INSTITUTO SUPERIOR DE TECNOLOGIAS AVANÇADAS DE LISBOA

Transparent Data Encryption (TDE) como ferramenta de *compliance* e proteção de dados: uma abordagem prática em sistemas Oracle

Alfredo Laureano Lourenço.

Dissertação para obtenção do Grau de Mestre em

ENGENHARIA INFORMÁTICA

Júri

Presidente: Professora Doutora Andreia Cristina Teles Vieira

Arguente: Professora Doutora Isabel Maria Surdinho Borges Alvarez

Orientador: Prof. Doutor Paulo André Reis Duarte Branco

Lisboa, 2025

Resumo

A crescente digitalização dos processos empresariais tornou os sistemas de gestão de bases de dados um dos principais alvos de ataques informáticos. A funcionalidade *Transparent Data Encryption* (TDE) do *Oracle Database*, disponível desde a versão *10g Release 2*, permite cifrar automaticamente os ficheiros de dados e os ficheiros de registo (*redo logs*), respondendo a requisitos de proteção definidos por normas como o Regulamento Geral sobre a Proteção de Dados (RGPD), o *Payment Card Industry Data Security Standard* (*PCI-DSS*) e a diretiva *NIS 2*. Apesar da sua maturidade, persistem dúvidas quanto ao impacto no desempenho e à eficácia operacional desta funcionalidade na versão *19c*, atualmente predominante nos ambientes empresariais.

Esta dissertação avalia, num ambiente laboratorial controlado, os efeitos da ativação da TDE em métricas como utilização do processador, memória, latência e operações de entrada e saída, comparando cenários com e sem encriptação. A abordagem segue um desenho quase experimental, com recurso a cargas de trabalho transacionais e analíticas geradas pela ferramenta *SwingBench* e a uma monitorização detalhada do sistema. Os resultados pretendem clarificar os custos, benefícios e boas práticas associados à utilização da TDE, fornecendo evidência empírica que apoie decisões informadas sobre a sua adoção em arquiteturas empresariais.

Palavras chave: *Transparent Data Encryption; Oracle Database*; encriptação; desempenho; proteção de dados; RGPD.

Abstract

Escalating reliance on data intensive workloads has turned database management systems into critical assets and prominent targets for cyberattacks. *Transparent Data Encryption* (TDE), a native feature of the *Oracle Database*, encrypts datafiles and redo log files transparently and is increasingly adopted to meet the security requirements established by the General Data Protection Regulation (GDPR), the *Payment Card Industry Data Security Standard* (PCI DSS) and the NIS 2 Directive. Despite its maturity, empirical evidence quantifying the operational cost of enabling TDE in the current *Oracle 19c* release remains limited, particularly in configurations that take advantage of modern cryptographic optimisations and hardware acceleration.

This dissertation presents a quasi experimental study that quantifies the performance impact and compliance benefits of TDE. Two identical *Oracle 19c* environments, one with TDE enabled and another without encryption, are subjected to transactional and analytical workloads generated by the *SwingBench* toolkit. Key system level metrics including processor utilisation, memory consumption, input output throughput and latency are captured through *Automatic Workload Repository* reports and operating system monitors. Audit trails and key management logs are mapped to GDPR and PCI DSS controls to assess the contribution of TDE to regulatory compliance. The results clarify the balance between security and performance and provide practical guidance for administrators intending to deploy TDE as part of a defence in depth strategy.

Keywords: Transparent Data Encryption; Oracle Database; data encryption; performance overhead; regulatory compliance; data protection.

Agradecimentos

Primeiramente, agradeço a Deus pela vida, pela proteção e pela provisão ao longo de todo o meu percurso académico, bem como pela força e discernimento concedidos nos momentos mais exigentes.

Agradeço profundamente à minha mãe, Delfina, pelo esforço incansável, pela dedicação à minha educação e pelo exemplo de resiliência e coragem que sempre me transmitiu. O seu apoio constante e os sacrifícios realizados foram determinantes para a concretização deste objetivo.

