha de base do cronograma registrada na OFB.	

Forma de acompanhamento	*Será subtraída a data de entrega dos produtos da OFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OFB.*
Periodicidade	*Para cada Ordem de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.*
Mecanismo de Cálculo (métrica)	***IAE = TEX – TEST*** *Onde:* ***IAE** – Indicador de Atraso de Entrega da OFB;* ***TEX** – Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB.* *A data de início será aquela constante na OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB.* *A data de entrega da OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OFB continua a correr, findando-se apenas quanto o Contratado entrega os produtos da OFB e haja aceitação por parte do fiscal técnico.* ***TEST** – Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência.*
Observações	*Obs1: Serão utilizados dias corridos na medição.* *Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.*
Início de Vigência	*A partir da emissão da OFB.*
Faixas de ajuste no pagamento e Sanções	*Para valores do indicador **IAE**:* *Menor ou igual a 0 – Pagamento integral da OFB;* *De 1 a 60 - aplicar-se-á glosa de 0,1666% por dia de atraso sobre o valor da OFB ou fração em atraso.* *Acima de 60 - aplicar-se-á glosa de 10% bem como multa de 2% sobre o valor OFB ou fração em atraso.*

6.12. O serviço de suporte será executado diretamente pela empresa Oracle, fabricante da solução, durante a vigência do contrato.

6.13. Os serviços de suporte serão prestados remotamente, quando possível, e presencialmente, sempre que se fizer necessário. A definição da necessidade de prestação de suporte presencial caberá a ANAC em conjunto com a CONTRATADA.

6.14. Os serviços de suporte serão demandados pela CONTRATANTE através da abertura de chamados.

6.15. Em até 15 (quinze) dias corridos após o início de execução do contrato, deverá ser fornecida Central de Atendimento (através de sítio na Internet, e-mail e telefone), sem custo adicional à CONTRATANTE, para aberturas de chamados, envio de arquivos para análise e consultas durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano.

6.16. A CONTRATANTE indicará profissionais autorizados a abrirem chamados diretamente com a fabricante.

6.17. Na ocasião de abertura dos chamados, serão fornecidas informações de identificação do produto, anormalidade observada, nome do responsável pela solicitação do serviço e severidade.

6.18. O início da contagem do tempo de atendimento se dará a partir do registro da criação do chamado pela CONTRATANTE.

6.19. O atendimento à resolução chamados deverá respeitar os tempos de atendimento previstos na seguinte tabela de severidades:

Tabela 2 - Níveis Mínimos de Serviço Exigidos para atendimento aos chamados do suporte técnico.

Severidade	**Descrição**	**Prazo de Resolução de Chamado (PRC)**	**Sanções**
Alta	Problemas graves que prejudicam a operação do produto ou limitação severa de suas funcionalidades com a paralisação parcial ou total da ferramenta.	Em até 04 (quatro) horas corridas, com exceção de defeitos que exijam a intervenção do laboratório da fabricante.	PRC > 4 Multa compensatória de 0,5% (cinco décimo por cento) do valor de base de cálculo, por hora de atraso, limitado ao percentual máximo de 10% (dez por cento) do valor da base de cálculo, por ocorrência.
Média	Problemas que criam restrições à operação da solução, mas não comprometem seu uso e funcionamento.	Em até 8 (oito) horas corridas, com exceção de defeitos que exijam a intervenção do laboratório da fabricante.	PRC > 8 Multa compensatória de 0,25% (vinte e cinco décimos por cento) do valor de base de cálculo, por hora de atraso, limitado ao percentual máximo de 5% (cinco por cento) do valor da base de cálculo, por ocorrência.
Baixa	Aplicado em situações de esclarecimento de dúvidas ou suporte relacionadas à instalação, configuração e uso dos produtos adquiridos, bem como na atualização de versão de programa e/ou componente de software integrante da solução.	Em até 36 (trinta e seis) horas comerciais, com exceção de defeitos que exijam a intervenção do laboratório da fabricante.	PRC > 36 Multa compensatória de 0,1% (um décimo por cento) do valor de base de cálculo, por hora de atraso, limitado ao percentual máximo de 3% (três por cento) do valor da base de cálculo, por ocorrência.
A base de cálculo para fins de sanções será de 1/12 (um doze avos) do valor total do contrato.			

6.20. O atendimento não poderá ser interrompido sem justificativa tempestiva, que por sua vez deverá ser avaliada e aceita pela equipe de fiscalização.

6.21. O Prazo de Resolução de Chamado (PRC) consiste no período em que um conjunto de esforços serão realizados para a solução do problema ou incidente de acordo com a severidade. A solução de contorno implica em situação temporária, quando houver necessidade de uma manutenção mais complexa e que demande um tempo maior na resolução, impedindo a paralisação total ou parcial dos serviços, até que o problema seja definitivamente solucionado.

6.22. Os chamados poderão ser escalados para níveis mais altos ou mais baixos, de acordo com a severidade do problema. Nesse caso, os prazos de resolução do problema, bem como as sanções, serão automaticamente ajustados para o novo nível de gravidade, considerando todo o tempo de atendimento gasto anteriormente.

6.23. Para os níveis de severidade "Alta" e "Média", o atendimento aos chamados não poderá ser interrompido até o completo restabelecimento do serviço, mesmo que se estenda para períodos noturnos, sábados, domingos e feriados. A interrupção de atendimento para um chamado dessa gravidade por parte da prestadora de serviço e que não tenha sido previamente autorizado pela CONTRATANTE, poderá ensejar em aplicação de penalidades previstas pela autoridade competente.

6.24. Todos os chamados registrados receberão código de identificação e serão controlados por sistema de informação da CONTRATADA ou de FABRICANTE, disponibilizado via web, ao qual A CONTRATANTE terá acesso para efeito de acompanhamento das providências em andamento e do tempo decorrido desde sua abertura.

6.25. O sistema deverá disponibilizar relatório dos chamados técnicos executados, os quais conterão as seguintes informações:

1. Relação de todos os chamados ocorridos no período, incluindo data e hora do início e término do atendimento; o Prazo de Resolução de Chamado (PRC); identificação do problema; severidade do chamado; tempo de solução do chamado; providências adotadas para o diagnóstico e solução aplicada; identificação do usuário que solicitou e validou o serviço; identificação do técnico responsável pela execução do serviço, bem como outras informações pertinentes.
2. Chamados fechados sem anuência do CONTRATANTE ou sem que os problemas tenham sido de fato resolvidos deverão ser reabertos e os prazos serão contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.

6.26. Se identificado interrupção do atendimento ao chamado, sem solicitação à CONTRATANTE, implicará em cancelamento do chamado e reabertura de novo chamado, incluindo o tempo de atendimento realizado do chamado anterior.

6.27. Sempre que os prazos de resolução de chamado não forem cumpridos, bem como surgir qualquer outra situação irregular, poderá ensejar em aplicação pela autoridade competente de penalidades previstas, em especial, as sanções previstas na Tabela 2 deste Termo de Referência.

6.28. A CONTRATADA será eximida de qualquer penalidade quanto ao não atendimento dos tempos de solução desde que comprovadas às seguintes situações:

1. Quando constatado que o problema está relacionado a defeito no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio.
2. Que a CONTRATADA tomou todas as medidas possíveis visando providenciar solução de contorno.

6.29. Não pode haver limitações de quantidade ou tempo para tratamento de chamados de suporte.

6.30. A frequência de aferição/ateste dos níveis de serviços será trimestral, por meio da apresentação pela CONTRATADA de Relatório de Chamados. A verificação será realizada por Equipe de Fiscalização devidamente designada pela CONTRATANTE, através da interface Web de relatórios, disponibilizada pela CONTRATADA ou por outro procedimento equivalente.

6.31. A CONTRATADA deverá enviar de forma trimestral Relatório de Chamados contendo todos os chamados técnicos concluídos no referido período e os que ainda continuam abertos juntamente com o *status* de cada chamado. Adicionalmente, devem ser enviadas justificativas e evidências suficientes para julgamento dos casos de descumprimento do indicador Prazo para Resolução de Chamados (PRC), caso existam.

6.32. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

Tabela 3 - Previsão de Penalidades e Sanções

Id	Ocorrência	Sanção
1	Não comparecer injustificadamente à Reunião Inicial.	Advertência.

		Em caso de reincidência, 0,01% sobre o valor total do Contrato.
2	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços/entrega dos materiais, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 72 horas úteis.	Multa de 0,01% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela CONTRATANTE, até o limite de 10 dias úteis.
		Após o limite de 10 dias úteis, aplicar-se-á multa de 0,02% do valor total do Contrato.
3	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas, etc.).	A CONTRATADA será declarada impedida de licitar e contratar no âmbito da Administração Pública federal, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
4	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado na fase de levantamento de requisitos e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	A CONTRATADA será declarada impedida de licitar e contratar no âmbito da Administração Pública federal, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
5	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	A CONTRATADA será declarada impedida de licitar e contratar no âmbito da Administração Pública federal, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
6	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da CONTRATANTE.	A CONTRATADA será declarada impedida de licitar e contratar no âmbito da Administração Pública federal, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
7	Não atender ao indicador de nível de serviço PRC (Prazo de Resolução de Chamado)	Tabela 2 do Termo de Referência.

6.33. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o Contratado:

6.33.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

6.33.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

7. Critérios de medição e pagamento

7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do Objeto

7.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

7.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 5 (cinco) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.3. O recebimento definitivo ocorrerá no prazo de 5 (cinco) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

7.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até 5 (cinco) dias úteis.

7.5. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

7.6. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.7. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

7.8. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Critérios de Aceitação

7.9. A verificação será feita por meio de acesso ao site do fabricante, a área de acesso exclusivo da CONTRATANTE, por meio de credenciais específicas, e verificação das licenças e quantidades disponibilizadas frente a proposta comercial da CONTRATADA e ao Termo de Referência.

7.10. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões “shareware” ou “trial”. O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.

7.11. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

Liquidação

7.12. A emissão da Nota Fiscal/Fatura pela CONTRATADA será precedida pela emissão do Termo de Recebimento Definitivo pela CONTRATANTE, conforme este Termo de Referência.

7.13. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

> 1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

7.14. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

a. 1. o prazo de validade;
b. 2. a data da emissão;

c. 3. os dados do contrato e do órgão Contratante;
d. 4. o período respectivo de execução do contrato;
e. 5. o valor a pagar; e
f. 6. eventual destaque do valor de retenções tributárias cabíveis.

7.15. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante;

7.16. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

7.17. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

7.18. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

7.19. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.20. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

7.21. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

7.22. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

7.23. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do **Índice de Custo da Tecnologia da Informação (ICTI)** de correção monetária.

Forma de pagamento

7.24. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

7.25. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.26. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.27. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

7.28. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Aditivo Contratual

7.29. Em caso de aditivo para acréscimo de licenças contratadas, deve-se observar todas as condições presentes no Acordo Corporativo N. 10/2022 SGD/ME - Oracle (SEI-ANAC n° 7379867) e suas atualizações, bem como a celebração de termo aditivo ao contrato.

Antecipação de pagamento

7.30. A presente contratação não permitirá a antecipação de pagamento, haja vista o curto tempo previsto para cumprimento integral do contrato e liquidação do pagamento.

Cessão de crédito

7.31. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de julho de 2020, conforme as regras deste presente tópico.

As cessões de crédito não fiduciárias dependerão de prévia aprovação do Contratante.

7.32. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

7.33. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, tudo nos termos do Parecer JL-01, de 18 de maio de 2020.

7.34. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

7.35. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do contratado.

8. Critérios de seleção do fornecedor

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

Forma de seleção e critério de julgamento da proposta

8.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo **MENOR PREÇO**.

8.2. Juntamente com a proposta comercial, a licitante vencedora deverá apresentar declaração, ou documento similar, da fabricante Oracle internacional, ou da Oracle Brasil, que indique ser uma representante e/ou revenda autorizada de produtos no Brasil.

8.3. Juntamente com a proposta comercial, a licitante vencedora deverá apresentar declaração que ateste **a não ocorrência do registro de oportunidade**, de modo a garantir o princípio da competitividade, conforme o disposto no art. 5º da Lei nº 14.133, de 2021, conforme modelo anexo a este termo de referência.

Exigências de habilitação

8.4. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Habilitação jurídica

8.5. **Pessoa física**: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

8.6. **Empresário individual**: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

8.7. **Microempreendedor Individual - MEI**: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br /empreendedor;

8.8. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI**: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

8.9. **Sociedade empresária estrangeira**: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

8.10. **Sociedade simples**: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

8.11. **Filial, sucursal ou agência de sociedade simples ou empresária**: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

8.12. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

8.13. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

8.14. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

8.15. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

8.16. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

8.17. Prova de inscrição no cadastro de contribuintes Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.18. Prova de regularidade com a Fazenda Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

8.19. Caso o fornecedor seja considerado isento dos tributos Municipal/Distrital relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

8.20. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

8.21. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

8.22. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

8.23. Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

I. 1. Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo)/(Passivo Circulante + Passivo Não Circulante);
II. 2. Solvência Geral (SG)= (Ativo Total)/(Passivo Circulante +Passivo não Circulante); e
III. 3. Liquidez Corrente (LC) = (Ativo Circulante)/(Passivo Circulante).

8.24. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de 10% do valor total estimado da contratação.

8.25. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

8.26. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º).

8.27. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

Qualificação Técnica

8.28. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

8.28.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

I) A licitante vencedora deverá comprovar aptidão para o fornecimento de licenças de software Oracle Advanced Security, em características e prazos compatíveis com o objeto desta licitação, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado, que comprove o fornecimento de, pelo menos, 3 (três) licenças do referido software.

8.28.2. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

8.28.3. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

8.28.4. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

8.29. Não será admitida a participação de cooperativas, , haja vista que o mercado de licenças de software não é compatível com as sociedades cooperativas.

Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência

8.30. Será assegurado o direito de preferência previsto no seu artigo 4º, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010.

8.31. Nas contratações de bens e serviços de informática e automação, nos termos da Lei nº 8.248, de 1991, as licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

9. Estimativas do Valor da Contratação

Valor (R$): 540.620,50

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1. O custo estimado total da contratação é de R$ 540.620,50 (quinhentos e quarenta mil seiscentos e vinte reais e cinquenta centavos), conforme custos unitários apostos na tabela abaixo.

9.2. Os valores unitário e global máximos a serem admitidos por esta Agência Reguladora para o objeto da pretensa aquisição **estão fixados na** tabela a seguir:

Tabela 4 - Estimativa de Preço da Contratação

Item	Descrição do Bem	Qtd	Unidade de medida	Valor unitário máximo (R$)	Valor total máximo (R$)
1	Licença Perpétua com Suporte e Atualização (SA) por 12 meses	7	unidade	77.231,50	540.620,50

10. Adequação orçamentária

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

10.2. A contratação será atendida pela seguinte dotação:

I) Gestão/Unidade: 20214/113240;

II) Fonte de Recursos: 1050000008;

III) Programa de Trabalho: 26.125.3004.2912.0001;

IV) Elemento de Despesa: 44.90.40.05 AQUISICAO DE SOFTWARE PRONTO;

V) Plano Interno: 2ATDTI22070;

10.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

10.4. *Cronograma Físico Financeiro*

Evento	Data/Prazo	Responsável	Valor
1. Assinatura do contrato	Conforme convocação da SAF/ANAC.	ANAC e CONTRATADA	R$ 0,00
2. Emissão da Ordem de Fornecimento de Bens (OFB)	Após evento (1) e conforme avaliação de oportunidade e conveniência da STI/ANAC	Fiscal Requisitante e Gestor do Contrato	R$ 0,00
3. Entrega das licenças de software	Até 20 (vinte) dias corridos após evento (2)	CONTRATADA	R$ 0,00
4. Emissão do Termo de Recebimento Provisório (TRP)	Até 2 (dois) dias úteis após evento (3)	Equipe de fiscalização	R$ 0,00

5. Avaliação do material recebido pela equipe de fiscalização	Até 5 (cinco) dias corridos após evento (4)	Equipe de fiscalização	R$ 0,00
6. Emissão do Termo de Recebimento Definitivo (TRD)	Até 5 (cinco) dias corridos após evento (4)	Equipe de fiscalização	R$ 0,00
7. Envio da documentação para pagamento	Até 2 (dois) dias úteis após evento (6)	Equipe de fiscalização	R$ 0,00
8. Pagamento	Até 30 dias corridos após evento (6)	Setor financeiro da ANAC	Conforme valor total do contrato.

11. Papéis e responsabilidades

11. PAPÉIS E RESPONSABILIDADES

11.1. São obrigações da **CONTRATANTE**:

1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;
3. receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável;
8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

11.2. São obrigações da **CONTRATADA**

1. indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do contrato;
2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
3. reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela Contratante;
4. propiciar todos os meios necessários à fiscalização do contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;
5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;
6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;
8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;
9. fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução dos serviços, quando for o caso.

12. Do reajuste

12. DO REAJUSTE

12.1. Não será admitido reajuste para está contratação.

13. Responsáveis

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

FELIPE SANTOS SARMANHO

Integrante Requisitante

Assinou eletronicamente em 31/08/2023 às 13:03:06.

WILLIAN ROCHA BICALHO

Integrante Técnico

Assinou eletronicamente em 01/09/2023 às 17:01:22.

ADERSON DE LIMA CALAZANS

Integrante Administrativo

Assinou eletronicamente em 31/08/2023 às 21:54:57.

Despacho: Aprovo este Termo de Rererência e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

FERNANDO ANDRE COELHO MITKIEWICZ

Autoridade máxima de TIC

Assinou eletronicamente em 01/09/2023 às 11:22:24.

ANEXO I

MODELO DE PROPOSTA COMERCIAL

À

AGENCIA NACIONAL DE AVIAÇÃO CIVIL (ANAC)

A proposta que faz a empresa _____, para contratação de solução de tecnologia da informação e comunicação para aquisição de licenças de uso perpétuas da Option Oracle Advanced Security – Processor Perpetual para segurança de banco de dados Oracle e implementação de criptografia de dados em repouso, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

Item	Descrição do Bem	Marca/modelo	Qtd	Unidade de medida	Valor unitário máximo (R$)	Valor total máximo (R$)
1	Licença Perpétua com Suporte e Atualização (SA) por 12 meses		7	unidade		

Assim sendo, o valor total da proposta é de R$ _____ **(por extenso).**

A presente proposta é baseada nas especificações, condições e prazos estabelecidos no edital de Pregão nº ___/2023-ANAC, os quais nos comprometemos a cumprir integralmente.

Prazo de validade da proposta: _____ dias (não inferior a sessenta dias)

Declaramos que estamos de pleno acordo com todas as condições estabelecidas no Edital e seus Anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas no Termo de Referência.

Declaramos que nos preços cotados estão incluídas todas as despesas que, direta ou indiretamente, fazem parte do presente objeto, tais como gastos da empresa com suporte técnico e administrativo, impostos, seguros, taxas, ou quaisquer outros que possam incidir sobre gastos da empresa, sem quaisquer acréscimos em virtude de expectativa inflacionária e deduzidos os descontos eventualmente concedidos.

Dados da empresa:

Razão Social		CNPJ (MF) nº	
Inscrição Estadual nº		Inscrição Municipal nº	
Endereço			
Telefone		Fax	
Cidade:		UF	

Dados do Representante para fim de apresentação da proposta e assinatura do contrato:

Nome			
CPF		Cargo/Função	
Carteira de Identidade		Expedido por	
Nacionalidade		Estado Civil	
Endereço			
Telefone		Fax	
Endereço Eletrônico			

Local e data

_____

Assinatura e carimbo

(Representante Legal)

ANEXO II - ORDEM DE FORNECIMENTO DE BENS

1. IDENTIFICAÇÃO

Nº da OS/OFB:	
Contrato nº	
Objeto do Contrato	
Contratada	
Preposto	
Início vigência	
Fim da vigência	
Área Requisitante da Solução:	

2. ESPECIFICAÇÃO DOS PRODUTOS / SERVIÇOS E VOLUMES

Id	PRODUTO / SERVIÇO	MÉTRICA	QUANTIDADE	Valor Total (R$)
	TOTAL:		----------	

3. INSTRUÇÕES COMPLEMENTARES

4. CRONOGRAMA

Id	TAREFA/ENTREGA	INÍCIO	FIM

5. ARTEFATOS / PRODUTOS

FORNECIDOS	A SEREM GERADOS E/OU ATUALIZADOS

6. ASSINATURA E ENCAMINHAMENTO DA DEMANDA

6.1. Autoriza-se a <execução dos serviços / entrega dos bens> correspondentes à presente <OS/OFB>, no período e nos quantitativos acima identificados.

CONTRATANTE	
Área/Fiscal Requisitante da Solução **Nome** **Matrícula**	**Gestor do Contrato** **Nome** **Matrícula**

Documento assinado eletronicamente por **Felipe Santos Sarmanho**, **Gerente**, em 13/06/2023, às 12:35, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Willian Rocha Bicalho**, **Analista Administrativo**, em 14/06/2023, às 10:11, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.anac.gov.br/sei/autenticidade, informando o código verificador **8071343** e o código CRC **997A622C**.

ANEXO III - TERMO DE RECEBIMENTO PROVISÓRIO

INTRODUÇÃO
O Termo de Recebimento Provisório declarará formalmente à Contratada que os serviços foram prestados ou que os bens foram recebidos para posterior análise das conformidades e qualidade, baseadas nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato. **Referência: Inciso XXI, Art. 2º, e alínea "a", inciso II, art. 33, da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO	
Contrato nº	
Nº da OS/ OFB:	
Objeto	
Contratante	
Contratada	

2 – ESPECIFICAÇÃO DOS PRODUTOS/BENS E VOLUMES DE EXECUÇÃO

SOLUÇÃO DE TIC

Nº da OS/OFB:	ID	PRODUTO	MODELO DE LICENCIAMENTO	MÉTRICA	QUANTIDADE	VALOR UNITÁRIO (R$)	VALOR TOTAL ANUAL (R$)

3 – RECEBIMENTO
Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 33, inciso II, alínea "a", da IN SGD/ME nº 94/2022, que os <serviços / bens> correspondentes à <OS/OFB> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram recebidos provisoriamente na presente data e serão objetos de avaliação por parte da **CONTRATANTE** quanto à adequação da entrega às condições contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato. Ressaltamos que o recebimento definitivo destes serviços ocorrerá após a verificação dos requisitos e demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**.

CONTRATANTE	CONTRATADA
Fiscal Técnico	**Preposto**
Nome Matrícula	Nome CPF

Documento assinado eletronicamente por **Felipe Santos Sarmanho**, **Gerente**, em 13/06/2023, às 12:35, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Willian Rocha Bicalho**, **Analista Administrativo**, em 14/06/2023, às 10:11, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.anac.gov.br/sei/autenticidade, informando o código verificador **8071211** e o código CRC **073F8A1C**.

ANEXO IV - TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO
O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem aos requisitos estabelecidos e aos critérios de aceitação. **Referência: Alínea "f", inciso II, e alínea "d", inciso III, do art. 33, da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO	
CONTRATO Nº	
Nº da OS/ OFB:	
OBJETO	
CONTRATANTE	
CONTRATADA	

2 – ESPECIFICAÇÃO DOS PRODUTOS/BENS E VOLUMES DE EXECUÇÃO

SOLUÇÃO DE TIC

Nº da OS/OFB:	ID	PRODUTO	MODELO DE LICENCIAMENTO	MÉTRICA	QUANTIDADE	VALOR UNITÁRIO (R$)	VALOR TOTAL ANUAL (R$)

3 – RECEBIMENTO

Por este instrumento atestamos, para fins de cumprimento do disposto na alínea "f", inciso II, e alínea "d", inciso III, do art. 33, da IN SGD/ME Nº 94/2022, que os <serviços / bens> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela **CONTRATADA** e atendem às condições contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Termo de Referência do Contrato acima indicado.

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.

Por conseguinte, o valor a liquidar correspondente à <OS/OFB> acima identificada monta em R$ <valor> (<valor por extenso>).
Referência: <Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>.

CONTRATANTE

FISCAL TÉCNICO	FISCAL REQUISITANTE
Nome Matrícula	Nome Matrícula

Documento assinado eletronicamente por **Felipe Santos Sarmanho**, **Gerente**, em 13/06/2023, às 12:35, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Willian Rocha Bicalho**, **Analista Administrativo**, em 14/06/2023, às 10:11, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.anac.gov.br/sei/autenticidade, informando o código verificador **8077012** e o código CRC **1479EE5C**.

ANEXO V - TERMO DE COMPROMISSO

O <*NOME DO ÓRGÃO*>, sediado em <*ENDEREÇO*>, CNPJ nº <*CNPJ*>, doravante denominado CONTRATANTE, e, de outro lado, a <*NOME DA EMPRESA*>, sediada em <*ENDEREÇO*>, CNPJ nº <*CNPJ*>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

1. **CLÁUSULA PRIMEIRA - DO OBJETO**

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo, bem como a Lei nº 13.709, de 14 de agosto de 2018, que trata da Proteção de Dados Pessoais.

2. **CLÁUSULA SEGUNDA - DOS CONCEITOS E DEFINIÇÕES**

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3. **CLÁUSULA TERCEIRA - DA INFORMAÇÃO SIGILOSA**

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

4. **CLÁUSULA QUARTA – DOS LIMITES DO SIGILO**

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5. **CLÁUSULA QUINTA – DOS DIREITOS E OBRIGAÇÕES**

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente;

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas; e

V – Respeitar as normas de segurança vigentes na Anac, em especial a Política de Segurança da Informação - PoSI.

6. **CLÁUSULA SEXTA – DA VIGÊNCIA**

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

7. **CLÁUSULA SÉTIMA – DAS PENALIDADES**

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 156 da Lei nº. 14.133/2021.

8. **CLÁUSULA OITAVA – DISPOSIÇÕES GERAIS**

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9. **CLÁUSULA NONA – DO FORO**

A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

DE ACORDO

Brasília (DF), _____de _____de _____.

Servidor Responsável *<Nome>* *<Cargo>* *<Matrícula>*	**Representante Legal da Empresa** *<Nome>* *<Qualificação>*	**Testemunha 1** *<Nome>* *<Qualificação>*	**Testemunha 2** *<Nome>* *<Qualificação>*

Documento assinado eletronicamente por **Felipe Santos Sarmanho**, **Gerente**, em 13/06/2023, às 12:35, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Willian Rocha Bicalho**, **Analista Administrativo**, em 14/06/2023, às 10:11, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.anac.gov.br/sei/autenticidade, informando o código verificador **8071135** e o código CRC **BA3D0515**.

ANEXO VI - TERMO DE CIÊNCIA

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, sob pena das sanções cabíveis nos termos da legislação vigente que assumo a responsabilidade por:

I - Tratar o(s) ativo(s) de informação como patrimônio da Agência Nacional de Aviação Civil (ANAC), guardando inteiro sigilo dos dados processados, reconhecendo serem estes de propriedade exclusiva da ANAC, sendo vedada a cessão, locação ou venda a terceiros;

II - Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço da ANAC;

III - Contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 27 de maio de 2020, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

IV - Utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas da ANAC;

V - Responder, perante a ANAC, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

VI - Ter ciência e atuar de acordo com o Termo de Compromisso celebrado entre a minha contratante e a ANAC em relação a ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto 7.845 de 14/11/2012 - 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.

VII - Respeitar as normas de segurança vigentes na Anac, em especial a Política de Segurança da Informação - PoSI.

Brasília (DF), _____de _____de _____.

_____ **Empregado** *<Nome>*	_____ **Preposto Administrativo** *<Nome>*

Documento assinado eletronicamente por **Felipe Santos Sarmanho**, **Gerente**, em 13/06/2023, às 12:35, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Willian Rocha Bicalho**, **Analista Administrativo**, em 14/06/2023, às 10:11, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Estudo Técnico Preliminar 11/2022

1. Informações Básicas

Número do processo: 00058.008005/2022-39

2. Título

Criptografia da dados em repouso para Banco de Dados Oracle

3. Descrição da necessidade

Solução de Criptografia de dados em Repouso para SGBD Oracle

É fato amplamente conhecido que a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), em vigor desde meados de 2020, prevê uma série de regras e práticas que buscam promover a proteção aos dados pessoais de todo cidadão em território brasileiro.

Neste contexto, todas as organizações, públicas ou privadas, devem adotar medidas diversas em relação à coleta, uso e compartilhamento dos dados pessoais por ela manipulados, seja em meio físico ou digital.

Especificamente, o artigo 46 da LGPD determina que os agentes de tratamento (coordenador e/ou operador) devem implementar controles internos para 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.

A Gerência Técnica de Gestão da Informação (GTGI) iniciou esforços para adequação da ANAC à LGPD. Dentre as principais iniciativas, destaca-se a produção de Relatórios de Inventário de Dados Pessoais que descrevem os procedimentos e resultados obtidos a partir de análise de bases que armazenam os dados da Agência.

Até o momento, as seguintes bases de dados foram analisadas:

Tabela 1- Inventário de Dados Pessoais realizado pela GTGI/ANAC

Base de dados/Sistema	Relatório de Diagnóstico e Recomendações	Tecnologia
AERONAUTA	Processo SEI nº 00058.011646/2021-90	Oracle
HABILITAÇÃO	Processo SEI nº 00058.021617/2021-36	Oracle
SISHAB	Processo SEI nº 00058.021766/2021-03	Oracle
CMA	Processo SEI nº 00058.021894/2021-49	SQL Server
SISMEDCRED	Processo SEI nº 00058.039351/2021-88	Oracle
Moodle	Processo SEI nº 00058.051198/2021-67	PostgreSQL
SIGRH	Processo SEI nº 00058.053008/2021-46	PostgreSQL

Observou-se que todos os relatórios presentes na Tabela 1 contêm uma seção intitulada "Recomendações" a qual apresenta orientações em relação à procedimentos e ações para cada dado pessoal ou conjunto de dados analisado. Tais orientações podem ser a eliminação do tratamento (coleta, processamento, armazenamento etc.) de dados sem fundamentação legal ou desnecessários, existência do prazo de guarda, ou até mesmo pseudonimização, anonimização ou criptografia.

Quanto a recomendação de criptografia, verifica-se que há sempre a mesma motivação, divergindo apenas quanto ao nome da base de dados e a quantidade de tabelas a serem criptografadas. O trecho abaixo foi retirado do documento SEI nº 5411816 que discorre sobre a base de dados do sistema Aeronauta:

> "A criptografia consiste em um processo por meio do qual um dado perde sua legibilidade. Desta forma, caso seja vazado, seu conteúdo não será lido com clareza, nitidez. Não se trata de uma medida de mitigação, mas de contingência. Em outras palavras, não impede que um vazamento ocorra, mas que caso ocorra os respectivos dados sejam inúteis. Esta técnica é totalmente pertinente

> e recomendada para a base de dados AERONAUTA, em função da grande quantidade de dados pessoais que ela armazena, alguns deles inclusive qualificados como sensíveis de acordo com a LGPD. Mais especificamente para as 30 tabelas que foram identificadas e sinalizadas por conterem dados sensíveis ou dados pessoais diretos, em um total de 100 existentes na base de dados.
>
> Importante salientar que há diversos controles de segurança implementados na ANAC como um todo (firewalls, antivírus, monitoramento e análise de rede, backup, ações de conscientização de servidores e colaboradores, dentre outras) que resultam em um elevado nível de segurança para as bases de dados como um todo.
>
> Mas apesar de todos os aspectos positivos acima descritos face ao elevado nível de adequação à LGPD, visando aumentar ainda mais a proteção aos direitos e liberdades fundamentais dos titulares dos dados, bem como diminuir riscos de violação de privacidade, recomenda-se criptografar as informações destas tabelas com dados sensíveis e dados pessoais diretos. Para as tabelas com dados pessoais indiretos, em função do esforço adicional de correlação de informações que seria necessário para identificar o titular à que pertencem, optou-se por não recomendar criptografá-las.
>
> Conclui-se, assim, por recomendar que as tabelas com dados pessoais sensíveis e dados pessoais diretos sejam criptografadas. Importante salientar que se trata de uma recomendação e não uma medida imprescindível."

Diante do Cenário apresentado, a STI elaborou Documento Oficial de Demanda SEI nº 6805759 com a seguinte necessidade de contratação:

> "Aquisição de licenças de uso perpétuas da Option Oracle Advanced Security - Processor Perpetual para segurança de banco de dados Oracle e implementação de criptografia de dados em repouso."

Apesar do assunto ser analisado em maior profundidade em seções futuras deste Estudo Técnico, destacam-se dois pontos importantes. O primeiro é relacionado ao nível de aplicação de criptografia, especificamente, dados em repouso. O segundo diz respeito a plataforma tecnológica na qual os dados sensíveis estão armazenados, em exclusivo, o Sistema Gerenciador de Banco de Dados (SGBD) Oracle Database Enterprise (designado como "SGBD Oracle" neste Estudo para fins de simplificação).

A criptografia de dados em repouso consiste em cifrar dados diretamente no sistema de arquivos (storage ou disco) no qual são armazenados. Este recurso representa uma importante medida de segurança para dificultar acesso não autorizado a dados sensíveis caso ocorra furto de arquivos do SGBD (*datafiles*) ou arquivos de backup nos quais estão armazenados. Entretanto, destaca-se que este tipo de criptografia não possui atuação sobre os dados em trânsito na rede ou dados manipulados em memória por servidores e/ou clientes (aplicações, sistemas, usuários e outros).

No que tange a plataforma tecnológica, aponta-se que, em resumo, um SGBD é um software responsável por prover acesso, armazenamento, persistência, manipulação e organização dos dados. a diversos clientes (aplicações, sistemas, usuários e outros) de forma a garantir segurança, desempenho e consistência.

A ANAC utiliza quatro SGBDs diferentes: SQL Server, Oracle, PostGres e Mysql. Levantamento realizado em fevereiro de 2022 constatou a seguinte distribuição de dados em SGBDs na Agência (em termos de armazenamento):

Tabela 2 -Levantamento sobre SGBDs da ANAC

SGBD	Servidores	Armazenamento (TB)[1,2]	Parcela Armazenamento (%)
Oracle	9	10	13,89
SQL Server	51	60	83,33
PostGres	14	2	2,78
Mysql	1	0,02	0,03
Total	**75**	**72**	-

[1]Os valores presentes representam totais brutos de armazenamento dos servidores virtuais (VMs) de bancos de dados e incluem o sistema operacional, arquivos temporários e demais presentes em discos dos ambientes de produção, validação e homologação da Agência.

[2]Ademais, aponta-se que houve erro de digitação no item 4.2 do Documento de Oficialização de Demanda (DOD) 6805759 no qual as quantidades de servidores e total de armazenamento constam como 75, mas deveriam ser 75 e 72 TB, respectivamente.

Com base em critérios de importância e criticidade, a STI/ANAC priorizou esforços para endereçar criptografia de dados em repouso em SGDBs através dos seguintes projetos previstos no PDTIC 2022-2023 (SEI nº 7410475):

Tabela 3 - Projetos relacionados a implementação de criptografia de dados em repouso presentes no PDTIC 2022-2023

#	Plano Interno	Nome Projeto	Objetivo estratégico atrelado	Início planejado	Término Planejado

Contratações Infraestrutura					
4	2ATDTI22070	Contratação de Criptografia de dados pessoais em repouso	E11: Aprimorar a gestão da informação para a tomada de decisão	jul/22	mar/23
Estruturantes Infraestrutura (GEIT)					
1	2XTDTI22037	Atualizar a infraestrutura do serviço de banco de dados SQL Server	E11: Aprimorar a gestão da informação para a tomada de decisão	fev/22	mai/22
15	2XTDTI22051	Criptografia de dados pessoais em repouso para SGBD SQL Server, PostgreSQL, MySQL	OE11: Aprimorar a gestão da informação para a tomada de decisão	out/22	dez/22
22	2XTDTI22041	Implantação da Criptografia em repouso	E13: Promover a alocação de recursos de forma estratégica e efetiva	nov/23	abr/24

Verifica-se que a previsão de projetos citados na Tabela 3 foi baseada na premissa presente no item 4.5 do Documento Oficial de Demanda SEI nº 6805759:

> "4.5. Para os SGBD com tecnologias Microsoft SQL Server, PostgreSQL e MySQL, a STI já identificou a possibilidade de implementação da criptografia de dados em repouso com os recursos existentes. Também já iniciou as ações e projetos necessários para realizar a criptografia dos dados nessas tecnologias. Contudo, para o SGBD na tecnologia Oracle, a solução atualmente contratada na ANAC não dispõe do mecanismo apropriado para criptografia de dados em repouso. Sendo assim, faz-se necessária a aquisição de licenciamento de software de componente adicional, também chamado "*option*", para implementar o referido mecanismo de segurança."

Portanto, enfatiza-se que o projeto 2ATDTI22070 ("Contratação de Criptografia de dados pessoais em repouso"), o qual deu origem ao DOD SEI nº 6805759 e a este Estudo Técnico, possui escopo de análise limitado ao SGBD Oracle, uma vez que a implementação de criptografia de dados em repouso nos demais SGBDs (SQL Server, PostgreSQL e MySQL) foi ou será endereçada em projetos diferentes, tais como: 2XTDTI22037 ("Atualizar a infraestrutura do serviço de banco de dados SQL Server") e 2XTDTI22051 ("Criptografia de dados pessoais em repouso para SGBD SQL Server, PostgreSQL, MySQL").

Para fins de completude, o projeto 2XTDTI22041 ("Implantação da Criptografia em repouso") tem como objeto a implementação da solução indicada ao fim deste Estudo Técnico. Sob tal ponto de vista, reforça-se que a criptografia de dados em repouso não é citada pela LGPD e não previne todos os tipos de ataques. No entanto, caso as barreiras de segurança de sistemas operacionais de servidores ou dispositivos de armazenamento nos quais dados sensíveis residam sejam violadas, a tal recuso irá impedir a visualização dos mesmos em formato legível por pessoas não autorizadas.

Logo, a STI/ANAC entende que, além de criptografia de dados em repouso em SGBDs, várias outras medidas técnicas e gerenciais, que não estão no escopo de Estudo Técnico, precisam ser adotadas para garantir atendimento aos requisitos provenientes da LGPD no que tange aos sistemas de informação da Agência.

4. Área requisitante

Área Requisitante	Responsável
Gerência de Infraestrutura Tecnológica	Felipe Santos Sarmanho

5. Necessidades de Negócio

Requisitos de Negócio

1. A solução deve ser contratada para todos os bancos de dados do fabricante Oracle que possuem dados pessoais elegíveis de tratamento pela LGPD.
2. Dados pessoais sensíveis não podem ser acessados fora do banco de dados e/ou por usuários sem privilégios adequados;
3. A solução deve permitir implementação de criptografia em repouso sem necessidade de alteração nas aplicações ou sistemas;
4. A solução não deve impactar de forma significativa a performance do acesso aos dados pelos sistemas e demais componentes do ponto de vista do usuário;
5. Não poderá haver perda ou corrompimento de dados criptografados;
6. A solução deve ter suporte e garantia do fabricante.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
Plano	**Objetivos Estratégicos**
Plano Estratégico da ANAC - 2020-2026	OE11: Aprimorar a gestão da informação para a tomada de decisão
	OE2: Garantir a segurança da aviação civil
	OE6: Fortalecer a gestão de riscos no sistema de aviação civil e a cultura de segurança
	OE13: Promover a alocação de recursos de forma estratégica e efetiva
Estratégia de Governo Digital - 2020 a 2022	Objetivo 10: Implementação da Lei Geral de Proteção de Dados - LGPD no Governo
	Objetivo 1: Oferta de serviços públicos digitais
	Objetivo 11: Garantia da segurança das plataformas de governo digital e de missão crítica

ALINHAMENTO AO PDTIC 2022-2023	
ID	**Ação do PDTIC**
2ATDTI22070	Contratação de Criptografia de dados pessoais em repouso

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
144	Contratação de Criptografia de dados pessoais em repouso

6. Necessidades Tecnológicas

Requisitos Tecnológicos

1. A solução deve ter integração e compatibilidade com as seguintes ferramentas Oracle utilizados pela ANAC:

- Oracle Database Enterprise - Versão 12c ou superior;
- Oracle Recovery manager (RMAN) - Versão 12c ou superior;
- Oracle RAC (Real Application Clusters) - Versão 12c ou superior;
- Tuning Pack - Versão 12c ou superior;
- Diagnostic Pack - Versão 12c ou superior;
- APEX (Oracle Application Express) - Versão 19.1 ou superior.

2. A solução deve ser capaz de encriptar/decriptar qualquer tipo de dado suportado pelo SGBD Oracle, tais como: números, datas, texto e outros;
3. A solução deve oferecer segurança contra tentativas de leitura de dados sensíveis a partir do sistema operacional de servidores Oracle, arquivos de backup (físicos e exports) ou furto de dispositivos físicos de armazenamento;
4. A solução deve utilizar de algoritmos de criptografia padrão de mercado e compatíveis com ePING ("Tabela 6 - Criptografa" do item 2.2 "Especificações Técnicas" do Documento SEI nº 7380334).;
5. A solução não pode exigir nenhum tipo de alteração ou modificação.no sistemas ou aplicações que utilizam o SGBD Oracle.
6. A solução deve possuir processos de criptografia e descriptografia automatizados (sem necessidade de interferência das sistemas ou aplicações)
7. A solução deve possuir mecanismo de armazenamento de chaves criptográficas históricas de forma a permitir rotação das mesmas.
8. A solução deve ser capaz de criptografar dados históricos forma online, ou seja, sem necessidade de desligamento do SGBD Oracle.

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

Não se aplica.

8. Estimativa da demanda - quantidade de bens e serviços

De acordo com o Requisitos de Negócio 2, a solução deve ser contratada para os bancos de dados que possuem dados pessoais armazenados.

Como pode ser visto no email SEI nº 7375362, em pesquisa realizada em março de 2022, a Gerência de Sistemas de Informação (GESI/ANAC), área responsável pela governança da dados da Agência, listou os servidores que se encontram na situação descrita no item anterior:

Tabela 4- Servidores de SGBDs Oracle que possuem dados pessoais na ANAC

ID	Servidor	TCP/IP	Versão	Instância	Banco	Quantidade de Núcleos de Processamento	Quantidade de Memória (GB)
1	SPBDF1034	10.161.50.206	12.2.0.1.0	PRODUCAO1	PRODUCAO	4	20
2	SPBDF1035	10.161.50.208	12.2.0.1.0	PRODUCAO2		4	20
3	SPBDF1087	10.161.50.202	11.2.0.4.0	PRODDW	PRODDW	2	16
4	SHBDF1014	10.161.50.29	12.2.0.1.0	VALIDACAO	VALIDACAO	4	16
				HOMOLOG	HOMOLOG		
				OPHOMOLG	OPHOMOLG		
				TREINA	TREINA		

O resumo de cada banco de dados segue abaixo:

PRODUCAO

O banco PRODUCAO está hospedado no Oracle Database Enterprise 12c e é utilizado pelas aplicações desenvolvidas através do Oracle APEX, tais como: ANAC+, Santos Dumond e outras. É o único da que utiliza tecnologia RAC (Real Application

Clusters) para suportar funcionamento de mais de um servidor (SPBDF1034 e SPBDF1035) de forma paralela com objetivo de prover alta disponibilidade e desempenho.

PRODW

O banco PRODDW está hospedado no Oracle Database Enterprise 11c (servidor SPBDF1087) e é utilizado para armazenar dados negociais gerados por rotinas de ETL (Extract, transform and load) de ferramentas tal como o Power Center.

VALIDAÇÃO

O servidor SHBDF1014 contém 4 bancos de dados, VALIDACAO, HOMOLOG, OPHOMOLG e TREINA, hospedados no Oracle Database Enterprise 12c.. O VALIDACAO representa uma cópia reduzida da base PROD (SPBDF1088) enquanto o HOMOLOG é uma cópia integral da base da base PRODUCAO (SPBDF1034 e SPBDF1035). Ambos são utilizados para realização de testes de recursos e atualizações das aplicações e sistemas antes que sejam submetido(a)s para o ambiente de produção.

Quanto ao OPHOMOLOG e ao TREINA, cabe ressaltar que o primeiro representa o banco de homologação do sistema IBM Open Pages (sistema de Fiscalização Integrada) e o segundo acomoda dados necessários para um ambiente de treinamento de aplicações.

9. Levantamento de soluções

Levantamento de Soluções

Inicialmente, verifica-se que o item 4.14 do Documento de Oficialização de Demanda (DOD) SEI nº 3951135 analisou e demonstrou a inviabilidade de substituição do SGBD Oracle pela ANAC:

> "*Quando da realização da contratação anterior em 2018, a Gerência de Sistemas e Informações - GESI, vinculada a Superintendência de Tecnologia da Informação - STI, foi consultada, e solicitamos que analisassem a possibilidade de refatoração dos sistemas que utilizam o banco de dados ORACLE, para que pudéssemos utilizar outro banco de dados que temos, o MS SQL da MICROSOFT, e nos informaram que os sistemas que utilizam o SGBD ORACLE não possuem uma camada de acesso a dados, necessitando que as camadas de acessos a dados desses sistemas fossem adaptadas para que pudessem utilizar o SGBD SQL Server, o que impactaria a maior parte das funcionalidades desses sistemas, e que redesenvolvimento dos sistemas baseados nas linguagens de programação ASP e JAVA teriam um alto custo (por volta de R$ 3.134.000,00, com base no valor do Ponto de Função do contrato nº 30/ANAC/2015), alto risco e demandariam um tempo considerável. Identificaram também, que as linhas de base desses sistemas somam por volta de 5100 pontos de função, e mesmo que esses sistemas sofressem uma manutenção adaptativa somente nas partes referentes de acesso aos dados, o impacto financeiro aumentaria, e que existem sistemas legados desenvolvidos em ASP.NET que utilizam ORACLE em algumas integrações, e estes também precisariam passar por manutenções adaptativas, para que pudessem ser migrados para o SGBD SQL Server*."

Ademais, os itens 2.1 a 2.3 do Estudo Técnico Premilinar (ETP - documento SEI nº 4120497) elaborado à época da contratação reali

> *"Em consulta realizada para a GESI/STI (área de desenvolvimento de sistemas corporativos) sobre a possibilidade de migração dos sistemas para o SQL Server, a mesma se posicionou que deveria ser mantido o SGBD Oracle por alguns anos. O levantamento foi feito juntamente com a Fábrica de Software (CAST).*
>
> *As aplicações em Java e ASP antigo utilizam predominantemente o SGBD Oracle como banco de dados. Estas, em sua maioria legadas, não possuem uma camada de acesso a dados. Dessa forma, seria necessário um refatoramento de todas estas aplicações. Além disso, boa parte das funcionalidades seriam impactadas, o que constitui um risco adicional para a tarefa. Existe também um custo de oportunidade pois enquanto a Fábrica de Software poderia estar desenvolvendo novos projetos ou demandas evolutivas, ela teria que gastar um esforço com refatoramento de sistemas legados que não atendem completamente aos requisitos dos usuários.*
>
> *Segundo levantamento mais recente realizado, existem 52 sistemas que ainda utilizam as bases de dados Oracle. Segue abaixo:"*

Sistema	***Nome do Projeto***	***Tecnologia***
Aeródromo	*-*	*ASP/SACI*
Agenda	*-*	*ASP.NET*
Alte	*Sistema de Apoio ao Registro Aeronáutico Brasileiro*	*ASP/SACI*
Bav	*-*	*JAVA/SINTAC*
Central de Envio	*-*	*ASP.NET*
Certificação de Centros Alunos	*Certificação de Centros - Alunos*	*ASP/SACI*
Certificação de Centros Escolas	*Gestão de Centros de Ensino da Aviação Civil*	*JAVA/SINTAC*
Civ	*CIV (Caderneta Individual de Voo) Eletrônica*	*ASP/SACI*
Cmbws	*Web Services de retorno da CMB*	*JAVA/SINTAC*
Consulta Aeronaves	*Consulta de Aeronaves*	*ASP/SACI*
Consulta de Licenças	*Consulta de Licença*	*ASP.NET*
Dados Aeronauta	*Atualização Cadastral de Aeronautas*	*ASP/SACI*
E-diam	*Declaração de Inspeção Anual de Manutenção Eletrônica*	*ASP/SACI*
Educator	*Sistema Educator*	*ASP.NET*
Empresa	*Empresa*	*JAVA/SINTAC*
Estatística	*Dados Econômicos e Operacionais das Empresas Aéreas*	*JAVA/SINTAC*
Examcred / Sishab	*Examinador credenciado*	*ASP/SACI*
Exames	*Resultado de Exame DAC*	*ASP/SACI*
GruInternet	*Portal GRU Internet (SIGEC)*	*JAVA/SINTAC*
Habilitação	*Gestão de Habilitações e Licenças de Pessoal da Aviação Civil*	*JAVA/SINTAC*
Hotran	*Horário de Transporte*	*JAVA/SINTAC*
Impressão CHT	*Impressão de CHT Pela Casa da Moeda*	*ASP/SACI*
Info	*Sistema de Informações*	*ASP/SACI*
Map	*Módulo de Aplicação de Provas*	*JAVA/SINTAC*
Nada Consta (Sigec)	*Portal Nada Consta (SIGEC)*	*ASP/SACI*
Parabéns	*Parabéns*	*ASP.NET*
Pel / SIAC	*Processo de Emissão de Licenças*	*ASP/SACI*
Pesqpo	*Pesquisa por Proprietario ou Operador*	*ASP/SACI*
Provas Online	*Provas Online*	*JAVA/SINTAC*
Rds	*Registro de Dificuldade em Serviço de Operações de Aeronaves*	*JAVA/SINTAC*
Registro de Capacitação	*Cadastro de Inspetores da Aviação Civil*	*ASP/SACI*
Reservas de Marcas	*Reserva de Marcas*	*ASP/SACI*
Saci	*Portal Saci*	*ASP*
Sca	*Sistema de Controle de Acesso*	*ASP/SACI*
Scprab	*Sistema Consulta Processual do RAB*	*ASP/SACI*
Sha	*Sistema de Homologação de Aeronaves*	*ASP/SACI*
Siavanac / Siavanac-n	*Sistema Integrado de Emissão e Controle de Autorização de Sobrevoo da ANAC*	*ASP/SACI*
Siavanac-n / Siavanac	*Sistema Autorização de Sobrevoo da Anac - Aeronaves Estrangeiras*	*ASP/SACI*
Siconfac	*Sistema Integrado de Controle e Fiscalização da Aviação Civil*	*ASP/SACI*
Sigad Ikhon	*Sistema Informatizado de Gestão Arquivística de Documentos*	*ASP.NET*
Sigec	*Sistema Integrado de Gestão de Créditos*	*ASP/SACI*
Sisad	*Sistema de Avaliação de Desempenho*	*ASP.NET*
Sishab	*Sistema de Habilitação (empresas aéreas)*	*ASP/SACI*
Sismedcred	*Sistema de Médicos Credenciados*	*ASP/SACI*
Sisrh	*Sistema de Recursos Humanos*	*JAVA/SINTAC*
Sme	*Sistema Modelo Experimental*	*ASP.NET*
Smi	*Sistema de Multas e Infrações 3.0*	*ASP.NET*
Spat	*Sistema de Pesquisa e Analise de Pendências*	*JAVA/SINTAC*
Ste	*Sistema de Departamento Técnico*	*ASP/SACI*

Sva	*Sistema de Vistorias de Aeronaves*	*ASP/SACI*
Upload de Arquivos	*Habilitação - Envio de Documentos*	*ASP/SACI*
Vlee	*Verificação de Licenças a Entidades Estrangeiras*	*ASP/SACI*

Uma vez verificada a necessidade de manutenção do SGBD Oracle na ANAC, acredita-se que alguns termos utilizados neste Estudo

Além disso, em resumo, o processo de criptografia consiste na aplicação de algoritmos complexos aos dados para, em seguida, conv

Os algoritmos simétricos usam uma única chave para proteger os dados e fornecem confidencialidade, integridade e autenticidade. A

Por outro lado, os algoritmos assimétricos utilizam uma chave pública e uma chave privada. A chave pública pode ser livremente dis

Neste Sentido, a importância do gerenciamento de chaves criptográficas deve ser corroborada. A menos que a criação, armazenamer

É importante enfatizar que, independente da solução, o uso de criptografia em SGBDs oferece segurança de perímetro, ou seja, evita

- *Ransonware*;
- *SQL Injection;*
- Comprometimento de chave criptográfica mestra (armazenada em arquivo com senha no sistema operacional do servidor do SGBD ou semelhante);
- Abuso de privilégios (SGBD);
- Privilégios excessivos ou esquecidos (SGBD);
- *DoS ou DDoS* - Negação de Serviço.

Uma vez alinhados os conceitos básicos, visualiza-se três soluções possíveis na ANAC para atender a proteção de dados almejada n

Identificação das Soluções

Tabela 5 - Identificação de Soluções

ID	Descrição da Solução
1	Criptografia no nível da solução de armazenamento (Storage)
2	Criptografia no nível do sistema operacional
3	Criptografia através de soluções de mercado

10. Análise comparativa de soluções

Análise Comparativa de Soluções

Solução 1 - Criptografia no nível da solução de armazenamento (Storage)

A ANAC utiliza solução de *storage* (armazenamento) composta por dois equipamentos Huawei OceanStor Dorado 5000 V3 (adquiridos em 2019 por meio do processo de contratação SEI nº 00058.002919/2018-18), um localizado na sede em Brasília e outro em processo de *moving* para o Centro de Treinamento da ANAC (também em Brasília). Dentre os principais recursos oferecidos pela solução, destaca-se a funcionalidade de criptografia de discos, conforme descrição do arquivo "*Disk Encryption User Guide*" (SEI nº 7571782):

> *"OceanStor Dorado V3 series storage systems support disk encryption, which provides secure storage services without impacting storage performance. The disk encryption function has the following characteristics:*
>
> - *Data in all disks is encrypted transparently without affecting other features such as mirroring, snapshot, deduplication, and compression.*
> - *Automatic key life cycle management and the Key Management Interoperability Protocol (KMIP) are supported, ensuring the openness of key management systems."*

Neste contexto, questionamento sobre a possibilidade de utilização do referido recurso de criptografia para proteção de dados pessoais no SGBD Oracle foi enviado a STI/CDRE (SEI nº 7571181). A resposta, cujo conteúdo completo pode ser visto no mesmo documento (SEI nº 7571181), enfatizou os seguintes pontos sobre o tipo de criptografia oferecido pela referida solução de *storage* :

- Os dados são criptografados quando “entram” em disco e imediatamente descriptografados quando "saem". Assim, nas demais camadas de acesso, incluindo o sistema operacional, os dados permanecem disponíveis em formato legível.
- Este nível de criptografia oferece proteção apenas contra acesso físico não autorizado aos equipamentos e respectivos discos.
- Os equipamentos de storage da ANAC estão armazenados em Salas Seguras com controle de acesso, CFTV (Circuito Fechado de Televisão) e monitoramento.

Além das características acima, a resposta ainda reforçou que a implementação de criptografia através da referida solução *storage* não é possível neste momento, pois tal opção não foi habilitada durante a implantação dos equipamentos na ANAC:

> *"Complementando, a criptografia só pode ser habilitada durante a criação de uma camada lógica sobre os discos físicos chamada Disk Domain. Na ANAC durante a instalação do Storage não existia nenhum requisito de criptografia dos dados no disco e optamos por não habilitar a criptografia. Ao habilitar esta opção criamos um ponto crítico no ambiente que é o gerenciamento de chaves. Caso ocorra algum imprevisto e tenhamos o extravio ou algum outro incidente grave com o gerenciamento de chaves os dados podem ficar inacessíveis e nem mesmo o Suporte da Huawei consegue liberar os dados.*"

Solução 2 - Criptografia no nível do Sistema Operacional

Todos os servidores de SGBD Oracle na ANAC utilizam sistema operacional Oracle Linux 7.9. Neste cenário, há alguns pacotes para implementação de criptografia de dados em repouso. A página "*Configuring and Using Data Encryption*" (SEI nº 7571818) do site oficial do referido sistema operacional lista duas opções:

- dm-crypt - Esse recurso criptografa partições ou discos inteiros (*block devices*) para que os dados fiquem inacessíveis quando o sistema operacional estiver desligado. Ao se iniciar o sistema operacional, caso senha apropriada seja fornecida, os dispositivos protegidos (partição e/ou disco) são descriptografados e seus dados ficam acessíveis.
- eCryptfs - Esse recurso criptografa arquivos e/ou diretórios (*file system*) para que os dados fiquem inacessíveis quando um diretório protegido estiver desmontado. Ao se montar o diretório protegido (no momento de uso), caso senha apropriada senha fornecida, os arquivos protegidos serão descriptografados e seus dados ficam acessíveis.

Ademais, ao realizar pesquisas no *Google*, outras opções de pacotes foram encontradas, tais como loop-AES, EncFS e TrueCrypt /VeraCryp. Porém, verificou-se que, as funcionalidades oferecidas pelos referidos pacotes são semelhantes (no tocante ao SGBD Oracle) e são baseados em dois métodos principais de implementação, *Block Device Encryption e Stacked Filesystem Encryption*, cujo quadro resumo de funcionalidades segue baixo:

Tabela 6 - Comparação entre métodos de criptografia de dados em repouso no Sistema Operacional Linux

	Block Device Encryption	**Stacked filesystem Encryption**
Granularidade da Criptografia	Dispositivo de Bloco (disco rígido, CD-ROM)	Arquivos
Container para dados criptografados	disco ou partição/ arquivo *loop device*	diretório em um sistema de arquivos existente
Relação com o sistema de arquivos	opera abaixo da camada do sistema de arquivos:	adiciona uma camada adicional a um sistema de arquivos existente
Criptografa metadados de arquivo	Sim (usar 'discard' pode revelar tamanhos de arquivo)	Parcial (somente os nomes são criptografados, todos os outros metadados são visíveis))
Pode ser usado para criptografar discos rígidos inteiros de forma personalizada (incluindo tabelas de partição)	Sim	Não
Pode ser usado para criptografar o swap space	Sim	Não
Pode ser usado sem pré-alocar uma quantidade fixa de espaço para o contêiner de dados	Não (usar 'discard' pode permitir contêineres alocados esparsamente, ao	Sim

criptografados	custo de revelar tamanhos de arquivo)	
Pode ser usado para proteger sistemas de arquivos existentes sem bloquear o acesso ao dispositivo (Compartilhamentos NFS ou Samba, armazenamento em nuvem e outros)	Não	Sim
Permite backup offline individual de arquivos criptografados	Não	Sim

A partir da análise das opções apresentadas acima, acredita-se que tais pacotes possuem limitações que dificultam ou impossibilitam o atendimento aos requisitos levantados neste Estudo Técnico. A proteção oferecida garante que os arquivos sensíveis sejam sempre armazenados em disco de forma criptografada. No entanto, uma vez desbloqueados por um mecanismo confiável (através de senha, arquivo e/ou outro), tais arquivos ficam disponíveis para o sistema operacional e os aplicativos em formato legível enquanto o sistema está em execução.

Além disso, não foi possível verificar se tais pacotes possuem serviço oficial de suporte, de forma que, não seria possível garantir o seu funcionamento adequado e/ou mesmo assegurar contratualmente que não ocorra perda de dados criptografados em caso de problemas técnicos avançados.

Solução 3 - Criptografia através de soluções de mercado

Por fim, analisa-se as soluções de mercado para criptografia de dados em repouso.

Em pesquisa realizada no Google, as principais soluções encontradas foram: Oracle Advanced Security, CipherTrust e Security Guardium.

Oracle Advanced Security

O Oracle Advanced Security (OAS) é um *software* categorizado como *Option* que deve contratado como "adicional" ao SGBD Oracle Enterprise para prover recursos avançados de segurança. Outras *Options* da Oracle já foram adquiridas pela ANAC e estão atualmente em utilização, tais como: *Oracle Real Application Clusters (RAC), Diagnostics Pack, Tuning Pack*. A funcionalidade de RAC serve para prover alta disponibilidade para o banco de dados através de utilização de *clusters*. Já as duas últimas servem para apoiar os profissionais de bancos de dados na gestão de eventos relevantes, em especial na identificação, análise e tratamento de problemas de desempenho.

O OAS criptografa os dados específicos dentro dos arquivos do banco de dados Oracle (*datafiles*) independente da infraestrutura de armazenamento ou sistema operacional. Portanto, ao contrário das soluções apresentadas anteriormente, os dados sensíveis permanecem em formato ilegível ao ambiente externo ao SGBD mesmo após inicialização de sistema operacional e montagem de diretórios.

Ademais, há uma outra grande diferença em relação as soluções anteriores: o nível de granularidade da aplicação da criptografia. Ao invés de operar em volumes ou diretórios inteiros, o OAS atua em níveis mais granulares: tablespaces (unidade lógica com um ou mais datafiles) ou coluna(s) (ambos dentro do SGBD Oracle). Apesar de algumas diferenças técnicas, ambas podem ser usadas para atender as recomendações presentes nos Relatórios de Inventário de Dados produzidos pela Gerência Técnica de Gestão da Informação (GTGI), conforme detalhado no item 2. "Descrição da Necessidade" deste Estudo Técnico.

Tal recurso representa um nível superior de proteção em relação as soluções analisadas anteriormente, uma vez que, além de proteção contra acesso físico não autorizado, adiciona-se a proteção contra acesso lógico não autorizado fora do SGBD, tais como o acesso de usuários privilegiados ao sistema operacional de servidores de SGBD Oracle ou acesso a unidades que armazenam arquivos de backup.

É necessário pontuar que o OAS oferece segurança de perímetro, ou seja, evita que tentativas de ataques externas ao SGBG Oracle obtenham visualização de dados protegidos em formato legível. No entanto, quando o usuário se autentica no SGBD, tal solução não pode ser usada para restringir acesso. Portanto, pode-se dizer que o OAS oferece proteção contra usuários do sistema operacional, porém, não possui ação sobre usuários do SGBD.

Reforça-se que a existência de usuários privilegiados em sistemas operacionais e SGBDs é necessária para realização tarefas de administrativas, tais como: realização de *backups/restores*, aplicação de atualizações de versões, modificações de estrutura etc. Atualmente, na ANAC, tais atividades são executadas por terceirizados da empresa Global Web (Contrato nº 21/ANAC/2021) e fiscalizadas por servidores da Agência (há usuários privilegiados em ambos os grupos).

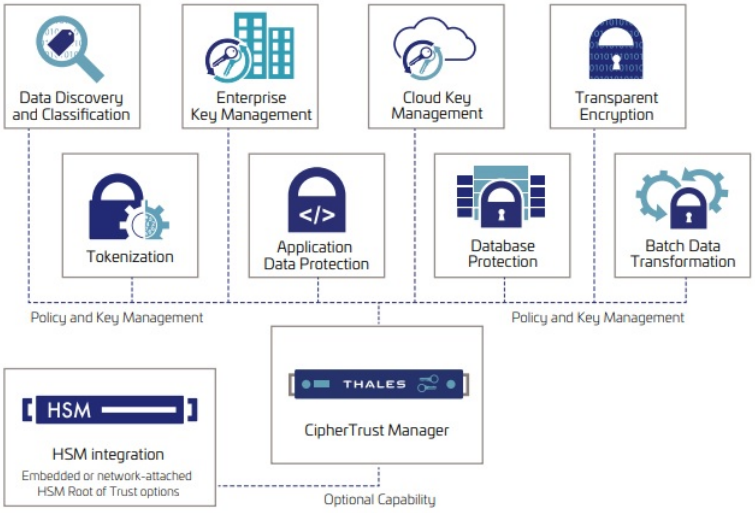
Outra característica importante está relacionada às necessidades de alteração ou adaptação das aplicações e sistemas que acessam dados criptografados. Ao declarar que a solução é transparente, a documentação do OAS confirma que não há impacto na interface SQL que os sistemas e aplicações usam (instruções SQL de entrada e resultados de instruções SQL de saída) devido a existência de processos automatizados de criptografia e a descriptografia gerenciados pelo SGBD.

Ademais, informa-se que o OAS é um *software* que está presente no código fonte do SGBD Oracle Enterprise, ou seja, não precisa de instalação adicional. No entanto, sua utilização depende de licenciamento, ativação e configuração. No caso da ANAC, toda a infraestrutura de SGBDs Oracle é local (instalada em Data Center da Agência) e, neste caso, a única opção de licenciamento é aquisição. Já a ativação e configuração devem seguir passos padronizados pelo Fabricante e incluem criação de um arquivo protegido por senha que contém a chaves criptográficas no sistema operacional dos servidores licenciados.

CipherTrust (antigo Vormetric Data Security Platform)

A solução CipherTrust da empresa Thales é uma *suite* composta por vários módulos que atendem à necessidades relacionadas a segurança da informação, como pode ser visto na imagem abaixo (retirada da página 6 do Documento SEI nº 7612243):

Imagem 1 - Módulos que compõem a solução CipherTrust



Ao contrário da OAS, que é um software específico do SGBD Oracle, CipherTrust é um amplo conjunto de tecnologias que podem ser usadas para proteção de vários tipos de solução de TIC, tais como: servidores de arquivos, servidores de emails, SGBDs e outros. No entanto, ressalta-se que este Estudo Técnico Preliminar analisou apenas os módulos (e respectivas funcionalidades) considerados essenciais para atendimento das necessidades presentes no DOD SEI nº 6805759 e os requisitos elencados em seções anteriores Documento.

Inicialmente, a documentação descreve que o módulo CipherTrust Manager é um *appliance* físico ou virtual que armazena e gerencia chaves de criptografia de dados, políticas de acesso a dados, domínios administrativos e perfis de administrador. É o elemento central e obrigatório da solução CipherTrust, do qual todos os outros componentes dependem.

Já o módulo CipherTrust Transparent Encryption (CTE), como o nome sugere, é o responsável por coordenar a criptografia dos dados em repouso e opera no sistema de arquivos ou no nível do volume de um servidor, independentemente da tecnologia de armazenamento subjacente, fornecendo proteção contra acesso fisco não autorizado.

Ademais, o CTE fornece proteção contra acesso lógico no nível do Sistema Operacional através de políticas de acesso a arquivos protegidos. Tais políticas permitem, dentre outras funcionalidades, a criação de *allow lists*, ou listas "confiáveis" que controlam os acessos e os privilégios a cada arquivo presente em um *Guard Point* (diretório protegido) com base em critérios diversos, tais com o identificação de processo e de usuário. Dessa forma, é possível criar regras que permitam que apenas os processos do SGBD Oracle e respectivo(s) usuário(s) tenham acesso aos arquivos sensíveis.

Através das políticas de acesso, também é possível implementar proteção contra acesso indevido ao conteúdo de arquivos sensíveis por usuários privilegiados do sistema operacional (incluindo o usuário root). Como exemplo, é possível criar regras que permitam que super usuários tenham acesso aos *Guard Point* para realizar tarefas administrativas (tais como: *backup, restore*, atualização de software e outros) sem aplicação de descriptografia por parte do CTE , ou seja, o conteúdo dos arquivos permanece cifrado e ilegível.

O módulo CTE exige que um software, chamado Agente CTE, seja instalado em cada servidor a ser protegido. Após ser instalado, o Agente CTE deve ser registrado no módulo CipherTrust Manager que, por sua vez, deve ser usado para especificar os dispositivos a serem protegidos, as chaves criptográficas a serem utilizadas, as políticas de acesso a serem aplicadas e outras configurações.

É importante ressaltar também que o CipherTrust Manager oferece acesso a um repositório de auditoria centralizado que permite rastrear e monitorar todas as tentativas de acesso aos dados protegidos, assim como oferece integração com soluções de SIEM (Gerenciamento e Correlação de Eventos de Segurança) e com sistemas centralizadores de logs.

Apesar de oferecer mais recursos que o OAS, é importante pontuar que o CTE também oferece apenas segurança de perímetro. Neste caso, vale a mesma regra descrita para a solução anterior, ou seja, tentativas de acesso não autorizadas provenientes do sistema operacional serão frustradas pela criptografia ou barradas pelas políticas de acesso. Porém, os usuários autenticados no SGBD não serão afeados ou terão acesso restringido pela solução.

Outro ponto importante que deve ser considerado neste Estudo Técnico é a necessidade de processamento de dados históricos que devem ser criptografados. Tais dados são decorrentes de anos de operação de sistemas e serviços de TI e, em alguns casos, podem ter volumes significativos. No caso da CipherTrust, para que seja possível realizar tal atividade de forma *online*, ou seja, sem a necessidade de desligar o SGBD Oracle, é necessário contratar um módulo chamado Batch Data Transformation.

Por fim, é importante pontuar que, de acordo com a documentação oficial, a solução CipherTrust opera de forma transparente, ou seja, sem necessidade de alteração de sistemas e serviços relacionados. Além disso, por se tratar de uma tecnologia nunca utilizada pela ANAC, a eventual contratação do CTE demandaria projeto(s) de instalação e implantação, capacitação de pessoal (de terceirizados e servidores), assim como a absorção no Contrato nº 21/ANAC/21 para fornecimento de serviços de operação e manutenção.

Security Guardium

A partir da análise da documentação oficial, verificou-se que apesar de ter nome diferente, a solução Security Guardium (SG), da empresa IBM, é a mesma solução CipherTrust (CT) da empresa Thales comercializada pela IBM através de um contrato do tipo OEM (Original Equipment Manufacturer). Neste sentido, foi encontrada página em site oficial da IBM contendo tabela de mapeamento dos nomes dos produtos entre as duas soluções (página 6 do anexo SEI nº 7626678).

Salvo entendimento equivocado, acredita-se que única diferença entre as soluções está na rede de vendas e serviços (incluindo suporte técnico) sendo a empresa Thales responsável pela CTE e a IBM pela SG.

A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública

Por se tratar de decisão interna e que não envolve contratação, não foi possível verificar ocorrência de implementação das Soluções 1 e 2 para a finalidade pretendida por este Estudo Técnico Preliminar.

Foi conduzida a pesquisa no sitio de Painel de Preços (https://paineldeprecos.planejamento.gov.br/) e ComprasNet (https://www.gov.br/compras/pt-br/acesso-a-informacao/consulta-detalhada) por contratações de soluções similares, voltadas para o SGBD Oracle.

No que tange a solução Oracle Advanced Security (OAS), foram encontrados os seguinte processos de Contratação:

- Tribunal Regional Eleitoral do Maranhão (Pregão Eletrônico nº 30/2021);
- Governo do Estado do Ceará (Pregões Eletrônicos nº 415/2021 e Ata de Registro de Preços nº 04/2018);
- Conselho Federal de Justiça no DF (Pregão Eletrônico nº 19/2019).

Por se tratarem da mesma solução, realizou-se pesquisa pelos termos CipherTrust e IBM Security Guardium. Foram encontradas as seguintes ocorrências de contratação de atualização de licenças e suporte técnico para o segundo:

- Banco Central do Brasil (Pregão Eletrônico nº 129/2021);
- Câmara dos Deputados (Pregão Eletrônico nº 116/2021).

As alternativas do mercado

A análise de alternativas de mercado foi realizada no tópico "Solução 3" do item 9 ("Análise Comparativa de Soluções") deste Estudo Técnico Preliminar.

A existência de software público brasileiro

Em pesquisa realizada em 01/07/2022 através da URL abaixo, não foi encontrado no Portal do Software Público Brasileiro solução(ões) que poderia(m) atender a totalidade das necessidades da ANAC, conforme especificações deste Estudo:

https://softwarepublico.gov.br/social/search/software_infos?utf8=%E2%9C%93&utf8=%E2%9C%93&display=&filter=&software_type=all&query=criptografia&commit=Filtro&software_display=15&sort=rating

As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis:

Não se aplica. No entanto, o suporte a algoritmos de criptografia recomendados na "Tabela 6 - Criptografa" do item 2.2 "Especificações Técnicas" do ePING foi considerado como requisito tecnológico obrigatório da solução neste Estudo Técnico Preliminar.

eMAG

Não se aplica.

Aderência às regulamentações da ICP-Brasil

Não se aplica.

Observância às orientações, premissas e especificações técnicas e funcionais definidas pelo e-ARQ Brasil

Não se aplica.

As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

Não se aplica.

A possibilidade de aquisição na forma de bens ou contratação como serviço;

Análise realizada no item 12 ("Descrição da solução de TIC a ser contratada").

Os diferentes modelos de prestação do serviço;

O Objeto deste Estudo é a aquisição de licenças de software. Toda a operacionalização será realizada pela empresa Global Web através do Contrato n. 21/ANAC/2021. Pontualmente, poderá haver prestação de serviço de suporte técnico pelo fabricante de forma remota, porém, tal programa é provido em formato único e pré-definido pelo fabricante sem margem de análise ou escolha de modelos por parte da ANAC.

Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

Não se aplica.

A ampliação ou substituição da solução implantada.

Conforme consta no item 4.14 do Documento de Oficialização de Demanda SEI nº 3951135, a Gerência de Sistemas (GESI) foi consultada sobre a possibilidade de fatoração (alteração) dos sistemas que utilizam o SGBD Oracle para um outro SGBD e a mesma declarou que tal iniciativa seria inviável por conta do alto custo, risco e tempo necessário.

Quadro resumo de comparação das soluções

Tabela 7- Quadro resumo de comparação das soluções

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1			X[1]
	Solução 2			X[1]
	Solução 3 (OAS)	X		
	Solução 3 (CT)			X[1]
	Solução 3 (SG)	X		
	Solução 1		X	

A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 2		X	
	Solução 3 (OAS)		X	
	Solução 3 (CT)		X	
	Solução 3 (SG)		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2	X		
	Solução 3 (OAS)		X	
	Solução 3 (CT)		X	
	Solução 3 (SG)		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
	Solução 3 (OAS)			X
	Solução 3 (CT)			X
	Solução 3 (SG)			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3 (OAS)			X
	Solução 3 (CT)			X
	Solução 3 (SG)			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
	Solução 3 (OAS)			X
	Solução 3 (CT)			X
	Solução 3 (SG)			X
Requisitos de Negócio	Solução 1		X	
	Solução 2		X	
	Solução 3 (OAS)	X		
	Solução 3 (CT)	X		
	Solução 3 (SG)	X		
Requisitos Tecnológicos	Solução 1		X	
	Solução 2		X	
	Solução 3 (OAS)	X		
	Solução 3 (CT)	X		
	Solução 3 (SG)	X		
Compatibilidade com o ambiente tecnológico da ANAC	Solução 1	X		
	Solução 2	X		
	Solução 3 (OAS)	X		
	Solução 3 (CT)		X	
	Solução 3 (SG)		X	

X[1] - Não foi possível identificar

11. Registro de soluções consideradas inviáveis

Soluções 1 e 2

Conforme registrado no item anterior ("Análise comparativa das soluções"), as Soluções 1 e 2 possuem escopos limitados e previnem apenas acessos não autorizados nas situações em que discos ou dispositivos de armazenamento:

- Possam ser acessados fisicamente devido a falta de segurança física das instalações;
- Possam ser furtados ou roubados;
- Possam sofrer algum tipo de manutenção externa a ANAC;
- Possam ser descartados de forma inapropriada (por defeito ou após fim do ciclo de vida).

Verifica-se que este nível de criptografia é insuficiente para a proteção de servidores SGBD Oracle. Quanto ao aspecto físico, registra-se que todos os servidores de SGBD da ANAC residem em salas seguras com controle de acesso, CFTV (Circuito fechado de televisão) e monitoramento. Quanto ao aspecto lógico, tais servidores precisam estar *online* 100% do tempo e, portanto, seus arquivos e dados sensíveis permaneceriam disponíveis de forma legível no sistema operacional.

Ademais, a Solução 1 não é passível de implementação atualmente, pois a solução de Storage Huawei OceanStor Dorado 5000 V3 não foi habilitada para implementar criptografia durante sua instalação na ANAC e tal configuração não pode ser alterada.

No que tange a Solução 2, verificou-se existir necessidade de intervenção (manual ou *scripts*) para realização dos processos de cifragem dos dados. Também merece destaque o fato de que não se identificou a existência de serviço de suporte oficial para os pacotes analisados, ao ponto que não seria possível garantir o pleno funcionamento dos mesmos em caso de problemas técnicos avançados ou falhas de desenvolvimento.

Pesquisas realizadas no Google não indicaram nenhuma implementação de criptografia de *datafiles* do SGBD Oracle com pacotes de sistema operacional por instituições públicas ou privadas. Entende-se que o referido SGBD possui características que impossibilitam a implementação de criptografia dessa forma, tal como a obrigatoriedade de utilização de *files system e logical volume manager* próprios da Oracle, chamados de Automatic Storage Management (ASM) para ambientes clusterizados, como o banco PRODUCAO (SPBDF1034 e SPBDF1035) que sustenta sistemas como ANAC+ e Santos Dumont na Agência.

Solução 3

No que tange as opções presentes na Solução 3, Oracle Advanced Security (OAS), CipherTrust (CT) e Security Guardium (SG), registra-se que todas atendem aos requisitos levantados neste Estudo Técnico Preliminar. Entretanto, tais soluções possuem nichos de atuação muito diferentes. Enquanto a OAS é um complemento (*option*) do SGBD Oracle com função específica de criptografar colunas e tablespaces sensíveis, a CT e a SG são soluções genéricas de segurança cibernética que possuem, além de recursos de criptografia de arquivos, várias funcionalidades que não fazem pare do escopo deste Estudo, tais como:

- Gerenciamento de ciclo de vida de chaves criptográficas de qualquer solução ou serviço de TI;
- Proteção contra ataques de *ransonware*;
- Criação de domínios administrativos para implementação de segregação de papéis (áreas administrativas);
- Possibilidade de integração com soluções de SIEM (Gerenciamento e Correlação de Eventos de Segurança) ou centralizadoras de logs.

De forma adicional, procedeu-se a análise de compatibilidade das soluções de mercado com o ambiente tecnológico da ANAC. Neste contexto, é importante introduzir de forma resumida os conceitos de sistema operacional (SO) e *kernel*:

- Sistema operacional: programa ou um conjunto de programas que possui duas funções principais: abstração do *hardware* , fazendo o papel de intermediário entre os programas (*software*) e os componentes físicos do computador (*hardware*) e gerenciamento de recursos, controlando as aplicações (processos) a executar, como, quando e com quais recursos (memória, disco, periféricos e outros).

- *Kernel :* núcleo ou componente central do sistema operacional que permite a execução das suas funções principais através de mecanismos de comunicação entre processos e chamadas de sistema.

De forma a possibilitar a análise pretendida, detalhou-se abaixo as características do SO utilizado pelos servidores que fazem parte do escopo deste Estudo Técnico Preliminar:

- **Servidores SPBDF1034 e SPBDF1035 (Cluster)**

  Operating System: Oracle Linux Server 7.9
  CPE OS Name: cpe:/o:oracle:linux:7:9:server

Kernel: Linux 4.14.35-2047.511.5.7.el7uek.x86_64
Architecture: x86-64

- **Servidor SPBDF1087**

Operating System: Oracle Linux Server 7.9
CPE OS Name: cpe:/o:oracle:linux:7:9:server
Kernel: Linux 4.14.35-2047.508.3.3.el7uek.x86_64
Architecture: x86-64

- **Servidor SHBDF1014**

Operating System: Oracle Linux Server 7.9
CPE OS Name: cpe:/o:oracle:linux:7:9:server
Kernel: Linux 4.14.35-2047.508.3.3.el7uek.x86_64
Architecture: x86-64

Como pode ser visto acima, o SO utilizado é o Oracle Linux Server 7.9 e o *kernel* base é Linux 4.14.35 do tipo UEK (Unbreakable Enterprise Linux). Este kernel é uma customização feita pela Oracle a partir do código fonte do Red Hat Enterprise Linux (RHEL) com o objetivo de prover recursos avançados de desempenho, segurança e integração entre os componentes de *hardware* e *software* da marca. Além disso, o Oracle Linux Server pode ser instalado e implantado sem custos de licenciamento em ambientes corporativos.
Uma vez coletadas as informações acima, as Matrizes de Compatibilidade e Matizes de Certificação das soluções OAS, CT e SG foram analisadas. A primeira, como já explicado anteriormente, faz parte do software Oracle Database Enterprise o qual está instalado e em utilização na ANAC há muitos anos. Mesmo assim, foi realizada busca no site oficial da fabricante e verificou-se que há formalização da compatibilidade entre o referido SGBD e o SO detalhado no parágrafo anterior (Anexo SEI nº 7869597).

A mesma análise foi realizada para as soluções CT e SG e uma incompatibilidade técnica foi encontrada. As referidas soluções não possuem suporte para o SO utilizado pelos servidores de SGBD Oracle da ANAC, conforme verificação realizada site oficial da fabricante Thales (Anexo SEI nº 7869691). Ao se listar as versões suportadas de *kernels* da plataforma RHEL 7.9, verifica-se que a versão utilizada pela ANAC não é exibida. Além disso, o seguinte aviso é apresentado: "*RHEL-7.9 Kernels (CentOS and OEL non-UEK Redhat like same kernel version is compatible.*)"

O problema reside no fato das soluções CT e SG não possuírem suporte para o *kernel* do tipo UEK (*Unbreakable Enterprise Kernel).* Neste contexto, é importante enfatizar que não é possível alterar o *kernel* de uma instalação de Linux do tipo UEK para tipo "não-UEK". Esse tipo de mudança exige a criação de um novo servidor com SO adequado e posterior migração completa do SGBD.

No entanto, a ANAC utiliza o recurso de virtualização chamado Oracle Virtual Machine (OVM), que permite que um equipamento servidor físico de grande capacidade de processamento seja dividido em servidores virtuais com menores capacidades de processamento. De acordo com o anexo SEI nº 8062351, a combinação do SO Oracle Linux com o virtualizador OVM é obrigatória para permitir que o licenciamento do Oracle Database seja realizado de acordo com a quantidade de núcleos de processamento dos servidores virtuais (vCPU) ao invés da quantidade total de núcleos de processamento do equipamento físico.

Na ANAC, as licenças do Oracle Database Enterprise (Contrato nº 35/ANAC/2018) e, posteriormente, do serviço de suporte técnico e direito de atualização (Contrato nº 23/ANAC/2020) foram dimensionadas com base na referida arquitetura. Portanto, qualquer alteração de tecnologia em relação ao sistema operacional ou ao virtualizador citados no parágrafo anterior colocaria a Agência em situação de irregularidade.

Ainda, reforça-se que apenas um banco de dados Oracle da ANAC, PRODUCAO (SPBDF1034 e SPBDF1035)**,** está atualmente configurado para ter alta disponibilidade na forma de cluster ativo-ativo, ou seja, com mínimo de indisponibilidade para falhas ou manutenções programadas. Dessa forma, uma eventual migração de servidores incorreria em períodos de indisponibilidade de sistemas e aplicações relacionados, além de possuir riscos técnicos difíceis de serem previstos por este Estudo Técnico, pois exigem análises de impacto de cada SO candidato a ser considerado.

Ademais, atualmente, na ANAC, todos os servidores de SGBD Oracle possuem o mesmo SO. Tal configuração facilita a manutenção e gestão dos ambientes. De tal forma, eventual decisão por alteração de SO afetaria não apenas os servidores que fazem parte do escopo deste Estudo, mas toda a infraestrutura de SGBDs Oracle da Agência.

A incompatibilidade dos produtos CT e SG com o ambiente da ANAC também foi apontada através de e-mail SEI nº 7787047 por uma das revendas que foram consultadas por ocasião da pesquisa de preços de mercado. Acredita-se que tal fato tenha desmotivado as empresas, pois mesmo tendo a STI enviado solicitações para várias delas, como pode ser visto no documento SEI nº 8070994, nenhuma cotação comercial foi obtida.

12. Análise comparativa de custos (TCO)

Entende-se que, dentre todas as soluções identificadas e analisadas neste Estudo Técnico Preliminar, apenas a Oracle Advanced Security (OAS) pode ser considerada viável, uma vez que, atende aos requisitos propostos e é compatível com o ambiente tecnológico da ANAC. Logo, apenas a referida solução será considerada na composição de preços neste Estudo Técnico Preliminar.

Os Catálogos de Soluções de TIC com Condições Padronizadas são instrumentos previstos na Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, com redação dada pela Instrução Normativa SGD/ME nº 202, de 18 de setembro de 2019. De acordo com § 3º, as estimativas de preços de itens constantes nos Catálogos de Soluções de TIC com Condições Padronizadas deverão utilizar como parâmetro o Preço Máximo de Compra de Item de TIC (PMC-TIC), salvo se a pesquisa de preços realizada nos termos deste artigo resultar em valor inferior ao PMC-TIC.

No momento de elaboração deste Estudo, o Catálogo do Acordo Corporativo N. 10/2021 firmado entre SGD/ME e Oracle (SEI nº 7379867) estabelece que o PMC-TIC para aquisição de uma licença perpétua do Oracle Advanced Security incluindo serviços de suporte e direito de atualização por 12 meses é R$ 77.231,50.

Ademais, foi realizada pesquisa de preços praticados em licitações semelhantes (SEI nº 7411376). Para manter a padronização, os valores apresentados estão precificados nas mesma condições do item acima:

Tabela 8 - Processos licitatórios semelhantes

ID	Item	Modelo de Licenciamento	Órgão	Pregão	Valor Unitário (R$)	Quantidade
1	Oracle Advanced Security	Licença Perpétua + Suporte e Atualização (SA)	TRE-MA	30/2021	67.500,00	4
			Estado do Ceará -ETICE	415/2021	65.943,00	10
			Conselho Federal de Justiça no DF[1]	29/2019	Não Definido	Ilimitada
			Estado do Ceará (ETICE)[2]	10/2017	59.999	24

[1] O processo de contratação do Conselho Federal de Justiça no DF (Pregão Eletrônico Nº 19/2019) contém o produto Oracle Advanced Security como um dos item do seu Objeto. Porém, não foi possível precificar as licenças de forma individual, pois foi utilizada a modalidade ilimitada, na qual o órgão pode instalar e utilizar, em seu parque tecnológico, qualquer quantidade dos produtos contratados pagando um valor "fixo".

[2] O Valor Unitário foi obtido a partir da ARP Nº 0004/2018. Devido a data do processo licitatório, esta cotação não será considerada.

Além disso, foram solicitadas propostas comerciais de vários fornecedores de produtos Oracle (SEI nº 7410419) e a compilação das respostas segue abaixo:

Tabela 9 - Resumo das cotações comercias do OAS

ID	Item	Modelo de Licenciamento	Vigência SA	Empresa	Valor Unitário (R$)	Quantidade	Valor Total (R$)
1	Oracle Advanced Security	Licença Perpétua + Suporte e Atualização (SA)	12 meses	LTA-RH Informática	116.712,61	7	816.988,27
				Accerte Tecnologia da Informação	143.391,01	7	1.003.737,07
				Bertini do Brasil	136.488,00	7	955.416,00
				VS Data	110.671,074	7	774.697,52
				IT One	102.957,09[1]	7	720.699,66
				Service IT	105.880,672[2]	7	741.164,69

[1] Para obtenção do valor unitário, os valores dos itens "Software Updates" e "Product Support" presentes na proposta e foram divididos por 7 e somados ao item "Licença Perpétua".
[2] Para obtenção do valor unitário, os valores dos itens "ORACLE ADVANCED SECURITY - PROCESSOR PERPETUAL", "ORACLE LICENÇA DE ATUALIZAÇÃO - 1 ANO" e "ORACLE SUPORTE - 1 ANO" presentes na proposta foram divididos por 7 e somados.

Com o objetivo de estimar o valor unitário da licenças do Oracle Advanced Security (OAS) foi realizada a média aritmética entre as seguintes cotações:

Tabela 10 - Média de preços unitários de licenças do do OAS

Origem	Tipo	Valor Unitário (R$)
TRE-MA (30/2021)	Processo Licitatório	67.500,00
Estado do Ceará - ETICE (415/2021)	Processo Licitatório	65.943,00
LTA-RH Informática	Proposta Comercial	116.712,61
Accerte Tecnologia da Informação	Proposta Comercial	143.391,01
Bertini do Brasil	Proposta Comercial	136.488,00
VS Data	Proposta Comercial	110.671,07
IT One	Proposta Comercial	102.957,09
Service IT	Proposta Comercial	105.880,67
Média		**105.553,20**

Como pode ser observado, apesar de todo esforço envolvido na pesquisa de processos de contratações similares e obtenção de cotações junto a fornecedores, o valor unitário obtido é superior ao PMC-TIC previsto no acordo Acordo Corporativo N. 10 /2021. Portanto, a referência unitária máxima para estimativa de preços de licenças do OAS neste Estudo será R$ 77.231,50.

Tabela 11 - Descrição do Cenário Viável

Cenário Viável

Descrição: Aquisição de licenças do Oracle Advanced Security (OAS) para os banco de dados PRODUCAO (SPBDF1034 e SPBDF1035), PRODDW (SPBDF1087) e VALIDACAO (SHBDF1014).

Aquisição de 7 licenças perpétuas do Oracle Advanced Security com suporte técnico e direito de atualização de 12 meses.

Os bancos de dados da Oracle com dados pessoais da ANAC estão cobertos.

Requisitos de Negócio são atendidos;

Requisitos Tecnológicos são atendidos.

Custo Total de Propriedade – Memória de Cálculo

ID	Item	Modelo de Licenciamento	Vigência SA	Valor Unitário (R$)	Quantidade	Valor Total (R$)
1	Oracle Advanced Security	Licença Perpétua + Suporte e Atualização (SA)	12 meses	77.231,50	7	540.620,50

13. Descrição da solução de TIC a ser contratada

A equipe de planejamento da contratação orienta pela contratação da solução Oracle Advanced Security, pois, conforme demonstrado ao longo dos itens 8, 9 e 10 deste Estudo Técnico Preliminar, é a única opção que atende aos requisitos propostos e é compatível com o ambiente tecnológico da ANAC.