Às minhas irmãs, Elisete e Marina, expresso o meu sincero agradecimento por serem uma fonte permanente de inspiração, orientação e exemplo, contribuindo de forma decisiva para o meu crescimento pessoal e académico.

Agradeço igualmente ao meu pai e a toda a minha família, que representam o principal motivo para eu procurar ser uma pessoa melhor a cada dia, tanto a nível pessoal como profissional.

À minha namorada, companheira presente ao longo deste percurso, agradeço o apoio, a compreensão e o incentivo constantes, especialmente nos períodos de maior exigência e dedicação.

Aos meus professores, em particular os meus orientadores, expresso o meu sincero agradecimento pela orientação, disponibilidade e contributos académicos ao longo do desenvolvimento desta dissertação.

Aos colegas da universidade, agradeço a partilha de conhecimentos, o apoio mútuo e o espírito de colaboração que marcaram esta etapa do meu percurso académico.

Aos meus amigos, deixo o meu reconhecimento pelo apoio, incentivo e companheirismo demonstrados ao longo deste caminho. A todos os que, direta ou indiretamente, contribuíram para a realização deste trabalho, o meu sincero agradecimento.

Índice

Acrónimos

ACID: Atomicidade, Consistência, Isolamento e Durabilidade. Conjunto de propriedades que garantem a fiabilidade das transações em sistemas de gestão de bases de dados.

AES: *Advanced Encryption Standard*. Algoritmo de encriptação simétrica amplamente utilizado para proteção de dados em repouso e em trânsito.

AES 256 GCM: *Advanced Encryption Standard* com chave de 256 bits no modo *Galois Counter Mode*. Modo de cifra autenticado que assegura confidencialidade e integridade.

CIA:
Confidencialidade, Integridade e Disponibilidade. Pilares fundamentais da segurança da informação.

DBA: Database Administrator. Profissional responsável pela administração, manutenção e segurança das bases de dados.

DEK: *Database Encryption Key*. Chave simétrica utilizada para cifrar os blocos de dados numa base de dados.

ENISA: *European Union Agency for Cybersecurity*. Agência europeia responsável por orientações e boas práticas em cibersegurança.

GCM: *Galois Counter Mode*. Modo de operação criptográfico que combina encriptação e autenticação de dados.

GDPR: *General Data Protection Regulation*. Regulamento europeu relativo à proteção de dados pessoais.

HIPAA: *Health Insurance Portability and Accountability Act*. Legislação dos Estados Unidos que regula a proteção de dados de saúde.

HSM: *Hardware Security Module*. Módulo físico dedicado ao armazenamento seguro e à gestão de chaves criptográficas.

Intel AES NI: *Advanced Encryption Standard New Instructions*. Conjunto de instruções de hardware que acelera operações criptográficas AES.
ISO IEC: *International Organization for Standardization* e *International Electrotechnical Commission.* Organismos internacionais responsáveis por normas técnicas e de segurança da informação.
I**SO 27001:** Norma internacional que define requisitos para sistemas de gestão da segurança da informação.

MEK: *Master Encryption Key*. Chave mestra utilizada para proteger as chaves de encriptação de dados.

NIS 2: Diretiva europeia relativa à segurança das redes e dos sistemas de informação, aplicável a operadores de serviços essenciais e fornecedores digitais.

NIST SP 800 30: Publicação do *National Institute of Standards and Technology* que estabelece diretrizes para gestão de riscos de segurança da informação.

NoSQL: *Not Only SQL*. Classe de bases de dados não relacionais orientadas a documentos, grafos ou pares chave valor.

OLAP: *Online Analytical Processing*. Tipo de processamento orientado à análise de grandes volumes de dados.

OLTP: *Online Transaction Processing*. Tipo de processamento orientado a transações curtas e frequentes.

PCI DSS: *Payment Card Industry Data Security Standard*. Norma de segurança para proteção de dados de titulares de cartões de pagamento.

PDB: *Pluggable Database*. Base de dados *pluggable* no modelo *multitenant* do Oracle.