Cumpre assinalar que todos os servidores de SGBD Oracle estão hospedados em salas seguras localizadas dentro da ANAC. Neste contexto, a única forma de contratação da solução Oracle Advanced Security é a aquisição de licenças de direito de uso perpétuo.

O serviço de suporte técnico por parte da fabricante e direito de atualização são essenciais para atendimento das requisitos levantados, especialmente no que diz respeito ao correção de eventuais falhas, erros ou bugs de código, assim como, apoio técnico do fabricante para solução de problemas avançados que podem comprometer a integridade e disponibilidade dos dados.

Além disso, como o OAS faz parte do software Oracle Database Enterprise, a não contratação do direito de atualização para o primeiro impedira atualização do SGBD nos servidores que compõe o escopo deste Estudo Técnico. Vale lembrar que há previsão de projeto identificado como 2XTDTI22056 no PDTI 2022-2023 cuja descrição é "Atualizar infraestrutura de Oracle para versão mais recente".

A Oracle Advanced Security foi precificado juntamente com serviço de suporte e direito de atualização por 12 meses como item único no Acordo Corporativo N. 10/2021 firmado entre SGD/ME e Oracle (SEI nº 7379867). Dessa forma, não se vislumbra possibilidade de parcelamento da solução.

14. Estimativa de custo total da contratação

Valor (R$): 540.620,50

A Oracle oferece duas formas de licenciamento dos seus produtos: as métricas *Named User Plus* e *Processor*. A primeira métrica utiliza o número de usuários do ambiente de banco de dados para calcular a quantidade de licenças necessárias. Nesse contexto, usuário é entendido como qualquer pessoa que interage direta ou indiretamente (através de uma interface *web*, por exemplo) com os dados armazenados no SGBD.

A segunda métrica, *Processor*, utiliza a quantidade de núcleos de processamento ou *cores* da máquina para o cálculo do licenciamento. A quantidade de licenças necessárias pode variar de acordo com o modelo específico do processador. Para a arquitetura de processamento atual da ANAC, *Intel Xeon*, existe uma proporção de 2 *cores* para 1 licença.

Conforme listado no item 8 "Levantamento de Soluções", os bancos de dados a serem atendidos pela solução Oracle Advanced Security (OAS) sustentam sistemas e serviços ofertados ao público externo, em especial regulados da ANAC. Como não é possível prever a quantidade de usuários que podem interagir com os dados, acredita-se que a opção *Processor* é a mais viável. Cabe ressaltar que tal característica está mais relacionada ao propósito dos bancos de dados envolvidos do que ao recurso de criptografia (OAS).

Neste sentido, é importante salientar que o Contrato nº 35/ANAC/2018 e o Contrato nº 20/ANAC/2020 optaram pela métrica *Processor*. O primeiro foi responsável pela aquisição de licenças perpétuas de SGBD Oracle Enterprise e tecnologias relacionadas, tais como: Oracle Real Application Clusters, Oracle Tuning Pack e Oracle Diagnostic Pack . Já o segundo teve como função contratar serviços de suporte técnico e direito de atualização para os referidos produtos após o fim do vigência do primeiro.

Por fim, Cumpre assinalar que os bancos de dados que constituem o escopo deste Estudo Técnico Preliminar estão detalhados no item 7 "Estimativa da demanda -quantidade de bens e serviços" totalizando 4 servidores com 14 núcleos de processamento, que no modelo de licenciamento escolhido, exigem a contratação de 7 licenças. Ademais, o valor unitário de R$ 77.231,50 inclui serviço de suporte técnico e direito de atualização por 12 meses e foi estimado de acordo com metodologia descrita no item 11 "Análise comparativa de custos (TCO)"

Portanto, segue abaixo a tabela resumo com a estimativa total do custo da contratação (TCO):

Tabela 12 - Estimativa Total do Custo da Contratação

ID	Item	Modelo de Licenciamento	Vigência SA	CÓD. PMC-TIC	Valor Unitário (R$)	Quantidade	Valor Total (R$)
1	Oracle Advanced Security	Licença Perpétua + Suporte e Atualização (SA)	12 meses		77.231,50	7	540.620,50

15. Justificativa técnica da escolha da solução

Conforme demonstrado ao longo dos itens 8, 9 e 10 deste Estudo Técnico Preliminar, dentre todas as soluções identificadas e analisadas, apenas a Oracle Advanced Security (OAS) pode ser considerada viável, uma vez que, atende aos requisitos propostos e é compatível com o ambiente tecnológico da ANAC.

No que tange a ferramentas de mercado, é importante enfatizar que as soluções CipherTrust da Thales e Security Guardium da IBM, grandes *players* mundiais, possuem incompatibilidade técnica com o sistema operacional utilizado pelos servidores SGBD Oracle da ANAC. De forma paralela, acredita-se que adoção de ferramentas não identificadas por este Estudo, especialmente, aquelas provenientes de fabricantes de menor porte, podem impor riscos semelhantes ou até mais graves.

Tal afirmativa é justificada pelo fato de que as soluções de criptografia externas ao SGBD criam uma dependência para a inicialização e funcionamento do último. Caso a solução de criptografia possua defeito ou incompatibilidade não identificada ou documentada, há risco de perda ou corrompimento de dados criptografados de forma definitiva. Neste caso hipotético, não haveria possibilidade de acionamento do serviço de suporte ou responsabilização da Oracle (fabricante do SGBD).

Cumpre assinalar que além de criptografar dados entrantes no banco de dados, a solução terá a responsabilidade de processar e criptografar todo o histórico de dados pessoais sensíveis em repouso no SGBD Oracle. Considerando que tais ativos sustentam sistemas e serviços importantes ao cumprimento da missão institucional da ANAC, acredita-se que a OAS pode prover o nível esperado de proteção contra vazamento de dados pelo sistema operacional enquanto garante a integridade e disponibilidade dos dados, uma vez que outros produtos da referida fabricante vêm sendo utilizados com alto grau de confiança pela STI desde a criação da Agência.

Por fim, cabe assinalar que a OAS oferece criptografia em nível colunar (colunas e tablespaces) de forma não invasiva e com o mínimo de impacto possível, pois não exige criação de estruturas auxiliares dentro do banco de dados, tais como: tabelas, gatilhos (*triggers*), visões (*views*) e esquemas (*schemas*) ou exige desenvolvimento de código interno PL/SQL (procedimentos, funções e outros). Entende-se que tais fatos representam grandes vantagens em termos de estabilidade, desempenho e eficiência de armazenamento.

16. Justificativa econômica da escolha da solução

Foram analisadas alternativas de criptografia de dados em repouso utilizando recurso atualmente disponíveis na ANAC, como a solução de armazenamento Huawei OceanStor Dorado 5000 V3 (Solução 1) e a utilização de ferramentas específicas do sistema operacional Linux (Solução 2). No entanto, ambas foram consideradas insuficientes para atendimento aos requisitos, pois, dentre outros motivos, proveem apenas proteção contra acesso físico não autorizado.

Por lado, as soluções de mercado analisadas, CipherTrust e Guardium Data Encryption, são tecnicamente incompatíveis com o *kernel* sistema operacional do ambiente Oracle da ANAC. Ressalta-se que a decisão pela mudança e migração dos servidores de banco dados Oracle para torna-los compatíveis com as referidas soluções violaria as regras de licenciamento do tipo *"hard*

partitioning", previstas no documento SEI nº 8062351, e colocaria ANAC em situação de irregularidade em relação ao licenciamento do Oracle Database Enterprise.

No que tange ao dimensionamento da solução escolhida, Oracle Advanced Security (OAS), salienta-se que foi realizado levantamento atualizado com a área de Governança de Dados (GESI/ANAC) em fevereiro de 2022 para se determinar cuidadosamente os bancos de dados da Oracle da Agência que possuem dados pessoais de forma a se estimar a quantidade mínima de licenças necessárias para atendimento aos requisitos.

Ademais, apesar de exigir ativação e configuração após aquisição das licenças, a solução Oracle Advanced Security não necessita de instalação, pois já faz parte do *software* do SGBD Oracle Database Enterprise. Dessa forma, os riscos e a complexidade do projeto de implantação são reduzidos, ao mesmo tempo que novas contratações ou aditivos contratuais são dispensados, pois tais atividades estão previstas no objeto do Contrato n. 21/ANAC/2021 (Global Web).

Por fim, como demonstrado no item 11 "Análise comparativa de custos TCO" deste Estudo, realizou-se extensiva pesquisa de propostas comercias e busca de processos de contratação semelhantes com a intenção de obter o mínimo valor unitário como estimativa, concluindo-se que a adoção do parâmetro Preço Máximo de Compra de Item de TIC (PMC-TIC) presente no Acordo Corporativo N 10-2021 (SEI nº 7379867) é a opção mais econômica.

17. Benefícios a serem alcançados com a contratação

Implementar criptografia de dados pessoais em repouso em SGBDs Oracle em auxílio ao atendimento à LGPD;

Impedir vazamento de dados pessoais sensíveis através do sistema operacional de servidores e dispositivos de armazenamento que armazenam datafiles os arquivos de backup.

Impedir extração de dados a partir do acesso a discos ou dispositivos de armazenamento perdidos, roubados ou desativados (defeituosos);

18. Providências a serem Adotadas

A implantação do Oracle Advanced Security (OAS) na ANAC foi prevista como projeto 2XTDTI22041 no PDTIC 2022-2023 com o título "Implantação da Criptografia em repouso" e será executado no escopo do Contrato Nº 21/ANAC/2021 (Global Web) com execução estimada para o primeiro semestre 2023, após a conclusão de processo de contratação em tela.

19. Declaração de Viabilidade

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

19.1. Justificativa da Viabilidade

Conforme demonstrado no decorrer deste Estudo Técnico Preliminar, foi verificada a solução do Oracle Advanced Security como tecnicamente viável, haja vista ser compatível com o ambiente tecnológico da ANAC além de que demonstra ter menor esforço operacional para implementação. Ademais, a solução do Oracle Advanced Security é padronizada quanto ao teto de preço pela SGD/ME, por meio de Acordo com Oracle.

20. Responsáveis

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

Despacho: Integrante Requisitante

FELIPE SANTOS SARMANHO

Agente de contratação

Assinou eletronicamente em 31/08/2023 às 13:04:01.

Despacho: Integrante Técnico

WILLIAN ROCHA BICALHO

Agente de contratação

Assinou eletronicamente em 31/08/2023 às 18:34:35.

Despacho: Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

FERNANDO ANDRE COELHO MITKIEWICZ

Autoridade Máxima de TIC - ANAC

Assinou eletronicamente em 31/08/2023 às 19:11:20.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - catalogo-oracle-2021-v3.pdf (1.26 MB)
- Anexo II - POC Delphix - Projeto 487738.pdf (687.92 KB)
- Anexo III - lifetime-support-technology-069183.pdf (372.89 KB)
- Anexo IV - Funcionalidade Data Redaction - Oracle Database 12c _ Oracle Brasil.pdf (770.3 KB)
- Anexo V - LGPD.pdf (871.09 KB)
- Anexo VI - Encryption and Redaction with OAS 19c.pdf (930.43 KB)
- Anexo VII - Oracle Advanced Security Data Redaction - FAQ.pdf (415.99 KB)

Anexo I - catalogo-oracle-2021-v3.pdf

CONTRATAÇÕES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

CATÁLOGO DE SOLUÇÕES DE TIC COM CONDIÇÕES PADRONIZADAS

(ORACLE)

MINISTÉRIO DA ECONOMIA
PÁTRIA AMADA BRASIL GOVERNO FEDERAL

Catálogo de Soluções de TIC com Condições Padronizadas - Oracle

Fabricante:	**Oracle do Brasil Sistemas Ltda.**
Versão do Catálogo:	3.0.0
Responsável pela elaboração e manutenção:	Secretaria de Governo Digital do Ministério da Economia (SGD).
Fundamento normativo:	Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, alterada pela Instrução Normativa SGD/ME nº 202, de 18 de setembro de 2019.
Data de publicação no DOU:	30/12/2021

Vigência:
Imediata a partir da publicação.

MINISTÉRIO DA ECONOMIA
Secretaria Especial de Desburocratização, Gestão e Governo Digital
Secretaria de Governo Digital

ANEXO I

CATÁLOGO DE PRODUTOS E SERVIÇOS

Acordo Corporativo nº 10/2021 - Processo nº 19974.100702/2019-21

1. Condições de utilização:

1.1. A existência deste Catálogo não obriga, direta ou indiretamente, qualquer órgão ou entidade que integre os poderes da União, Estados ou Municípios a celebrar qualquer contrato para a aquisição ou fornecimento de licenças ou serviços Oracle.

1.2. O órgão ou entidade, a partir de sua necessidade, deve realizar os estudos técnicos preliminares, analisando soluções alternativas e demais orientações previstas nas leis e normas que regem as contratações de soluções de tecnologia da informação e comunicação.

CATÁLOGO DE TIC COM CONDIÇÕES PADRONIZADAS – ORACLE					
Item	**Categoria**	**Descrição**	**Modelo de Licenciamento**	**PMC-TIC(1)**	**Vigência SA**
OR-001	Plataforma de Dados	Oracle Database Enterprise Edition	Licença Perpétua + Suporte e Atualização (SA)	R$ 244.566,43	12 meses
OR-002	Plataforma de Dados	Oracle Tuning Pack	Licença Perpétua + Suporte e Atualização (SA)	R$ 25.743,85	12 meses
OR-003	Plataforma de Dados	Oracle Real Application Clusters	Licença Perpétua + Suporte e Atualização (SA)	R$ 118.421,62	12 meses
OR-004	Plataforma de Dados	Oracle Partitioning	Licença Perpétua + Suporte e Atualização (SA)	R$ 59.210,84	12 meses
OR-005	Plataforma de Dados	Oracle Diagnostics Pack	Licença Perpétua + Suporte e Atualização (SA)	R$ 38.615,72	12 meses
OR-006	Plataforma de Dados	Oracle Active Data Guard	Licença Perpétua + Suporte e Atualização (SA)	R$ 59.210,82	12 meses

OR-007	Plataforma de Dados	Oracle Advanced Security	Licença Perpétua + Suporte e Atualização (SA)	R$ 77.231,50	12 meses
OR-008	Plataforma de Dados	Oracle Data Masking and Subsetting Pack	Licença Perpétua + Suporte e Atualização (SA)	R$ 59.210,82	12 meses
OR-009	Plataforma de Dados	Oracle Audit Vault and Database Firewall	Licença Perpétua + Suporte e Atualização (SA)	R$ 30.892,60	12 meses
OR-010	Plataforma de Dados	Oracle Database Vault	Licença Perpétua + Suporte e Atualização (SA)	R$ 59.210,82	12 meses
OR-011	Plataforma de Dados	Oracle Label Security	Licença Perpétua + Suporte e Atualização (SA)	R$ 59.210,82	12 meses
OR-012	Plataforma de Dados	Oracle Multitenant	Licença Perpétua + Suporte e Atualização (SA)	R$ 90.103,42	12 meses
OR-013	Plataforma de Dados	Oracle Key Vault	Licença Perpétua + Suporte e Atualização (SA)	R$ 514.876,70	12 meses
OR-014	Plataforma de Dados	Oracle GoldenGate	Licença Perpétua + Suporte e Atualização (SA)	R$ 90.103,42	12 meses
OR-015	Plataforma de Dados	Oracle GoldenGate for Non Oracle Database	Licença Perpétua + Suporte e Atualização (SA)	R$ 90.103,42	12 meses
OR-016	Plataforma de Dados	Oracle GoldenGate for Mainframe	Licença Perpétua + Suporte e Atualização (SA)	R$ 514.876,70	12 meses
OR-017	Plataforma de Dados	Oracle GoldenGate for Big Data	Licença Perpétua + Suporte e Atualização (SA)	R$ 102.975,34	12 meses
OR-018	Plataforma de Dados	Oracle Management Pack for Oracle GoldenGate	Licença Perpétua + Suporte e Atualização (SA)	R$ 18.020,68	12 meses
OR-019	Plataforma de Dados	Oracle GoldenGate Foundation Suite	Licença Perpétua + Suporte e Atualização (SA)	R$ 38.615,75	12 meses

(1) - O Preço Máximo de Compra de Item de TIC (PMC-TIC) possui validade conforme previsto na Cláusula Quinta "Da Vigência", do Acordo Corporativo nº 10/2021, considerando seus termos aditivos.

Documento assinado eletronicamente por **Ulysses César Amaro de Melo**, **Secretário(a) Substituto(a)**, em 28/12/2021, às 18:19, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Cristiano Jorge Poubel de Castro**, **Coordenador(a)-Geral**, em 28/12/2021, às 18:48, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Tony Gomes Tonete**, **Usuário Externo**, em 29/12/2021, às 10:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Daniel Darlen Corrêa Ribeiro**, **Usuário Externo**, em 29/12/2021, às 11:47, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.economia.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **21289993** e o código CRC **7B1EC427**.

Referência: Processo nº 19974.100702/2019-21. SEI nº 21289993

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 30/12/2021 | Edição: 246 | Seção: 3 | Página: 59

Órgão: Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de Governo Digital

EXTRATO DE TERMO ADITIVO

a) Espécie: Primeiro Termo Aditivo ao Acordo Corporativo nº 10/2021 que celebram a União, por intermédio da Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, e a empresa Oracle do Brasil Sistemas Ltda.

b) Processo SEI/ME: nº 19974.100702/2019-21.

c) Objeto: Atualização do Anexo I ao Acordo Corporativo nº 10/2021, visando à inclusão de novos produtos e serviços em conformidade com as condições comerciais pactuadas no instrumento principal.

d) Fundamentação Legal: Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, alterada pela Instrução Normativa SGD/ME nº 202, de 18 de setembro de 2019.

e) Despesa: O presente Termo Aditivo não contempla repasse de recursos financeiros entre os partícipes.

f) Prazo de vigência: O Primeiro Termo Aditivo ao Acordo Corporativo nº 10/2021 terá validade a partir da publicação no Diário Oficial da União.

g) Data de Assinatura: 29 de dezembro de 2021. Signatários: Ulysses Cesar Amaro de Melo, Secretário de Governo Digital Substituto da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, e Tony Gomes Tonete, Procurador da Oracle do Brasil Sistemas Ltda.

MINISTÉRIO DA
ECONOMIA

PÁTRIA AMADA
BRASIL
GOVERNO FEDERAL

www.economia.gov.br

Anexo II - POC Delphix - Projeto 487738.pdf

Willian Rocha Bicalho

De: portaldeservicos@anac.gov.br
Enviado em: sexta-feira, 4 de março de 2022 16:20
Para: Willian Rocha Bicalho
Assunto: Projeto 487738 - Entregável Aprovado
Anexos: REC_FROM_GED_164640.docx; REC_FROM_GED_161432.xlsx

Prezados(as),

Informamos que foi concluída a etapa "Realizar Fiscalização do Projeto" do projeto número 487738 pela ANAC - Agência Nacional de Aviação Civil, e como resultado, o **entregável foi aprovado.**

Segue abaixo algumas informações:

- **Solicitante do Projeto**: Felipe Santos Sarmanho
- **Número**: 487738
- **Serviço**: Atender Demanda de TI - Projetizada
- **Descrição**: Prezados,

  a pedido do Superintendente, Gustavo Sanches, e do Gerente, Marcelo Lino, solicito o apoio para a realização da POV/POC da ferramenta DELPHIX.

  Esta demanda envolve as seguintes ações:
  Ação 1: A ANAC tem que definir a data aproximada de instalação, para geração do link, e também, se vai realizar a POV somente nos dados abertos do RAB ou se vai usar a base de dados Oracle do RAB (envolve o curador dos dados);
  Ação 2: A BLUE solicitará ao fabricante a disponibilização de um link para download de uma imagem de máquina virtual (OVA) contendo a aplicação;
  Ação 3: A BLUE e a DELPHIX necessitarão de duas agendas (de 1 hora cada, por meio de videoconferência) com a equipe de infraestrutura para realizar a instalação. Existe a necessidade de duas agendas por conta de um teste intermediário;
  Ação 4: A BLUE e a DELPHIX necessitará de uma agenda (por meio de videoconferência) com a equipe de banco de dados e/ou área de dados e/ou administrador do sistema a ser utilizado na POV. Nesta etapa os dados são realmente ingeridos pela plataforma.

  Apoio da GlobalWeb é necessário especificamente para a Ação 3 e 4.
  Quanto as Ações 1 e 2, ainda estão em tratativas pela gestão da ANAC. Então solicito aguardar estas ações.

  Oportunamente iremos passar o contato da empresa Blue (representante da Delphix) para que a equipe da GlobalWeb entre em contato faça o agendamento para implantação da ferramenta.

  Para esta demanda,
  - solicito que NÃO seja elaborado o documento de planejamento técnico.
  - solicito que seja enviado por e-mail, depois do alinhamento com a empresa Blue, o cronograma de atividades e prazos acordados.

Atenciosamente,

Gestão de Projetos GlobalWeb
Superintendência de Tecnologia da Informação - STI

Telefones para contato, Interno: 9000 e Externo: 0800-617767
E-mail para contato: portaldeservicos@anac.gov.br

Anexo III - lifetime-support-technology-069183.pdf

ORACLE

Oracle Technology Products

Oracle Lifetime Support Policy

January 20, 2022 | Version 1.00

TABLE OF CONTENTS

ORACLE LIFETIME SUPPORT: 3

From Five Years to Forever 3

ORACLE LIFETIME SUPPORT: 5

Oracle Essbase Releases 6

Oracle SQL Developer Data Modeler Releases 7

Oracle REST Data Services (formerly Application Express Listener) 8

Oracle's Ikan Releases 9

Oracle Collaboration Suite Releases 10

Oracle Beehive Releases 10

Oracle Enterprise Manager Releases 10

Oracle Business Transaction Management Releases (Formerly Amberpoint) 11

Oracle Real User Experience Insight Releases (Formerly Moniforce) 12

Oracle Application Testing Suite Releases 13

Oracle's mValent Releases 14

Oracle Rdb Database Releases 15

Oracle CODASYL DBMS Database Release 15

Oracle TimesTen In-Memory Database Releases 15

Oracle Berkeley DB (Formerly Sleepycat) Releases 16

Oracle Database Lite Releases 18

Oracle Database Mobile Server 18

Oracle Reliaty Backup Releases 18

Oracle Secure Backup Releases 19

Oracle Warehouse Builder Releases 19

Oracle's JD Edwards EnterpriseOne Extended Process Integration (XPI) Releases 19

Oracle's Auptyma Release 20

Oracle Express Server Release 20

Oracle Gateway Release's 20

Oracle's TripleHop Releases 23

Oracle Secure Enterprise Search 23

Oracle Application Express (Formerly HTML DB) 23

Oracle Zero Data Loss Appliance Releases 24

Oracle Fail Safe Releases 24

Oracle's ClearApp Releases 25

Oracle Virtual Iron Releases 25

Oracle's Secerno Releases 26

Oracle Audit Vault and Database Firewall Releases 27

Oracle Key Vault Releases 27

Oracle's MySQL Releases 27

Oracle's NoSQL Database Release 28

Oracle Big Data Appliance 29

Oracle Big Data SQL 29

Oracle Big Data Connectors 29

Oracle Big Data Spatial and Graph 30

Oracle Exadata Storage Server Software 31

ORACLE TECHNOLOGY

Maximize your support investment, unlock the full value of your Oracle products, and control your upgrade strategy—with the industry's leading support policy.

Simple, predictable, flexible, and the most comprehensive support policy available, the Oracle Lifetime Support Policy helps drive your business success. Oracle's industry leading support policy covers your entire technology environment, from database to middleware to applications—an industry first, only from Oracle.

Oracle's Lifetime Support Policy also puts you in control of your upgrade strategy. Our flexible support policy stages make it easier for you to plan and budget for Oracle's exclusive product upgrades. You'll enjoy continued peace of mind, knowing that we'll always be there to support your business. When it's time to upgrade, you'll have rights to major product releases, so you can benefit from Oracle's technology leadership and keep pace with the world of business.

Expect lifetime support. Expect control of your technology future—with Oracle's Lifetime Support Policy.

ORACLE LIFETIME SUPPORT:

From Five Years to Forever

Oracle Lifetime Support Policy

With Oracle Support, you know up front and with certainty how long your Oracle products are supported. The Lifetime Support Policy provides access to technical experts for as long as you license your Oracle products and consists of three support stages: Premier Support, Extended Support, and Sustaining Support. It delivers maximum value by providing you with rights to major product releases so you can take full advantage of technology and product enhancements. Your technology and your business keep moving forward together.

Premier Support provides a standard five-year support policy for Oracle Technology products. You can extend support for an additional three years with Extended Support for specific releases or receive indefinite technical support with Sustaining Support.

Premier Support

As an Oracle customer, you can expect the best with Premier Support, our award-winning, nextgeneration support program. Premier Support provides you with maintenance and support for your Oracle Database products for five years from their general availability date. You benefit from

- Major product and technology releases
- Technical support
- My Oracle Support
- Updates, fixes, security alerts, data fixes, and critical patch updates
- Tax, legal, and regulatory updates
- Upgrade scripts
- Certification with most new third-party products/versions
- Certification with most new Oracle products

Extended Support

Your technology future is assured with Oracle's Extended Support. Extended Support lets you stay competitive, with the freedom to upgrade on your timetable. If you take advantage of Extended Support, it provides you with an extra three years of support for specific Oracle releases for an additional fee. You benefit from

- Major product and technology releases
- Technical support
- My Oracle Support
- Updates, fixes, security alerts, data fixes, and critical patch updates
- Tax, legal, and regulatory updates
- Upgrade scripts
- Certification with most existing third-party products/versions
- Certification with most existing Oracle products

Extended Support may not include certification with some new third-party products/versions.

Sustaining Support

Sustaining Support puts you in control of your upgrade strategy. When Premier Support expires, if you choose not to purchase Extended Support, or when Extended Support expires, Sustaining Support will be available for as long as you license your Oracle products. With Sustaining Support, you receive technical support, including access to our online support tools, knowledgebases, and technical support experts. You benefit from

- Major product and technology releases
- Technical support
- Access to My Oracle Support
- Fixes, updates, and critical patch updates created during Premier Support and Extended Support (if offered and only after the Extended Support period ends)
- Upgrade scripts created during the Premier Support stage

Sustaining Support does not include

- New updates, fixes, security alerts, data fixes, and critical patch updates
- New tax, legal, and regulatory updates
- New upgrade scripts
- Certification with new third-party products/versions
- Certification with new Oracle products

For more specifics on Premier Support, Extended Support, and Sustaining Support, please refer to Oracle's 'Technical Support Policies'.

ORACLE LIFETIME SUPPORT:

Coverage for Oracle Technology Products

Oracle Database Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
8.1.7	Sept 2000	Dec 2004	Dec 2006	Indefinite
9.2	Jul 2002	Jul 2007	Jul 2010	Indefinite
10.1	Jan 2004	Jan 2009	Jan 2012	Indefinite
10.2	Jul 2005	Jul 2010	Jul 2013	Indefinite
11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
11.2	Sep 2009	Jan 2015	Dec 2020	Indefinite
Enterprise Edition 12.1 [2]	Jun 2013	Jul 2018	Jul 2022	Indefinite
Standard Edition (SE) 12.1	Jun 2013	Aug 2016	Not Available	Indefinite
Standard Edition One (SE1) 12.1	Jun 2013	Aug 2016	Not Available	Indefinite
Standard Edition 2 (SE2) 12.1 [2]	Sep 2015	Jul 2018	Jul 2022	Indefinite
12.2.0.1 [1]	Mar 2017	Nov 30, 2020 (Limited Error Correction Period for 12.2.0.1 – Dec 1, 2020 – Mar 31, 2022)	Not Available	Indefinite

[1] Oracle Database 12.2.0.1: Premier Support error correction provided for the period of December 1, 2020 through March 31, 2022 will be limited to Severity 1 production fixes and security fixes delivered via the Quarterly Release Update (RU) process. Error Correction support will be available only for the following platforms: Linux x86-64, Solaris x86-64, Solaris SPARC, IBM AIX on Power Systems, IBM Linux on System Z (ZLinux), HP-UX Itanium, Fujitsu BS2000 and Microsoft Windows x64. This extension excludes:

- Functional upgrades of any kind, issues associated with Third-Party software, and certifications with new versions of the OS; embedded components in the Oracle Database that rely upon de-supported releases of Java products; updates to any cryptography related functionality, including, but not limited to, Transport Layer Security (TLS), network encryption, and other forms of secured communications.
- Embedded components in the Oracle Database that rely upon de-supported releases of Java products; updates to any cryptography related functionality, including, but not limited to, Transport Layer Security (TLS), network encryption, and other forms of secured communications.

[2] Oracle Database 12.1.0.2 : Extended Support is offered for the period August 2021 through July 2022 for the following platforms: Linux x86-64, Linux on IBM Z, IBM AIX on POWER Systems (64 bit), HP-UX Itanium, Fujitsu BS2000, Oracle Solaris on SPARC, Oracle Solaris on x86-64 and Microsoft Windows x64. Please note that the Microsoft Windows 2008 version used for building the Oracle Database 12.1.0.2 Windows platform reached end-of-life support on January 14, 2020. However, we will make reasonable efforts to deliver patches for Database 12.1.0.2 for Windows until July 2022, as long as our tooling continues to function.

Oracle Database Releases (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
18c	Jul 2018	Jun 2021	Not Available	Indefinite
19c (Long Term Release)	Apr 2019	Apr 2024	Apr 2027	Indefinite
21c (Innovation Release)	Aug 2021	Apr 2024	Not Available	Indefinite

For more detailed information on bug fix and patch release policies and dates, please refer to the Database Error Correction Support Policy (Doc ID 209768.1) and the Release Schedule of Current Database Releases (Doc ID 742060.1)

Information on upgrade paths can be found in the Database Upgrade Guide for the release you plan to upgrade to. Product documentation can be found at https://docs.oracle.com in the Oracle Help Center.

Oracle Essbase Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Essbase 21.x	Dec 2020	Aug 2025	Not Available	Indefinite

For previous Oracle Essbase releases, please see the Middleware and Applications LSP.

Oracle SQL Developer Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
1.0	Mar 2006	Mar 2011	Not Available	Indefinite
1.1	Dec 2006	Mar 2011	Not Available	Indefinite
1.2	Jun 2007	Jun 2012	Not Available	Indefinite
1.5	Apr 2008	Apr 2013	Not Available	Indefinite
2.1	Dec 2009	Dec 2014	Not Available	Indefinite
3.0	Mar 2011	Mar 2016	Not Available	Indefinite
3.1	Feb 2012	Feb 2017	Not Available	Indefinite
3.2	Aug 2012	Aug 2017	Not Available	Indefinite
4.0	Sep 2014	Sep 2019	Not Available	Indefinite

Oracle SQL Developer Releases (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
4.1	May 2015	May 2020	Not Available	Indefinite
4.2	Apr 2017	Apr 2022	Not Available	Indefinite
17.2	Jul 2017	Jul 2022	Not Available	Indefinite
17.3	Oct 2017	Oct 2022	Not Available	Indefinite
17.4	Dec 2017	Dec 2022	Not Available	Indefinite
18.1	Apr 2018	Apr 2023	Not Available	Indefinite
18.2	Jul 2018	Jul 2023	Not Available	Indefinite
18.3	Oct 2018	Oct 2023	Not Available	Indefinite
18.4	Jan 2019	Jan 2024	Not Available	Indefinite
19.1	Apr 2019	Apr 2024	Not Available	Indefinite
19.2	Sep 2019	Sep 2024	Not Available	Indefinite
19.4	Dec 2019	Dec 2024	Not Available	Indefinite
20.2	Jun 2020	Jun 2025	Not Available	Indefinite
20.4	Jan 2021	Jan 2026	Not Available	Indefinite
21.2	Jul 2021	Jul 2026	Not Available	Indefinite

Oracle SQL Developer Data Modeler Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
2.0	Jul 2009	Jul 2014	Not Available	Indefinite
3.0	Jan 2011	Jan 2016	Not Available	Indefinite
3.1	Feb 2012	Feb 2017	Not Available	Indefinite
3.3	Mar 2013	Mar 2018	Not Available	Indefinite

Oracle SQL Developer Data Modeler Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
4.0	Sep 2014	Sep 2019	Not Available	Indefinite
4.1	May 2015	May 2020	Not Available	Indefinite
4.2	Apr 2017	Apr 2022	Not Available	Indefinite
17.2	Jul 2017	Jul 2022	Not Available	Indefinite
17.3	Oct 2017	Oct 2022	Not Available	Indefinite
17.4	Dec 2017	Dec 2022	Not Available	Not Available
18.1	Apr 2018	Apr 2023	Not Available	Not Available
18.2	Jul 2018	Jul 2023	Not Available	Not Available
18.3	Oct 2018	Oct 2023	Not Available	Not Available
18.4	Jan 2019	Jan 2024	Not Available	Not Available
19.1	Apr 2019	Apr 2024	Not Available	Not Available
19.2	Aug 2019	Aug 2024	Not Available	Not Available
19.4	Nov 2019	Nov 2024	Not Available	Indefinite
20.2	Jun 2020	Jun 2025	Not Available	Indefinite
20.3	Oct 2020	Oct 2025	Not Available	Indefinite
20.4	Jan 2021	Jan 2026	Not Available	Indefinite
21.1	Apr 2021	Apr 2026	Not Available	Indefinite
21.2	Jul 2021	Jul 2026	Not Available	Indefinite

Oracle REST Data Services (formerly Application Express Listener)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
1.0	Jul 2010	Jul 2015	Not available	Indefinite
1.1	Mar 2011	Mar 2016	Not available	Indefinite

Oracle REST Data Services (formerly Application Express Listener) (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
2.0	Dec 2012	Dec 2017	Not available	Indefinite
3.0	Jun 2015	Jun 2020	Not available	Indefinite
17.4	Dec 2017	Dec 2022	Not available	Indefinite
18.1	Apr 2018	Apr 2023	Not available	Indefinite
18.2	Jul 2018	Jul 2023	Not available	Indefinite
18.3	Oct 2018	Oct 2023	Not available	Indefinite
18.4	Jan 2019	Jan 2024	Not available	Indefinite
19.1	Apr 2019	Apr 2024	Not available	Indefinite
19.2	Aug 2019	Aug 2024	Not available	Indefinite
19.4	Dec 2019	Dec 2024	Not Available	Indefinite
20.2	Jul 2020	Jul 2025	Not Available	Indefinite
20.3	Oct 2020	Oct 2025	Not Available	Indefinite
20.4	Jan 2021	Jan 2026	Not Available	Indefinite
21.1	Jan 2021	Jan 2026	Not Available	Indefinite
21.2	Jul 2021	Jul 2026	Not Available	Indefinite

Oracle's Ikan Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
CWD4ALL (All releases)	Not Available	Not Available	Not Available	Aug 2009
Oracle-Branded Releases				
Oracle SQL Developer Data Modeler 2.0.0.57.0	Jul 2009	Jul 2014	Jul 2017	Indefinite

Support for all CWD4ALL releases will end August 31, 2009. Customers are advised to use the Oracle-branded product, Oracle SQL Developer Data Modeling.

Oracle Collaboration Suite Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
9.0.3	Dec 2002	Oct 2005	Not Available	Not Available
9.0.4	Apr 2004	Mar 2007	Not Available	Mar 2010
10.1	Aug 2005	Aug 2010	Aug 2013	Indefinite

Support retirement dates have already been announced for Oracle Collaboration Suite 9.0. For more detailed information on bug fix and patch release policies and dates, please refer to the Database Error Correction Support Policy (Doc ID 209768.1)

Oracle Beehive Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Beehive 2.0	Feb 2010	Feb 2015	Feb 2018	Indefinite
Beehive Voicemail for 2.0	Feb 2010	Feb 2015	Not Available	Indefinite

Oracle Enterprise Manager Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Enterprise Manager Grid Control 10.1	Feb 2004	Feb 2009	Feb 2012	Indefinite
Enterprise Manager Grid Control 10.2	Oct 2005	Nov 2011	Nov 2014	Indefinite
Enterprise Manager Grid Control 11.1	Apr 2010	Apr 2015	Apr 2018	Indefinite
Enterprise Manager Cloud Control 12.1	Oct 2011	Oct 2016	Oct 2020	Indefinite
Enterprise Manager Cloud Control 13.x	Dec 2015	Dec 2023	Dec 2026	Indefinite

Oracle Business Transaction Management Releases (Formerly Amberpoint)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
AMS 5.0 and Earlier	Not Available	Not Available	Not Available	Not Available
AMS 6.0.5.1	Feb 2010	Mar 2012	Not Available	Not Available
AMS 6.1.4.1	Feb 2010	Mar 2012	Not Available	Indefinite
AMS 6.5.3.x	Feb 2010	Mar 2012	Not Available	Indefinite
SNMP Adapter 1.0.1.1	Feb 2010	Mar 2012	Not Available	Indefinite
Datapower Observer 1.0.2.0	Feb 2010	Mar 2012	Not Available	Indefinite
BW Observer 2.2.1.0	Feb 2010	Mar 2012	Not Available	Indefinite
Cisco AXG Observer (All Versions)	Not Available	Not Available	Not Available	Not Available
BMC Adapter (All Versions)	Not Available	Not Available	Not Available	Not Available
HPOVO Adapter (All Versions)	Not Available	Not Available	Not Available	Not Available
Internal Tools (All Versions)	Not Available	Not Available	Not Available	Not Available
Jigsaw Tools (All Versions)	Not Available	Not Available	Not Available	Not Available
MOM Adapter (All Versions)	Not Available	Not Available	Not Available	Not Available
SCOM Adapter (All Versions)	Not Available	Not Available	Not Available	Not Available
SiteScope Adapter (All Versions)	Not Available	Not Available	Not Available	Not Available
TEC Adapter (All Versions)	Not Available	Not Available	Not Available	Not Available
Oracle Branded Releases				
Oracle Business Transaction Management 6.5.4.x	Apr 2010	Apr 2012	Apr 2014	Indefinite
Oracle Business Transaction Management 11.1.x	Mar 2011	Mar 2016	Mar 2019	Indefinite
Oracle Business Transaction Management 12.1.x	Oct 2011	Oct 2016	Oct 2019	Indefinite

Note: No Certification will be provided to new OS and 3rd Party products for legacy AmberPoint releases and any AMS 6.0.x, 6.1.x and 6.5.x release not listed will receive indefinite sustaining support.

Oracle Real User Experience Insight Releases (Formerly Moniforce)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
UXinsight 4.3x	Oct 2007	Jun 2008	Not Available	Not Available
UXinsight 4.4	Feb 2008	Dec 2008	Not Available	Not Available
webProbe 3.2.x 32bit	Jun 2005	Not Available	Not Available	Dec 2010
webProbe 3.6.x (32 and 64 bit)	Jun 2007	Not Available	Not Available	Dec 2010
webProbe 3.6.4 64bit	Jan 2008	Dec 2009	Not Available	Dec 2010
webSensor Enterprise 3.2.x 32bit	Jun 2005	Not Available	Not Available	Dec 2010
webSensor Enterprise 3.6.x (32 and 64 bit)	June 2007	Not Available	Not Available	Dec 2010
webSensor Enterprise 3.6.4 64bit	Jan 2008	Dec 2009	Not Available	Dec 2010
webSensor Commerce 3.2.x 32bit	Jun 2005	Not Available	Not Available	Not Available
webSensor Commerce 3.6.x (32 and 64 bit)	Jun 2007	Not Available	Not Available	Not Available
webSensor Commerce 3.6.4 64bit	Jan 2008	Jan 2009	Jan 2009	Jan 2009
webAlarm	Not Available	Jan 2009	Jan 2009	Jan 2009
Oracle Branded Releases				
Oracle Real User Experience Insight 4.4.1	Mar 2008	Dec 2009	Dec 2010	Dec 2011
Oracle Real User Experience Insight 4.5.x	Sep 2008	Sep 2010	Sep 2012	Indefinite
Oracle Real User Experience Insight 5.x	Apr 2009	Apr 2011	Apr 2013	Indefinite
Oracle Real User Experience Insight 6.0.x	Nov 2009	Nov 2011	Nov 2013	Indefinite
Oracle Real User Experience Insight 6.5.x	Apr 2010	Apr 2012	Apr 2014	Indefinite
Oracle Real User Experience Insight 11.1.x	Oct 2010	Oct 2015	Oct 2018	Indefinite
Oracle Real User Experience Insight 12.1.x	Oct 2011	Oct 2016	Oct 2019	Indefinite
Oracle Real User Experience Insight 13.x	Dec 2015	Dec 2023	Dec 2026	Indefinite

The migration path for webAlarm is to use Oracle's existing service-level monitoring solution.

Oracle Application Testing Suite Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
e-TEST suite 5.x and earlier	Not Available	Not Available	Not Available	Not Available
e-TEST suite 6.x	Not Available	Not Available	Not Available	Not Available
e-TEST suite 7.x	Not Available	Not Available	Not Available	Not Available
e-TEST suite 8.0	Mar 2005	Not Available	Not Available	Not Available
e-TEST suite 8.1	Jun 2006	Not Available	Not Available	Not Available
e-TEST suite 8.2	Apr 2007	Not Available	Not Available	Jun 2009
Oracle Application Testing Suite 8.3	Jun 2008	Jun 2010	June 2012	Indefinite
Oracle Application Testing Suite 8.4	Sep 2008	Sep 2010	Sep 2012	Indefinite
Oracle Application Testing Suite 8.5	Jan 2009	Jan 2011	Jan 2013	Indefinite

Oracle Application Testing Suite Releases (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Application Testing Suite 9.0	Sep 2009	Sep 2011	Sep 2013	Indefinite
Oracle Application Testing Suite 9.1	Apr 2010	Apr 2015	Apr 2018	Indefinite
Oracle Application Testing Suite 9.2	Nov 2010	Nov 2015	Nov 2018	Indefinite
Oracle Application Testing Suite 9.3	Aug 2011	Aug 2016	Aug 2019	Indefinite
Oracle Application Testing Suite 12.x	May 2012	May 2017	May 2020	Indefinite
Oracle Application Testing Suite 13.x	Jun 2017	Jun 2022	Jun 2025	Indefinite

Oracle's mValent Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
mValent Integrity 3.x and earlier	Jan 2006	Not Available	Not Available	Not Available
mValent Integrity 4.0	Jan 2006	Not Available	Not Available	Not Available
mValent Integrity 4.1.x	Jan 2006	Not Available	Not Available	Not Available
mValent Integrity 4.2.x	Dec 2007	Not Available	Not Available	Not Available
mValent Integrity 5.0.x	Dec 2007	Not Available	Not Available	Dec 2011
mValent Integrity 5.1.x	Sep 2008	Not Available	Not Available	Dec 2011
mValent Integrity 5.2.x	Dec 2008	Not Available	Not Available	Dec 2012
mValent Integrity 5.3.x	Feb 2009	Dec 2011	Dec 2013	Indefinite

Oracle Rdb Database Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
7.0	Oct 1996	Aug 2007	Aug 2009	Indefinite
7.1	Jul 2001	Dec 2007	Dec 2010	Indefinite
7.2	Jan 2006	Jul 2015	Jul 2017	Indefinite
7.3	Mar 2011	Sep 2020	Sep 2023	Indefinite
7.4	Aug 2020	Sep 2023	Not Available	Indefinite

Oracle CODASYL DBMS Database Release

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
7.0	Oct 1996	Aug 2007	Aug 2009	Indefinite
7.1	Jul 2001	Dec 2007	Dec 2010	Indefinite
7.2	Jan 2006	Jul 2015	Jul 2017	Indefinite
7.3	Mar 2011	Sep 2020	Sep 2023	Indefinite
7.4	Nov 2021	Sep 2023	Not Available	Indefinite

Oracle TimesTen In-Memory Database Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
5.0	Nov 2003	Nov 2005	Not Available	Not Available
5.1	Oct 2004	Oct 2006	Not Available	Not Available
6.0	Sep 2005	Sep 2008	Sep 2009	Indefinite
7.0	Feb 2007	Feb 2012	Feb 2015	Indefinite
11.2.1	May 2009	May 2014	May 2017	Indefinite
11.2.2	Jan 2012	Jan 2021	Jan 2023	Indefinite
18.1	May 2018	May 2023	May 2026	Indefinite
22.1	Nov 2021	Nov 2026	Nov 2029	Indefinite

The releases of the Oracle Database Enterprise Edition Option TimesTen Application-Tier Database Cache will follow the same support timeframe as the associated Oracle TimesTen In-Memory Database releases.

Oracle Berkeley DB (Formerly Sleepycat) Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
3.1.14	Jun 2000	Dec 2006	Dec 2007	Indefinite
3.1.17	Aug 2000	Dec 2000	Dec 2007	Indefinite
3.2.9	Jan 2001	Dec 2006	Dec 2007	Indefinite
3.3.11	Jul 2001	Dec 2007	Dec 2010	Indefinite
4.0.14	Dec 2001	Dec 2008	Dec 2011	Indefinite
4.1.25	Sep 2002	Dec 2008	Dec 2011	Indefinite
4.2.52	Nov 2003	Dec 2008	Dec 2011	Indefinite
4.3.29	Nov 2004	Dec 2009	Dec 2012	Indefinite
4.4.20	Nov 2005	Dec 2010	Dec 2013	Indefinite
4.5	Sep 2006	Sep 2011	Sep 2014	Indefinite
4.6.21	Nov 2007	Nov 2012	Nov 2015	Indefinite
4.7.25	May 2008	May 2013	May 2016	Indefinite
4.8.30	Apr 2010	Apr 2015	Apr 2018	Indefinite
Berkeley DB 11.2.5.0	Nov 2010	Nov 2015	Nov 2018	Indefinite
Berkeley DB 11.2.5.1	Jan 2011	Jan 2016	Jan 2019	Indefinite
Berkeley DB 11.2.5.2	Jun 2011	Jun 2016	Jun 2019	Indefinite
Berkeley DB 11.2.5.3	Dec 2011	Dec 2016	Dec 2019	Indefinite
Berkeley DB 12.1.6.0	Jun 2013	Jun 2018	Jun 2021	Indefinite
Berkeley DB 12.1.6.1	Jun 2014	Jun 2019	Jun 2022	Indefinite
Berkeley DB 12.1.6.2	Jan 2016	Jan 2021	Jan 2024	Indefinite
Berkeley DB XML 1.2.1	Feb 2004	Dec 2007	Dec 2010	Indefinite
Berkeley DB XML 2.0.9	Jan 2005	Dec 2008	Dec 2011	Indefinite

Oracle Berkeley DB (Formerly Sleepycat) Releases (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Berkeley DB XML 2.1.8	May 2005	Dec 2008	Dec 2011	Indefinite
Berkeley DB XML 2.2.13	Jan 2006	Jan 2009	Jan 2012	Indefinite
Berkeley DB XML 2.3	Jan 2007	Jan 2012	Jan 2015	Indefinite
Berkeley DB XML 2.4	Apr 2008	Apr 2013	Apr 2016	Indefinite
Berkeley DB XML 11.2.2.5	Aug 2009	Aug 2014	Aug 2017	Indefinite
Berkeley DB XML 12.1.6.0	Sep 2014	Sep 2019	Sep 2022	Indefinite
Berkeley DB Java Edition 1.7.1	Feb 2005	Feb 2008	Not Available	Indefinite
Berkeley DB Java Edition 2.0.42	Jun 2005	Jun 2008	Jun 2010	Indefinite
Berkeley DB Java Edition 2.0.54	Jul 2005	Jul 2008	Jul 2010	Indefinite
Berkeley DB Java Edition 2.0.90	Nov 2005	Nov 2008	Nov 2010	Indefinite
Berkeley DB Java Edition 2.1.30	Jan 2006	Jan 2011	Jan 2014	Indefinite
Berkeley DB Java Edition 3.0.11	May 2006	May 2011	May 2014	Indefinite
Berkeley DB Java Edition 3.1.0	Sep 2006	Sep 2011	Sep 2014	Indefinite
Berkeley DB Java Edition 3.1.25	Oct 2006	Oct 2011	Oct 2014	Indefinite
Berkeley DB Java Edition 3.2	Dec 2006	Dec 2011	Dec 2014	Indefinite
Berkeley DB Java Edition 3.3	Jun 2008	Jun 2013	Jun 2016	Indefinite
Berkeley DB Java Edition 4.0	Dec 2009	Dec 2014	Dec 2017	Indefinite
Berkeley DB Java Edition 11.2.4	Nov 2010	Nov 2015	Nov 2018	Indefinite
Berkeley DB Java Edition 11.2.5	Dec 2011	Dec 2016	Dec 2019	Indefinite
Berkeley DB Java Edition 12.1.6	May 2014	May 2019	May 2022	Indefinite

Older releases of Oracle Berkeley DB, Oracle Berkeley DB XML, and Oracle Berkeley DB Java Edition not listed will receive indefinite Sustaining Support.

Oracle Database Lite Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
10.0	Jul 2004	Dec 2008	Dec 2010	Indefinite
10.2	Sep 2005	Dec 2009	Dec 2011	Indefinite
10.3	Apr 2007	Dec 2012	Dec 2015	Indefinite

Oracle Database Lite releases will follow the support time frames for the most recent Oracle Fusion Middleware version for which the Oracle Database Lite release is certified.

For Oracle products which require or embed Oracle Database Lite (for example Oracle Mobile Field Service and Oracle E-Business Suite), Oracle Database Lite will be supported according to the support schedule of those products, even if the support dates extend beyond those for Oracle Database Lite support.

Oracle Database Mobile Server

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
11.1	Oct 2011	Oct 2016	Oct 2019	Indefinite
11.2	Oct 2012	Oct 2017	Oct 2020	Indefinite
11.3	Oct 2013	Oct 2018	Oct 2021	Indefinite
12.1	Apr 2015	Apr 2020	Apr 2023	Indefinite

Oracle Reliaty Backup Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
3.1.3.x	Not Available	Aug 2007	Not Available	Indefinite

Customers should plan to migrate to Oracle Secure Backup 10.1.

Oracle Secure Backup Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
10.1	Apr 2006	Dec 2008	Not Available	Indefinite
10.2	Nov 2007	May 2010	Not Available	Indefinite
10.3	Jun 2009	Dec 2012	Not Available	Indefinite
10.4	Oct 2011	Oct 2016	Not Available	Indefinite
12.1	Feb 2015	Feb 2020	Not Available	Indefinite
12.2	Jan 2018	Jan 2023	Not Available	Indefinite
18.1	Dec 2019	Jan 2024	Not Available	Indefinite

Oracle Warehouse Builder Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
9.2	Jul 2003	Oct 2007	Not Available	Oct 2010
10.1	Apr 2004	Jul 2007	Not Available	Jul 2010

As of 10gR2 (10.2) Oracle Warehouse Builder (OWB) ships as a part of the Database release. So from 10.2 onwards the lifecycle dates for OWB will be the same as for the Database release it ships with.

Oracle's JD Edwards EnterpriseOne Extended Process Integration (XPI) Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
8.92	Dec 2003	Jun 2008	Not Available	Not Available
8.94	Dec 2004	Dec 2008	Not Available	Not Available

Oracle's Auptyma Release

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Java Application Monitoring (All Releases)	Dec 2005	Jan 2008	Jan 2008	Not Available

Support for all legacy Auptyma products ended on January 31, 2008. Customers are advised to upgrade to the Oracle-branded product, Oracle Enterprise Manager 10gR4 (10.2.0.4).

Oracle Express Server Release

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Express Server 6.3.4	Jul 2002	Dec 2007	Not Available	Dec 2010

Oracle Gateway Release's

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Gateway Release 9.2				
Oracle Access Manager for AS/400 9.2	Jul 2002	Jul 2007	Not Available	Indefinite
Oracle Transparent Gateway for DB2/400 9.2	Jul 2002	Jul 2007	Not Available	Indefinite
Oracle Transparent Gateway for DRDA 9.2	Jul 2002	Jul 2007	Not Available	Indefinite
Oracle Procedural Gateway for APPC 9.2	Jul 2002	Jul 2007	Not Available	Indefinite
Oracle Procedural Gateway for IBM MQ Series 9.2	Jul 2002	Jul 2007	Not Available	Indefinite
Oracle Transparent Gateway for DB2 9.2	Jul 2002	Jul 2007	Not Available	Indefinite

Oracle Gateway Release's (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Gateway Release 10.1				
Oracle Access Manager for AS/400 10.1	Jan 2004	Jan 2009	Not Available	Indefinite
Oracle Transparent Gateway for DB2/400 10.1	Jan 2004	Jan 2009	Not Available	Indefinite
Oracle Transparent Gateway for DRDA 10.1	Jan 2004	Jan 2009	Not Available	Indefinite
Oracle Procedural Gateway for APPC 10.1	Jan 2004	Jan 2009	Not Available	Indefinite
Oracle Transparent Gateway for DB2 10.1	Jan 2004	Jan 2009	Not Available	Indefinite
Oracle Gateway Release 10.2				
Oracle Access Manager for AS/400 10.2	Jul 2005	Jul 2010	Not Available	Indefinite
Oracle Transparent Gateway for DB2/400 10.2	Jul 2005	Jul 2010	Not Available	Indefinite
Oracle Transparent Gateway for DRDA 10.2	Jul 2005	Jul 2010	Not Available	Indefinite
Oracle Procedural Gateway for APPC 10.2	Jul 2005	Jul 2010	Not Available	Indefinite
Oracle Procedural Gateway for WebSphere MQ 10.2	Jul 2005	Jul 2010	Not Available	Indefinite
Oracle Transparent Gateway for DB2 10.2	Jul 2005	Jul 2011	Not Available	Indefinite
Oracle Gateway Release 11.1				
Oracle Database Gateway for Websphere MQ 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for APPC 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for DRDA 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for VSAM 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for Adabas 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for SQL Server 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for Teradata 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for Informix 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for Sybase 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite

Oracle Gateway Release's (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Gateway Release 11.2				
Oracle Database Gateway for Websphere MQ 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for APPC 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for DRDA 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for VSAM 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for IMS 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for Adabas 11.2	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for SQL Server 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for Teradata 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for Informix 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for Sybase 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Gateway Release 12.1				
Oracle Database Gateway for Websphere MQ 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Database Gateway for APPC 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Database Gateway for DRDA 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Database Gateway for SQL Server 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Database Gateway for Teradata 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Database Gateway for Sybase 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Database Gateway for Informix 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite

Oracle Access Manager for AS/400 10.2 is the terminal release.

Oracle Transparent Gateway for DB2/400 10.2 is the terminal release, customers should migrate to Oracle Database gateway for DRDA .

Oracle's TripleHop Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
MatchPoint 2.x	Jun 2002	Not Available	Not Available	Not Available
MatchPoint 3.x	Oct 2003	Not Available	Not Available	Sep 2008

Customers should plan to migrate to latest version of Oracle Secure Enterprise Search.

Oracle Secure Enterprise Search

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Secure Enterprise Search 10.1.8	Apr 2007	Jan 2012	Not Available	Indefinite
Secure Enterprise Search 11.1	Feb 2010	Feb 2015	Not Available	Indefinite
Secure Enterprise Search 11.2	Jul 2013	Jan 2018	Not Available	Indefinite

Oracle Application Express (Formerly HTML DB)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
1.6	Jul 2005	Dec 2008	Not Available	Indefinite
2.0	Sep 2005	Dec 2008	Not Available	Indefinite
2.2	Aug 2006	Aug 2009	Not Available	Indefinite
3.0	Mar 2007	Mar 2010	Not Available	Indefinite
3.1	Feb 2008	Feb 2011	Not Available	Indefinite
3.2	Feb 2009	Feb 2012	Not Available	Indefinite
4.0	Jun 2010	Jun 2015	Not Available	Indefinite
4.1	Aug 2011	Aug 2016	Not Available	Indefinite
4.2	Oct 2012	Oct 2017	Not Available	Indefinite

Oracle Application Express (Formerly HTML DB) (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
5.0	Apr 2015	Apr 2020	Not Available	Indefinite
5.1	Dec 2016	Dec 2021	Not Available	Indefinite
18.x	May 2018	May 2023	Not Available	Indefinite
19.x	Mar 2019	Sep 2024	Not Available	Indefinite
20.x	Apr 2020	Apr 2025	Not Available	Indefinite
21.x	May 2021	May 2024	Not Available	Indefinite

Oracle Zero Data Loss Appliance Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Zero Data Loss Appliance Software 12.2	Aug 2018	Dec 2021	Not Available	Indefinite
Zero Data Loss Appliance Software 19.2	Aug 2019	Aug 2022	Not Available	Indefinite

Oracle Fail Safe Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Fail Safe 3.3.2	Nov 2002	Jul 2007	Not Available	Indefinite
Oracle Fail Safe 3.3.3	Apr 2004	Mar 2009	Not Available	Indefinite
Oracle Fail Safe 3.3.4	Nov 2005	Jul 2010	Not Available	Indefinite
Oracle Fail Safe 3.4.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Fail Safe 3.4.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Fail Safe 4.1.x	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Fail Safe 4.2.x	Apr 2018	Apr 2024	Apr 2027	Indefinite

Oracle's ClearApp Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Acsera Manager 5.1	Not Available	Not Available	Not Available	Not Available
QuickVision 6.0	Not Available	Not Available	Not Available	Jun 2010
QuickVision 6.1	Not Available	Not Available	Not Available	Indefinite
QuickVision 7.0	Not Available	Dec 2009	Dec 2010	Indefinite
QuickVision 7.5	Sep 2008	Dec 2010	Dec 2011	Indefinite
Oracle-Branded Releases				
Oracle Composite Application Monitor and Modeler 10.2.0.4	Nov 2008	Oct 2010	Oct 2013	Indefinite

The migration path for QuickVision 7.5 is to use Oracle Composite Application Monitor and Modeler. Oracle Composite Application Monitor and Modeler is part of Oracle Grid Control release 10.2.x. To be eligible for Premier Support and Extended Support coverage, a mandatory patch for QuickVision 7.0 must be applied.

Oracle Virtual Iron Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.0.4 and earlier	Sep 2007	Not Availalble	Not Availalble	Not Availalble
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.0.5	Sep 2007	Not Availalble	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.1.4	Oct 2007	Not Availalble	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.2.9	Dec 2007	Not Availalble	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.2.11	Jan 2008	Not Availalble	Not Availalble	Indefinite

Oracle Virtual Iron Releases (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.2.13	Jan 2008	Not Availalble	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.2.14	Feb 2008	Not Availalble	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.3.8	Apr 2008	Not Availalble	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition 4.4.13	Sep 2008	Sep 2009	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition 4.4.15	Oct 2008	Oct 2009	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition 4.5.13	Jan 2009	Jan 2010	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition 4.5.16	Feb 2009	Feb 2010	Not Availalble	Indefinite

Oracle's Secerno Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Previous Secerno Releases	Various	Jan 2012	Not Available	Indefinite

Oracle Audit Vault and Database Firewall Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Database Firewall 5.x	Jan 2011	Jan 2016	Not Available	Indefinite
Oracle Audit Vault 10.2.3	Jun 2008	Jun 2013	Not Available	Indefinite
Oracle Audit Vault 10.3	Dec 2011	Dec 2016	Not Available	Indefinite
Oracle Audit Vault and Database Firewall 12.1	Dec 2012	Dec 2017	Not Available	Indefinite
Oracle Audit Vault and Database Firewall 12.2	Dec 2015	Mar 2021	Not Available	Indefinite
Oracle Audit Vault and Database Firewall 20.x	Jul 2020	Jul 2024	Not Available	Indefinite

Oracle Key Vault Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Key Vault 12.2	Feb 2016	Sep 2020	Not Available	Indefinite
Oracle Key Vault 18	Apr 2019	Apr 2022	Not Available	Indefinite
Oracle Key Vault 21	Jan 2021	Jul 2024	Not Available	Indefinite

Oracle's MySQL Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
MySQL Database 5.0	Oct 2005	Dec 2011	Not Available	Indefinite
MySQL Database 5.1	Dec 2008	Dec 2013	Not Available	Indefinite
MySQL Database 5.5	Dec 2010	Dec 2015	Dec 2018	Indefinite
MySQL Database 5.6	Feb 2013	Feb 2018	Feb 2021	Indefinite
MySQL Database 5.7	Oct 2015	Oct 2020	Oct 2023	Indefinite

Oracle's MySQL Releases (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
MySQL Database 8.0	Apr 2018	Apr 2023	Apr 2026	Indefinite
MySQL Cluster 6	Aug 2007	Mar 2013	Not Available	Indefinite
MySQL Cluster 7.0	Apr 2009	Apr 2014	Not Available	Indefinite
MySQL Cluster 7.1	Apr 2010	Apr 2015	Not Available	Indefinite
MySQL Cluster 7.2	Feb 2012	Feb 2017	Feb 2020	Indefinite
MySQL Cluster 7.3	Jun 2013	Jun 2018	Jun 2021	Indefinite
MySQL Cluster 7.4	Feb 2015	Feb 2020	Feb 2023	Indefinite
MySQL Cluster 7.5	Oct 2016	Oct 2021	Oct 2024	Indefinite
MySQL Cluster 7.6	May 2018	May 2023	May 2026	Indefinite
MySQL Cluster 8.0	Jan 2020	Jan 2025	Jan 2028	Indefinite

Oracle's NoSQL Database Release

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
11.2.1	Oct 2011	Oct 2016	Oct 2019	Indefinite
11.2.2	Nov 2012	Nov 2017	Nov 2020	Indefinite
12.1.2	Jul 2013	Jul 2018	Jul 2021	Indefinite
12.1.3	Mar 2014	Mar 2019	Mar 2022	Indefinite
12.1.4	Jun 2016	Jun 2021	Jun 2024	Indefinite
12.2.4.x	Apr 2017	Apr 2023	Apr 2026	Indefinite
18.x	Apr 2018	Apr 2023	Apr 2026	Indefinite
19.x	Apr 2019	Apr 2024	Apr 2027	Indefinite
20.x	Apr 2020	Apr 2025	Apr 2028	Indefinite
21.x	Apr 2021	Apr 2026	Apr 2029	Indefinite

Oracle Big Data Appliance

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Big Data Appliance 3.x	Jun 2012	Jun 2017	Not Available	Jan 2025
Oracle Big Data Appliance 4.x	Apr 2014	Jan 2022	Not Available	Jan 2025
Oracle Big Data Appliance 5.x	Nov 2019	Jan 2025	Not Available	Not Available

For more detailed information on specific release and support dates, refer to MyOracle Support.

Oracle Big Data SQL

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Big Data SQL 1.x	Sep 2013	Sep 2018	Sep 2021	Indefinite
Oracle Big Data SQL 2.x	Oct 2015	Oct 2020	Oct 2023	Indefinite
Oracle Big Data SQL 3.x	Mar 2016	Mar 2021	Mar 2024	Indefinite
Oracle Big Data SQL 4.x	Jul 2019	Jul 2024	Jan 2025	Indefinite

Oracle Big Data Connectors

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Big Data Connectors 3.x	Apr 2014	Apr 2019	Not Available	Indefinite
Oracle Big Data Connectors 4.1 – 4.5	Sep 2014	Sep 2019	Not Available	Indefinite
Big Data Connectors 4.6	Aug 2016	Aug 2021	Not Available	Indefinite
Big Data Connectors 4.9	Jun 2017	Jun 2022	Not Available	Indefinite
Big Data Connectors 4.12	Nov 2018	Nov 2023	Not Available	Indefinite
Big Data Connectors 5.1	May 2020	May 2025	Not Available	Indefinite

Oracle Big Data Spatial and Graph

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Big Data Spatial and Graph 1.x	May 2015	May 2020	Not Available	Indefinite
Oracle Big Data Spatial and Graph 2.x	Nov 2016	Nov 2021	Not Available	Indefinite
Oracle Big Data Spatial and Graph 3.x	Oct 2019	Oct 2024	Not Available	Indefinite

LIFETIME SUPPORT POLICY:

Our Commitment to Deliver a Superior Ownership Experience

Oracle Exadata Storage Server Software

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
11.1.x	Sep 2008	Sep 2013	Not Available	Indefinite
11.2.x	Sep 2009	Sep 2014	Sep 2017	Indefinite
12.1	Dec 2013	Dec 2018	Dec 2021	Indefinite
12.2	Jan 2017	Jan 2022	Jan 2023	Indefinite
18.1	Sep 2017	Sep 2022	Sep 2023	Indefinite
19.1	Oct 2018	Oct 2023	Not Available	Indefinite
19.2	Feb 2019	Oct 2023	Not Available	Indefinite
19.3	Sep 2019	Oct 2023	Not Available	Indefinite
20.1	Jun 2020	Oct 2023	Not Available	Indefinite
21.2	May 2021	May 2024	Not Available	Indefinite

Now, you can have even greater peace of mind knowing that your business strategy is driving your upgrade strategy with more control, more choice, and more certainty. It all amounts to an Oracle Superior Ownership Experience—available only with the industry's most advanced support offering, Oracle Lifetime Support.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Anexo IV - Funcionalidade Data Redaction - Oracle Database 12c _ Oracle Brasil.pdf

Data Redaction

Funcionalidade Data Redaction - Oracle Database 12c

Por OraWorld,
Postado em Maio 2014

No *Oracle Database 12c*, foi introduzida uma nova funcionalidade, chamada de *Oracle Data Redaction*. Esta nova funcionalidade faz parte do pacote *Advanced Security* e permite a proteção dos dados mostrados ao usuário em tempo real, sem necessidade de modificações na aplicação.

O *Oracle Database 12c* aplica a proteção em tempo de execução, no momento em que os usuários do aplicativo tentam acessar os dados, isto se chama *at query-execution time*. Os dados armazenados permanecem inalterados, enquanto os dados a serem exibidos são transformados *on-the-fly* antes de deixarem o banco de dados.

Desde a versão 11G, existe o *Oracle Data Masking*, onde os dados são transformados usando formatos de máscaras e este dado mascarado atualizado é armazenado em novos blocos de dados. Isto é adequado para ambientes de não-produção (desenvolvimento, homologação, treinamento, etc)

Segue abaixo algumas outras *features* que já existiam para auxiliar a tornar os dados mais seguros:

Virtual Private Database (VPD) - permite controlar os acessos em nível de registro e coluna, adicionando uma cláusula WHERE dinâmica em uma instrução SQL.
Oracle Label Security – Permite adicionar valores definidos pelo usuário para os registros e usar o VPD para controlar o acesso com base nestes valores.
Database Vault – o *Data Redaction* não impede que usuários privilegiados como DBAs não tenham acesso ao conteúdo das colunas que estão sendo protegidas. Para resolver isso, pode-se utilizar o *Database Vault*.
Considerando as questões de licenciamento, o *Oracle Data Masking* só está disponível no banco *Enterprise Edition* e com a aquisição do pacote *Advanced Security*.

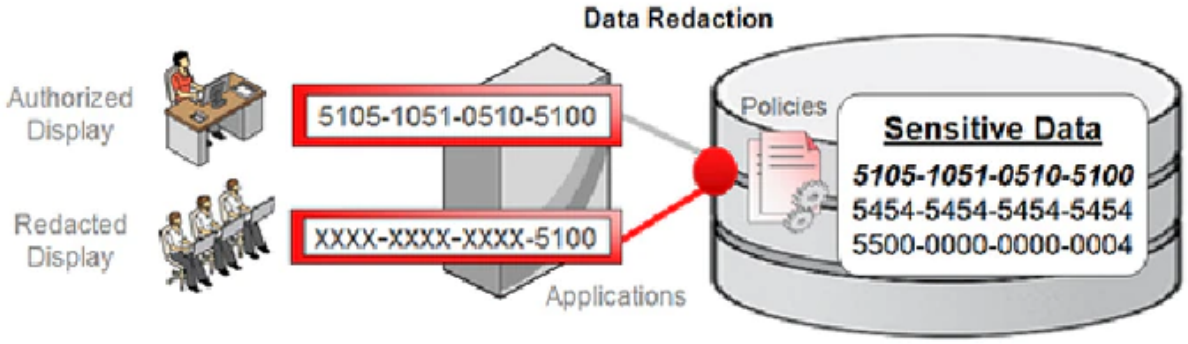
Como funciona:

Podemos criar ***redaction policies*** que basicamente gerenciam que condição deve ser atendida antes dos dados serem protegidos, quais colunas da tabela e o tipo de proteção.

A *package* utilizada para criar as regras de proteção se chama DBMS_REDACT, que inclui 5 procedures para gerir as regras e mais uma *procedure* para alterar o valor default da *full redaction policy*.

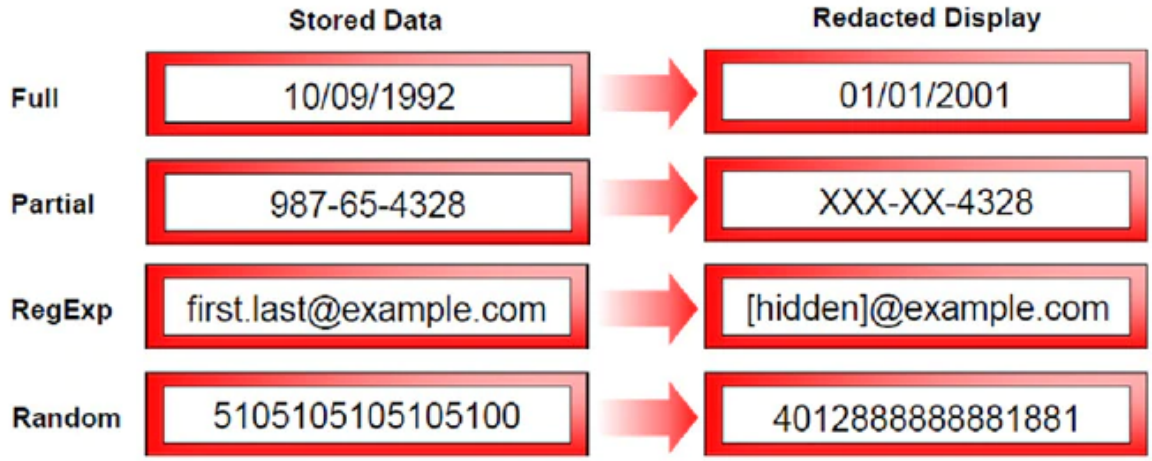
DBMS_REDACT.ALTER_POLICY – permite fazer mudanças nas políticas existentes.
DBMS_REDACT.DISABLE_POLICY – desativa uma política existente.
DBMS_REDACT.DROP_POLICY – elimina uma política existente.

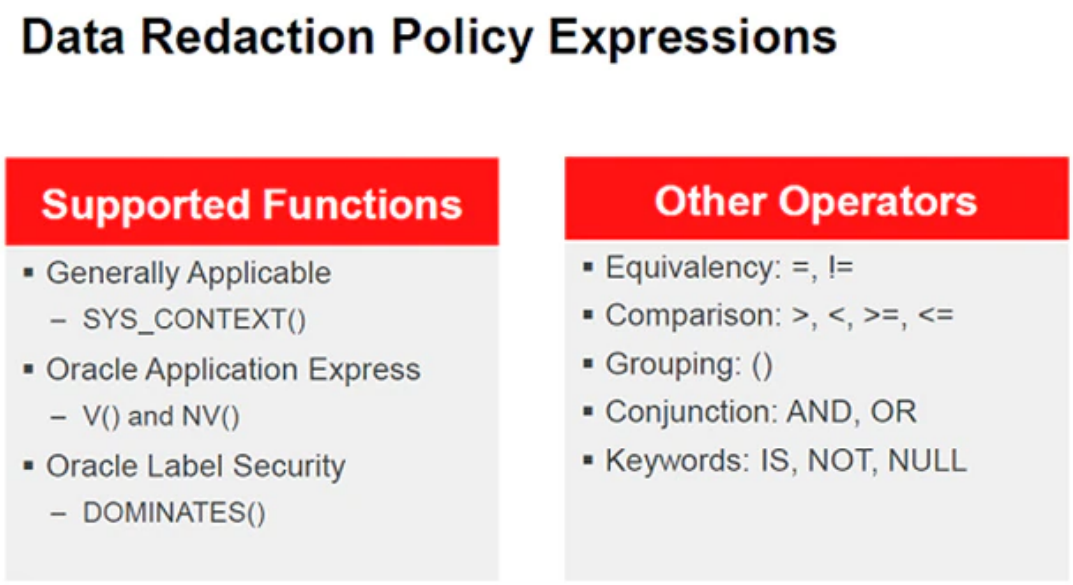
DBMS_REDACT.ENABLE_POLICY – ativa uma política existente.
DBMS_REDACT.UPDATE_FULL_REDACTION_VALUES – altera o valor *default* de retorno para *full redaction*. É necessário reiniciar o banco de dados para ter efeito.



Você pode proteger os dados da coluna, utilizando um dos seguintes métodos:

Full redaction – Todo conteúdo da coluna é protegido e o tipo de valor devolvido depende do tipo de dados da coluna. Para campos numéricos, será devolvido o valor zero, para campos do tipo *character*, será devolvido um espaço. Essa definição pode ser alterada a nível de banco de dados.
Partial redaction – Apenas uma parte da informação é alterada, como por exemplo, os primeiros dígitos do número de cartão de crédito são trocados por asterisco.
Regular expressions - Você pode usar expressões regulares para procurar padrões de dados para proteger.
Random redaction – os valores retornados são aleatórios; cada vez que é feita uma consulta os valores retornados são diferentes.
No redaction - permite testar o funcionamento interno de suas políticas de redação, sem nenhum efeito sobre os resultados das consultas em tabelas. Muito utilizado para testar as políticas antes de colocar em produção.





O Data Redaction pode ajudar a cumprir com as regulamentações de segurança, como Payment Card Industry Data Security Standard (PCI DSS) e da Lei Sarbanes-Oxley.

O Data Redaction pode ser utilizado com os seguintes tipos de colunas: NUMBER, BINARY_FLOAT, BINARY_DOUBLE, CHAR, VARCHAR2, NCHAR, NVARCHAR2, DATE, TIMESTAMP, TIMESTAMP WITH TIME ZONE, BLOB, CLOB e NCLOB.

Views do dicionário:

Podemos utilizar as seguintes views do dicionário de dados do Oracle para obter informações sobre o *Oracle Data Redaction*:

REDACTION_POLICIES
REDACTION_COLUMNS
REDACTION_VALUES_FOR_TYPE_FULL

Data Redaction e o utilitário Data Pump:

A *role* ***DATAPUMP_EXP_FULL_DATABASE*** inclui o privilégio de sistema ***EXEMPT REDACTION POLICY.*** Com isso, um DBA ao exportar as tabelas, estará exportando os dados reais e não os mascarados.

Se você tentar exportar uma tabela sem ter o privilégio EXEMPT REDACTION POLICY, receberá o seguinte erro:

```
ORA-28081: Insufficient privileges - the command references a redacted object
```

Copy

Para exportar apenas os *metadados* relacionados com as políticas do *Oracle Data Redaction*, você pode usar os seguintes parâmetros do EXPDP:

CONTENT=METADATA_ONLY INCLUDE=RADM_FPTM,RADM_POLICY

Data Redaction e Create tables as select (CTAS):

Um usuário não pode criar uma tabela fazendo SELECT a partir de uma tabela com uma *policy* ativa, se ele não tiver privilégio para ver os valores mascarados

PDB utilizada para os exemplos com o EM12c:

Acessando o *Oracle Data Redaction*:

Tela de gerenciamento das políticas:

Criando uma política para não mostrar o salário, caso o usuário do sistema não seja o Supervisor:

Verificando se a política funciona:

```
SQL*Plus: Release 12.1.0.1.0 Production on Wed Apr 2 10:22:46 2014
Copyright (c) 1982, 2013, Oracle.  All rights reserved.

Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics
and Real Application Testing options

SQL> select EMPLOYEE_ID, FIRST_NAME, SALARY from hr.employees WHERE ROWNUM < 5

EMPLOYEE_ID FIRST_NAME               SALARY
----------- -------------------- ----------
        100 Steven                        0
        101 Neena                         0
        102 Lex                           0
        103 Alexander                     0
```

Copy

Verificando a mesma tabela, agora com o usuário SUPERVISOR:

```
[oracle@dibutu ~]$ sqlplus supervisor/senha@localhost:1521/testpdb

SQL*Plus: Release 12.1.0.1.0 Production on Wed Apr 2 10:26:04 2014
Copyright (c) 1982, 2013, Oracle.  All rights reserved.

Connected to:
```

```
Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics
and Real Application Testing options

SQL> select EMPLOYEE_ID, FIRST_NAME, SALARY from hr.employees WHERE ROWNUM < 5

EMPLOYEE_ID FIRST_NAME               SALARY
----------- -------------------- ----------
        100 Steven                    24000
        101 Neena                     17000
        102 Lex                       17000
        103 Alexander                  9000
```

Copy

Criando a mesma política utilizando o SQL*Plus:

```
SQL>
BEGIN
DBMS_REDACT.ADD_POLICY
(OBJECT_SCHEMA =>'HR',  object_name => 'EMPLOYEES',  policy_name => 'POLITICA_
expression => 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') != ''SUPERVISOR''');
DBMS_REDACT.ALTER_POLICY
(OBJECT_SCHEMA => 'HR',  object_name => 'EMPLOYEES',  policy_name => 'POLITICA
action => DBMS_REDACT.ADD_COLUMN,  column_name => '"SALARY"',  function_type =
END;
/
PL/SQL procedure successfully completed.
```

Copy

Criando a mesma política utilizando o *SQLDeveloper*:

OraWorld é um grupo que está constantemente trabalhando com a comunidade Oracle por meio de artigos, conferências, webinars e cursos de Banco de Dados Oracle. O OraWorld possui membros "Oracle Certified Masters" e "Oracle ACEs".

Você pode seguir este grupo através dos seguintes links:

https://www.facebook.com/oraworldteam

https://twitter.com/oraworld_team

http://www.oraworld-team.com

Anexo V - LGPD.pdf

Presidência da República
Secretaria-Geral
Subchefia para Assuntos Jurídicos

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

Texto compilado

Mensagem de veto

Vigência

~~Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).~~

Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019) Vigência

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

~~II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;~~

~~II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

~~b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;~~
~~b) acadêmicos;~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

~~§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.~~
~~§ 2º O tratamento dos dados a que se refere o inciso III do **caput** por pessoa jurídica de direito privado só será admitido em procedimentos sob a tutela de pessoa jurídica de direito público, hipótese na qual será observada a limitação de que trata o § 3º.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

~~§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.~~
~~§ 3º Os dados pessoais constantes de bancos de dados constituídos para os fins de que trata o inciso III do **caput** não poderão ser tratados em sua totalidade por pessoas jurídicas de direito privado, não incluídas as controladas pelo Poder Público.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

~~§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado.~~ ~~(Revogado pela Medida Provisória nº 869, de 2018)~~

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

~~VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;~~

~~VIII - encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

~~XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;~~

~~XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

~~XIX - autoridade nacional: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.~~

~~XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

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;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

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.

CAPÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS

Seção I
Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

~~VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;~~

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

~~§ 1º Nos casos de aplicação do disposto nos incisos II e III do caput deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, o titular será informado das hipóteses em que será admitido o tratamento de seus dados.~~ (Revogado pela Medida Provisória nº 869, de 2018)

§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)

~~§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do caput do art. 23 desta Lei poderá ser especificada pela autoridade nacional. (Revogado pela Medida Provisória nº 869, de 2018)~~

§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Seção II
Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

~~f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou~~

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

~~§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.~~

~~§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses de: (Redação dada pela Medida Provisória nº 869, de 2018)~~

~~I - portabilidade de dados quando consentido pelo titular; ou (Incluído pela Medida Provisória nº 869, de 2018)~~

~~II - necessidade de comunicação para a adequada prestação de serviços de saúde suplementar. (Incluído pela Medida Provisória nº 869, de 2018)~~

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) Vigência

I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019) Vigência

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Seção III
Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Seção IV
Do Término do Tratamento de Dados

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CAPÍTULO III
DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

~~V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;~~

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

~~Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.~~

~~Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

§ 3º (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO IV
DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I
Das Regras

Art. 23. 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;

II - (VETADO); e

~~III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.~~

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

IV - (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal , terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ;

II - (VETADO);

~~III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.~~
~~III - se for indicado um encarregado para as operações de tratamento de dados pessoais, nos termos do art. 39;~~ ~~Redação dada pela Medida Provisória nº 869, de 2018)~~

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

~~IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;~~ ~~(Incluído pela Medida Provisória nº 869, de 2018)~~
~~V - na hipótese de a transferência dos dados objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados; ou~~ ~~(Incluído pela Medida Provisória nº 869, de 2018)~~

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019) Vigência

~~VI - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.~~ ~~(Incluído pela Medida Provisória nº 869, de 2018)~~

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

~~Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:~~
~~Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa jurídica de direito privado dependerá de consentimento do titular, exceto:~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 28. (VETADO).

~~Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, às entidades do Poder Público, a realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.~~
~~Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do Poder Público a realização de operações de tratamento de dados pessoais, as informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Seção II
Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

CAPÍTULO V
DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as 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) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

CAPÍTULO VI
DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I
Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II
Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

§ 4º (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

Seção III
Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

CAPÍTULO VII
DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I
Da Segurança e do Sigilo de Dados

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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II
Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

CAPÍTULO VIII
DA FISCALIZAÇÃO

Seção I
Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

~~X - (VETADO); (Incluído pela Lei nº 13.853, de 2019)~~ (Promulgação partes vetadas)
~~XI - (VETADO); (Incluído pela Lei nº 13.853, de 2019)~~ (Promulgação partes vetadas)
~~XII - (VETADO). (Incluído pela Lei nº 13.853, de 2019)~~ (Promulgação partes vetadas)

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

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;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

~~§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.~~

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. (Redação dada pela Lei nº 13.853, de 2019) Vigência

~~§ 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal) , na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa) , e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .~~

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011. (Redação dada pela Lei nº 13.853, de 2019)

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. (Incluído pela Lei nº 13.853, de 2019)

~~§ 6º (VETADO). (Incluído pela Lei nº 13.853, de 2019)~~ (Promulgação partes vetadas)

§ 6º As sanções previstas nos incisos X, XI e XII do **caput** deste artigo serão aplicadas: (Incluído pela Lei nº 13.853, de 2019)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do **caput** deste artigo para o mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. (Incluído pela Lei nº 13.853, de 2019)

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. (Vigência)

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento. (Vigência)

CAPÍTULO IX
DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I
Da Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55. (VETADO).

~~Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados - ANPD, órgão da administração pública federal, integrante da Presidência da República.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-B. É assegurada autonomia técnica à ANPD.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-C. ANPD é composta por:~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~I - Conselho Diretor, órgão máximo de direção;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~III - Corregedoria;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~IV - Ouvidoria;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~V - órgão de assessoramento jurídico próprio; e~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei."~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-D. O Conselho Diretor da ANPD será composto por cinco diretores, incluído o Diretor-Presidente.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 1º Os membros do Conselho Diretor da ANPD serão nomeados pelo Presidente da República e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superior - DAS de nível 5.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros, de reputação ilibada, com nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 3º O mandato dos membros do Conselho Diretor será de quatro anos.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de dois, de três, de quatro, de cinco e de seis anos, conforme estabelecido no ato de nomeação.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 1º Nos termos do **caput** , cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 2º Compete ao Presidente da República determinar o afastamento preventivo, caso necessário, e proferir o julgamento.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013 .~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Parágrafo único. A infração ao disposto no **caput** caracteriza ato de improbidade administrativa.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art.55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Parágrafo único. Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-J. Compete à ANPD:~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~I - zelar pela proteção dos dados pessoais;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~II - editar normas e procedimentos sobre a proteção de dados pessoais;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~III - deliberar, na esfera administrativa, sobre a interpretação desta Lei, suas competências e os casos omissos;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~IV - requisitar informações, a qualquer momento, aos controladores e operadores de dados pessoais que realizem operações de tratamento de dados pessoais; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~V - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VI - fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VII - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VIII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei praticado por órgãos e entidades da administração pública federal; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~IX - difundir na sociedade o conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre as medidas de segurança; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~X - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos controladores; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XI - elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XII - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XIII - realizar consultas públicas para colher sugestões sobre temas de relevante interesse público na área de atuação da ANPD; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XIV - realizar, previamente à edição de resoluções, a oitiva de entidades ou órgãos da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XV - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XVI - elaborar relatórios de gestão anuais acerca de suas atividades. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 1º A ANPD, na edição de suas normas, deverá observar a exigência de mínima intervenção, assegurados os fundamentos e os princípios previstos nesta Lei e o disposto no art. 170 da Constituição. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 2º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 3º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 4º No exercício das competências de que trata o **caput** , a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei, sob pena de responsabilidade. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 5º As reclamações colhidas conforme o disposto no inciso V do **caput** poderão ser analisadas de forma agregada e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, cujas demais competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Parágrafo único. A ANPD articulará sua atuação com o Sistema Nacional de Defesa do Consumidor do Ministério da Justiça e com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais, e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Lei nº 13.853, de 2019)

§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. (Incluído pela Lei nº 13.853, de 2019)

§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-B. É assegurada autonomia técnica e decisória à ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-C. A ANPD é composta de: (Incluído pela Lei nº 13.853, de 2019)

I - Conselho Diretor, órgão máximo de direção; (Incluído pela Lei nº 13.853, de 2019)

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - Corregedoria; (Incluído pela Lei nº 13.853, de 2019)

IV - Ouvidoria; (Incluído pela Lei nº 13.853, de 2019)

V - órgão de assessoramento jurídico próprio; e (Incluído pela Lei nº 13.853, de 2019)

VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Lei nº 13.853, de 2019)

§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. (Incluído pela Lei nº 13.853, de 2019)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. (Incluído pela Lei nº 13.853, de 2019)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, somente quando assim recomendado pela comissão especial de que trata o § 1º deste artigo, e proferir o julgamento. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A infração ao disposto no caput deste artigo caracteriza ato de improbidade administrativa. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. (Incluído pela Lei nº 13.853, de 2019)

§ 2º O Conselho Diretor disporá sobre o regimento interno da ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019)

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019)

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019)

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (Incluído pela Lei nº 13.853, de 2019)

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (Incluído pela Lei nº 13.853, de 2019)

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Lei nº 13.853, de 2019)

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (Incluído pela Lei nº 13.853, de 2019)

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Lei nº 13.853, de 2019)

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (Incluído pela Lei nº 13.853, de 2019)

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; (Incluído pela Lei nº 13.853, de 2019)

XII - elaborar relatórios de gestão anuais acerca de suas atividades; (Incluído pela Lei nº 13.853, de 2019)

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (Incluído pela Lei nº 13.853, de 2019)

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; (Incluído pela Lei nº 13.853, de 2019)

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019)

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; (Incluído pela Lei nº 13.853, de 2019)

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); (Incluído pela Lei nº 13.853, de 2019)

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei nº 13.853, de 2019)

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Lei nº 13.853, de 2019)

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; (Incluído pela Lei nº 13.853, de 2019)

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Lei nº 13.853, de 2019)

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. (Incluído pela Lei nº 13.853, de 2019)

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. (Incluído pela Lei nº 13.853, de 2019)

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-L. Constituem receitas da ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; (Incluído pela Lei nº 13.853, de 2019)

II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados; (Incluído pela Lei nº 13.853, de 2019)

III - os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade; (Incluído pela Lei nº 13.853, de 2019)

IV - os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo; (Incluído pela Lei nº 13.853, de 2019)

V - (VETADO); (Incluído pela Lei nº 13.853, de 2019)

VI - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; (Incluído pela Lei nº 13.853, de 2019)

VII - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. (Incluído pela Lei nº 13.853, de 2019)

Art. 56. (VETADO).

Art. 5 7. (VETADO).

Seção II
Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Art. 58. (VETADO).

~~Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por vinte e três representantes, titulares suplentes, dos seguintes órgãos: (Incluído pela Medida Provisória nº 869, de 2018)~~
~~I - seis do Poder Executivo federal; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~II - um do Senado Federal; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~III - um da Câmara dos Deputados; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~IV - um do Conselho Nacional de Justiça; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~V - um do Conselho Nacional do Ministério Público; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~VI - um do Comitê Gestor da Internet no Brasil; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~VII - quatro de entidades da sociedade civil com atuação comprovada em proteção de dados pessoais; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~VIII - quatro de instituições científicas, tecnológicas e de inovação; e (Incluído pela Medida Provisória nº 869, de 2018)~~
~~IX - quatro de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais. (Incluído pela Medida Provisória nº 869, de 2018)~~
~~§ 1º Os representantes serão designados pelo Presidente da República. (Incluído pela Medida Provisória nº 869, de 2018)~~
~~§ 2º Os representantes de que tratam os incisos I a VI do **caput** e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Medida Provisória nº 869, de 2018)~~
~~§ 3º Os representantes de que tratam os incisos VII, VIII e IX do **caput** e seus suplentes: (Incluído pela Medida Provisória nº 869, de 2018)~~
~~I - serão indicados na forma de regulamento; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~II - terão mandato de dois anos, permitida uma recondução; e (Incluído pela Medida Provisória nº 869, de 2018)~~
~~III - não poderão ser membros do Comitê Gestor da Internet no Brasil. (Incluído pela Medida Provisória nº 869, de 2018)~~
~~§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Medida Provisória nº 869, de 2018)~~
~~Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Medida Provisória nº 869, de 2018)~~
~~I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Medida Provisória nº 869, de 2018)~~
~~V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: (Incluído pela Lei nº 13.853, de 2019)

I - 5 (cinco) do Poder Executivo federal; (Incluído pela Lei nº 13.853, de 2019)

II - 1 (um) do Senado Federal; (Incluído pela Lei nº 13.853, de 2019)

III - 1 (um) da Câmara dos Deputados; (Incluído pela Lei nº 13.853, de 2019)

IV - 1 (um) do Conselho Nacional de Justiça; (Incluído pela Lei nº 13.853, de 2019)

V - 1 (um) do Conselho Nacional do Ministério Público; (Incluído pela Lei nº 13.853, de 2019)

VI - 1 (um) do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)

VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; (Incluído pela Lei nº 13.853, de 2019)

VIII - 3 (três) de instituições científicas, tecnológicas e de inovação; (Incluído pela Lei nº 13.853, de 2019)

IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; (Incluído pela Lei nº 13.853, de 2019)

X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e (Incluído pela Lei nº 13.853, de 2019)

XI - 2 (dois) de entidades representativas do setor laboral. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os representantes de que tratam os incisos I, II, III, IV, V e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Lei nº 13.853, de 2019)

§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes: (Incluído pela Lei nº 13.853, de 2019)

I - serão indicados na forma de regulamento; (Incluído pela Lei nº 13.853, de 2019)

II - não poderão ser membros do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)

III - terão mandato de 2 (dois) anos, permitida 1 (uma) recondução. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Lei nº 13.853, de 2019)

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Lei nº 13.853, de 2019)

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Lei nº 13.853, de 2019)

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Lei nº 13.853, de 2019)

IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Lei nº 13.853, de 2019)

V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população. (Incluído pela Lei nº 13.853, de 2019)

Art. 59. (VETADO).