PL SQL :P*rocedural Language SQL*. Linguagem procedural integrada no Oracle *Database*.

RGPD: Regulamento Geral sobre a Proteção de Dados. Designação em português do GDPR.

RSA: Algoritmo criptográfico assimétrico baseado em chaves pública e privada.

SGBD: Sistema de Gestão de Bases de Dados. Software responsável pela criação, gestão e segurança das bases de dados.

SQL: *Structured Query Language.* Linguagem padrão para definição e manipulação de dados em bases de dados relacionais.

TDE: *Transparent Data Encryption*. Funcionalidade do Oracle Database que cifra automaticamente dados em repouso.

Índice de Figuras

Índice de Tabelas

1. Introdução

1.1 Importância da segurança da informação

Nas últimas duas décadas, o volume global de dados tem crescido de forma exponencial, impulsionado pela computação em nuvem, pela Internet das Coisas e pela digitalização de processos críticos. A *International Data Corporation* projeta que a esfera digital ultrapasse os 180 *zettabytes* de informação antes do final da década [6]. Esta enorme massa de dados, concentrada sobretudo em sistemas de gestão de bases de dados, tornou-se simultaneamente um ativo estratégico e um alvo preferencial de ciberataques. Em média, cada violação de dados representa perdas superiores a quatro milhões de dólares, valor que inclui paralisações operacionais, sanções legais e danos reputacionais [10].

A norma ISO/IEC 27000 define segurança da informação como o conjunto de processos destinados a preservar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a responsabilidade dos dados ao longo de todo o seu ciclo de vida [1]. Estes atributos constituem a base das políticas organizacionais e dos controlos técnicos, que visam mitigar riscos, assegurar a conformidade regulamentar e manter a confiança de clientes e parceiros. A adoção de medidas de proteção robustas tornou-se imperativa, sobretudo após a entrada em vigor do Regulamento Geral sobre a Proteção de Dados, que exige salvaguardas "adequadas ao risco", destacando-se entre elas a encriptação de dados em repouso [13].

O termo "segurança" provém do latim *securitas*, que expressa a condição de estar livre de preocupação ou perigo. Já "informação" deriva de *informatio*, ou seja, o ato de dar forma ou estruturar o conhecimento. Em conjunto, o conceito remete para o esforço contínuo de proteger dados relevantes contra acessos não autorizados, alterações indevidas ou indisponibilidade. Esta missão implica múltiplas camadas de defesa, desde políticas de acesso e autenticação multifator até à encriptação de dados e à monitorização contínua.

Para compreender a aplicação prática destas salvaguardas, é essencial revisitar os princípios fundamentais que sustentam esta disciplina. Nos capítulos seguintes analisam-se os cinco pilares clássicos: confidencialidade, integridade, disponibilidade, autenticidade e responsabilidade. A estes juntam-se extensões contemporâneas como a posse ou controlo e o

não repúdio, elementos que reforçam a fiabilidade e a resiliência dos sistemas num cenário de ameaças em constante evolução.

1.2 Objetivos da pesquisa

1.2.1 Objetivo geral

Avaliar de forma empírica como a implementação da *Transparent Data Encryption* (TDE) em ambientes Oracle contribui para a segurança da informação e para o cumprimento de requisitos regulamentares.

1.2.2 Objetivos específicos

a) Medir o impacto da TDE no desempenho de cargas OLTP em Oracle 19c.

b) Verificar o grau de adesão das configurações testadas aos requisitos do RGPD, da NIS 2 e da PCI-DSS.

c) Analisar a integração da TDE com outros controlos Oracle (*Database Vault, Unified Audit*, gestão externa de chaves) na perspetiva de uma estratégia de defesa em profundidade.

1.3 Perguntas de investigação

1. De que forma a utilização da *Transparent Data Encryption (TDE)* em bases de dados Oracle melhora a segurança e apoia a conformidade com regulamentos como o RGPD?

2. Como a TDE se integra com outras ferramentas e processos de segurança do ecossistema Oracle para constituir uma estratégia abrangente?