CAPÍTULO X
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações: Vigência

"Art. 7º .....

.....

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

....." (NR)

"Art. 16. .....

.....

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

~~Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 . (Revogado pela Medida Provisória nº 869, de 2018)~~

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 .

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

~~Art. 65. Esta Lei entra em vigor após decorridos 18 (dezoito) meses de sua publicação oficial .~~
~~Art. 65. Esta Lei entra em vigor: (Redação dada pela Medida Provisória nº 869, de 2018)~~
~~I - quanto aos art. 55-A, art. 55-B, art. 55-C, art. 55-D, art. 55-E, art. 55-F, art. 55-G, art. 55-H, art. 55-I, art. 55-J, art. 55-K, art. 58-A e art. 58-B, no dia 28 de dezembro de 2018; e (Incluído pela Medida Provisória nº 869, de 2018)~~
~~II - vinte e quatro meses após a data de sua publicação quanto aos demais artigos. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)

I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)

~~II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)~~
~~II - em 3 de maio de 2021, quanto aos demais artigos. (Redação dada pela Medida Provisória nº 959, de 2020)~~ (Convertida na Lei nº 14.058, de 2020)

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

Brasília , 14 de agosto de 2018; 197º da Independência e 130º da República.

MICHEL TEMER
Torquato Jardim
Aloysio Nunes Ferreira Filho
Eduardo Refinetti Guardia
Esteves Pedro Colnago Junior
Gilberto Magalhães Occhi
Gilberto Kassab
Wagner de Campos Rosário
Gustavo do Vale Rocha
Ilan Goldfajn
Raul Jungmann
Eliseu Padilha

Este texto não substitui o publicado no DOU de 15.8.2018, e republicado parcialmente em 15.8.2018 - Edição extra

*

Anexo VI - Encryption and Redaction with OAS 19c.pdf

19c ORACLE Database

Encryption and Redaction with Oracle Advanced Security

Preventive controls to encrypt data at rest and redact sensitive information

WHITE PAPER / AUGUST 29, 2019

ORACLE

PURPOSE STATEMENT

This document provides an overview of features and enhancements included in latest releases of Oracle Advanced Security Option. It is intended solely to help you assess the business benefits of using Oracle Advanced Security preventive controls and to plan your Data Security / I.T. projects.

DISCLAIMER

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

TABLE OF CONTENTS

Purpose Statement 2

Introduction 5

Preventing Database Bypass with Encryption 6

- Oracle Advanced Security Transparent Data Encryption 6
- Protecting Entire Applications Using TDE Tablespace Encryption 7
- Protecting Sensitive Data Using TDE Column Encryption 8
- Performance Characteristics 8
- Built-In Key Management 8
- Encryption Impact for Common Operational Activities 9

Limiting Sensitive Data Exposure with Data Redaction 10

- Oracle Advanced Security Data Redaction 11
- Policies and Transformations 11
- Performance Characteristics 12
- Security Considerations 12
- Easy to Deploy Data Redaction 13
- Comparison to Alternative Approaches 13

Applying Encryption and Redaction in Oracle Multitenant Architecture 14

Data Encryption in the Oracle Cloud 14

Conclusion 14

INTRODUCTION

Rising security threats, expanding compliance requirements, consolidation, and cloud computing are just a few of the reasons why data security has become critical. Nearly 20 years after the first U.S. breach notification law, the need for strong preventive controls continues to increase as access to data expands. Initiatives such as the European Union's General Data Protection Regulation (GDPR) help ensure data security remains a top priority for organizations. Stolen client devices, including tablets and smartphones, have the potential to easily expose sensitive information as users move beyond the laptop. Outsourcing, offshoring, corporate mergers, and nearly continuous organizational change create additional risks by making it easier for malicious insiders to obtain sensitive data and for outside hackers to gain access to servers using social engineering attacks. These growing trends are just one reason why centralized and efficient protection of sensitive data, regardless of the applications being used, is more important than ever. Implementing security measures that consistently protect sensitive data at the source becomes a critical control as stored data continues to proliferate and access to data expands beyond traditional boundaries. Protecting data requires a defense in depth, multi-layered approach that encompasses controls to evaluate security postures, prevent data loss, detect suspicious activities and apply data access controls at the source through data-driven security. Oracle Database 19c strengthens Oracle's industry-leading database security solution by providing important new security measures in each of these areas.

Oracle Advanced Security option with Oracle Database delivers two essential preventive controls covering encryption of data-at-rest and redaction of sensitive data. These controls help protect sensitive data from being exposed directly from storage or through applications. Oracle Advanced Security Transparent Data Encryption (TDE) helps prevent attacks that attempt to bypass the database and read sensitive information from data files at the operating system level, from database backups, or from database exports. Oracle Advanced Security Data Redaction

"On our path towards EU GDPR compliance, we chose Oracle Database Security solutions including Oracle Advanced Security, Oracle Key Vault, Oracle Database Vault, Oracle Audit Vault and Oracle Database Firewall to streamline and simplify our Oracle deployment. With Oracle, we minimize risk and further enhance our overall security.

Henrique Zacarias
CIO
NOS

complements TDE by redacting sensitive data in query results before the data leaves the database, thus reducing the risk of unauthorized data exposure in applications. This white paper describes TDE and Data Redaction and explains how these valuable preventive controls can work together to help secure your sensitive data.

PREVENTING DATABASE BYPASS WITH ENCRYPTION

Data-at-rest encryption is an important control for blocking unauthorized access to sensitive data using methods that circumvent the database. Privileged operating system accounts are just one of the vehicles used by attackers and malicious insiders to gain access to sensitive information directly in physical storage.

Oracle Advanced Security Transparent Data Encryption (TDE) stops attackers from bypassing the database and reading sensitive information from storage by encrypting data in the database layer. Applications and users authenticated to the database continue to have access to application data transparently, while unauthenticated users attempting to circumvent the database are denied access to clear text data. To understand this better, consider the fact that privileged operating system users can access database tablespace files and extract sensitive data using simple shell commands. In addition, consider the possibility of attacks that read sensitive data from lost, stolen, or improperly decommissioned disks or backups. Figure 1 shows an example of extracting customer credit card numbers directly from storage using the common Linux "strings" command and a search pattern.

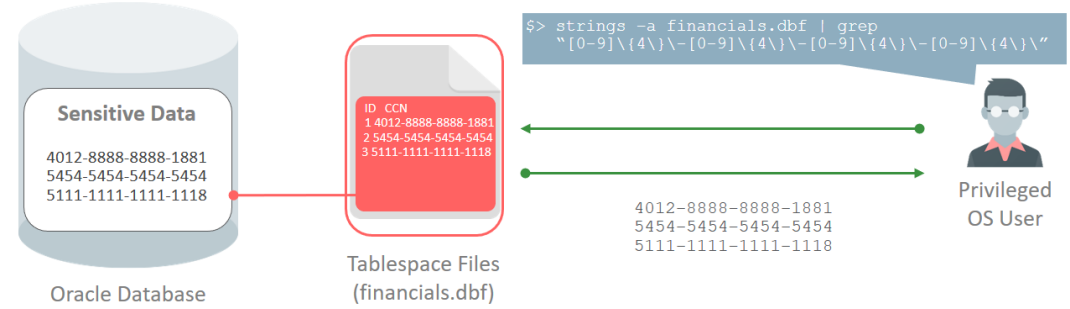


Figure 1. Extracting customer credit card numbers from Oracle database tablespace files

Oracle Advanced Security Transparent Data Encryption

Transparent Data Encryption resides at an optimal layer within the database to prevent database bypass while maintaining application transparency. TDE deploys quickly and encrypts application tablespaces, or entire databases including SYSTEM, SYSAUX, TEMP and UNDO tablespaces. It is transparent to applications because the encryption and decryption processes do not require any application changes, and the application users do not have to directly deal with encrypted data. Most importantly, TDE's built-in two-tier key architecture enables key rotation without downtime, and provides full key lifecycle management, tracking the keys across their lifetime with helpful meta-data attributes. Figure 2 shows how encrypting an Oracle database using TDE prevents database bypass.

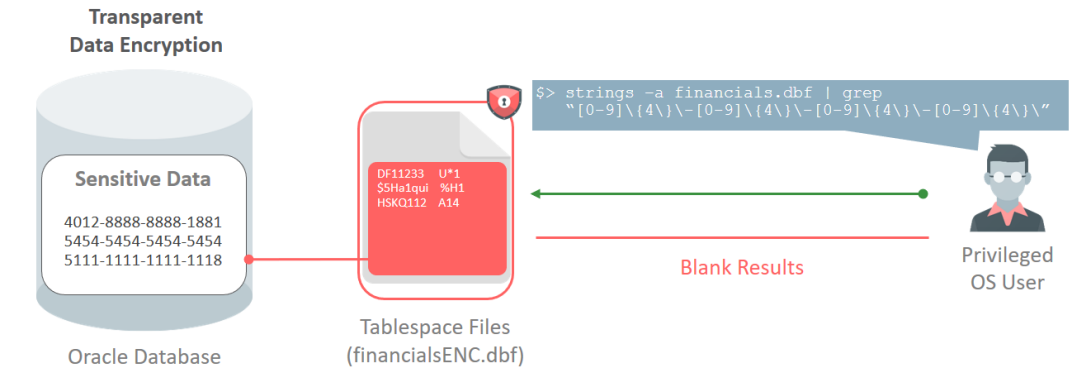


Figure 2. Encrypting with Transparent Data Encryption to prevent database bypass

TDE is unique when compared to alternative approaches that encrypt entire storage volumes or require new toolkits and programming APIs. These approaches do not protect against many bypass attacks, may require significant application changes, have complex (or no) key management, and are not integrated with complementary technologies such as Oracle Advanced Compression, Oracle Real Application Cluster (RAC), Oracle Recovery Manager (RMAN), Oracle Multitenant, Oracle GoldenGate, and Oracle Data Guard.

The high level of protection provided by TDE follows common standards for strong encryption as described in the figure below. With Oracle Database 19c, TDE supports operation with a FIPS 140-2 Level 1 cryptographic module, using only approved encryption suites.

Standard encryption and hashing algorithms used by TDE

ENCRYPTION ALGORITHMS	KEY LENGTH
Advanced Encryption Standard (AES)	128, 192, 256 bits
Triple Data Encryption Standard (TDES)	168 bits
ARIA (Korea)	128, 192, 256 bits
SEED (Korea)	128 bits
GOST (Russia)	256 bits

Protecting Entire Applications Using TDE Tablespace Encryption

Oracle Advanced Security TDE tablespace encryption protects entire application tables by encrypting the underlying tablespaces and indexes. It encrypts application tablespaces regardless of the data's sensitivity and irrespective of its data type. Tablespace encryption simplifies the encryption process because there is no need to identify specific database columns. It is useful when the database contains a large amount of sensitive data to be encrypted and the columns reside in many different locations. Due all these reasons, TDE tablespace encryption has become our customers' encryption method of choice.

Protecting Sensitive Data Using TDE Column Encryption

Oracle Advanced Security also provides TDE column encryption. TDE column encryption can be used to encrypt specific data in application tables such as credit card numbers and U.S. Social Security numbers. Customers identify columns within their application schema containing sensitive or regulated data, and then encrypt only those columns. This approach is useful when the database tables are large, only a small number of columns must be encrypted, and the columns are known. TDE column encryption is typically useful for warehouse applications where each query is likely to return a very different set of data. Data encrypted using TDE column encryption remains encrypted on backup media and discarded disk drives, helping prevent unauthorized access and potential data breaches that bypass the database.

Performance Characteristics

TDE's cryptographic operations are extremely fast and well integrated with related Oracle Database features. TDE leverages CPU-based hardware cryptographic acceleration available in Intel® AES-NI and Oracle SPARC T4 and newer platforms to increase performance significantly. The block-level operations of TDE tablespace encryption receive an additional performance boost from database buffering and caching. Tablespace encryption integrates seamlessly with Oracle Advanced Compression, ensuring that compression occurs before encryption. Tablespace encryption also integrates with the advanced technologies in Oracle Exadata such as Exadata Hybrid Columnar Compression (EHCC) and Smart Scans, which offload certain cryptographic processing to storage cells for fast parallel execution.

Built-In Key Management

Key management is critical to the security of the encryption solution. Oracle Advanced Security TDE provides an out-of-the-box, two-tier key management architecture consisting of data encryption keys and a master encryption key. The data encryption keys are managed automatically by the database and are in-turn encrypted by the master encryption key. The master encryption key is stored and managed outside of the database within an Oracle Wallet, a standards-based PKCS12 file that protects keys, or in Oracle Key Vault, a centralized key management platform that complies with the industry standard OASIS Key Management Interoperability Protocol (KMIP). Keeping the master key separate from the encrypted data mitigates attacks because both the keys and the encrypted data must be separately compromised to gain access to clear data. The two-tier key architecture also enables rotation of master keys without having to re-encrypt all of the sensitive data.

Either to help you to address regulatory requirements or to comply with your own company policy, Oracle Database 18c introduced support for Bring Your Own Key (BYOK). This feature allows you to bring a user-generated key and use it as the master encryption key for Advanced Security Option Transparent Data Encryption. Those external keys can be ingested by TDE directly, or they can be batch-uploaded into OKV for later use by TDE-enabled databases.

Oracle Database has a dedicated SYSKM privilege that may run all key management operations including initializing TDE, rotating master keys and changing the keystore password. This role can be optionally delegated to a designated user account to enable separation of duty for these functions. Oracle Enterprise Manager provides a convenient graphical user interface for creating, rotating, and managing TDE master keys as shown in the figure below.

Oracle Key Vault is the only enterprise-grade key management platform that provides continuous key availability by clustering up to 16 active OKV instances across geographically distributed datacenters; it is a full-stack, security-hardened software appliance which provides centralized management of encryption keys, Oracle Wallets, Java Keystores, ACFS volume encryption keys, Solaris crypto keys, and credential files. Oracle Key Vault works with Oracle Database and MySQL TDE to automate the management of TDE master keys including creation, rotation, and expiration. Oracle Key Vault

centrally manages TDE master keys over a direct network connection, eliminating the need for local wallet files, reducing operational and security challenges of wallet file management such as periodic password rotation, wallet file backups, and wallet file recovery. Using Oracle Key Vault with TDE enables sites to scale their TDE deployments to hundreds or thousands of databases in different locations while improving operational efficiencies, reducing TCO, and enabling consistent key management policies. A RESTful API allows for secure, automated on-boarding of any number of current or future TDE-enabled databases without any further intervention by the OKV administrators.

Oracle Key Vault also integrates with popular Hardware Security Modules (HSM) from nCipher and Safenet (now Thales) to establish a Root of Trust (RoT) relationship where the secret that unlocks OKV is stored on a tamper-resistant, specialized, FIPS 140-2 level 3 certified hardware module.

Oracle Key Vault supports hybrid cloud deployments, so organizations migrating to the Oracle Cloud can use it to support TDE deployments in both their cloud and on premises databases.

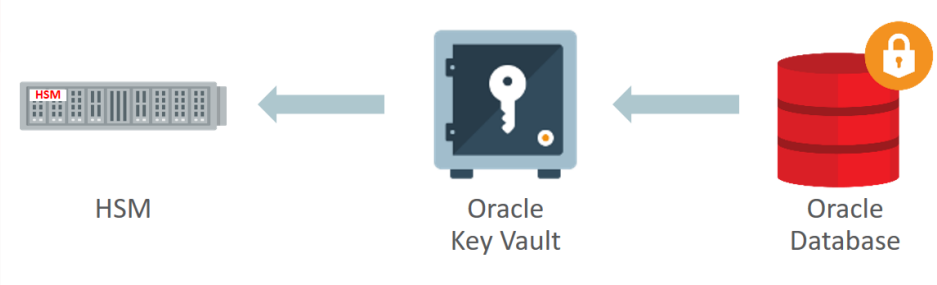


Figure 3. Oracle Key Vault and HSM as Root of Trust for TDE

Encryption Impact for Common Operational Activities

Essential day-to-day database operational activities can potentially leak sensitive data when not performed properly, making bypass easy. Examples of these activities include database backup and restore, data movement, high-availability clustering, and replication.

Example integrations with Oracle Advanced Security TDE

DATABASE TECHNOLOGIES	EXAMPLE POINTS OF INTEGRATION	TDE SUPPORT
High-Availability Clusters	Oracle Real Application Clusters (RAC), Oracle Data Guard	✓
Backup and Restore	Oracle Recovery Manager (RMAN), Oracle Secure Backup	✓
Export and Import	Oracle Data Pump Export and Import	✓
Database Replication	Oracle GoldenGate	✓
Pluggable Databases	Oracle Multitenant	✓
Engineered Systems	Oracle Exadata Smart Scan	✓
Storage Management	Oracle Automatic Storage Management (ASM) and ASM Cluster File System (ACFS)	✓
Data Compression	Oracle Standard, Advanced , and Hybrid Columnar Compression	✓

Oracle Advanced Security TDE supports these critical database operational activities and helps ensure that the data remains encrypted. Tablespace encryption integrates with Oracle Recovery Manager (backup and restore), Oracle Data Pump (data movement), Oracle Data Guard (redundancy and failover), and Oracle GoldenGate (replication). TDE also integrates with internal features of the database such as redo to prevent possible data leakage in logs. This fully integrated approach to database encryption makes the solution easy to deploy in complex real-world environments while protecting against bypass attacks that attempt to take advantage of gaps in operational processes.

Oracle Database 19c TDE provides two options for performing tablespace conversions from clear-text to encrypted tablespaces. For deployments which require conversion to be performed with no downtime, online tablespace encryption runs in the background to convert tablespaces from clear text to encrypted text while systems remain operational. TDE also offers an offline tablespace conversion mode which efficiently converts tablespaces with no storage overhead.

LIMITING SENSITIVE DATA EXPOSURE WITH DATA REDACTION

Privacy and compliance require a cost-effective approach to managing data exposure in applications. The embrace of smartphone and tablet devices make the issue of sensitive data exposure even more urgent as data access beyond the traditional office environment becomes commonplace. Even traditional applications require a more comprehensive solution for reducing exposure to sensitive data, for example, a call center application with a screen that exposes customer credit card information and personally identifiable information to call center operators. Exposing that information, even to valid application users, may violate privacy regulations and put the data at unnecessary risk.

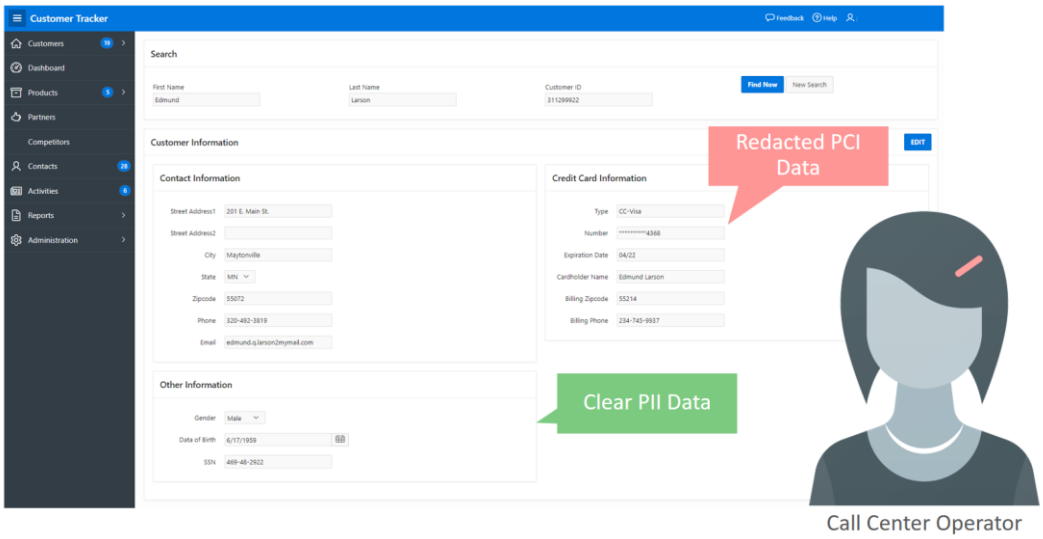


Figure 4. Clear and redacted information displayed in a call center application

Oracle Advanced Security Data Redaction

Oracle Advanced Security Data Redaction provides selective, on-the-fly redaction of sensitive data in database query results prior to display by applications so that unauthorized users cannot view the sensitive data. The stored data remains unaltered, while displayed data is transformed and redacted on-the-fly before it leaves the database. Data Redaction reduces exposure of sensitive information and helps prevent exploitation of application flaws that may disclose sensitive data in application pages. It is well suited for both new and legacy applications that need to limit exposure of sensitive data without invasive application changes. Oracle Data Redaction is particularly suited for reporting applications and other applications that are read-only.

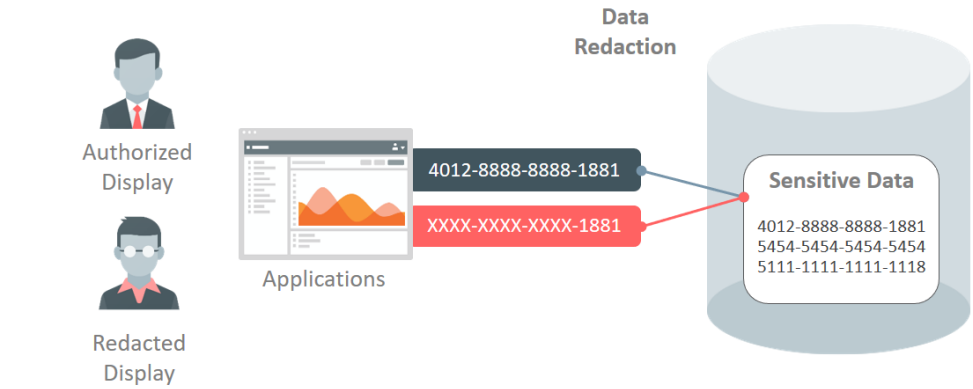


Figure 5. Redacting sensitive data displayed by applications using Data Redaction

Policies and Transformations

Oracle Advanced Security Data Redaction supports a number of different transformations that can redact all data in specified columns, preserve certain pieces of the data, or randomly generate replacement data. Examples of the supported data transformations are shown below.

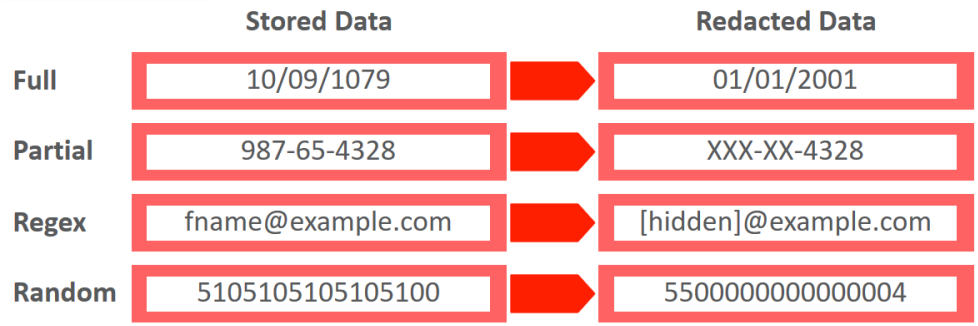


Figure 6. Example Data Redaction transformations

Data Redaction makes the business need-to-know decision based on declarative policy conditions that utilize rich runtime contexts available from the database and from the applications themselves. Examples include user identifiers, user roles, and client IP addresses.

Context information available from Oracle Application Express (APEX), Oracle Real Application Security, and Oracle Label Security also can be utilized to define redaction policies. Redacting APEX

applications is straightforward because policy conditions can leverage the application users and application identifiers that APEX automatically tracks.

Multiple runtime conditions can be joined together within a data redaction policy for fine-grained control over when redaction occurs. The policies are stored and managed inside of the database, and they go into effect immediately upon being enabled.

Performance Characteristics

High-speed performance is crucial for Data Redaction because the target databases typically will be production systems. Data needs to be transformed on-the-fly at runtime, without altering data stored on disk or in caches and buffers. Because the transformations will execute on production environments and will be repeated frequently, the performance overhead must be small.

One important performance characteristic of Data Redaction is that it supports only data transformations with proven high performance. These are a subset of all the possible operations that could be used to transform data in non-production environments. This specific subset avoids long-running and processor intensive operations.

Data Redaction also leverages performance optimizations of the Oracle Database that are only possible by being part of the database kernel. The implementation ensures that data transformations are fast in-memory computations. Policy information is cached in memory, and policy expressions are evaluated only once per execution, so there is no per row performance impact.

Security Considerations

Another benefit resulting from Data Redaction being part of the database kernel is tighter security. This implementation avoids potential vulnerabilities that plague other redaction techniques due to their dependence on proxies that can be meddled with. Additionally, Data Redaction in the kernel continues protecting sensitive data even when other security measures may be compromised. For example, runtime conditions in policies can narrow the impact of a SQL Injection attack by continuing to redact sensitive data even when the attack has bypassed other preventive controls in the application and database.

Data Redaction also avoids obvious sources of leakage where the redaction policy could be bypassed by copying data into a new table that does not have a policy. Certain mass copy operations that touch redacted data are blocked by default, and this behavior can be overridden where necessary using a Data Redaction exempt privilege.

Although Data Redaction can be used to prevent accidental viewing of sensitive data by privileged database users such as DBAs, it is intended primarily for redacting data displayed by software applications. Data Redaction does not prevent privileged users from connecting directly to the database and running ad hoc queries that back into pieces of sensitive data (i.e. it does not stop exhaustive ad hoc queries or other inference attacks). However, Data Redaction is fully compatible with Oracle Database security solutions that control and monitor privileged database user access, including DBAs. It can be deployed in tandem with other solutions such as Oracle Database Vault or Oracle Audit Vault and Database Firewall to provide defense-in-depth security. Data Redaction can also be used with database encryption as well, and it is a great complement to TDE.

Easy to Deploy Data Redaction

Data Redaction can be deployed for existing applications quickly using either a command line API or Oracle Enterprise Manager. The command line API is a PL/SQL procedure that accepts protected columns, transformation types, and conditions. Oracle Enterprise Manager provides a convenient Policy Expression Builder that enables administrators to define and apply redaction policies on existing applications. As shown below, the Policy Expression Builder dialog guides the user through creating policy conditions that use context obtained from applications, the database, the APEX framework, and other database security solutions.

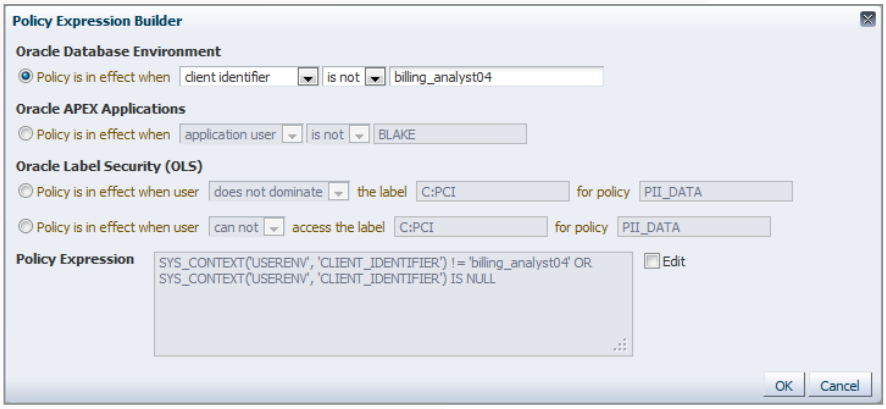


Figure 7. Using Oracle Enterprise Manager Policy Expression Builder to create Data Redaction policies

Predefined column templates also are available in Oracle Enterprise Manager for redacting common sensitive data such as credit card numbers and U.S. Social Security numbers. Oracle Enterprise Manager Sensitive Data Discovery assists in locating columns to be redacted inside of complex application schemas.

Another reason why Data Redaction is easy to deploy is its transparency to applications and the database. For application transparency, Data Redaction supports the column data types that are frequently used by applications and various database objects including tables, views, and materialized views. Redacted values retain key characteristics of the original data such as the data type and optional formatting characters. Random redaction values are drawn from data ranges defined by the existing column data. For transparency to the database, Data Redaction avoids impacting essential database operational activities. It does not affect administrative tasks such as data movement (Oracle Data Pump) or database backup and restore (Oracle Recovery Manager). It does not interfere with database cluster configurations such as Oracle Real Application Clusters, Oracle Data Guard, and Oracle GoldenGate. Data Redaction does not get in the way of existing database triggers or Oracle Virtual Private Database (VPD) policies. In addition, because Data Redaction is part of the database kernel, no separate installation is required.

Comparison to Alternative Approaches

Traditional approaches to redacting sensitive data typically relied on application coding or installing third-party software on the database server to modify its behavior. These alternatives have important drawbacks compared to Data Redaction.

Approaches that require coding new application logic, modifying existing SQL statements, or authoring custom application scripts are likely to result in disparate solutions that are inconsistent across the enterprise and costly to maintain over their lifetime. In addition, strict controls must be placed on new application development to make sure that custom application code and new objects are properly

accessed. The code also needs to take into consideration multiple factors under which the redaction policies are enforced while maintaining the performance and semantics of the application.

Approaches that add new components to the Oracle Database, overwrite existing components, establish proxies, and modify basic behavior of the database also are fraught with problems. Not only do the new components introduce new attack surfaces, but they also can create performance overhead, impact operational activities of the database, and may fail when attempting to transform complex database queries that are generated by applications. In contrast, redacting directly in the Oracle Database kernel using Data Redaction has tighter security, superior performance, and better compatibility with a range of database configurations, use cases, and workloads.

APPLYING ENCRYPTION AND REDACTION IN ORACLE MULTITENANT ARCHITECTURE

Oracle Advanced Security fully supports the Oracle Database multitenant architecture. Both TDE and Data Redaction attributes automatically follow Pluggable Databases (PDB) as they move between multitenant Container Databases (CDB). When moving a PDB that has redaction policies, the policies transfer directly to the new container as part of the PDB. When moving an encrypted PDB, the TDE master keys for that PDB are transferred separately from the encrypted data to maintain proper security separation during transit. Encryption and redaction immediately resume their normal operation after the PDB has been plugged in and configured.

DATA ENCRYPTION IN THE ORACLE CLOUD

In Oracle Database Cloud Service databases, data security is provided for data in transit and data at rest. Security of data in transit is achieved through network encryption. Security of data at rest is achieved through encryption of data stored in database data files and backups using Oracle Advanced Security Transparent Data Encryption. By default, all new tablespaces that are user created in a Database Cloud Service databases are encrypted. For multitenant deployments in the Oracle Cloud, TDE supports a keystore per pluggable database. This design offers greater isolation between tenants and enables independent key management operations.

In addition, to give customers the possibility to control their own master encryption keys, Oracle Key Vault supports hybrid cloud deployments. In this scenario, Oracle Key Vault can be deployed on-premises to support TDE deployments in both cloud and on-premises databases.

CONCLUSION

As data exposed in applications continues to rapidly expand, enterprises must have strong controls in place to protect data no matter what devices or applications are used. Oracle Database 19c, now available in the cloud and on-premises, helps organizations keep their sensitive information safe in this increasingly complex environment by delivering critical controls that enforce data security in the database.

Oracle Advanced Security with Oracle Database 19c provides two critical preventive controls. Transparent Data Encryption encrypts data at rest to stop database bypass attacks from accessing sensitive information in storage. Data Redaction reduces exposure of sensitive information in applications by redacting database query results on-the-fly, according to defined policies. Together these two controls form the foundation of a multi-layered, defense-in-depth approach. They further establish Oracle Database 19c Release as the world's most advanced database solution.

ORACLE CORPORATION

Worldwide Headquarters
500 Oracle Parkway, Redwood Shores, CA 94065 USA

Worldwide Inquiries
TELE + 1.650.506.7000 + 1.800.ORACLE1
FAX + 1.650.506.7200
oracle.com

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com. Outside North America, find your local office at oracle.com/contact.

 blogs.oracle.com/cloudsecurity/db-sec

 facebook.com/oracle

 twitter.com/oracle

Integrated Cloud Applications & Platform Services

White Paper: Encryption and Redaction with Oracle Advanced Security
August 2019

 Oracle is committed to developing practices and products that help protect the environment

ORACLE

Anexo VII - Oracle Advanced Security Data Redaction - FAQ.pdf

18c ORACLE Database

Oracle Advanced Security Transparent Data Encryption (TDE)

Frequently Asked Questions (FAQ)

MARCH 2018

ORACLE

Product Overview

Q. What does Transparent Data Encryption (TDE) provide?

A: TDE transparently encrypts data at rest in Oracle Databases. It stops unauthorized attempts from the operating system to access database data stored in files, without impacting how applications access the data using SQL.

TDE can encrypt entire application tablespaces or specific sensitive columns. Tablespace encryption is useful when you want to encrypt all data irrespective of columns. With tablespace encryption, you do not need to consider column characteristics such as indexes and constraints. Column encryption is useful in cases where only a handful of sensitive columns must be encrypted.

TDE is fully integrated with Oracle database. Encrypted data remains encrypted in the database, whether it is in tablespace storage files, temporary tablespaces, undo tablespaces, or other files that Oracle Database 18c relies on such as redo logs. Also, TDE can encrypt entire database backups and Data Pump exports. Oracle Recovery Manager (RMAN) and Data Pump Export/Import both integrate with TDE encryption to pass through previously encrypted data.

Q. How are TDE encryption keys managed?

A: TDE creates and manages multiple keys used for encryption. These keys must be protected because, if an attacker obtains encrypted data and matching keys, they can easily decrypt to see clear data.

TDE has a two-tier key architecture, with data encryption keys that are wrapped by a single database master key. Data encryption keys are managed by Oracle Database 18c behind the scenes. The master key is separated from encrypted data, stored outside of the database, and directly managed by the database security administrator in a keystore.

Two keystore options are available for TDE to support diverse customer environments. By default, TDE stores its master key in an Oracle Wallet, a PKCS#12 standards-based key storage file. Wallets provide an easy solution for small numbers of encrypted databases. Customers with many Oracle databases and other encrypted Oracle servers can leverage Oracle Key Vault, a security hardened software appliance that provides centralized key and wallet management for the enterprise. It uses industry standard OASIS Key Management Interoperability Protocol (KMIP) for communications. Customers can keep their local Oracle Wallets and Java Keystores, using Key Vault as a central location to periodically back them up, or they can remove keystore files from their environment entirely in favor of always-on Key Vault connections. All network connections between Key Vault and database servers are encrypted and mutually authenticated using SSL/TLS.

TDE master keys can be rotated periodically according to your security policies with zero downtime and without having to re-encrypt any stored data. Historical master keys are retained in the keystore in case encrypted database backups must be restored later. Master keys in the keystore are managed using a set of SQL commands (introduced in Oracle Database 12*c*). For separation of duties, these commands are accessible only to security administrators who hold the new SYSKM administrative privilege or higher. In addition to using SQL commands, you can manage TDE master keys using Oracle Enterprise Manager 12*c* or 13*c*.

Q. How does TDE impact database performance?

A: For Oracle Database 18c systems with modern hardware, the performance overhead from TDE typically is very low and not noticeable to end-users. The TDE page on Oracle Technology Network links to several real-world customer testimonials describing how TDE performs in live production environments.

TDE tablespace encryption leverages cryptographic circuitry present in most modern Intel® and Oracle SPARC processors and cores to accelerate encrypt and decrypt operations by 5-10 times. Oracle Database 18c further caches decrypted tablespace data to make repeated queries faster. For applications that run full table scans, the performance impact may be higher. More memory and bigger caches will improve performance in these

situations. As TDE works at tablespace level, one could consider moving all non-sensitive tables to a clear tablespace.

TDE column encryption can be narrowed to certain columns containing your most sensitive data to minimize overall performance impact. In this approach, only a few columns must be decrypted – even for complex analytical queries that scan large data sets. Column encryption also leverages CPU cryptographic acceleration.

Q. How transparent is TDE to business applications?

A: TDE is transparent to business applications and does not require application changes. Encryption and decryption occur at the database storage level, with no impact to the SQL interface that applications use (neither inbound SQL statements, nor outbound SQL query results).

Note that TDE is certified for use with common packaged applications. These certifications are mainly for profiling TDE performance under different application workloads and for capturing application deployment tips, scripts, and best practices.

Q. How transparent is TDE to database operations?

A: TDE is tightly integrated with frequently used Oracle Database 18c technologies to make it transparent to your database operations. For example, it is integrated with Oracle Advanced Compression, Oracle Real Application Clusters (RAC), Oracle Data Guard, Oracle Active Data Guard (primary/standby), Oracle Golden Gate (replication), and Oracle Multitenant (pluggable databases). Note that for unattended startup in database cluster configurations, TDE provides a key management option, auto-login wallet that allows the database to open its keystore and access its master key without a human operator.

Q. How does TDE integrate with Oracle Exadata?

A: TDE tablespace encryption leverages Oracle Exadata to further boost performance. For example, Exadata Smart Scans parallelize cryptographic processing across multiple storage cells, resulting in faster queries on encrypted data. TDE also benefits from support of hardware cryptographic acceleration on server processors in Exadata. TDE integration with Exadata Hybrid Columnar Compression (EHCC) compresses data first, improving cryptographic performance by greatly reducing the total amount of data to encrypt and decrypt.

Deployment Considerations

Q. What is the process to set up TDE?

As TDE is part of the database kernel, no separate installation is required. To deploy and configure TDE: 1) Setup a keystore and create an initial master key, 2) Enable encryption for tablespaces or columns in your database.

All steps can be executed using SQL commands or Oracle Enterprise Manager 12*c* or 13*c* GUI. All data that is added to those encrypted tablespaces is automatically encrypted. Column encryption however, can be applied to both new and existing tables. See the next question for information about encrypted existing clear data. For detailed information about setup steps, tuning, and migration, please refer to the product documentation for TDE.

Q. How do I migrate existing clear data to TDE encrypted data?

A: TDE provides multiple techniques to migrate existing clear data to encrypted tablespaces or columns. Solutions are available for both online and offline migration.

Existing tablespaces can be encrypted online with zero downtime on production systems or encrypted offline with no storage overhead during a maintenance period. Online tablespace conversion is available on Oracle Database 12.2.0.1 and above whereas offline tablespace conversion has been backported on Oracle Database 11.2.0.4 and 12.1.0.2.

Alternatively, you can copy existing clear data into a new encrypted tablespace with Oracle Online Table Redefinition (DBMS_REDEFINITION). It copies in the background with no downtime. This approach works for both 11*g* and 12*c* databases. This approach includes certain restrictions described in Oracle Database 12*c* product documentation.

Customers with Oracle Data Guard can use Data Guard and Oracle Data Pump to encrypt existing clear data with near zero downtime (see details here). This procedure encrypts on standby first (using DataPump Export/Import), switches over, and then encrypts on the new standby. Database downtime is limited to the time it takes to perform Data Guard switch over. Multiple synchronization points along the way capture updates to data from queries that executed during the process.

If you plan to migrate to encrypted tablespaces offline during a scheduled maintenance period, then you can use Data Pump to migrate in bulk. You also can use SQL commands such as ALTER TABLE MOVE, ALTER INDEX REBUILD (to move an index), and CREATE TABLE AS SELECT to migrate individual objects.

With TDE column encryption, you can encrypt an existing clear column in the background using a single SQL command such as ALTER TABLE MODIFY. This is a fully online operation.

Q. How much extra storage space is needed for TDE encrypted data?

A: For TDE tablespace encryption, the storage overhead is practically none.

The storage overhead associated with TDE column encryption is between 1 and 52 bytes per row for each encrypted column, depending on the following factors:

- Padding [Mandatory] - Padding to the next 16 bytes (for AES). With 3DES168, padding is to the next 8 bytes. For example, if a value requires 9 bytes of storage, then encrypting this value with 3DES168 requires an additional 7 bytes of storage.
- MAC [Optional] - If MAC is specified on the encrypted column, then 20 bytes are added to each value to support integrity checking using SHA. MAC is on by default.
- SALT [Optional] - If SALT is specified for TDE column level encryption, then an additional 16 bytes per value is added. Randomly generated 16 bytes SALT is on by default.

These numbers are important for storage planning. Note that when a column is marked as encrypted, any cryptographic expansion of the cipher data is handled by TDE transparently.

Q. Does TDE support Hardware Security Modules (HSM)?

A: TDE customers optionally may store their master keys in an external device such as HSM using the PKCS #11 interface. In this setup, master keys are stored directly in the third-party device rather than in Oracle Key Vault or Oracle Wallet.

When using PKCS #11, the third-party vendor provides the storage device, PKCS #11 software client library, secure communication from the device to the PKCS #11 client (running on the database server), authentication, auditing, and other related functionality. The vendor also is responsible for testing and ensuring high-availability

of the master encryption key in diverse database server environments, configurations, and versions. Customers should contact the device vendor to receive assistance for any related issues. We do not certify or validate third-party HSMs due to the above challenges.

Standards and Compliance

Q. Which encryption algorithms does TDE support?

A: TDE encryption uses international standards such as Advanced Encryption Standard (AES) and 3DES. Customers can choose their preferred data encryption algorithm and key length.

Q. What industry standards key management does TDE use?

A: TDE master key management uses standards such as PKCS #12 and PKCS #5 for Oracle Wallet keystore. Oracle Key Vault uses OASIS Key Management Interoperability Protocol (KMIP) and PKCS #11 standards for communications. Customers can choose Oracle Wallet or Oracle Key Vault as their preferred keystore.

Q. What security certifications and validations does TDE have?

A: The cryptographic library that TDE uses in Oracle Database 18c is validated for U.S. FIPS 140-2. See here for the library's FIPS 140 certificate (search for the text "Crypto-C Micro Edition"; TDE uses version 4.0). Also, see here for up-to-date summary information regarding Oracle Database certifications and validations.

Q. How does TDE help customers comply with Payment Card Industry (PCI) standards, healthcare data privacy laws (U.S. HIPAA/HITECH), and other security regulations?

A: TDE is an important database security control that helps Oracle customers comply with diverse standards, laws, and regulations that mandate data privacy and security. It provides essential encryption for data at rest in Oracle Databases, enabling customers to address a growing list of regulations in different geographies and industries and remain in compliance as regulations evolve. TDE often is deployed in conjunction with its key management options (Oracle Key Vault and Oracle Wallet) to address specific terms of PCI-DSS Requirement #3 - Protect Stored Cardholder Data. In healthcare context for HIPAA, customers use TDE to encrypt sensitive patient data stored in the database.

Comparison to Other Approaches

Q. How does TDE compare to encrypting in the application tier?

Encrypting in the application tier may be desirable for certain extremely sensitive columns where it is essential that only the application be able to access the data. However, this approach requires high-cost custom coding for proper encryption/decryption and management of keys. Furthermore, all application server nodes need to access the encryption keys making their management and protection difficult. It also increases the chances of corruption if users or the application can update any row/column without appropriate control.

Encryption in the application tier also adversely impacts core database query capabilities because you can only use the database to perform equivalency searches on encrypted columns. Common analytical queries that match against data ranges or computed values will not work. Application tier encryption does not benefit from Oracle Database In-Memory and Exadata high performance architecture.

TDE can be used to encrypt very diverse data all at once in database storage files and does not have these limitations.

Q. How does TDE compare to encrypting host directories or volumes?

Encrypting Oracle Database 18c tablespace files using file or volume encryption software running on the host may initially seem desirable with its support for diverse use cases and platforms; however, because these

technologies are not tuned for high I/O database operations, they can have dramatic impact on core database components. For example, if you attempt to store database redo logs in an encrypted directory or volume, this redo component will incur performance overhead, leading to increasing wait times for log switches, delayed archive file writes, accelerating memory consumption, and possible database stoppage (see details on My Oracle Support).

If you use third-party products that require installing invasive operating system and/or file system modules, this software can crash the database host. These modules may conflict with other running security programs (e.g. anti-virus, intrusion detection) and lead to system crashes. They may also disrupt your patching policies, preventing you from applying a critical patch to the host operating system or file system until a matching patch is available from the encryption vendor. Sensitive data in encrypted file storage may be presented as clear data to non-database programs and users running on the host, exposing your sensitive information to attacks that circumvent the database.

In addition, these solutions cannot limit encryption overhead to specific sets of database tables or columns, and they do not benefit from Oracle Database In-Memory and Exadata high performance architecture.

Note that TDE is fully supported on all operating system platforms including Oracle engineered systems. For addressing data at rest encryption outside of Oracle Databases, TDE can be paired with complementary Oracle technologies.

If a third-party vendor solution causes problems with your database environment, Oracle Support may request you to decrypt data, uninstall third-party software, and reproduce your issue before providing assistance. For questions about third-party encryption products or any support inquiries, you will be asked to consult with your vendor. Oracle provides no support for third-party solutions encrypting tablespace files on Oracle engineered systems such as Oracle Exadata and Oracle Database Appliance.

Q. How does TDE compare to encrypting in disk drives or SAN?

A: Encrypting Oracle Database 18c tablespace files using encryption features of disk drives or SAN storage arrays may seem desirable due to their support for diverse use cases outside of Oracle Databases. However, sensitive data in encrypted disks or SAN may be presented as clear data to non-database programs and users running on the host, exposing your sensitive information to attacks that circumvent the database. These solutions cannot limit encryption overhead to specific sets of database tables or columns, and they do not benefit from Oracle Database In-Memory and Exadata architectures. You typically must purchase new premium price hardware and/or software with optional add-ons. Troubleshooting data I/O issues becomes nearly impossible on encrypted storage arrays.

Complementary Technologies

Q. Can TDE be paired with other data at rest encryption technologies?

A: Oracle provides additional data at rest encryption technologies that can be paired with TDE to protect unstructured file data, storage files of non-Oracle databases, and more as shown in the table below.

Use Case	Oracle Technology
Encrypt files (non-tablespace) using Oracle file systems and operating systems	• Oracle ZFS - An encrypting file system for Solaris and other operating systems • Oracle ACFS - An encrypting file system that runs on Oracle Automatic Storage Management (ASM)

	• Oracle Linux native encryption modules including dm-crypt and eCryptFS
Encrypt files (non-tablespace) using Oracle Database 18c	Oracle Secure Files in combination with TDE. Support for Secure File LOBs is a core feature of the database
Encrypt data programmatically in the database tier	Oracle Database package encryption toolkit (DBMS_CRYPTO) for encrypting database columns using PL/SQL
Encrypt data programmatically in the application tier	Oracle Java (JCA/JCE), application tier encryption may limit certain query functionality of the database. Consider suitability for your use cases in advance

Table 1 – Complementary Oracle Data at Rest Encryption Technologies

Oracle provides solutions to encrypt sensitive data in the application tier – although this has implications for databases that you must consider in advance (see details here). Note that TDE is the only recommended solution specifically for encrypting data stored in Oracle Database 18c tablespace files.

Q. What security controls typically are configured alongside TDE?

A: It is recommended to use TDE in combination with other detective and preventive security controls available for Oracle Database 18c.

Preventive controls help you stop many common threats. Good prevention starts by granting only appropriate privileges and roles to database user accounts, following the security principle of least privilege. You also should encrypt database network connections using SQLNet encryption or built-in support for SSL/TLS. Next, you can add restrictions for privileged user accounts, limit display of sensitive application data, and sanitize copies of production data used in testing and development environments. Details about these preventive controls are shown below.

Preventive Control	**Description**
Oracle Database Vault	Reduces risk exposure coming from powerful database users such as DBA and privileged application connections. Restricts operations these privileged accounts can perform
Oracle Data Redaction	Redacts sensitive data from query results prior to display by applications. Enforces redaction at runtime, with low overhead, and according to conditions set in policies. Part of the same license as TDE (Oracle Advanced Security)
Oracle Data Masking and Subsetting	Makes it easy to create masked and subsetted copies of production data for use in non-production environments such as testing and development databases. Available as an add-on pack for Oracle Enterprise Manager
Oracle Label Security	Implements Multi-Level Security (MLS) enabling rows with differing sensitivity to reside in the same table. Explicitly labels rows with group, compartment, and sensitivity levels – then matches them with user labels

Table 2 – Oracle Database Preventive Controls Typically Used In Combination with TDE

Detective controls start with database auditing to capture records of database actions. You can deploy Oracle Audit Vault and Database Firewall to move audit information to a central repository where you can run database activity reports, detect anomalies, and generate security alerts. Oracle Audit Vault and Database Firewall also provides database firewall and monitoring capabilities that track inbound SQL statements, giving you early warning of unauthorized database activity and blocking threats before they cause harm.

Please refer to the Oracle Database Security page on Oracle Technology Network for more information about database security controls to use alongside TDE.

More Information

Q. How is TDE licensed?

TDE is part of Oracle Advanced Security license for Oracle Database Enterprise Edition. For on-premises databases, Advanced Security can be licensed by server core count or by named user plus (see pricing information here).

The Advanced Security license includes data redaction, tablespace encryption, column encryption, and wallet-based master key management. Centralized key and wallet management using Oracle Key Vault is licensed separately. Note that creating encrypted database backups (RMAN) and Data Pump exports also requires a license for Advanced Security if you do not already have one.

Q. Where can I learn more about TDE?

A: For more information about the benefits of TDE, please see the product page on Oracle Technology Network. A variety of helpful information is available on this page including product data sheet, customer references, videos, tutorials, and more.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services

CONTRATAÇÕES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

CATÁLOGO DE SOLUÇÕES DE TIC COM CONDIÇÕES PADRONIZADAS

(ORACLE)

MINISTÉRIO DA ECONOMIA
PÁTRIA AMADA BRASIL GOVERNO FEDERAL

Catálogo de Soluções de TIC com Condições Padronizadas - Oracle

Fabricante:	**Oracle do Brasil Sistemas Ltda.**
Versão do Catálogo:	3.0.0
Responsável pela elaboração e manutenção:	Secretaria de Governo Digital do Ministério da Economia (SGD).
Fundamento normativo:	Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, alterada pela Instrução Normativa SGD/ME nº 202, de 18 de setembro de 2019.
Data de publicação no DOU:	30/12/2021

Vigência:
Imediata a partir da publicação.

MINISTÉRIO DA ECONOMIA
Secretaria Especial de Desburocratização, Gestão e Governo Digital
Secretaria de Governo Digital

ANEXO I

CATÁLOGO DE PRODUTOS E SERVIÇOS

Acordo Corporativo nº 10/2021 - Processo nº 19974.100702/2019-21

1. Condições de utilização:

1.1. A existência deste Catálogo não obriga, direta ou indiretamente, qualquer órgão ou entidade que integre os poderes da União, Estados ou Municípios a celebrar qualquer contrato para a aquisição ou fornecimento de licenças ou serviços Oracle.

1.2. O órgão ou entidade, a partir de sua necessidade, deve realizar os estudos técnicos preliminares, analisando soluções alternativas e demais orientações previstas nas leis e normas que regem as contratações de soluções de tecnologia da informação e comunicação.

CATÁLOGO DE TIC COM CONDIÇÕES PADRONIZADAS – ORACLE					
Item	**Categoria**	**Descrição**	**Modelo de Licenciamento**	**PMC-TIC(1)**	**Vigência SA**
OR-001	Plataforma de Dados	Oracle Database Enterprise Edition	Licença Perpétua + Suporte e Atualização (SA)	R$ 244.566,43	12 meses
OR-002	Plataforma de Dados	Oracle Tuning Pack	Licença Perpétua + Suporte e Atualização (SA)	R$ 25.743,85	12 meses
OR-003	Plataforma de Dados	Oracle Real Application Clusters	Licença Perpétua + Suporte e Atualização (SA)	R$ 118.421,62	12 meses
OR-004	Plataforma de Dados	Oracle Partitioning	Licença Perpétua + Suporte e Atualização (SA)	R$ 59.210,84	12 meses
OR-005	Plataforma de Dados	Oracle Diagnostics Pack	Licença Perpétua + Suporte e Atualização (SA)	R$ 38.615,72	12 meses
OR-006	Plataforma de Dados	Oracle Active Data Guard	Licença Perpétua + Suporte e Atualização (SA)	R$ 59.210,82	12 meses

OR-007	Plataforma de Dados	Oracle Advanced Security	Licença Perpétua + Suporte e Atualização (SA)	R$ 77.231,50	12 meses
OR-008	Plataforma de Dados	Oracle Data Masking and Subsetting Pack	Licença Perpétua + Suporte e Atualização (SA)	R$ 59.210,82	12 meses
OR-009	Plataforma de Dados	Oracle Audit Vault and Database Firewall	Licença Perpétua + Suporte e Atualização (SA)	R$ 30.892,60	12 meses
OR-010	Plataforma de Dados	Oracle Database Vault	Licença Perpétua + Suporte e Atualização (SA)	R$ 59.210,82	12 meses
OR-011	Plataforma de Dados	Oracle Label Security	Licença Perpétua + Suporte e Atualização (SA)	R$ 59.210,82	12 meses
OR-012	Plataforma de Dados	Oracle Multitenant	Licença Perpétua + Suporte e Atualização (SA)	R$ 90.103,42	12 meses
OR-013	Plataforma de Dados	Oracle Key Vault	Licença Perpétua + Suporte e Atualização (SA)	R$ 514.876,70	12 meses
OR-014	Plataforma de Dados	Oracle GoldenGate	Licença Perpétua + Suporte e Atualização (SA)	R$ 90.103,42	12 meses
OR-015	Plataforma de Dados	Oracle GoldenGate for Non Oracle Database	Licença Perpétua + Suporte e Atualização (SA)	R$ 90.103,42	12 meses
OR-016	Plataforma de Dados	Oracle GoldenGate for Mainframe	Licença Perpétua + Suporte e Atualização (SA)	R$ 514.876,70	12 meses
OR-017	Plataforma de Dados	Oracle GoldenGate for Big Data	Licença Perpétua + Suporte e Atualização (SA)	R$ 102.975,34	12 meses
OR-018	Plataforma de Dados	Oracle Management Pack for Oracle GoldenGate	Licença Perpétua + Suporte e Atualização (SA)	R$ 18.020,68	12 meses
OR-019	Plataforma de Dados	Oracle GoldenGate Foundation Suite	Licença Perpétua + Suporte e Atualização (SA)	R$ 38.615,75	12 meses

(1) - O Preço Máximo de Compra de Item de TIC (PMC-TIC) possui validade conforme previsto na Cláusula Quinta "Da Vigência", do Acordo Corporativo nº 10/2021, considerando seus termos aditivos.

Documento assinado eletronicamente por **Ulysses César Amaro de Melo**, **Secretário(a) Substituto(a)**, em 28/12/2021, às 18:19, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Cristiano Jorge Poubel de Castro**, **Coordenador(a)-Geral**, em 28/12/2021, às 18:48, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Tony Gomes Tonete**, **Usuário Externo**, em 29/12/2021, às 10:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Daniel Darlen Corrêa Ribeiro**, **Usuário Externo**, em 29/12/2021, às 11:47, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.economia.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **21289993** e o código CRC **7B1EC427**.

Referência: Processo nº 19974.100702/2019-21. SEI nº 21289993

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 30/12/2021 | Edição: 246 | Seção: 3 | Página: 59

Órgão: Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de Governo Digital

EXTRATO DE TERMO ADITIVO

a) Espécie: Primeiro Termo Aditivo ao Acordo Corporativo nº 10/2021 que celebram a União, por intermédio da Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, e a empresa Oracle do Brasil Sistemas Ltda.

b) Processo SEI/ME: nº 19974.100702/2019-21.

c) Objeto: Atualização do Anexo I ao Acordo Corporativo nº 10/2021, visando à inclusão de novos produtos e serviços em conformidade com as condições comerciais pactuadas no instrumento principal.

d) Fundamentação Legal: Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, alterada pela Instrução Normativa SGD/ME nº 202, de 18 de setembro de 2019.

e) Despesa: O presente Termo Aditivo não contempla repasse de recursos financeiros entre os partícipes.

f) Prazo de vigência: O Primeiro Termo Aditivo ao Acordo Corporativo nº 10/2021 terá validade a partir da publicação no Diário Oficial da União.

g) Data de Assinatura: 29 de dezembro de 2021. Signatários: Ulysses Cesar Amaro de Melo, Secretário de Governo Digital Substituto da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, e Tony Gomes Tonete, Procurador da Oracle do Brasil Sistemas Ltda.

MINISTÉRIO DA
ECONOMIA

PÁTRIA AMADA
BRASIL
GOVERNO FEDERAL

www.economia.gov.br

Willian Rocha Bicalho

De: portaldeservicos@anac.gov.br
Enviado em: sexta-feira, 4 de março de 2022 16:20
Para: Willian Rocha Bicalho
Assunto: Projeto 487738 - Entregável Aprovado
Anexos: REC_FROM_GED_164640.docx; REC_FROM_GED_161432.xlsx

Prezados(as),

Informamos que foi concluída a etapa "Realizar Fiscalização do Projeto" do projeto número 487738 pela ANAC - Agência Nacional de Aviação Civil, e como resultado, o **entregável foi aprovado.**

Segue abaixo algumas informações:

- **Solicitante do Projeto**: Felipe Santos Sarmanho
- **Número**: 487738
- **Serviço**: Atender Demanda de TI - Projetizada
- **Descrição**: Prezados,

  a pedido do Superintendente, Gustavo Sanches, e do Gerente, Marcelo Lino, solicito o apoio para a realização da POV/POC da ferramenta DELPHIX.

  Esta demanda envolve as seguintes ações:
  Ação 1: A ANAC tem que definir a data aproximada de instalação, para geração do link, e também, se vai realizar a POV somente nos dados abertos do RAB ou se vai usar a base de dados Oracle do RAB (envolve o curador dos dados);
  Ação 2: A BLUE solicitará ao fabricante a disponibilização de um link para download de uma imagem de máquina virtual (OVA) contendo a aplicação;
  Ação 3: A BLUE e a DELPHIX necessitarão de duas agendas (de 1 hora cada, por meio de videoconferência) com a equipe de infraestrutura para realizar a instalação. Existe a necessidade de duas agendas por conta de um teste intermediário;
  Ação 4: A BLUE e a DELPHIX necessitará de uma agenda (por meio de videoconferência) com a equipe de banco de dados e/ou área de dados e/ou administrador do sistema a ser utilizado na POV. Nesta etapa os dados são realmente ingeridos pela plataforma.

  Apoio da GlobalWeb é necessário especificamente para a Ação 3 e 4.
  Quanto as Ações 1 e 2, ainda estão em tratativas pela gestão da ANAC. Então solicito aguardar estas ações.

  Oportunamente iremos passar o contato da empresa Blue (representante da Delphix) para que a equipe da GlobalWeb entre em contato faça o agendamento para implantação da ferramenta.

  Para esta demanda,
  - solicito que NÃO seja elaborado o documento de planejamento técnico.
  - solicito que seja enviado por e-mail, depois do alinhamento com a empresa Blue, o cronograma de atividades e prazos acordados.

Atenciosamente,

Gestão de Projetos GlobalWeb
Superintendência de Tecnologia da Informação - STI

Telefones para contato, Interno: 9000 e Externo: 0800-617767
E-mail para contato: portaldeservicos@anac.gov.br

ORACLE

Oracle Technology Products

Oracle Lifetime Support Policy

January 20, 2022 | Version 1.00

TABLE OF CONTENTS

ORACLE LIFETIME SUPPORT: 3

From Five Years to Forever 3

ORACLE LIFETIME SUPPORT: 5

Oracle Essbase Releases 6

Oracle SQL Developer Data Modeler Releases 7

Oracle REST Data Services (formerly Application Express Listener) 8

Oracle's Ikan Releases 9

Oracle Collaboration Suite Releases 10

Oracle Beehive Releases 10

Oracle Enterprise Manager Releases 10

Oracle Business Transaction Management Releases (Formerly Amberpoint) 11

Oracle Real User Experience Insight Releases (Formerly Moniforce) 12

Oracle Application Testing Suite Releases 13

Oracle's mValent Releases 14

Oracle Rdb Database Releases 15

Oracle CODASYL DBMS Database Release 15

Oracle TimesTen In-Memory Database Releases 15

Oracle Berkeley DB (Formerly Sleepycat) Releases 16

Oracle Database Lite Releases 18

Oracle Database Mobile Server 18

Oracle Reliaty Backup Releases 18

Oracle Secure Backup Releases 19

Oracle Warehouse Builder Releases 19

Oracle's JD Edwards EnterpriseOne Extended Process Integration (XPI) Releases 19

Oracle's Auptyma Release 20

Oracle Express Server Release 20

Oracle Gateway Release's 20

Oracle's TripleHop Releases 23

Oracle Secure Enterprise Search 23

Oracle Application Express (Formerly HTML DB) 23

Oracle Zero Data Loss Appliance Releases 24

Oracle Fail Safe Releases 24

Oracle's ClearApp Releases 25

Oracle Virtual Iron Releases 25

Oracle's Secerno Releases 26

Oracle Audit Vault and Database Firewall Releases 27

Oracle Key Vault Releases 27

Oracle's MySQL Releases 27

Oracle's NoSQL Database Release 28

Oracle Big Data Appliance 29

Oracle Big Data SQL 29

Oracle Big Data Connectors 29

Oracle Big Data Spatial and Graph 30

Oracle Exadata Storage Server Software 31

ORACLE TECHNOLOGY

Maximize your support investment, unlock the full value of your Oracle products, and control your upgrade strategy—with the industry's leading support policy.

Simple, predictable, flexible, and the most comprehensive support policy available, the Oracle Lifetime Support Policy helps drive your business success. Oracle's industry leading support policy covers your entire technology environment, from database to middleware to applications—an industry first, only from Oracle.

Oracle's Lifetime Support Policy also puts you in control of your upgrade strategy. Our flexible support policy stages make it easier for you to plan and budget for Oracle's exclusive product upgrades. You'll enjoy continued peace of mind, knowing that we'll always be there to support your business. When it's time to upgrade, you'll have rights to major product releases, so you can benefit from Oracle's technology leadership and keep pace with the world of business.

Expect lifetime support. Expect control of your technology future—with Oracle's Lifetime Support Policy.

ORACLE LIFETIME SUPPORT:

From Five Years to Forever

Oracle Lifetime Support Policy

With Oracle Support, you know up front and with certainty how long your Oracle products are supported. The Lifetime Support Policy provides access to technical experts for as long as you license your Oracle products and consists of three support stages: Premier Support, Extended Support, and Sustaining Support. It delivers maximum value by providing you with rights to major product releases so you can take full advantage of technology and product enhancements. Your technology and your business keep moving forward together.

Premier Support provides a standard five-year support policy for Oracle Technology products. You can extend support for an additional three years with Extended Support for specific releases or receive indefinite technical support with Sustaining Support.

Premier Support

As an Oracle customer, you can expect the best with Premier Support, our award-winning, nextgeneration support program. Premier Support provides you with maintenance and support for your Oracle Database products for five years from their general availability date. You benefit from

- Major product and technology releases
- Technical support
- My Oracle Support
- Updates, fixes, security alerts, data fixes, and critical patch updates
- Tax, legal, and regulatory updates
- Upgrade scripts
- Certification with most new third-party products/versions
- Certification with most new Oracle products

Extended Support

Your technology future is assured with Oracle's Extended Support. Extended Support lets you stay competitive, with the freedom to upgrade on your timetable. If you take advantage of Extended Support, it provides you with an extra three years of support for specific Oracle releases for an additional fee. You benefit from

- Major product and technology releases
- Technical support
- My Oracle Support
- Updates, fixes, security alerts, data fixes, and critical patch updates
- Tax, legal, and regulatory updates
- Upgrade scripts
- Certification with most existing third-party products/versions
- Certification with most existing Oracle products

Extended Support may not include certification with some new third-party products/versions.

Sustaining Support

Sustaining Support puts you in control of your upgrade strategy. When Premier Support expires, if you choose not to purchase Extended Support, or when Extended Support expires, Sustaining Support will be available for as long as you license your Oracle products. With Sustaining Support, you receive technical support, including access to our online support tools, knowledgebases, and technical support experts. You benefit from

- Major product and technology releases
- Technical support
- Access to My Oracle Support
- Fixes, updates, and critical patch updates created during Premier Support and Extended Support (if offered and only after the Extended Support period ends)
- Upgrade scripts created during the Premier Support stage

Sustaining Support does not include

- New updates, fixes, security alerts, data fixes, and critical patch updates
- New tax, legal, and regulatory updates
- New upgrade scripts
- Certification with new third-party products/versions
- Certification with new Oracle products

For more specifics on Premier Support, Extended Support, and Sustaining Support, please refer to Oracle's 'Technical Support Policies'.

ORACLE LIFETIME SUPPORT:

Coverage for Oracle Technology Products

Oracle Database Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
8.1.7	Sept 2000	Dec 2004	Dec 2006	Indefinite
9.2	Jul 2002	Jul 2007	Jul 2010	Indefinite
10.1	Jan 2004	Jan 2009	Jan 2012	Indefinite
10.2	Jul 2005	Jul 2010	Jul 2013	Indefinite
11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
11.2	Sep 2009	Jan 2015	Dec 2020	Indefinite
Enterprise Edition 12.1 [2]	Jun 2013	Jul 2018	Jul 2022	Indefinite
Standard Edition (SE) 12.1	Jun 2013	Aug 2016	Not Available	Indefinite
Standard Edition One (SE1) 12.1	Jun 2013	Aug 2016	Not Available	Indefinite
Standard Edition 2 (SE2) 12.1 [2]	Sep 2015	Jul 2018	Jul 2022	Indefinite
12.2.0.1 [1]	Mar 2017	Nov 30, 2020 (Limited Error Correction Period for 12.2.0.1 – Dec 1, 2020 – Mar 31, 2022)	Not Available	Indefinite

[1] Oracle Database 12.2.0.1: Premier Support error correction provided for the period of December 1, 2020 through March 31, 2022 will be limited to Severity 1 production fixes and security fixes delivered via the Quarterly Release Update (RU) process. Error Correction support will be available only for the following platforms: Linux x86-64, Solaris x86-64, Solaris SPARC, IBM AIX on Power Systems, IBM Linux on System Z (ZLinux), HP-UX Itanium, Fujitsu BS2000 and Microsoft Windows x64. This extension excludes:

- Functional upgrades of any kind, issues associated with Third-Party software, and certifications with new versions of the OS; embedded components in the Oracle Database that rely upon de-supported releases of Java products; updates to any cryptography related functionality, including, but not limited to, Transport Layer Security (TLS), network encryption, and other forms of secured communications.
- Embedded components in the Oracle Database that rely upon de-supported releases of Java products; updates to any cryptography related functionality, including, but not limited to, Transport Layer Security (TLS), network encryption, and other forms of secured communications.

[2] Oracle Database 12.1.0.2 : Extended Support is offered for the period August 2021 through July 2022 for the following platforms: Linux x86-64, Linux on IBM Z, IBM AIX on POWER Systems (64 bit), HP-UX Itanium, Fujitsu BS2000, Oracle Solaris on SPARC, Oracle Solaris on x86-64 and Microsoft Windows x64. Please note that the Microsoft Windows 2008 version used for building the Oracle Database 12.1.0.2 Windows platform reached end-of-life support on January 14, 2020. However, we will make reasonable efforts to deliver patches for Database 12.1.0.2 for Windows until July 2022, as long as our tooling continues to function.

Oracle Database Releases (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
18c	Jul 2018	Jun 2021	Not Available	Indefinite
19c (Long Term Release)	Apr 2019	Apr 2024	Apr 2027	Indefinite
21c (Innovation Release)	Aug 2021	Apr 2024	Not Available	Indefinite

For more detailed information on bug fix and patch release policies and dates, please refer to the Database Error Correction Support Policy (Doc ID 209768.1) and the Release Schedule of Current Database Releases (Doc ID 742060.1)

Information on upgrade paths can be found in the Database Upgrade Guide for the release you plan to upgrade to. Product documentation can be found at https://docs.oracle.com in the Oracle Help Center.

Oracle Essbase Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Essbase 21.x	Dec 2020	Aug 2025	Not Available	Indefinite

For previous Oracle Essbase releases, please see the Middleware and Applications LSP.

Oracle SQL Developer Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
1.0	Mar 2006	Mar 2011	Not Available	Indefinite
1.1	Dec 2006	Mar 2011	Not Available	Indefinite
1.2	Jun 2007	Jun 2012	Not Available	Indefinite
1.5	Apr 2008	Apr 2013	Not Available	Indefinite
2.1	Dec 2009	Dec 2014	Not Available	Indefinite
3.0	Mar 2011	Mar 2016	Not Available	Indefinite
3.1	Feb 2012	Feb 2017	Not Available	Indefinite
3.2	Aug 2012	Aug 2017	Not Available	Indefinite
4.0	Sep 2014	Sep 2019	Not Available	Indefinite

Oracle SQL Developer Releases (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
4.1	May 2015	May 2020	Not Available	Indefinite
4.2	Apr 2017	Apr 2022	Not Available	Indefinite
17.2	Jul 2017	Jul 2022	Not Available	Indefinite
17.3	Oct 2017	Oct 2022	Not Available	Indefinite
17.4	Dec 2017	Dec 2022	Not Available	Indefinite
18.1	Apr 2018	Apr 2023	Not Available	Indefinite
18.2	Jul 2018	Jul 2023	Not Available	Indefinite
18.3	Oct 2018	Oct 2023	Not Available	Indefinite
18.4	Jan 2019	Jan 2024	Not Available	Indefinite
19.1	Apr 2019	Apr 2024	Not Available	Indefinite
19.2	Sep 2019	Sep 2024	Not Available	Indefinite
19.4	Dec 2019	Dec 2024	Not Available	Indefinite
20.2	Jun 2020	Jun 2025	Not Available	Indefinite
20.4	Jan 2021	Jan 2026	Not Available	Indefinite
21.2	Jul 2021	Jul 2026	Not Available	Indefinite

Oracle SQL Developer Data Modeler Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
2.0	Jul 2009	Jul 2014	Not Available	Indefinite
3.0	Jan 2011	Jan 2016	Not Available	Indefinite
3.1	Feb 2012	Feb 2017	Not Available	Indefinite
3.3	Mar 2013	Mar 2018	Not Available	Indefinite

Oracle SQL Developer Data Modeler Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
4.0	Sep 2014	Sep 2019	Not Available	Indefinite
4.1	May 2015	May 2020	Not Available	Indefinite
4.2	Apr 2017	Apr 2022	Not Available	Indefinite
17.2	Jul 2017	Jul 2022	Not Available	Indefinite
17.3	Oct 2017	Oct 2022	Not Available	Indefinite
17.4	Dec 2017	Dec 2022	Not Available	Not Available
18.1	Apr 2018	Apr 2023	Not Available	Not Available
18.2	Jul 2018	Jul 2023	Not Available	Not Available
18.3	Oct 2018	Oct 2023	Not Available	Not Available
18.4	Jan 2019	Jan 2024	Not Available	Not Available
19.1	Apr 2019	Apr 2024	Not Available	Not Available
19.2	Aug 2019	Aug 2024	Not Available	Not Available
19.4	Nov 2019	Nov 2024	Not Available	Indefinite
20.2	Jun 2020	Jun 2025	Not Available	Indefinite
20.3	Oct 2020	Oct 2025	Not Available	Indefinite
20.4	Jan 2021	Jan 2026	Not Available	Indefinite
21.1	Apr 2021	Apr 2026	Not Available	Indefinite
21.2	Jul 2021	Jul 2026	Not Available	Indefinite

Oracle REST Data Services (formerly Application Express Listener)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
1.0	Jul 2010	Jul 2015	Not available	Indefinite
1.1	Mar 2011	Mar 2016	Not available	Indefinite

Oracle REST Data Services (formerly Application Express Listener) (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
2.0	Dec 2012	Dec 2017	Not available	Indefinite
3.0	Jun 2015	Jun 2020	Not available	Indefinite
17.4	Dec 2017	Dec 2022	Not available	Indefinite
18.1	Apr 2018	Apr 2023	Not available	Indefinite
18.2	Jul 2018	Jul 2023	Not available	Indefinite
18.3	Oct 2018	Oct 2023	Not available	Indefinite
18.4	Jan 2019	Jan 2024	Not available	Indefinite
19.1	Apr 2019	Apr 2024	Not available	Indefinite
19.2	Aug 2019	Aug 2024	Not available	Indefinite
19.4	Dec 2019	Dec 2024	Not Available	Indefinite
20.2	Jul 2020	Jul 2025	Not Available	Indefinite
20.3	Oct 2020	Oct 2025	Not Available	Indefinite
20.4	Jan 2021	Jan 2026	Not Available	Indefinite
21.1	Jan 2021	Jan 2026	Not Available	Indefinite
21.2	Jul 2021	Jul 2026	Not Available	Indefinite

Oracle's Ikan Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
CWD4ALL (All releases)	Not Available	Not Available	Not Available	Aug 2009
Oracle-Branded Releases				
Oracle SQL Developer Data Modeler 2.0.0.57.0	Jul 2009	Jul 2014	Jul 2017	Indefinite

Support for all CWD4ALL releases will end August 31, 2009. Customers are advised to use the Oracle-branded product, Oracle SQL Developer Data Modeling.

Oracle Collaboration Suite Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
9.0.3	Dec 2002	Oct 2005	Not Available	Not Available
9.0.4	Apr 2004	Mar 2007	Not Available	Mar 2010
10.1	Aug 2005	Aug 2010	Aug 2013	Indefinite

Support retirement dates have already been announced for Oracle Collaboration Suite 9.0. For more detailed information on bug fix and patch release policies and dates, please refer to the Database Error Correction Support Policy (Doc ID 209768.1)

Oracle Beehive Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Beehive 2.0	Feb 2010	Feb 2015	Feb 2018	Indefinite
Beehive Voicemail for 2.0	Feb 2010	Feb 2015	Not Available	Indefinite

Oracle Enterprise Manager Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Enterprise Manager Grid Control 10.1	Feb 2004	Feb 2009	Feb 2012	Indefinite
Enterprise Manager Grid Control 10.2	Oct 2005	Nov 2011	Nov 2014	Indefinite
Enterprise Manager Grid Control 11.1	Apr 2010	Apr 2015	Apr 2018	Indefinite
Enterprise Manager Cloud Control 12.1	Oct 2011	Oct 2016	Oct 2020	Indefinite
Enterprise Manager Cloud Control 13.x	Dec 2015	Dec 2023	Dec 2026	Indefinite

Oracle Business Transaction Management Releases (Formerly Amberpoint)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
AMS 5.0 and Earlier	Not Available	Not Available	Not Available	Not Available
AMS 6.0.5.1	Feb 2010	Mar 2012	Not Available	Not Available
AMS 6.1.4.1	Feb 2010	Mar 2012	Not Available	Indefinite
AMS 6.5.3.x	Feb 2010	Mar 2012	Not Available	Indefinite
SNMP Adapter 1.0.1.1	Feb 2010	Mar 2012	Not Available	Indefinite
Datapower Observer 1.0.2.0	Feb 2010	Mar 2012	Not Available	Indefinite
BW Observer 2.2.1.0	Feb 2010	Mar 2012	Not Available	Indefinite
Cisco AXG Observer (All Versions)	Not Available	Not Available	Not Available	Not Available
BMC Adapter (All Versions)	Not Available	Not Available	Not Available	Not Available
HPOVO Adapter (All Versions)	Not Available	Not Available	Not Available	Not Available
Internal Tools (All Versions)	Not Available	Not Available	Not Available	Not Available
Jigsaw Tools (All Versions)	Not Available	Not Available	Not Available	Not Available
MOM Adapter (All Versions)	Not Available	Not Available	Not Available	Not Available
SCOM Adapter (All Versions)	Not Available	Not Available	Not Available	Not Available
SiteScope Adapter (All Versions)	Not Available	Not Available	Not Available	Not Available
TEC Adapter (All Versions)	Not Available	Not Available	Not Available	Not Available
Oracle Branded Releases				
Oracle Business Transaction Management 6.5.4.x	Apr 2010	Apr 2012	Apr 2014	Indefinite
Oracle Business Transaction Management 11.1.x	Mar 2011	Mar 2016	Mar 2019	Indefinite
Oracle Business Transaction Management 12.1.x	Oct 2011	Oct 2016	Oct 2019	Indefinite

Note: No Certification will be provided to new OS and 3rd Party products for legacy AmberPoint releases and any AMS 6.0.x, 6.1.x and 6.5.x release not listed will receive indefinite sustaining support.

Oracle Real User Experience Insight Releases (Formerly Moniforce)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
UXinsight 4.3x	Oct 2007	Jun 2008	Not Available	Not Available
UXinsight 4.4	Feb 2008	Dec 2008	Not Available	Not Available
webProbe 3.2.x 32bit	Jun 2005	Not Available	Not Available	Dec 2010
webProbe 3.6.x (32 and 64 bit)	Jun 2007	Not Available	Not Available	Dec 2010
webProbe 3.6.4 64bit	Jan 2008	Dec 2009	Not Available	Dec 2010
webSensor Enterprise 3.2.x 32bit	Jun 2005	Not Available	Not Available	Dec 2010
webSensor Enterprise 3.6.x (32 and 64 bit)	June 2007	Not Available	Not Available	Dec 2010
webSensor Enterprise 3.6.4 64bit	Jan 2008	Dec 2009	Not Available	Dec 2010
webSensor Commerce 3.2.x 32bit	Jun 2005	Not Available	Not Available	Not Available
webSensor Commerce 3.6.x (32 and 64 bit)	Jun 2007	Not Available	Not Available	Not Available
webSensor Commerce 3.6.4 64bit	Jan 2008	Jan 2009	Jan 2009	Jan 2009
webAlarm	Not Available	Jan 2009	Jan 2009	Jan 2009
Oracle Branded Releases				
Oracle Real User Experience Insight 4.4.1	Mar 2008	Dec 2009	Dec 2010	Dec 2011
Oracle Real User Experience Insight 4.5.x	Sep 2008	Sep 2010	Sep 2012	Indefinite
Oracle Real User Experience Insight 5.x	Apr 2009	Apr 2011	Apr 2013	Indefinite
Oracle Real User Experience Insight 6.0.x	Nov 2009	Nov 2011	Nov 2013	Indefinite
Oracle Real User Experience Insight 6.5.x	Apr 2010	Apr 2012	Apr 2014	Indefinite
Oracle Real User Experience Insight 11.1.x	Oct 2010	Oct 2015	Oct 2018	Indefinite
Oracle Real User Experience Insight 12.1.x	Oct 2011	Oct 2016	Oct 2019	Indefinite
Oracle Real User Experience Insight 13.x	Dec 2015	Dec 2023	Dec 2026	Indefinite

The migration path for webAlarm is to use Oracle's existing service-level monitoring solution.

Oracle Application Testing Suite Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
e-TEST suite 5.x and earlier	Not Available	Not Available	Not Available	Not Available
e-TEST suite 6.x	Not Available	Not Available	Not Available	Not Available
e-TEST suite 7.x	Not Available	Not Available	Not Available	Not Available
e-TEST suite 8.0	Mar 2005	Not Available	Not Available	Not Available
e-TEST suite 8.1	Jun 2006	Not Available	Not Available	Not Available
e-TEST suite 8.2	Apr 2007	Not Available	Not Available	Jun 2009
Oracle Application Testing Suite 8.3	Jun 2008	Jun 2010	June 2012	Indefinite
Oracle Application Testing Suite 8.4	Sep 2008	Sep 2010	Sep 2012	Indefinite
Oracle Application Testing Suite 8.5	Jan 2009	Jan 2011	Jan 2013	Indefinite

Oracle Application Testing Suite Releases (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Application Testing Suite 9.0	Sep 2009	Sep 2011	Sep 2013	Indefinite
Oracle Application Testing Suite 9.1	Apr 2010	Apr 2015	Apr 2018	Indefinite
Oracle Application Testing Suite 9.2	Nov 2010	Nov 2015	Nov 2018	Indefinite
Oracle Application Testing Suite 9.3	Aug 2011	Aug 2016	Aug 2019	Indefinite
Oracle Application Testing Suite 12.x	May 2012	May 2017	May 2020	Indefinite
Oracle Application Testing Suite 13.x	Jun 2017	Jun 2022	Jun 2025	Indefinite

Oracle's mValent Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
mValent Integrity 3.x and earlier	Jan 2006	Not Available	Not Available	Not Available
mValent Integrity 4.0	Jan 2006	Not Available	Not Available	Not Available
mValent Integrity 4.1.x	Jan 2006	Not Available	Not Available	Not Available
mValent Integrity 4.2.x	Dec 2007	Not Available	Not Available	Not Available
mValent Integrity 5.0.x	Dec 2007	Not Available	Not Available	Dec 2011
mValent Integrity 5.1.x	Sep 2008	Not Available	Not Available	Dec 2011
mValent Integrity 5.2.x	Dec 2008	Not Available	Not Available	Dec 2012
mValent Integrity 5.3.x	Feb 2009	Dec 2011	Dec 2013	Indefinite

Oracle Rdb Database Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
7.0	Oct 1996	Aug 2007	Aug 2009	Indefinite
7.1	Jul 2001	Dec 2007	Dec 2010	Indefinite
7.2	Jan 2006	Jul 2015	Jul 2017	Indefinite
7.3	Mar 2011	Sep 2020	Sep 2023	Indefinite
7.4	Aug 2020	Sep 2023	Not Available	Indefinite

Oracle CODASYL DBMS Database Release

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
7.0	Oct 1996	Aug 2007	Aug 2009	Indefinite
7.1	Jul 2001	Dec 2007	Dec 2010	Indefinite
7.2	Jan 2006	Jul 2015	Jul 2017	Indefinite
7.3	Mar 2011	Sep 2020	Sep 2023	Indefinite
7.4	Nov 2021	Sep 2023	Not Available	Indefinite

Oracle TimesTen In-Memory Database Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
5.0	Nov 2003	Nov 2005	Not Available	Not Available
5.1	Oct 2004	Oct 2006	Not Available	Not Available
6.0	Sep 2005	Sep 2008	Sep 2009	Indefinite
7.0	Feb 2007	Feb 2012	Feb 2015	Indefinite
11.2.1	May 2009	May 2014	May 2017	Indefinite
11.2.2	Jan 2012	Jan 2021	Jan 2023	Indefinite
18.1	May 2018	May 2023	May 2026	Indefinite
22.1	Nov 2021	Nov 2026	Nov 2029	Indefinite

The releases of the Oracle Database Enterprise Edition Option TimesTen Application-Tier Database Cache will follow the same support timeframe as the associated Oracle TimesTen In-Memory Database releases.

Oracle Berkeley DB (Formerly Sleepycat) Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
3.1.14	Jun 2000	Dec 2006	Dec 2007	Indefinite
3.1.17	Aug 2000	Dec 2000	Dec 2007	Indefinite
3.2.9	Jan 2001	Dec 2006	Dec 2007	Indefinite
3.3.11	Jul 2001	Dec 2007	Dec 2010	Indefinite
4.0.14	Dec 2001	Dec 2008	Dec 2011	Indefinite
4.1.25	Sep 2002	Dec 2008	Dec 2011	Indefinite
4.2.52	Nov 2003	Dec 2008	Dec 2011	Indefinite
4.3.29	Nov 2004	Dec 2009	Dec 2012	Indefinite
4.4.20	Nov 2005	Dec 2010	Dec 2013	Indefinite
4.5	Sep 2006	Sep 2011	Sep 2014	Indefinite
4.6.21	Nov 2007	Nov 2012	Nov 2015	Indefinite
4.7.25	May 2008	May 2013	May 2016	Indefinite
4.8.30	Apr 2010	Apr 2015	Apr 2018	Indefinite
Berkeley DB 11.2.5.0	Nov 2010	Nov 2015	Nov 2018	Indefinite
Berkeley DB 11.2.5.1	Jan 2011	Jan 2016	Jan 2019	Indefinite
Berkeley DB 11.2.5.2	Jun 2011	Jun 2016	Jun 2019	Indefinite
Berkeley DB 11.2.5.3	Dec 2011	Dec 2016	Dec 2019	Indefinite
Berkeley DB 12.1.6.0	Jun 2013	Jun 2018	Jun 2021	Indefinite
Berkeley DB 12.1.6.1	Jun 2014	Jun 2019	Jun 2022	Indefinite
Berkeley DB 12.1.6.2	Jan 2016	Jan 2021	Jan 2024	Indefinite
Berkeley DB XML 1.2.1	Feb 2004	Dec 2007	Dec 2010	Indefinite
Berkeley DB XML 2.0.9	Jan 2005	Dec 2008	Dec 2011	Indefinite

Oracle Berkeley DB (Formerly Sleepycat) Releases (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Berkeley DB XML 2.1.8	May 2005	Dec 2008	Dec 2011	Indefinite
Berkeley DB XML 2.2.13	Jan 2006	Jan 2009	Jan 2012	Indefinite
Berkeley DB XML 2.3	Jan 2007	Jan 2012	Jan 2015	Indefinite
Berkeley DB XML 2.4	Apr 2008	Apr 2013	Apr 2016	Indefinite
Berkeley DB XML 11.2.2.5	Aug 2009	Aug 2014	Aug 2017	Indefinite
Berkeley DB XML 12.1.6.0	Sep 2014	Sep 2019	Sep 2022	Indefinite
Berkeley DB Java Edition 1.7.1	Feb 2005	Feb 2008	Not Available	Indefinite
Berkeley DB Java Edition 2.0.42	Jun 2005	Jun 2008	Jun 2010	Indefinite
Berkeley DB Java Edition 2.0.54	Jul 2005	Jul 2008	Jul 2010	Indefinite
Berkeley DB Java Edition 2.0.90	Nov 2005	Nov 2008	Nov 2010	Indefinite
Berkeley DB Java Edition 2.1.30	Jan 2006	Jan 2011	Jan 2014	Indefinite
Berkeley DB Java Edition 3.0.11	May 2006	May 2011	May 2014	Indefinite
Berkeley DB Java Edition 3.1.0	Sep 2006	Sep 2011	Sep 2014	Indefinite
Berkeley DB Java Edition 3.1.25	Oct 2006	Oct 2011	Oct 2014	Indefinite
Berkeley DB Java Edition 3.2	Dec 2006	Dec 2011	Dec 2014	Indefinite
Berkeley DB Java Edition 3.3	Jun 2008	Jun 2013	Jun 2016	Indefinite
Berkeley DB Java Edition 4.0	Dec 2009	Dec 2014	Dec 2017	Indefinite
Berkeley DB Java Edition 11.2.4	Nov 2010	Nov 2015	Nov 2018	Indefinite
Berkeley DB Java Edition 11.2.5	Dec 2011	Dec 2016	Dec 2019	Indefinite
Berkeley DB Java Edition 12.1.6	May 2014	May 2019	May 2022	Indefinite

Older releases of Oracle Berkeley DB, Oracle Berkeley DB XML, and Oracle Berkeley DB Java Edition not listed will receive indefinite Sustaining Support.

Oracle Database Lite Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
10.0	Jul 2004	Dec 2008	Dec 2010	Indefinite
10.2	Sep 2005	Dec 2009	Dec 2011	Indefinite
10.3	Apr 2007	Dec 2012	Dec 2015	Indefinite

Oracle Database Lite releases will follow the support time frames for the most recent Oracle Fusion Middleware version for which the Oracle Database Lite release is certified.

For Oracle products which require or embed Oracle Database Lite (for example Oracle Mobile Field Service and Oracle E-Business Suite), Oracle Database Lite will be supported according to the support schedule of those products, even if the support dates extend beyond those for Oracle Database Lite support.

Oracle Database Mobile Server

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
11.1	Oct 2011	Oct 2016	Oct 2019	Indefinite
11.2	Oct 2012	Oct 2017	Oct 2020	Indefinite
11.3	Oct 2013	Oct 2018	Oct 2021	Indefinite
12.1	Apr 2015	Apr 2020	Apr 2023	Indefinite

Oracle Reliaty Backup Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
3.1.3.x	Not Available	Aug 2007	Not Available	Indefinite

Customers should plan to migrate to Oracle Secure Backup 10.1.

Oracle Secure Backup Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
10.1	Apr 2006	Dec 2008	Not Available	Indefinite
10.2	Nov 2007	May 2010	Not Available	Indefinite
10.3	Jun 2009	Dec 2012	Not Available	Indefinite
10.4	Oct 2011	Oct 2016	Not Available	Indefinite
12.1	Feb 2015	Feb 2020	Not Available	Indefinite
12.2	Jan 2018	Jan 2023	Not Available	Indefinite
18.1	Dec 2019	Jan 2024	Not Available	Indefinite

Oracle Warehouse Builder Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
9.2	Jul 2003	Oct 2007	Not Available	Oct 2010
10.1	Apr 2004	Jul 2007	Not Available	Jul 2010

As of 10gR2 (10.2) Oracle Warehouse Builder (OWB) ships as a part of the Database release. So from 10.2 onwards the lifecycle dates for OWB will be the same as for the Database release it ships with.

Oracle's JD Edwards EnterpriseOne Extended Process Integration (XPI) Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
8.92	Dec 2003	Jun 2008	Not Available	Not Available
8.94	Dec 2004	Dec 2008	Not Available	Not Available

Oracle's Auptyma Release

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Java Application Monitoring (All Releases)	Dec 2005	Jan 2008	Jan 2008	Not Available

Support for all legacy Auptyma products ended on January 31, 2008. Customers are advised to upgrade to the Oracle-branded product, Oracle Enterprise Manager 10gR4 (10.2.0.4).

Oracle Express Server Release

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Express Server 6.3.4	Jul 2002	Dec 2007	Not Available	Dec 2010

Oracle Gateway Release's

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Gateway Release 9.2				
Oracle Access Manager for AS/400 9.2	Jul 2002	Jul 2007	Not Available	Indefinite
Oracle Transparent Gateway for DB2/400 9.2	Jul 2002	Jul 2007	Not Available	Indefinite
Oracle Transparent Gateway for DRDA 9.2	Jul 2002	Jul 2007	Not Available	Indefinite
Oracle Procedural Gateway for APPC 9.2	Jul 2002	Jul 2007	Not Available	Indefinite
Oracle Procedural Gateway for IBM MQ Series 9.2	Jul 2002	Jul 2007	Not Available	Indefinite
Oracle Transparent Gateway for DB2 9.2	Jul 2002	Jul 2007	Not Available	Indefinite

Oracle Gateway Release's (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Gateway Release 10.1				
Oracle Access Manager for AS/400 10.1	Jan 2004	Jan 2009	Not Available	Indefinite
Oracle Transparent Gateway for DB2/400 10.1	Jan 2004	Jan 2009	Not Available	Indefinite
Oracle Transparent Gateway for DRDA 10.1	Jan 2004	Jan 2009	Not Available	Indefinite
Oracle Procedural Gateway for APPC 10.1	Jan 2004	Jan 2009	Not Available	Indefinite
Oracle Transparent Gateway for DB2 10.1	Jan 2004	Jan 2009	Not Available	Indefinite
Oracle Gateway Release 10.2				
Oracle Access Manager for AS/400 10.2	Jul 2005	Jul 2010	Not Available	Indefinite
Oracle Transparent Gateway for DB2/400 10.2	Jul 2005	Jul 2010	Not Available	Indefinite
Oracle Transparent Gateway for DRDA 10.2	Jul 2005	Jul 2010	Not Available	Indefinite
Oracle Procedural Gateway for APPC 10.2	Jul 2005	Jul 2010	Not Available	Indefinite
Oracle Procedural Gateway for WebSphere MQ 10.2	Jul 2005	Jul 2010	Not Available	Indefinite
Oracle Transparent Gateway for DB2 10.2	Jul 2005	Jul 2011	Not Available	Indefinite
Oracle Gateway Release 11.1				
Oracle Database Gateway for Websphere MQ 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for APPC 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for DRDA 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for VSAM 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for Adabas 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for SQL Server 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for Teradata 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for Informix 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for Sybase 11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite

Oracle Gateway Release's (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Gateway Release 11.2				
Oracle Database Gateway for Websphere MQ 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for APPC 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for DRDA 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for VSAM 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for IMS 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for Adabas 11.2	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Database Gateway for SQL Server 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for Teradata 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for Informix 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Database Gateway for Sybase 11.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Gateway Release 12.1				
Oracle Database Gateway for Websphere MQ 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Database Gateway for APPC 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Database Gateway for DRDA 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Database Gateway for SQL Server 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Database Gateway for Teradata 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Database Gateway for Sybase 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Database Gateway for Informix 12.1	Jun 2013	Jun 2018	Jun 2021	Indefinite

Oracle Access Manager for AS/400 10.2 is the terminal release.

Oracle Transparent Gateway for DB2/400 10.2 is the terminal release, customers should migrate to Oracle Database gateway for DRDA .

Oracle's TripleHop Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
MatchPoint 2.x	Jun 2002	Not Available	Not Available	Not Available
MatchPoint 3.x	Oct 2003	Not Available	Not Available	Sep 2008

Customers should plan to migrate to latest version of Oracle Secure Enterprise Search.

Oracle Secure Enterprise Search

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Secure Enterprise Search 10.1.8	Apr 2007	Jan 2012	Not Available	Indefinite
Secure Enterprise Search 11.1	Feb 2010	Feb 2015	Not Available	Indefinite
Secure Enterprise Search 11.2	Jul 2013	Jan 2018	Not Available	Indefinite

Oracle Application Express (Formerly HTML DB)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
1.6	Jul 2005	Dec 2008	Not Available	Indefinite
2.0	Sep 2005	Dec 2008	Not Available	Indefinite
2.2	Aug 2006	Aug 2009	Not Available	Indefinite
3.0	Mar 2007	Mar 2010	Not Available	Indefinite
3.1	Feb 2008	Feb 2011	Not Available	Indefinite
3.2	Feb 2009	Feb 2012	Not Available	Indefinite
4.0	Jun 2010	Jun 2015	Not Available	Indefinite
4.1	Aug 2011	Aug 2016	Not Available	Indefinite
4.2	Oct 2012	Oct 2017	Not Available	Indefinite

Oracle Application Express (Formerly HTML DB) (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
5.0	Apr 2015	Apr 2020	Not Available	Indefinite
5.1	Dec 2016	Dec 2021	Not Available	Indefinite
18.x	May 2018	May 2023	Not Available	Indefinite
19.x	Mar 2019	Sep 2024	Not Available	Indefinite
20.x	Apr 2020	Apr 2025	Not Available	Indefinite
21.x	May 2021	May 2024	Not Available	Indefinite

Oracle Zero Data Loss Appliance Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Zero Data Loss Appliance Software 12.2	Aug 2018	Dec 2021	Not Available	Indefinite
Zero Data Loss Appliance Software 19.2	Aug 2019	Aug 2022	Not Available	Indefinite

Oracle Fail Safe Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Fail Safe 3.3.2	Nov 2002	Jul 2007	Not Available	Indefinite
Oracle Fail Safe 3.3.3	Apr 2004	Mar 2009	Not Available	Indefinite
Oracle Fail Safe 3.3.4	Nov 2005	Jul 2010	Not Available	Indefinite
Oracle Fail Safe 3.4.1	Aug 2007	Aug 2012	Aug 2015	Indefinite
Oracle Fail Safe 3.4.2	Sep 2009	Jan 2015	Jan 2018	Indefinite
Oracle Fail Safe 4.1.x	Jun 2013	Jun 2018	Jun 2021	Indefinite
Oracle Fail Safe 4.2.x	Apr 2018	Apr 2024	Apr 2027	Indefinite

Oracle's ClearApp Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Acsera Manager 5.1	Not Available	Not Available	Not Available	Not Available
QuickVision 6.0	Not Available	Not Available	Not Available	Jun 2010
QuickVision 6.1	Not Available	Not Available	Not Available	Indefinite
QuickVision 7.0	Not Available	Dec 2009	Dec 2010	Indefinite
QuickVision 7.5	Sep 2008	Dec 2010	Dec 2011	Indefinite
Oracle-Branded Releases				
Oracle Composite Application Monitor and Modeler 10.2.0.4	Nov 2008	Oct 2010	Oct 2013	Indefinite

The migration path for QuickVision 7.5 is to use Oracle Composite Application Monitor and Modeler. Oracle Composite Application Monitor and Modeler is part of Oracle Grid Control release 10.2.x. To be eligible for Premier Support and Extended Support coverage, a mandatory patch for QuickVision 7.0 must be applied.

Oracle Virtual Iron Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.0.4 and earlier	Sep 2007	Not Availalble	Not Availalble	Not Availalble
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.0.5	Sep 2007	Not Availalble	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.1.4	Oct 2007	Not Availalble	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.2.9	Dec 2007	Not Availalble	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.2.11	Jan 2008	Not Availalble	Not Availalble	Indefinite

Oracle Virtual Iron Releases (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.2.13	Jan 2008	Not Availalble	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.2.14	Feb 2008	Not Availalble	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition and Virtual Iron Enterprise Edition 4.3.8	Apr 2008	Not Availalble	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition 4.4.13	Sep 2008	Sep 2009	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition 4.4.15	Oct 2008	Oct 2009	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition 4.5.13	Jan 2009	Jan 2010	Not Availalble	Indefinite
Virtual Iron Extended Enterprise Edition 4.5.16	Feb 2009	Feb 2010	Not Availalble	Indefinite

Oracle's Secerno Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Previous Secerno Releases	Various	Jan 2012	Not Available	Indefinite

Oracle Audit Vault and Database Firewall Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Database Firewall 5.x	Jan 2011	Jan 2016	Not Available	Indefinite
Oracle Audit Vault 10.2.3	Jun 2008	Jun 2013	Not Available	Indefinite
Oracle Audit Vault 10.3	Dec 2011	Dec 2016	Not Available	Indefinite
Oracle Audit Vault and Database Firewall 12.1	Dec 2012	Dec 2017	Not Available	Indefinite
Oracle Audit Vault and Database Firewall 12.2	Dec 2015	Mar 2021	Not Available	Indefinite
Oracle Audit Vault and Database Firewall 20.x	Jul 2020	Jul 2024	Not Available	Indefinite

Oracle Key Vault Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Key Vault 12.2	Feb 2016	Sep 2020	Not Available	Indefinite
Oracle Key Vault 18	Apr 2019	Apr 2022	Not Available	Indefinite
Oracle Key Vault 21	Jan 2021	Jul 2024	Not Available	Indefinite

Oracle's MySQL Releases

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
MySQL Database 5.0	Oct 2005	Dec 2011	Not Available	Indefinite
MySQL Database 5.1	Dec 2008	Dec 2013	Not Available	Indefinite
MySQL Database 5.5	Dec 2010	Dec 2015	Dec 2018	Indefinite
MySQL Database 5.6	Feb 2013	Feb 2018	Feb 2021	Indefinite
MySQL Database 5.7	Oct 2015	Oct 2020	Oct 2023	Indefinite

Oracle's MySQL Releases (continued)

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
MySQL Database 8.0	Apr 2018	Apr 2023	Apr 2026	Indefinite
MySQL Cluster 6	Aug 2007	Mar 2013	Not Available	Indefinite
MySQL Cluster 7.0	Apr 2009	Apr 2014	Not Available	Indefinite
MySQL Cluster 7.1	Apr 2010	Apr 2015	Not Available	Indefinite
MySQL Cluster 7.2	Feb 2012	Feb 2017	Feb 2020	Indefinite
MySQL Cluster 7.3	Jun 2013	Jun 2018	Jun 2021	Indefinite
MySQL Cluster 7.4	Feb 2015	Feb 2020	Feb 2023	Indefinite
MySQL Cluster 7.5	Oct 2016	Oct 2021	Oct 2024	Indefinite
MySQL Cluster 7.6	May 2018	May 2023	May 2026	Indefinite
MySQL Cluster 8.0	Jan 2020	Jan 2025	Jan 2028	Indefinite

Oracle's NoSQL Database Release

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
11.2.1	Oct 2011	Oct 2016	Oct 2019	Indefinite
11.2.2	Nov 2012	Nov 2017	Nov 2020	Indefinite
12.1.2	Jul 2013	Jul 2018	Jul 2021	Indefinite
12.1.3	Mar 2014	Mar 2019	Mar 2022	Indefinite
12.1.4	Jun 2016	Jun 2021	Jun 2024	Indefinite
12.2.4.x	Apr 2017	Apr 2023	Apr 2026	Indefinite
18.x	Apr 2018	Apr 2023	Apr 2026	Indefinite
19.x	Apr 2019	Apr 2024	Apr 2027	Indefinite
20.x	Apr 2020	Apr 2025	Apr 2028	Indefinite
21.x	Apr 2021	Apr 2026	Apr 2029	Indefinite

Oracle Big Data Appliance

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Big Data Appliance 3.x	Jun 2012	Jun 2017	Not Available	Jan 2025
Oracle Big Data Appliance 4.x	Apr 2014	Jan 2022	Not Available	Jan 2025
Oracle Big Data Appliance 5.x	Nov 2019	Jan 2025	Not Available	Not Available

For more detailed information on specific release and support dates, refer to MyOracle Support.

Oracle Big Data SQL

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Big Data SQL 1.x	Sep 2013	Sep 2018	Sep 2021	Indefinite
Oracle Big Data SQL 2.x	Oct 2015	Oct 2020	Oct 2023	Indefinite
Oracle Big Data SQL 3.x	Mar 2016	Mar 2021	Mar 2024	Indefinite
Oracle Big Data SQL 4.x	Jul 2019	Jul 2024	Jan 2025	Indefinite

Oracle Big Data Connectors

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Big Data Connectors 3.x	Apr 2014	Apr 2019	Not Available	Indefinite
Oracle Big Data Connectors 4.1 – 4.5	Sep 2014	Sep 2019	Not Available	Indefinite
Big Data Connectors 4.6	Aug 2016	Aug 2021	Not Available	Indefinite
Big Data Connectors 4.9	Jun 2017	Jun 2022	Not Available	Indefinite
Big Data Connectors 4.12	Nov 2018	Nov 2023	Not Available	Indefinite
Big Data Connectors 5.1	May 2020	May 2025	Not Available	Indefinite

Oracle Big Data Spatial and Graph

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
Oracle Big Data Spatial and Graph 1.x	May 2015	May 2020	Not Available	Indefinite
Oracle Big Data Spatial and Graph 2.x	Nov 2016	Nov 2021	Not Available	Indefinite
Oracle Big Data Spatial and Graph 3.x	Oct 2019	Oct 2024	Not Available	Indefinite

LIFETIME SUPPORT POLICY:

Our Commitment to Deliver a Superior Ownership Experience

Oracle Exadata Storage Server Software

Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends
11.1.x	Sep 2008	Sep 2013	Not Available	Indefinite
11.2.x	Sep 2009	Sep 2014	Sep 2017	Indefinite
12.1	Dec 2013	Dec 2018	Dec 2021	Indefinite
12.2	Jan 2017	Jan 2022	Jan 2023	Indefinite
18.1	Sep 2017	Sep 2022	Sep 2023	Indefinite
19.1	Oct 2018	Oct 2023	Not Available	Indefinite
19.2	Feb 2019	Oct 2023	Not Available	Indefinite
19.3	Sep 2019	Oct 2023	Not Available	Indefinite
20.1	Jun 2020	Oct 2023	Not Available	Indefinite
21.2	May 2021	May 2024	Not Available	Indefinite

Now, you can have even greater peace of mind knowing that your business strategy is driving your upgrade strategy with more control, more choice, and more certainty. It all amounts to an Oracle Superior Ownership Experience—available only with the industry's most advanced support offering, Oracle Lifetime Support.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Data Redaction

Funcionalidade Data Redaction - Oracle Database 12c

Por OraWorld,
Postado em Maio 2014

No *Oracle Database 12c*, foi introduzida uma nova funcionalidade, chamada de *Oracle Data Redaction*. Esta nova funcionalidade faz parte do pacote *Advanced Security* e permite a proteção dos dados mostrados ao usuário em tempo real, sem necessidade de modificações na aplicação.

O *Oracle Database 12c* aplica a proteção em tempo de execução, no momento em que os usuários do aplicativo tentam acessar os dados, isto se chama *at query-execution time*. Os dados armazenados permanecem inalterados, enquanto os dados a serem exibidos são transformados *on-the-fly* antes de deixarem o banco de dados.

Desde a versão 11G, existe o *Oracle Data Masking*, onde os dados são transformados usando formatos de máscaras e este dado mascarado atualizado é armazenado em novos blocos de dados. Isto é adequado para ambientes de não-produção (desenvolvimento, homologação, treinamento, etc)

Segue abaixo algumas outras *features* que já existiam para auxiliar a tornar os dados mais seguros:

Virtual Private Database (VPD) - permite controlar os acessos em nível de registro e coluna, adicionando uma cláusula WHERE dinâmica em uma instrução SQL.
Oracle Label Security – Permite adicionar valores definidos pelo usuário para os registros e usar o VPD para controlar o acesso com base nestes valores.
Database Vault – o *Data Redaction* não impede que usuários privilegiados como DBAs não tenham acesso ao conteúdo das colunas que estão sendo protegidas. Para resolver isso, pode-se utilizar o *Database Vault*.
Considerando as questões de licenciamento, o *Oracle Data Masking* só está disponível no banco *Enterprise Edition* e com a aquisição do pacote *Advanced Security*.

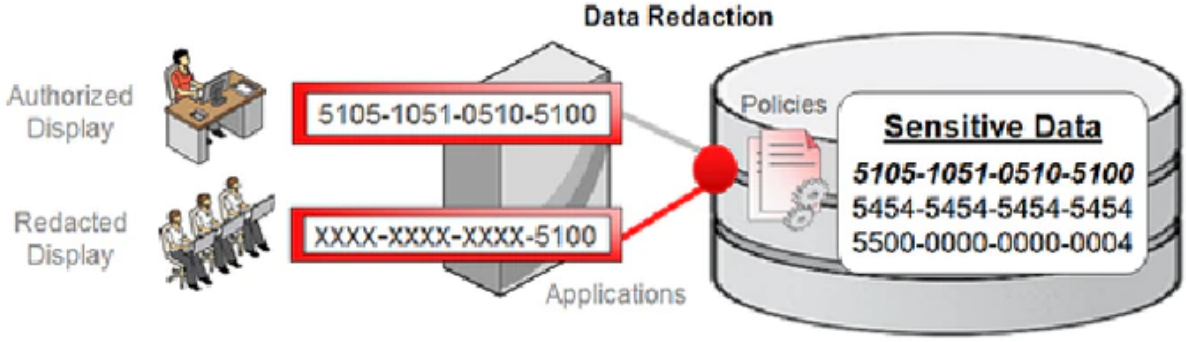
Como funciona:

Podemos criar ***redaction policies*** que basicamente gerenciam que condição deve ser atendida antes dos dados serem protegidos, quais colunas da tabela e o tipo de proteção.

A *package* utilizada para criar as regras de proteção se chama DBMS_REDACT, que inclui 5 procedures para gerir as regras e mais uma *procedure* para alterar o valor default da *full redaction policy*.

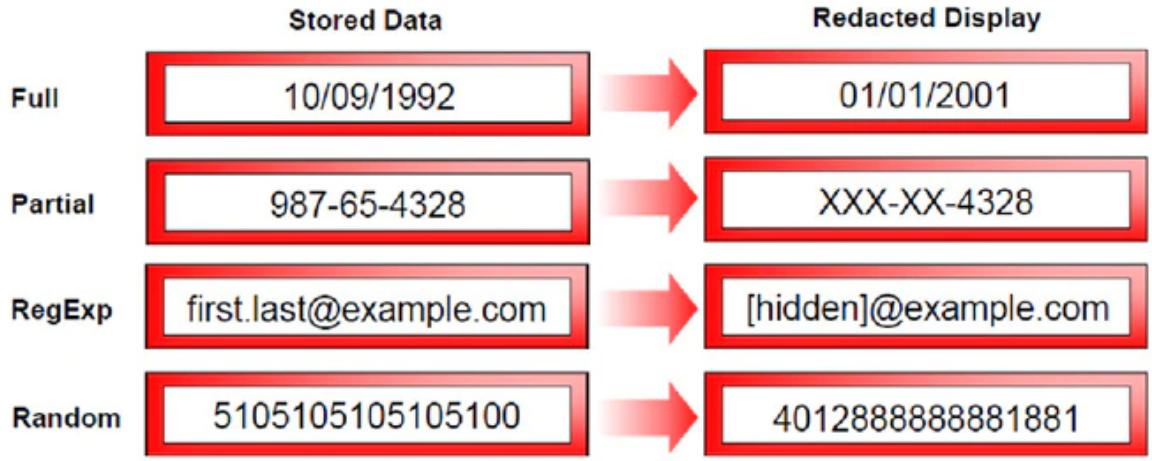
DBMS_REDACT.ALTER_POLICY – permite fazer mudanças nas políticas existentes.
DBMS_REDACT.DISABLE_POLICY – desativa uma política existente.
DBMS_REDACT.DROP_POLICY – elimina uma política existente.

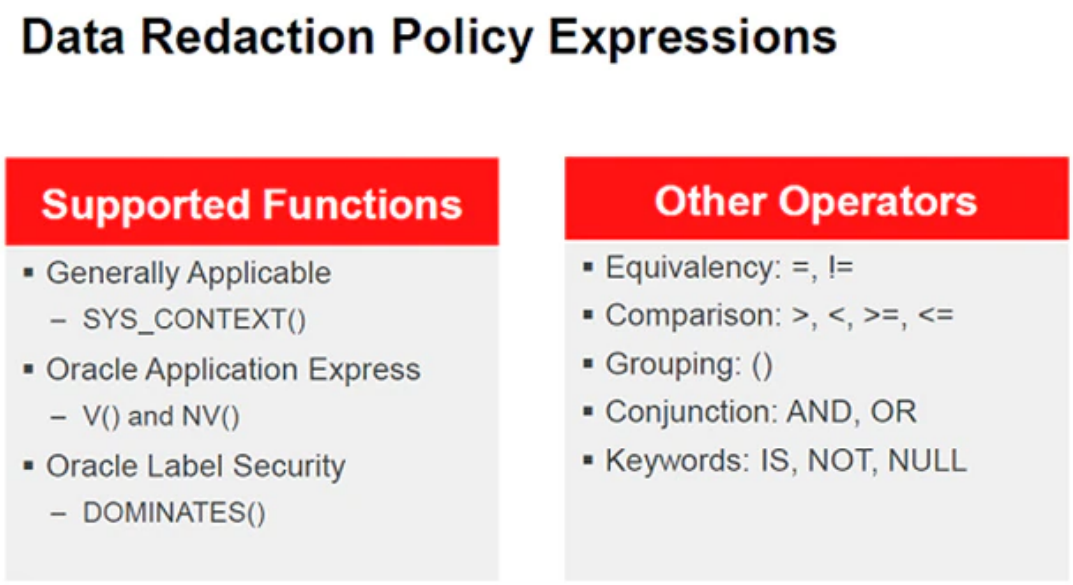
DBMS_REDACT.ENABLE_POLICY – ativa uma política existente.
DBMS_REDACT.UPDATE_FULL_REDACTION_VALUES – altera o valor *default* de retorno para *full redaction*. É necessário reiniciar o banco de dados para ter efeito.



Você pode proteger os dados da coluna, utilizando um dos seguintes métodos:

Full redaction – Todo conteúdo da coluna é protegido e o tipo de valor devolvido depende do tipo de dados da coluna. Para campos numéricos, será devolvido o valor zero, para campos do tipo *character*, será devolvido um espaço. Essa definição pode ser alterada a nível de banco de dados.
Partial redaction – Apenas uma parte da informação é alterada, como por exemplo, os primeiros dígitos do número de cartão de crédito são trocados por asterisco.
Regular expressions - Você pode usar expressões regulares para procurar padrões de dados para proteger.
Random redaction – os valores retornados são aleatórios; cada vez que é feita uma consulta os valores retornados são diferentes.
No redaction - permite testar o funcionamento interno de suas políticas de redação, sem nenhum efeito sobre os resultados das consultas em tabelas. Muito utilizado para testar as políticas antes de colocar em produção.





O Data Redaction pode ajudar a cumprir com as regulamentações de segurança, como Payment Card Industry Data Security Standard (PCI DSS) e da Lei Sarbanes-Oxley.

O Data Redaction pode ser utilizado com os seguintes tipos de colunas: NUMBER, BINARY_FLOAT, BINARY_DOUBLE, CHAR, VARCHAR2, NCHAR, NVARCHAR2, DATE, TIMESTAMP, TIMESTAMP WITH TIME ZONE, BLOB, CLOB e NCLOB.

Views do dicionário:

Podemos utilizar as seguintes views do dicionário de dados do Oracle para obter informações sobre o *Oracle Data Redaction*:

REDACTION_POLICIES
REDACTION_COLUMNS
REDACTION_VALUES_FOR_TYPE_FULL

Data Redaction e o utilitário Data Pump:

A *role* ***DATAPUMP_EXP_FULL_DATABASE*** inclui o privilégio de sistema ***EXEMPT REDACTION POLICY.*** Com isso, um DBA ao exportar as tabelas, estará exportando os dados reais e não os mascarados.

Se você tentar exportar uma tabela sem ter o privilégio EXEMPT REDACTION POLICY, receberá o seguinte erro:

```
ORA-28081: Insufficient privileges - the command references a redacted object
```

Copy

Para exportar apenas os *metadados* relacionados com as políticas do *Oracle Data Redaction*, você pode usar os seguintes parâmetros do EXPDP:

CONTENT=METADATA_ONLY INCLUDE=RADM_FPTM,RADM_POLICY

Data Redaction e Create tables as select (CTAS):

Um usuário não pode criar uma tabela fazendo SELECT a partir de uma tabela com uma *policy* ativa, se ele não tiver privilégio para ver os valores mascarados

PDB utilizada para os exemplos com o EM12c:

Acessando o *Oracle Data Redaction*:

Tela de gerenciamento das políticas:

Criando uma política para não mostrar o salário, caso o usuário do sistema não seja o Supervisor:

Verificando se a política funciona:

```
SQL*Plus: Release 12.1.0.1.0 Production on Wed Apr 2 10:22:46 2014
Copyright (c) 1982, 2013, Oracle.  All rights reserved.

Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics
and Real Application Testing options

SQL> select EMPLOYEE_ID, FIRST_NAME, SALARY from hr.employees WHERE ROWNUM < 5

EMPLOYEE_ID FIRST_NAME               SALARY
----------- -------------------- ----------
        100 Steven                        0
        101 Neena                         0
        102 Lex                           0
        103 Alexander                     0
```

Copy

Verificando a mesma tabela, agora com o usuário SUPERVISOR:

```
[oracle@dibutu ~]$ sqlplus supervisor/senha@localhost:1521/testpdb

SQL*Plus: Release 12.1.0.1.0 Production on Wed Apr 2 10:26:04 2014
Copyright (c) 1982, 2013, Oracle.  All rights reserved.

Connected to:
```

```
Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics
and Real Application Testing options

SQL> select EMPLOYEE_ID, FIRST_NAME, SALARY from hr.employees WHERE ROWNUM < 5

EMPLOYEE_ID FIRST_NAME               SALARY
----------- -------------------- ----------
        100 Steven                    24000
        101 Neena                     17000
        102 Lex                       17000
        103 Alexander                  9000
```

Copy

Criando a mesma política utilizando o SQL*Plus:

```
SQL>
BEGIN
DBMS_REDACT.ADD_POLICY
(OBJECT_SCHEMA =>'HR',  object_name => 'EMPLOYEES',  policy_name => 'POLITICA_
expression => 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') != ''SUPERVISOR''');
DBMS_REDACT.ALTER_POLICY
(OBJECT_SCHEMA => 'HR',  object_name => 'EMPLOYEES',  policy_name => 'POLITICA
action => DBMS_REDACT.ADD_COLUMN,  column_name => '"SALARY"',  function_type =
END;
/
PL/SQL procedure successfully completed.
```

Copy

Criando a mesma política utilizando o *SQLDeveloper*:

OraWorld é um grupo que está constantemente trabalhando com a comunidade Oracle por meio de artigos, conferências, webinars e cursos de Banco de Dados Oracle. O OraWorld possui membros "Oracle Certified Masters" e "Oracle ACEs".

Você pode seguir este grupo através dos seguintes links:

https://www.facebook.com/oraworldteam

https://twitter.com/oraworld_team

http://www.oraworld-team.com

Presidência da República
Secretaria-Geral
Subchefia para Assuntos Jurídicos

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

Texto compilado

Mensagem de veto

Vigência

~~Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).~~

Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019) Vigência

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

~~II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;~~

~~II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

~~b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;~~
~~b) acadêmicos;~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

~~§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.~~
~~§ 2º O tratamento dos dados a que se refere o inciso III do **caput** por pessoa jurídica de direito privado só será admitido em procedimentos sob a tutela de pessoa jurídica de direito público, hipótese na qual será observada a limitação de que trata o § 3º.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

~~§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.~~
~~§ 3º Os dados pessoais constantes de bancos de dados constituídos para os fins de que trata o inciso III do **caput** não poderão ser tratados em sua totalidade por pessoas jurídicas de direito privado, não incluídas as controladas pelo Poder Público.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

~~§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado.~~ ~~(Revogado pela Medida Provisória nº 869, de 2018)~~

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

~~VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;~~

~~VIII - encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

~~XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;~~

~~XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

~~XIX - autoridade nacional: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.~~

~~XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

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;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

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.

CAPÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS

Seção I
Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

~~VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;~~

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

~~§ 1º Nos casos de aplicação do disposto nos incisos II e III do caput deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, o titular será informado das hipóteses em que será admitido o tratamento de seus dados.~~ (Revogado pela Medida Provisória nº 869, de 2018)

§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)

~~§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do caput do art. 23 desta Lei poderá ser especificada pela autoridade nacional. (Revogado pela Medida Provisória nº 869, de 2018)~~

§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Seção II
Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

~~f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou~~

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

~~§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.~~

~~§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses de: (Redação dada pela Medida Provisória nº 869, de 2018)~~

~~I - portabilidade de dados quando consentido pelo titular; ou (Incluído pela Medida Provisória nº 869, de 2018)~~

~~II - necessidade de comunicação para a adequada prestação de serviços de saúde suplementar. (Incluído pela Medida Provisória nº 869, de 2018)~~

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) Vigência

I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019) Vigência

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Seção III
Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Seção IV
Do Término do Tratamento de Dados

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CAPÍTULO III
DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

~~V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;~~

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

~~Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.~~

~~Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

§ 3º (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO IV
DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I
Das Regras

Art. 23. 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;

II - (VETADO); e

~~III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.~~

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

IV - (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal , terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ;

II - (VETADO);

~~III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.~~
~~III - se for indicado um encarregado para as operações de tratamento de dados pessoais, nos termos do art. 39;~~ ~~Redação dada pela Medida Provisória nº 869, de 2018)~~

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

~~IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;~~ ~~(Incluído pela Medida Provisória nº 869, de 2018)~~
~~V - na hipótese de a transferência dos dados objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados; ou~~ ~~(Incluído pela Medida Provisória nº 869, de 2018)~~

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019) Vigência

~~VI - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.~~ ~~(Incluído pela Medida Provisória nº 869, de 2018)~~

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

~~Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:~~
~~Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa jurídica de direito privado dependerá de consentimento do titular, exceto:~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 28. (VETADO).

~~Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, às entidades do Poder Público, a realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.~~
~~Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do Poder Público a realização de operações de tratamento de dados pessoais, as informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Seção II
Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

CAPÍTULO V
DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as 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) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

CAPÍTULO VI
DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I
Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II
Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

§ 4º (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

Seção III
Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

CAPÍTULO VII
DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I
Da Segurança e do Sigilo de Dados

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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II
Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

CAPÍTULO VIII
DA FISCALIZAÇÃO

Seção I
Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

~~X - (VETADO); (Incluído pela Lei nº 13.853, de 2019)~~ (Promulgação partes vetadas)
~~XI - (VETADO); (Incluído pela Lei nº 13.853, de 2019)~~ (Promulgação partes vetadas)
~~XII - (VETADO). (Incluído pela Lei nº 13.853, de 2019)~~ (Promulgação partes vetadas)

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

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;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

~~§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.~~

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. (Redação dada pela Lei nº 13.853, de 2019) Vigência

~~§ 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal) , na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa) , e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .~~

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011. (Redação dada pela Lei nº 13.853, de 2019)

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. (Incluído pela Lei nº 13.853, de 2019)

~~§ 6º (VETADO). (Incluído pela Lei nº 13.853, de 2019)~~ (Promulgação partes vetadas)

§ 6º As sanções previstas nos incisos X, XI e XII do **caput** deste artigo serão aplicadas: (Incluído pela Lei nº 13.853, de 2019)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do **caput** deste artigo para o mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. (Incluído pela Lei nº 13.853, de 2019)

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. (Vigência)

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento. (Vigência)

CAPÍTULO IX
DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I
Da Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55. (VETADO).

~~Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados - ANPD, órgão da administração pública federal, integrante da Presidência da República.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-B. É assegurada autonomia técnica à ANPD.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-C. ANPD é composta por:~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~I - Conselho Diretor, órgão máximo de direção;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~III - Corregedoria;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~IV - Ouvidoria;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~V - órgão de assessoramento jurídico próprio; e~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei."~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-D. O Conselho Diretor da ANPD será composto por cinco diretores, incluído o Diretor-Presidente.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 1º Os membros do Conselho Diretor da ANPD serão nomeados pelo Presidente da República e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superior - DAS de nível 5.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros, de reputação ilibada, com nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 3º O mandato dos membros do Conselho Diretor será de quatro anos.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de dois, de três, de quatro, de cinco e de seis anos, conforme estabelecido no ato de nomeação.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 1º Nos termos do **caput** , cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~§ 2º Compete ao Presidente da República determinar o afastamento preventivo, caso necessário, e proferir o julgamento.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013 .~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Parágrafo único. A infração ao disposto no **caput** caracteriza ato de improbidade administrativa.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art.55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Parágrafo único. Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente.~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~Art. 55-J. Compete à ANPD:~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~I - zelar pela proteção dos dados pessoais;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~II - editar normas e procedimentos sobre a proteção de dados pessoais;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~III - deliberar, na esfera administrativa, sobre a interpretação desta Lei, suas competências e os casos omissos;~~ (Incluído pela Medida Provisória nº 869, de 2018)

~~IV - requisitar informações, a qualquer momento, aos controladores e operadores de dados pessoais que realizem operações de tratamento de dados pessoais; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~V - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VI - fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VII - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VIII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei praticado por órgãos e entidades da administração pública federal; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~IX - difundir na sociedade o conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre as medidas de segurança; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~X - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos controladores; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XI - elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XII - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XIII - realizar consultas públicas para colher sugestões sobre temas de relevante interesse público na área de atuação da ANPD; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XIV - realizar, previamente à edição de resoluções, a oitiva de entidades ou órgãos da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XV - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XVI - elaborar relatórios de gestão anuais acerca de suas atividades. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 1º A ANPD, na edição de suas normas, deverá observar a exigência de mínima intervenção, assegurados os fundamentos e os princípios previstos nesta Lei e o disposto no art. 170 da Constituição. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 2º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 3º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 4º No exercício das competências de que trata o **caput** , a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei, sob pena de responsabilidade. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 5º As reclamações colhidas conforme o disposto no inciso V do **caput** poderão ser analisadas de forma agregada e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, cujas demais competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Parágrafo único. A ANPD articulará sua atuação com o Sistema Nacional de Defesa do Consumidor do Ministério da Justiça e com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais, e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Lei nº 13.853, de 2019)

§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. (Incluído pela Lei nº 13.853, de 2019)

§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-B. É assegurada autonomia técnica e decisória à ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-C. A ANPD é composta de: (Incluído pela Lei nº 13.853, de 2019)

I - Conselho Diretor, órgão máximo de direção; (Incluído pela Lei nº 13.853, de 2019)

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - Corregedoria; (Incluído pela Lei nº 13.853, de 2019)

IV - Ouvidoria; (Incluído pela Lei nº 13.853, de 2019)

V - órgão de assessoramento jurídico próprio; e (Incluído pela Lei nº 13.853, de 2019)

VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Lei nº 13.853, de 2019)

§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. (Incluído pela Lei nº 13.853, de 2019)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. (Incluído pela Lei nº 13.853, de 2019)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, somente quando assim recomendado pela comissão especial de que trata o § 1º deste artigo, e proferir o julgamento. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A infração ao disposto no caput deste artigo caracteriza ato de improbidade administrativa. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. (Incluído pela Lei nº 13.853, de 2019)

§ 2º O Conselho Diretor disporá sobre o regimento interno da ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019)

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019)

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019)

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (Incluído pela Lei nº 13.853, de 2019)

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (Incluído pela Lei nº 13.853, de 2019)

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Lei nº 13.853, de 2019)

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (Incluído pela Lei nº 13.853, de 2019)

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Lei nº 13.853, de 2019)

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (Incluído pela Lei nº 13.853, de 2019)

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; (Incluído pela Lei nº 13.853, de 2019)

XII - elaborar relatórios de gestão anuais acerca de suas atividades; (Incluído pela Lei nº 13.853, de 2019)

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (Incluído pela Lei nº 13.853, de 2019)

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; (Incluído pela Lei nº 13.853, de 2019)

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019)

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; (Incluído pela Lei nº 13.853, de 2019)

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); (Incluído pela Lei nº 13.853, de 2019)

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei nº 13.853, de 2019)

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Lei nº 13.853, de 2019)

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; (Incluído pela Lei nº 13.853, de 2019)

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Lei nº 13.853, de 2019)

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. (Incluído pela Lei nº 13.853, de 2019)

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. (Incluído pela Lei nº 13.853, de 2019)

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-L. Constituem receitas da ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; (Incluído pela Lei nº 13.853, de 2019)

II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados; (Incluído pela Lei nº 13.853, de 2019)

III - os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade; (Incluído pela Lei nº 13.853, de 2019)

IV - os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo; (Incluído pela Lei nº 13.853, de 2019)

V - (VETADO); (Incluído pela Lei nº 13.853, de 2019)

VI - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; (Incluído pela Lei nº 13.853, de 2019)

VII - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. (Incluído pela Lei nº 13.853, de 2019)

Art. 56. (VETADO).

Art. 5 7. (VETADO).

Seção II
Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Art. 58. (VETADO).

~~Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por vinte e três representantes, titulares suplentes, dos seguintes órgãos: (Incluído pela Medida Provisória nº 869, de 2018)~~
~~I - seis do Poder Executivo federal; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~II - um do Senado Federal; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~III - um da Câmara dos Deputados; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~IV - um do Conselho Nacional de Justiça; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~V - um do Conselho Nacional do Ministério Público; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~VI - um do Comitê Gestor da Internet no Brasil; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~VII - quatro de entidades da sociedade civil com atuação comprovada em proteção de dados pessoais; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~VIII - quatro de instituições científicas, tecnológicas e de inovação; e (Incluído pela Medida Provisória nº 869, de 2018)~~
~~IX - quatro de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais. (Incluído pela Medida Provisória nº 869, de 2018)~~
~~§ 1º Os representantes serão designados pelo Presidente da República. (Incluído pela Medida Provisória nº 869, de 2018)~~
~~§ 2º Os representantes de que tratam os incisos I a VI do **caput** e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Medida Provisória nº 869, de 2018)~~
~~§ 3º Os representantes de que tratam os incisos VII, VIII e IX do **caput** e seus suplentes: (Incluído pela Medida Provisória nº 869, de 2018)~~
~~I - serão indicados na forma de regulamento; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~II - terão mandato de dois anos, permitida uma recondução; e (Incluído pela Medida Provisória nº 869, de 2018)~~
~~III - não poderão ser membros do Comitê Gestor da Internet no Brasil. (Incluído pela Medida Provisória nº 869, de 2018)~~
~~§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Medida Provisória nº 869, de 2018)~~
~~Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Medida Provisória nº 869, de 2018)~~
~~I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Medida Provisória nº 869, de 2018)~~
~~IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Medida Provisória nº 869, de 2018)~~
~~V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: (Incluído pela Lei nº 13.853, de 2019)

I - 5 (cinco) do Poder Executivo federal; (Incluído pela Lei nº 13.853, de 2019)

II - 1 (um) do Senado Federal; (Incluído pela Lei nº 13.853, de 2019)

III - 1 (um) da Câmara dos Deputados; (Incluído pela Lei nº 13.853, de 2019)

IV - 1 (um) do Conselho Nacional de Justiça; (Incluído pela Lei nº 13.853, de 2019)

V - 1 (um) do Conselho Nacional do Ministério Público; (Incluído pela Lei nº 13.853, de 2019)

VI - 1 (um) do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)

VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; (Incluído pela Lei nº 13.853, de 2019)

VIII - 3 (três) de instituições científicas, tecnológicas e de inovação; (Incluído pela Lei nº 13.853, de 2019)

IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; (Incluído pela Lei nº 13.853, de 2019)

X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e (Incluído pela Lei nº 13.853, de 2019)

XI - 2 (dois) de entidades representativas do setor laboral. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os representantes de que tratam os incisos I, II, III, IV, V e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Lei nº 13.853, de 2019)

§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes: (Incluído pela Lei nº 13.853, de 2019)

I - serão indicados na forma de regulamento; (Incluído pela Lei nº 13.853, de 2019)

II - não poderão ser membros do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)

III - terão mandato de 2 (dois) anos, permitida 1 (uma) recondução. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Lei nº 13.853, de 2019)

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Lei nº 13.853, de 2019)

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Lei nº 13.853, de 2019)

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Lei nº 13.853, de 2019)

IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Lei nº 13.853, de 2019)

V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população. (Incluído pela Lei nº 13.853, de 2019)

Art. 59. (VETADO).

CAPÍTULO X
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações: Vigência

"Art. 7º .....

.....

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

....." (NR)

"Art. 16. .....

.....

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

~~Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 . (Revogado pela Medida Provisória nº 869, de 2018)~~

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 .

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

~~Art. 65. Esta Lei entra em vigor após decorridos 18 (dezoito) meses de sua publicação oficial .~~
~~Art. 65. Esta Lei entra em vigor: (Redação dada pela Medida Provisória nº 869, de 2018)~~
~~I - quanto aos art. 55-A, art. 55-B, art. 55-C, art. 55-D, art. 55-E, art. 55-F, art. 55-G, art. 55-H, art. 55-I, art. 55-J, art. 55-K, art. 58-A e art. 58-B, no dia 28 de dezembro de 2018; e (Incluído pela Medida Provisória nº 869, de 2018)~~
~~II - vinte e quatro meses após a data de sua publicação quanto aos demais artigos. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)

I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)

~~II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)~~
~~II - em 3 de maio de 2021, quanto aos demais artigos. (Redação dada pela Medida Provisória nº 959, de 2020)~~ (Convertida na Lei nº 14.058, de 2020)

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

Brasília , 14 de agosto de 2018; 197º da Independência e 130º da República.

MICHEL TEMER
Torquato Jardim
Aloysio Nunes Ferreira Filho
Eduardo Refinetti Guardia
Esteves Pedro Colnago Junior
Gilberto Magalhães Occhi
Gilberto Kassab
Wagner de Campos Rosário
Gustavo do Vale Rocha
Ilan Goldfajn
Raul Jungmann
Eliseu Padilha

Este texto não substitui o publicado no DOU de 15.8.2018, e republicado parcialmente em 15.8.2018 - Edição extra

*

19c ORACLE Database

Encryption and Redaction with Oracle Advanced Security

Preventive controls to encrypt data at rest and redact sensitive information

WHITE PAPER / AUGUST 29, 2019

ORACLE

PURPOSE STATEMENT

This document provides an overview of features and enhancements included in latest releases of Oracle Advanced Security Option. It is intended solely to help you assess the business benefits of using Oracle Advanced Security preventive controls and to plan your Data Security / I.T. projects.

DISCLAIMER

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

TABLE OF CONTENTS

Purpose Statement 2

Introduction 5

Preventing Database Bypass with Encryption 6

- Oracle Advanced Security Transparent Data Encryption 6
- Protecting Entire Applications Using TDE Tablespace Encryption 7
- Protecting Sensitive Data Using TDE Column Encryption 8
- Performance Characteristics 8
- Built-In Key Management 8
- Encryption Impact for Common Operational Activities 9

Limiting Sensitive Data Exposure with Data Redaction 10

- Oracle Advanced Security Data Redaction 11
- Policies and Transformations 11
- Performance Characteristics 12
- Security Considerations 12
- Easy to Deploy Data Redaction 13
- Comparison to Alternative Approaches 13

Applying Encryption and Redaction in Oracle Multitenant Architecture 14

Data Encryption in the Oracle Cloud 14

Conclusion 14

INTRODUCTION

Rising security threats, expanding compliance requirements, consolidation, and cloud computing are just a few of the reasons why data security has become critical. Nearly 20 years after the first U.S. breach notification law, the need for strong preventive controls continues to increase as access to data expands. Initiatives such as the European Union's General Data Protection Regulation (GDPR) help ensure data security remains a top priority for organizations. Stolen client devices, including tablets and smartphones, have the potential to easily expose sensitive information as users move beyond the laptop. Outsourcing, offshoring, corporate mergers, and nearly continuous organizational change create additional risks by making it easier for malicious insiders to obtain sensitive data and for outside hackers to gain access to servers using social engineering attacks. These growing trends are just one reason why centralized and efficient protection of sensitive data, regardless of the applications being used, is more important than ever. Implementing security measures that consistently protect sensitive data at the source becomes a critical control as stored data continues to proliferate and access to data expands beyond traditional boundaries. Protecting data requires a defense in depth, multi-layered approach that encompasses controls to evaluate security postures, prevent data loss, detect suspicious activities and apply data access controls at the source through data-driven security. Oracle Database 19c strengthens Oracle's industry-leading database security solution by providing important new security measures in each of these areas.

Oracle Advanced Security option with Oracle Database delivers two essential preventive controls covering encryption of data-at-rest and redaction of sensitive data. These controls help protect sensitive data from being exposed directly from storage or through applications. Oracle Advanced Security Transparent Data Encryption (TDE) helps prevent attacks that attempt to bypass the database and read sensitive information from data files at the operating system level, from database backups, or from database exports. Oracle Advanced Security Data Redaction

"On our path towards EU GDPR compliance, we chose Oracle Database Security solutions including Oracle Advanced Security, Oracle Key Vault, Oracle Database Vault, Oracle Audit Vault and Oracle Database Firewall to streamline and simplify our Oracle deployment. With Oracle, we minimize risk and further enhance our overall security.

Henrique Zacarias
CIO
NOS

complements TDE by redacting sensitive data in query results before the data leaves the database, thus reducing the risk of unauthorized data exposure in applications. This white paper describes TDE and Data Redaction and explains how these valuable preventive controls can work together to help secure your sensitive data.

PREVENTING DATABASE BYPASS WITH ENCRYPTION

Data-at-rest encryption is an important control for blocking unauthorized access to sensitive data using methods that circumvent the database. Privileged operating system accounts are just one of the vehicles used by attackers and malicious insiders to gain access to sensitive information directly in physical storage.

Oracle Advanced Security Transparent Data Encryption (TDE) stops attackers from bypassing the database and reading sensitive information from storage by encrypting data in the database layer. Applications and users authenticated to the database continue to have access to application data transparently, while unauthenticated users attempting to circumvent the database are denied access to clear text data. To understand this better, consider the fact that privileged operating system users can access database tablespace files and extract sensitive data using simple shell commands. In addition, consider the possibility of attacks that read sensitive data from lost, stolen, or improperly decommissioned disks or backups. Figure 1 shows an example of extracting customer credit card numbers directly from storage using the common Linux "strings" command and a search pattern.

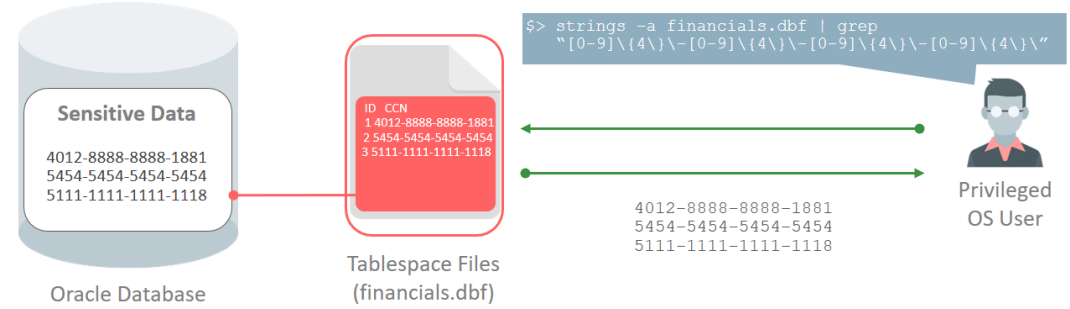


Figure 1. Extracting customer credit card numbers from Oracle database tablespace files

Oracle Advanced Security Transparent Data Encryption

Transparent Data Encryption resides at an optimal layer within the database to prevent database bypass while maintaining application transparency. TDE deploys quickly and encrypts application tablespaces, or entire databases including SYSTEM, SYSAUX, TEMP and UNDO tablespaces. It is transparent to applications because the encryption and decryption processes do not require any application changes, and the application users do not have to directly deal with encrypted data. Most importantly, TDE's built-in two-tier key architecture enables key rotation without downtime, and provides full key lifecycle management, tracking the keys across their lifetime with helpful meta-data attributes. Figure 2 shows how encrypting an Oracle database using TDE prevents database bypass.

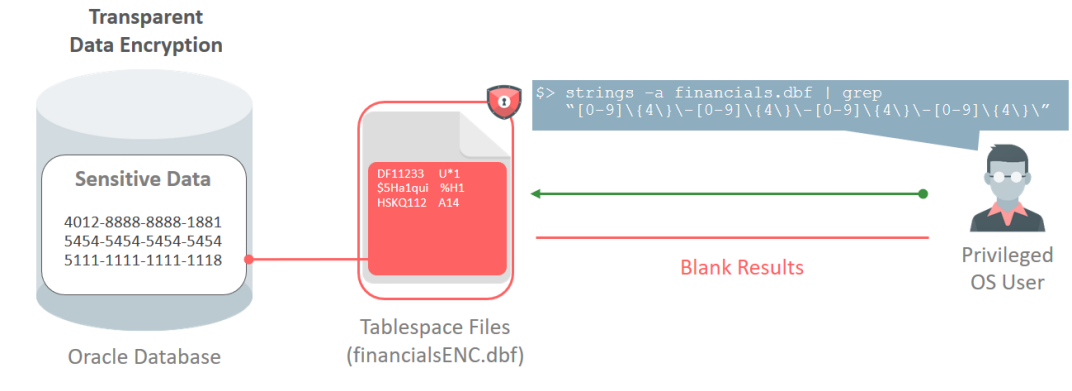


Figure 2. Encrypting with Transparent Data Encryption to prevent database bypass

TDE is unique when compared to alternative approaches that encrypt entire storage volumes or require new toolkits and programming APIs. These approaches do not protect against many bypass attacks, may require significant application changes, have complex (or no) key management, and are not integrated with complementary technologies such as Oracle Advanced Compression, Oracle Real Application Cluster (RAC), Oracle Recovery Manager (RMAN), Oracle Multitenant, Oracle GoldenGate, and Oracle Data Guard.

The high level of protection provided by TDE follows common standards for strong encryption as described in the figure below. With Oracle Database 19c, TDE supports operation with a FIPS 140-2 Level 1 cryptographic module, using only approved encryption suites.

Standard encryption and hashing algorithms used by TDE

ENCRYPTION ALGORITHMS	KEY LENGTH
Advanced Encryption Standard (AES)	128, 192, 256 bits
Triple Data Encryption Standard (TDES)	168 bits
ARIA (Korea)	128, 192, 256 bits
SEED (Korea)	128 bits
GOST (Russia)	256 bits

Protecting Entire Applications Using TDE Tablespace Encryption

Oracle Advanced Security TDE tablespace encryption protects entire application tables by encrypting the underlying tablespaces and indexes. It encrypts application tablespaces regardless of the data's sensitivity and irrespective of its data type. Tablespace encryption simplifies the encryption process because there is no need to identify specific database columns. It is useful when the database contains a large amount of sensitive data to be encrypted and the columns reside in many different locations. Due all these reasons, TDE tablespace encryption has become our customers' encryption method of choice.

Protecting Sensitive Data Using TDE Column Encryption

Oracle Advanced Security also provides TDE column encryption. TDE column encryption can be used to encrypt specific data in application tables such as credit card numbers and U.S. Social Security numbers. Customers identify columns within their application schema containing sensitive or regulated data, and then encrypt only those columns. This approach is useful when the database tables are large, only a small number of columns must be encrypted, and the columns are known. TDE column encryption is typically useful for warehouse applications where each query is likely to return a very different set of data. Data encrypted using TDE column encryption remains encrypted on backup media and discarded disk drives, helping prevent unauthorized access and potential data breaches that bypass the database.

Performance Characteristics

TDE's cryptographic operations are extremely fast and well integrated with related Oracle Database features. TDE leverages CPU-based hardware cryptographic acceleration available in Intel® AES-NI and Oracle SPARC T4 and newer platforms to increase performance significantly. The block-level operations of TDE tablespace encryption receive an additional performance boost from database buffering and caching. Tablespace encryption integrates seamlessly with Oracle Advanced Compression, ensuring that compression occurs before encryption. Tablespace encryption also integrates with the advanced technologies in Oracle Exadata such as Exadata Hybrid Columnar Compression (EHCC) and Smart Scans, which offload certain cryptographic processing to storage cells for fast parallel execution.

Built-In Key Management

Key management is critical to the security of the encryption solution. Oracle Advanced Security TDE provides an out-of-the-box, two-tier key management architecture consisting of data encryption keys and a master encryption key. The data encryption keys are managed automatically by the database and are in-turn encrypted by the master encryption key. The master encryption key is stored and managed outside of the database within an Oracle Wallet, a standards-based PKCS12 file that protects keys, or in Oracle Key Vault, a centralized key management platform that complies with the industry standard OASIS Key Management Interoperability Protocol (KMIP). Keeping the master key separate from the encrypted data mitigates attacks because both the keys and the encrypted data must be separately compromised to gain access to clear data. The two-tier key architecture also enables rotation of master keys without having to re-encrypt all of the sensitive data.

Either to help you to address regulatory requirements or to comply with your own company policy, Oracle Database 18c introduced support for Bring Your Own Key (BYOK). This feature allows you to bring a user-generated key and use it as the master encryption key for Advanced Security Option Transparent Data Encryption. Those external keys can be ingested by TDE directly, or they can be batch-uploaded into OKV for later use by TDE-enabled databases.

Oracle Database has a dedicated SYSKM privilege that may run all key management operations including initializing TDE, rotating master keys and changing the keystore password. This role can be optionally delegated to a designated user account to enable separation of duty for these functions. Oracle Enterprise Manager provides a convenient graphical user interface for creating, rotating, and managing TDE master keys as shown in the figure below.

Oracle Key Vault is the only enterprise-grade key management platform that provides continuous key availability by clustering up to 16 active OKV instances across geographically distributed datacenters; it is a full-stack, security-hardened software appliance which provides centralized management of encryption keys, Oracle Wallets, Java Keystores, ACFS volume encryption keys, Solaris crypto keys, and credential files. Oracle Key Vault works with Oracle Database and MySQL TDE to automate the management of TDE master keys including creation, rotation, and expiration. Oracle Key Vault

centrally manages TDE master keys over a direct network connection, eliminating the need for local wallet files, reducing operational and security challenges of wallet file management such as periodic password rotation, wallet file backups, and wallet file recovery. Using Oracle Key Vault with TDE enables sites to scale their TDE deployments to hundreds or thousands of databases in different locations while improving operational efficiencies, reducing TCO, and enabling consistent key management policies. A RESTful API allows for secure, automated on-boarding of any number of current or future TDE-enabled databases without any further intervention by the OKV administrators.

Oracle Key Vault also integrates with popular Hardware Security Modules (HSM) from nCipher and Safenet (now Thales) to establish a Root of Trust (RoT) relationship where the secret that unlocks OKV is stored on a tamper-resistant, specialized, FIPS 140-2 level 3 certified hardware module.

Oracle Key Vault supports hybrid cloud deployments, so organizations migrating to the Oracle Cloud can use it to support TDE deployments in both their cloud and on premises databases.

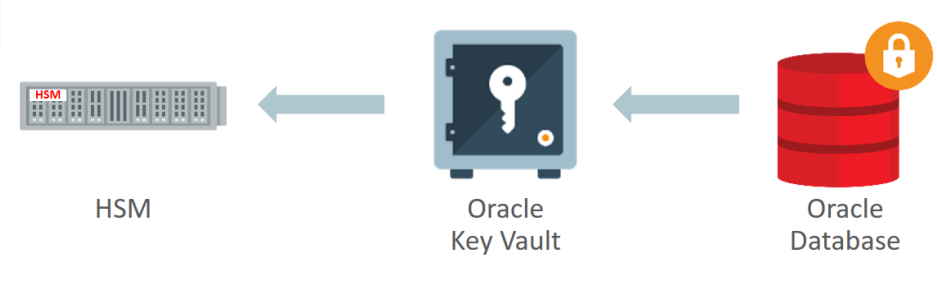


Figure 3. Oracle Key Vault and HSM as Root of Trust for TDE

Encryption Impact for Common Operational Activities

Essential day-to-day database operational activities can potentially leak sensitive data when not performed properly, making bypass easy. Examples of these activities include database backup and restore, data movement, high-availability clustering, and replication.

Example integrations with Oracle Advanced Security TDE

DATABASE TECHNOLOGIES	EXAMPLE POINTS OF INTEGRATION	TDE SUPPORT
High-Availability Clusters	Oracle Real Application Clusters (RAC), Oracle Data Guard	✓
Backup and Restore	Oracle Recovery Manager (RMAN), Oracle Secure Backup	✓
Export and Import	Oracle Data Pump Export and Import	✓
Database Replication	Oracle GoldenGate	✓
Pluggable Databases	Oracle Multitenant	✓
Engineered Systems	Oracle Exadata Smart Scan	✓
Storage Management	Oracle Automatic Storage Management (ASM) and ASM Cluster File System (ACFS)	✓
Data Compression	Oracle Standard, Advanced , and Hybrid Columnar Compression	✓

Oracle Advanced Security TDE supports these critical database operational activities and helps ensure that the data remains encrypted. Tablespace encryption integrates with Oracle Recovery Manager (backup and restore), Oracle Data Pump (data movement), Oracle Data Guard (redundancy and failover), and Oracle GoldenGate (replication). TDE also integrates with internal features of the database such as redo to prevent possible data leakage in logs. This fully integrated approach to database encryption makes the solution easy to deploy in complex real-world environments while protecting against bypass attacks that attempt to take advantage of gaps in operational processes.

Oracle Database 19c TDE provides two options for performing tablespace conversions from clear-text to encrypted tablespaces. For deployments which require conversion to be performed with no downtime, online tablespace encryption runs in the background to convert tablespaces from clear text to encrypted text while systems remain operational. TDE also offers an offline tablespace conversion mode which efficiently converts tablespaces with no storage overhead.

LIMITING SENSITIVE DATA EXPOSURE WITH DATA REDACTION

Privacy and compliance require a cost-effective approach to managing data exposure in applications. The embrace of smartphone and tablet devices make the issue of sensitive data exposure even more urgent as data access beyond the traditional office environment becomes commonplace. Even traditional applications require a more comprehensive solution for reducing exposure to sensitive data, for example, a call center application with a screen that exposes customer credit card information and personally identifiable information to call center operators. Exposing that information, even to valid application users, may violate privacy regulations and put the data at unnecessary risk.

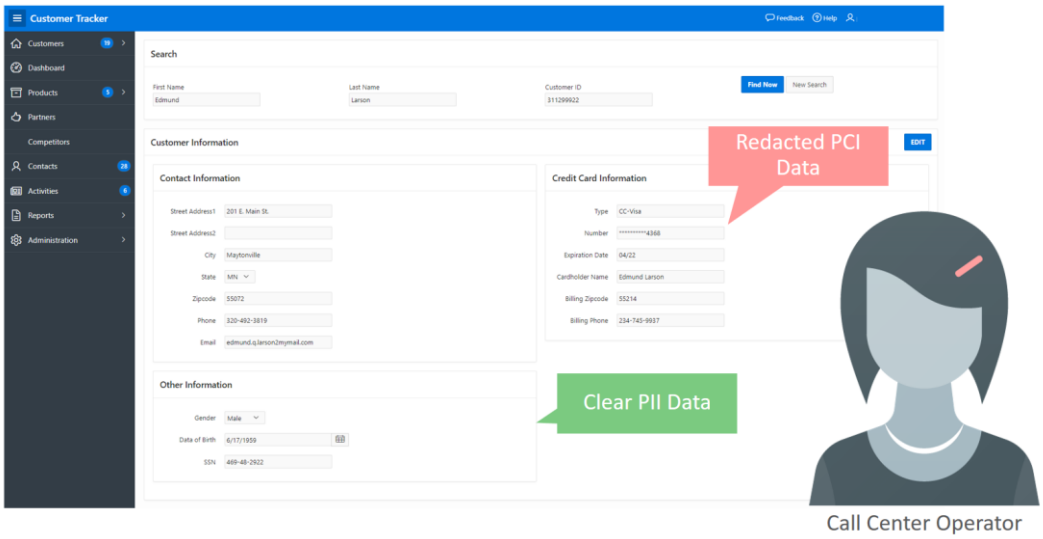


Figure 4. Clear and redacted information displayed in a call center application

Oracle Advanced Security Data Redaction

Oracle Advanced Security Data Redaction provides selective, on-the-fly redaction of sensitive data in database query results prior to display by applications so that unauthorized users cannot view the sensitive data. The stored data remains unaltered, while displayed data is transformed and redacted on-the-fly before it leaves the database. Data Redaction reduces exposure of sensitive information and helps prevent exploitation of application flaws that may disclose sensitive data in application pages. It is well suited for both new and legacy applications that need to limit exposure of sensitive data without invasive application changes. Oracle Data Redaction is particularly suited for reporting applications and other applications that are read-only.

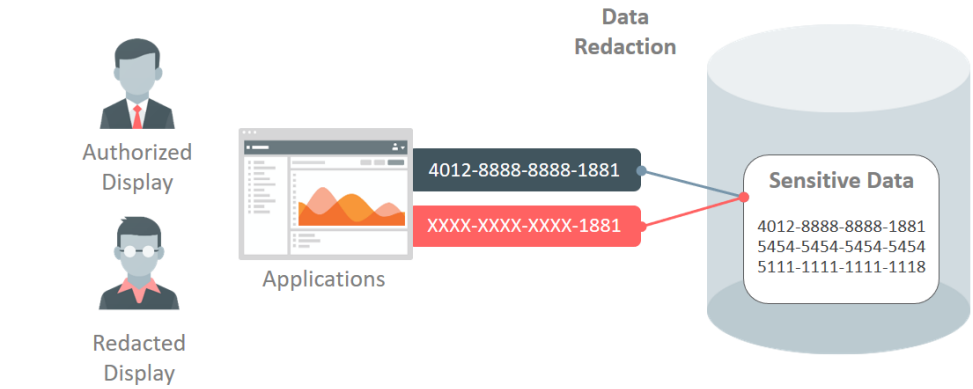


Figure 5. Redacting sensitive data displayed by applications using Data Redaction

Policies and Transformations

Oracle Advanced Security Data Redaction supports a number of different transformations that can redact all data in specified columns, preserve certain pieces of the data, or randomly generate replacement data. Examples of the supported data transformations are shown below.

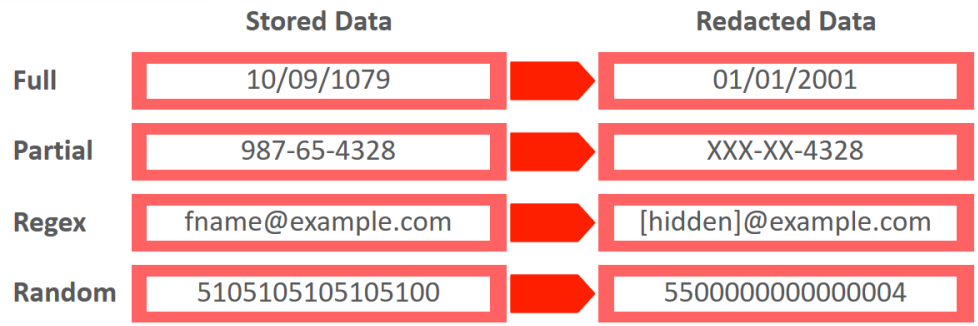


Figure 6. Example Data Redaction transformations

Data Redaction makes the business need-to-know decision based on declarative policy conditions that utilize rich runtime contexts available from the database and from the applications themselves. Examples include user identifiers, user roles, and client IP addresses.

Context information available from Oracle Application Express (APEX), Oracle Real Application Security, and Oracle Label Security also can be utilized to define redaction policies. Redacting APEX

applications is straightforward because policy conditions can leverage the application users and application identifiers that APEX automatically tracks.

Multiple runtime conditions can be joined together within a data redaction policy for fine-grained control over when redaction occurs. The policies are stored and managed inside of the database, and they go into effect immediately upon being enabled.

Performance Characteristics

High-speed performance is crucial for Data Redaction because the target databases typically will be production systems. Data needs to be transformed on-the-fly at runtime, without altering data stored on disk or in caches and buffers. Because the transformations will execute on production environments and will be repeated frequently, the performance overhead must be small.

One important performance characteristic of Data Redaction is that it supports only data transformations with proven high performance. These are a subset of all the possible operations that could be used to transform data in non-production environments. This specific subset avoids long-running and processor intensive operations.

Data Redaction also leverages performance optimizations of the Oracle Database that are only possible by being part of the database kernel. The implementation ensures that data transformations are fast in-memory computations. Policy information is cached in memory, and policy expressions are evaluated only once per execution, so there is no per row performance impact.

Security Considerations

Another benefit resulting from Data Redaction being part of the database kernel is tighter security. This implementation avoids potential vulnerabilities that plague other redaction techniques due to their dependence on proxies that can be meddled with. Additionally, Data Redaction in the kernel continues protecting sensitive data even when other security measures may be compromised. For example, runtime conditions in policies can narrow the impact of a SQL Injection attack by continuing to redact sensitive data even when the attack has bypassed other preventive controls in the application and database.

Data Redaction also avoids obvious sources of leakage where the redaction policy could be bypassed by copying data into a new table that does not have a policy. Certain mass copy operations that touch redacted data are blocked by default, and this behavior can be overridden where necessary using a Data Redaction exempt privilege.

Although Data Redaction can be used to prevent accidental viewing of sensitive data by privileged database users such as DBAs, it is intended primarily for redacting data displayed by software applications. Data Redaction does not prevent privileged users from connecting directly to the database and running ad hoc queries that back into pieces of sensitive data (i.e. it does not stop exhaustive ad hoc queries or other inference attacks). However, Data Redaction is fully compatible with Oracle Database security solutions that control and monitor privileged database user access, including DBAs. It can be deployed in tandem with other solutions such as Oracle Database Vault or Oracle Audit Vault and Database Firewall to provide defense-in-depth security. Data Redaction can also be used with database encryption as well, and it is a great complement to TDE.

Easy to Deploy Data Redaction

Data Redaction can be deployed for existing applications quickly using either a command line API or Oracle Enterprise Manager. The command line API is a PL/SQL procedure that accepts protected columns, transformation types, and conditions. Oracle Enterprise Manager provides a convenient Policy Expression Builder that enables administrators to define and apply redaction policies on existing applications. As shown below, the Policy Expression Builder dialog guides the user through creating policy conditions that use context obtained from applications, the database, the APEX framework, and other database security solutions.

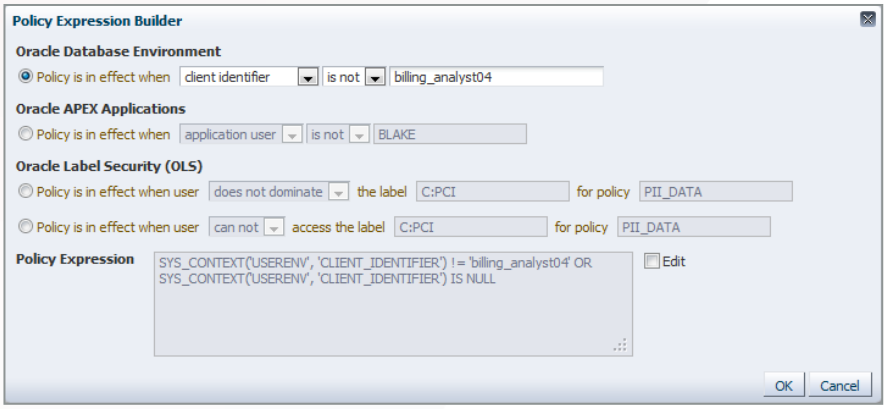


Figure 7. Using Oracle Enterprise Manager Policy Expression Builder to create Data Redaction policies

Predefined column templates also are available in Oracle Enterprise Manager for redacting common sensitive data such as credit card numbers and U.S. Social Security numbers. Oracle Enterprise Manager Sensitive Data Discovery assists in locating columns to be redacted inside of complex application schemas.

Another reason why Data Redaction is easy to deploy is its transparency to applications and the database. For application transparency, Data Redaction supports the column data types that are frequently used by applications and various database objects including tables, views, and materialized views. Redacted values retain key characteristics of the original data such as the data type and optional formatting characters. Random redaction values are drawn from data ranges defined by the existing column data. For transparency to the database, Data Redaction avoids impacting essential database operational activities. It does not affect administrative tasks such as data movement (Oracle Data Pump) or database backup and restore (Oracle Recovery Manager). It does not interfere with database cluster configurations such as Oracle Real Application Clusters, Oracle Data Guard, and Oracle GoldenGate. Data Redaction does not get in the way of existing database triggers or Oracle Virtual Private Database (VPD) policies. In addition, because Data Redaction is part of the database kernel, no separate installation is required.

Comparison to Alternative Approaches

Traditional approaches to redacting sensitive data typically relied on application coding or installing third-party software on the database server to modify its behavior. These alternatives have important drawbacks compared to Data Redaction.

Approaches that require coding new application logic, modifying existing SQL statements, or authoring custom application scripts are likely to result in disparate solutions that are inconsistent across the enterprise and costly to maintain over their lifetime. In addition, strict controls must be placed on new application development to make sure that custom application code and new objects are properly

accessed. The code also needs to take into consideration multiple factors under which the redaction policies are enforced while maintaining the performance and semantics of the application.

Approaches that add new components to the Oracle Database, overwrite existing components, establish proxies, and modify basic behavior of the database also are fraught with problems. Not only do the new components introduce new attack surfaces, but they also can create performance overhead, impact operational activities of the database, and may fail when attempting to transform complex database queries that are generated by applications. In contrast, redacting directly in the Oracle Database kernel using Data Redaction has tighter security, superior performance, and better compatibility with a range of database configurations, use cases, and workloads.

APPLYING ENCRYPTION AND REDACTION IN ORACLE MULTITENANT ARCHITECTURE

Oracle Advanced Security fully supports the Oracle Database multitenant architecture. Both TDE and Data Redaction attributes automatically follow Pluggable Databases (PDB) as they move between multitenant Container Databases (CDB). When moving a PDB that has redaction policies, the policies transfer directly to the new container as part of the PDB. When moving an encrypted PDB, the TDE master keys for that PDB are transferred separately from the encrypted data to maintain proper security separation during transit. Encryption and redaction immediately resume their normal operation after the PDB has been plugged in and configured.

DATA ENCRYPTION IN THE ORACLE CLOUD

In Oracle Database Cloud Service databases, data security is provided for data in transit and data at rest. Security of data in transit is achieved through network encryption. Security of data at rest is achieved through encryption of data stored in database data files and backups using Oracle Advanced Security Transparent Data Encryption. By default, all new tablespaces that are user created in a Database Cloud Service databases are encrypted. For multitenant deployments in the Oracle Cloud, TDE supports a keystore per pluggable database. This design offers greater isolation between tenants and enables independent key management operations.

In addition, to give customers the possibility to control their own master encryption keys, Oracle Key Vault supports hybrid cloud deployments. In this scenario, Oracle Key Vault can be deployed on-premises to support TDE deployments in both cloud and on-premises databases.

CONCLUSION

As data exposed in applications continues to rapidly expand, enterprises must have strong controls in place to protect data no matter what devices or applications are used. Oracle Database 19c, now available in the cloud and on-premises, helps organizations keep their sensitive information safe in this increasingly complex environment by delivering critical controls that enforce data security in the database.

Oracle Advanced Security with Oracle Database 19c provides two critical preventive controls. Transparent Data Encryption encrypts data at rest to stop database bypass attacks from accessing sensitive information in storage. Data Redaction reduces exposure of sensitive information in applications by redacting database query results on-the-fly, according to defined policies. Together these two controls form the foundation of a multi-layered, defense-in-depth approach. They further establish Oracle Database 19c Release as the world's most advanced database solution.

ORACLE CORPORATION

Worldwide Headquarters
500 Oracle Parkway, Redwood Shores, CA 94065 USA

Worldwide Inquiries
TELE + 1.650.506.7000 + 1.800.ORACLE1
FAX + 1.650.506.7200
oracle.com

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com. Outside North America, find your local office at oracle.com/contact.

 blogs.oracle.com/cloudsecurity/db-sec

 facebook.com/oracle

 twitter.com/oracle

Integrated Cloud Applications & Platform Services

White Paper: Encryption and Redaction with Oracle Advanced Security
August 2019

 Oracle is committed to developing practices and products that help protect the environment

ORACLE

18c ORACLE Database

Oracle Advanced Security Transparent Data Encryption (TDE)

Frequently Asked Questions (FAQ)

MARCH 2018

ORACLE

Product Overview

Q. What does Transparent Data Encryption (TDE) provide?

A: TDE transparently encrypts data at rest in Oracle Databases. It stops unauthorized attempts from the operating system to access database data stored in files, without impacting how applications access the data using SQL.

TDE can encrypt entire application tablespaces or specific sensitive columns. Tablespace encryption is useful when you want to encrypt all data irrespective of columns. With tablespace encryption, you do not need to consider column characteristics such as indexes and constraints. Column encryption is useful in cases where only a handful of sensitive columns must be encrypted.

TDE is fully integrated with Oracle database. Encrypted data remains encrypted in the database, whether it is in tablespace storage files, temporary tablespaces, undo tablespaces, or other files that Oracle Database 18c relies on such as redo logs. Also, TDE can encrypt entire database backups and Data Pump exports. Oracle Recovery Manager (RMAN) and Data Pump Export/Import both integrate with TDE encryption to pass through previously encrypted data.

Q. How are TDE encryption keys managed?

A: TDE creates and manages multiple keys used for encryption. These keys must be protected because, if an attacker obtains encrypted data and matching keys, they can easily decrypt to see clear data.

TDE has a two-tier key architecture, with data encryption keys that are wrapped by a single database master key. Data encryption keys are managed by Oracle Database 18c behind the scenes. The master key is separated from encrypted data, stored outside of the database, and directly managed by the database security administrator in a keystore.

Two keystore options are available for TDE to support diverse customer environments. By default, TDE stores its master key in an Oracle Wallet, a PKCS#12 standards-based key storage file. Wallets provide an easy solution for small numbers of encrypted databases. Customers with many Oracle databases and other encrypted Oracle servers can leverage Oracle Key Vault, a security hardened software appliance that provides centralized key and wallet management for the enterprise. It uses industry standard OASIS Key Management Interoperability Protocol (KMIP) for communications. Customers can keep their local Oracle Wallets and Java Keystores, using Key Vault as a central location to periodically back them up, or they can remove keystore files from their environment entirely in favor of always-on Key Vault connections. All network connections between Key Vault and database servers are encrypted and mutually authenticated using SSL/TLS.

TDE master keys can be rotated periodically according to your security policies with zero downtime and without having to re-encrypt any stored data. Historical master keys are retained in the keystore in case encrypted database backups must be restored later. Master keys in the keystore are managed using a set of SQL commands (introduced in Oracle Database 12*c*). For separation of duties, these commands are accessible only to security administrators who hold the new SYSKM administrative privilege or higher. In addition to using SQL commands, you can manage TDE master keys using Oracle Enterprise Manager 12*c* or 13*c*.

Q. How does TDE impact database performance?

A: For Oracle Database 18c systems with modern hardware, the performance overhead from TDE typically is very low and not noticeable to end-users. The TDE page on Oracle Technology Network links to several real-world customer testimonials describing how TDE performs in live production environments.

TDE tablespace encryption leverages cryptographic circuitry present in most modern Intel® and Oracle SPARC processors and cores to accelerate encrypt and decrypt operations by 5-10 times. Oracle Database 18c further caches decrypted tablespace data to make repeated queries faster. For applications that run full table scans, the performance impact may be higher. More memory and bigger caches will improve performance in these

situations. As TDE works at tablespace level, one could consider moving all non-sensitive tables to a clear tablespace.

TDE column encryption can be narrowed to certain columns containing your most sensitive data to minimize overall performance impact. In this approach, only a few columns must be decrypted – even for complex analytical queries that scan large data sets. Column encryption also leverages CPU cryptographic acceleration.

Q. How transparent is TDE to business applications?

A: TDE is transparent to business applications and does not require application changes. Encryption and decryption occur at the database storage level, with no impact to the SQL interface that applications use (neither inbound SQL statements, nor outbound SQL query results).

Note that TDE is certified for use with common packaged applications. These certifications are mainly for profiling TDE performance under different application workloads and for capturing application deployment tips, scripts, and best practices.

Q. How transparent is TDE to database operations?

A: TDE is tightly integrated with frequently used Oracle Database 18c technologies to make it transparent to your database operations. For example, it is integrated with Oracle Advanced Compression, Oracle Real Application Clusters (RAC), Oracle Data Guard, Oracle Active Data Guard (primary/standby), Oracle Golden Gate (replication), and Oracle Multitenant (pluggable databases). Note that for unattended startup in database cluster configurations, TDE provides a key management option, auto-login wallet that allows the database to open its keystore and access its master key without a human operator.

Q. How does TDE integrate with Oracle Exadata?

A: TDE tablespace encryption leverages Oracle Exadata to further boost performance. For example, Exadata Smart Scans parallelize cryptographic processing across multiple storage cells, resulting in faster queries on encrypted data. TDE also benefits from support of hardware cryptographic acceleration on server processors in Exadata. TDE integration with Exadata Hybrid Columnar Compression (EHCC) compresses data first, improving cryptographic performance by greatly reducing the total amount of data to encrypt and decrypt.

Deployment Considerations

Q. What is the process to set up TDE?

As TDE is part of the database kernel, no separate installation is required. To deploy and configure TDE: 1) Setup a keystore and create an initial master key, 2) Enable encryption for tablespaces or columns in your database.

All steps can be executed using SQL commands or Oracle Enterprise Manager 12*c* or 13*c* GUI. All data that is added to those encrypted tablespaces is automatically encrypted. Column encryption however, can be applied to both new and existing tables. See the next question for information about encrypted existing clear data. For detailed information about setup steps, tuning, and migration, please refer to the product documentation for TDE.

Q. How do I migrate existing clear data to TDE encrypted data?

A: TDE provides multiple techniques to migrate existing clear data to encrypted tablespaces or columns. Solutions are available for both online and offline migration.

Existing tablespaces can be encrypted online with zero downtime on production systems or encrypted offline with no storage overhead during a maintenance period. Online tablespace conversion is available on Oracle Database 12.2.0.1 and above whereas offline tablespace conversion has been backported on Oracle Database 11.2.0.4 and 12.1.0.2.

Alternatively, you can copy existing clear data into a new encrypted tablespace with Oracle Online Table Redefinition (DBMS_REDEFINITION). It copies in the background with no downtime. This approach works for both 11*g* and 12*c* databases. This approach includes certain restrictions described in Oracle Database 12*c* product documentation.

Customers with Oracle Data Guard can use Data Guard and Oracle Data Pump to encrypt existing clear data with near zero downtime (see details here). This procedure encrypts on standby first (using DataPump Export/Import), switches over, and then encrypts on the new standby. Database downtime is limited to the time it takes to perform Data Guard switch over. Multiple synchronization points along the way capture updates to data from queries that executed during the process.

If you plan to migrate to encrypted tablespaces offline during a scheduled maintenance period, then you can use Data Pump to migrate in bulk. You also can use SQL commands such as ALTER TABLE MOVE, ALTER INDEX REBUILD (to move an index), and CREATE TABLE AS SELECT to migrate individual objects.

With TDE column encryption, you can encrypt an existing clear column in the background using a single SQL command such as ALTER TABLE MODIFY. This is a fully online operation.

Q. How much extra storage space is needed for TDE encrypted data?

A: For TDE tablespace encryption, the storage overhead is practically none.

The storage overhead associated with TDE column encryption is between 1 and 52 bytes per row for each encrypted column, depending on the following factors:

- Padding [Mandatory] - Padding to the next 16 bytes (for AES). With 3DES168, padding is to the next 8 bytes. For example, if a value requires 9 bytes of storage, then encrypting this value with 3DES168 requires an additional 7 bytes of storage.
- MAC [Optional] - If MAC is specified on the encrypted column, then 20 bytes are added to each value to support integrity checking using SHA. MAC is on by default.
- SALT [Optional] - If SALT is specified for TDE column level encryption, then an additional 16 bytes per value is added. Randomly generated 16 bytes SALT is on by default.

These numbers are important for storage planning. Note that when a column is marked as encrypted, any cryptographic expansion of the cipher data is handled by TDE transparently.

Q. Does TDE support Hardware Security Modules (HSM)?

A: TDE customers optionally may store their master keys in an external device such as HSM using the PKCS #11 interface. In this setup, master keys are stored directly in the third-party device rather than in Oracle Key Vault or Oracle Wallet.

When using PKCS #11, the third-party vendor provides the storage device, PKCS #11 software client library, secure communication from the device to the PKCS #11 client (running on the database server), authentication, auditing, and other related functionality. The vendor also is responsible for testing and ensuring high-availability

of the master encryption key in diverse database server environments, configurations, and versions. Customers should contact the device vendor to receive assistance for any related issues. We do not certify or validate third-party HSMs due to the above challenges.

Standards and Compliance

Q. Which encryption algorithms does TDE support?

A: TDE encryption uses international standards such as Advanced Encryption Standard (AES) and 3DES. Customers can choose their preferred data encryption algorithm and key length.

Q. What industry standards key management does TDE use?

A: TDE master key management uses standards such as PKCS #12 and PKCS #5 for Oracle Wallet keystore. Oracle Key Vault uses OASIS Key Management Interoperability Protocol (KMIP) and PKCS #11 standards for communications. Customers can choose Oracle Wallet or Oracle Key Vault as their preferred keystore.

Q. What security certifications and validations does TDE have?

A: The cryptographic library that TDE uses in Oracle Database 18c is validated for U.S. FIPS 140-2. See here for the library's FIPS 140 certificate (search for the text "Crypto-C Micro Edition"; TDE uses version 4.0). Also, see here for up-to-date summary information regarding Oracle Database certifications and validations.

Q. How does TDE help customers comply with Payment Card Industry (PCI) standards, healthcare data privacy laws (U.S. HIPAA/HITECH), and other security regulations?

A: TDE is an important database security control that helps Oracle customers comply with diverse standards, laws, and regulations that mandate data privacy and security. It provides essential encryption for data at rest in Oracle Databases, enabling customers to address a growing list of regulations in different geographies and industries and remain in compliance as regulations evolve. TDE often is deployed in conjunction with its key management options (Oracle Key Vault and Oracle Wallet) to address specific terms of PCI-DSS Requirement #3 - Protect Stored Cardholder Data. In healthcare context for HIPAA, customers use TDE to encrypt sensitive patient data stored in the database.

Comparison to Other Approaches

Q. How does TDE compare to encrypting in the application tier?

Encrypting in the application tier may be desirable for certain extremely sensitive columns where it is essential that only the application be able to access the data. However, this approach requires high-cost custom coding for proper encryption/decryption and management of keys. Furthermore, all application server nodes need to access the encryption keys making their management and protection difficult. It also increases the chances of corruption if users or the application can update any row/column without appropriate control.

Encryption in the application tier also adversely impacts core database query capabilities because you can only use the database to perform equivalency searches on encrypted columns. Common analytical queries that match against data ranges or computed values will not work. Application tier encryption does not benefit from Oracle Database In-Memory and Exadata high performance architecture.

TDE can be used to encrypt very diverse data all at once in database storage files and does not have these limitations.

Q. How does TDE compare to encrypting host directories or volumes?

Encrypting Oracle Database 18c tablespace files using file or volume encryption software running on the host may initially seem desirable with its support for diverse use cases and platforms; however, because these

technologies are not tuned for high I/O database operations, they can have dramatic impact on core database components. For example, if you attempt to store database redo logs in an encrypted directory or volume, this redo component will incur performance overhead, leading to increasing wait times for log switches, delayed archive file writes, accelerating memory consumption, and possible database stoppage (see details on My Oracle Support).

If you use third-party products that require installing invasive operating system and/or file system modules, this software can crash the database host. These modules may conflict with other running security programs (e.g. anti-virus, intrusion detection) and lead to system crashes. They may also disrupt your patching policies, preventing you from applying a critical patch to the host operating system or file system until a matching patch is available from the encryption vendor. Sensitive data in encrypted file storage may be presented as clear data to non-database programs and users running on the host, exposing your sensitive information to attacks that circumvent the database.

In addition, these solutions cannot limit encryption overhead to specific sets of database tables or columns, and they do not benefit from Oracle Database In-Memory and Exadata high performance architecture.

Note that TDE is fully supported on all operating system platforms including Oracle engineered systems. For addressing data at rest encryption outside of Oracle Databases, TDE can be paired with complementary Oracle technologies.

If a third-party vendor solution causes problems with your database environment, Oracle Support may request you to decrypt data, uninstall third-party software, and reproduce your issue before providing assistance. For questions about third-party encryption products or any support inquiries, you will be asked to consult with your vendor. Oracle provides no support for third-party solutions encrypting tablespace files on Oracle engineered systems such as Oracle Exadata and Oracle Database Appliance.

Q. How does TDE compare to encrypting in disk drives or SAN?

A: Encrypting Oracle Database 18c tablespace files using encryption features of disk drives or SAN storage arrays may seem desirable due to their support for diverse use cases outside of Oracle Databases. However, sensitive data in encrypted disks or SAN may be presented as clear data to non-database programs and users running on the host, exposing your sensitive information to attacks that circumvent the database. These solutions cannot limit encryption overhead to specific sets of database tables or columns, and they do not benefit from Oracle Database In-Memory and Exadata architectures. You typically must purchase new premium price hardware and/or software with optional add-ons. Troubleshooting data I/O issues becomes nearly impossible on encrypted storage arrays.

Complementary Technologies

Q. Can TDE be paired with other data at rest encryption technologies?

A: Oracle provides additional data at rest encryption technologies that can be paired with TDE to protect unstructured file data, storage files of non-Oracle databases, and more as shown in the table below.

Use Case	Oracle Technology
Encrypt files (non-tablespace) using Oracle file systems and operating systems	• Oracle ZFS - An encrypting file system for Solaris and other operating systems • Oracle ACFS - An encrypting file system that runs on Oracle Automatic Storage Management (ASM)

	• Oracle Linux native encryption modules including dm-crypt and eCryptFS
Encrypt files (non-tablespace) using Oracle Database 18c	Oracle Secure Files in combination with TDE. Support for Secure File LOBs is a core feature of the database
Encrypt data programmatically in the database tier	Oracle Database package encryption toolkit (DBMS_CRYPTO) for encrypting database columns using PL/SQL
Encrypt data programmatically in the application tier	Oracle Java (JCA/JCE), application tier encryption may limit certain query functionality of the database. Consider suitability for your use cases in advance

Table 1 – Complementary Oracle Data at Rest Encryption Technologies

Oracle provides solutions to encrypt sensitive data in the application tier – although this has implications for databases that you must consider in advance (see details here). Note that TDE is the only recommended solution specifically for encrypting data stored in Oracle Database 18c tablespace files.

Q. What security controls typically are configured alongside TDE?

A: It is recommended to use TDE in combination with other detective and preventive security controls available for Oracle Database 18c.

Preventive controls help you stop many common threats. Good prevention starts by granting only appropriate privileges and roles to database user accounts, following the security principle of least privilege. You also should encrypt database network connections using SQLNet encryption or built-in support for SSL/TLS. Next, you can add restrictions for privileged user accounts, limit display of sensitive application data, and sanitize copies of production data used in testing and development environments. Details about these preventive controls are shown below.

Preventive Control	**Description**
Oracle Database Vault	Reduces risk exposure coming from powerful database users such as DBA and privileged application connections. Restricts operations these privileged accounts can perform
Oracle Data Redaction	Redacts sensitive data from query results prior to display by applications. Enforces redaction at runtime, with low overhead, and according to conditions set in policies. Part of the same license as TDE (Oracle Advanced Security)
Oracle Data Masking and Subsetting	Makes it easy to create masked and subsetted copies of production data for use in non-production environments such as testing and development databases. Available as an add-on pack for Oracle Enterprise Manager
Oracle Label Security	Implements Multi-Level Security (MLS) enabling rows with differing sensitivity to reside in the same table. Explicitly labels rows with group, compartment, and sensitivity levels – then matches them with user labels

Table 2 – Oracle Database Preventive Controls Typically Used In Combination with TDE

Detective controls start with database auditing to capture records of database actions. You can deploy Oracle Audit Vault and Database Firewall to move audit information to a central repository where you can run database activity reports, detect anomalies, and generate security alerts. Oracle Audit Vault and Database Firewall also provides database firewall and monitoring capabilities that track inbound SQL statements, giving you early warning of unauthorized database activity and blocking threats before they cause harm.

Please refer to the Oracle Database Security page on Oracle Technology Network for more information about database security controls to use alongside TDE.

More Information

Q. How is TDE licensed?

TDE is part of Oracle Advanced Security license for Oracle Database Enterprise Edition. For on-premises databases, Advanced Security can be licensed by server core count or by named user plus (see pricing information here).

The Advanced Security license includes data redaction, tablespace encryption, column encryption, and wallet-based master key management. Centralized key and wallet management using Oracle Key Vault is licensed separately. Note that creating encrypted database backups (RMAN) and Data Pump exports also requires a license for Advanced Security if you do not already have one.

Q. Where can I learn more about TDE?

A: For more information about the benefits of TDE, please see the product page on Oracle Technology Network. A variety of helpful information is available on this page including product data sheet, customer references, videos, tutorials, and more.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services