1.4 Justificação

Relatórios recentes indicam que mais de 70 por cento das credenciais vendidas em mercados clandestinos têm origem em extratos de bases de dados obtidos sem uma encriptação adequada [11]. Embora a funcionalidade TDE esteja disponível desde a versão 10g, continua a haver escassez de estudos que quantifiquem o seu impacto no desempenho da versão 19c, atualmente predominante em ambientes corporativos [9]. Esta investigação procura colmatar essa lacuna, oferecendo métricas reproduzíveis e orientações práticas para administradores e decisores.

1.5 Estrutura do trabalho

O **Capítulo 2** desenvolve a revisão da literatura. São abordados os princípios fundamentais da segurança da informação, os mecanismos de encriptação de dados em repouso, o enquadramento regulamentar aplicável (como o RGPD e outras normas relevantes) e as principais lacunas identificadas na investigação atual.

O **Capítulo 3** descreve a metodologia experimental. Explica-se o ambiente de testes utilizado, as ferramentas aplicadas e as métricas selecionadas para avaliar o impacto da TDE no desempenho do sistema.

O **Capítulo 4** apresenta os resultados obtidos. Estes são analisados à luz dos objetivos traçados, procurando evidenciar os efeitos da ativação da TDE e as suas implicações práticas.

O **Capítulo 5** encerra o trabalho com uma síntese dos principais achados. São reconhecidas as limitações do estudo e sugeridas direções para futuras investigações nesta área.

2.Revisão da literatura

2.1 Pilares da segurança da informação

A ISO/IEC 27000 define segurança da informação como a preservação, ao longo de todo o ciclo de vida dos dados, dos atributos de confidencialidade, integridade, disponibilidade, autenticidade e responsabilidade [1]. Estes atributos, consagrados no modelo "CIA", formam a base sobre a qual se constroem políticas, controlos técnicos e requisitos regulatórios.

A confidencialidade assegura que apenas sujeitos autorizados acedem à informação. Em bases de dados isto traduz-se na aplicação de encriptação, autenticação multifator e classificação de dados. O modelo de Bell e LaPadula formaliza a política "*no read up, no write down*", ainda usada em contextos governamentais e replicada em mecanismos Oracle como *Virtual Private Database* [2].

Integridade garante exatidão e completude dos registos. *Triggers, constraints* e funções *hash* detetam alterações não autorizadas, enquanto os modelos de Biba e de Clark–Wilson impõem transações bem-formadas e separação de deveres, reduzindo o risco de corrupção acidental ou maliciosa [3][4].

Disponibilidade exige que os dados estejam acessíveis quando necessário. Redundância de *hardware*, Oracle *Data Guard*, planos de continuidade de negócio e testes de recuperação regular sustentam este pilar, conferindo resiliência perante falhas físicas ou lógicas [1].

Embora o triângulo CIA permaneça central, Parker propôs a inclusão de autenticidade, posse ou controlo, utilidade e não repúdio, formando o chamado hexágono de Parker [5]. Entre estes, dois destacam-se em ambientes regulados.

A autenticidade confirma, sem ambiguidades, a identidade de utilizadores e processos. Implementa-se com certificados digitais, Kerberos e registos unificados de auditoria. No Oracle *Database* o *Unified Audit* associa cada comando SQL a um utilizador autenticado, apoiando a rastreabilidade exigida pelo RGPD [13].

Responsabilidade (não repúdio) assegura que o autor de uma ação não possa negar posteriormente a sua execução. Assinaturas digitais, carimbos de tempo e *logs* imutáveis

servem como prova em auditorias internas ou externas, mitigando litígios e exigências de conformidade.

Regulamentações recentes, como o RGPD, introduzem também o conceito de privacidade, que impõe exigências como a minimização de dados, a pseudonimização e a encriptação robusta dos dados em repouso. A privacidade pode ser entendida como um requisito de alto nível, alcançado pela combinação dos pilares clássicos da segurança da informação, e reforçado por práticas como o mascaramento dinâmico e a gestão de consentimento.

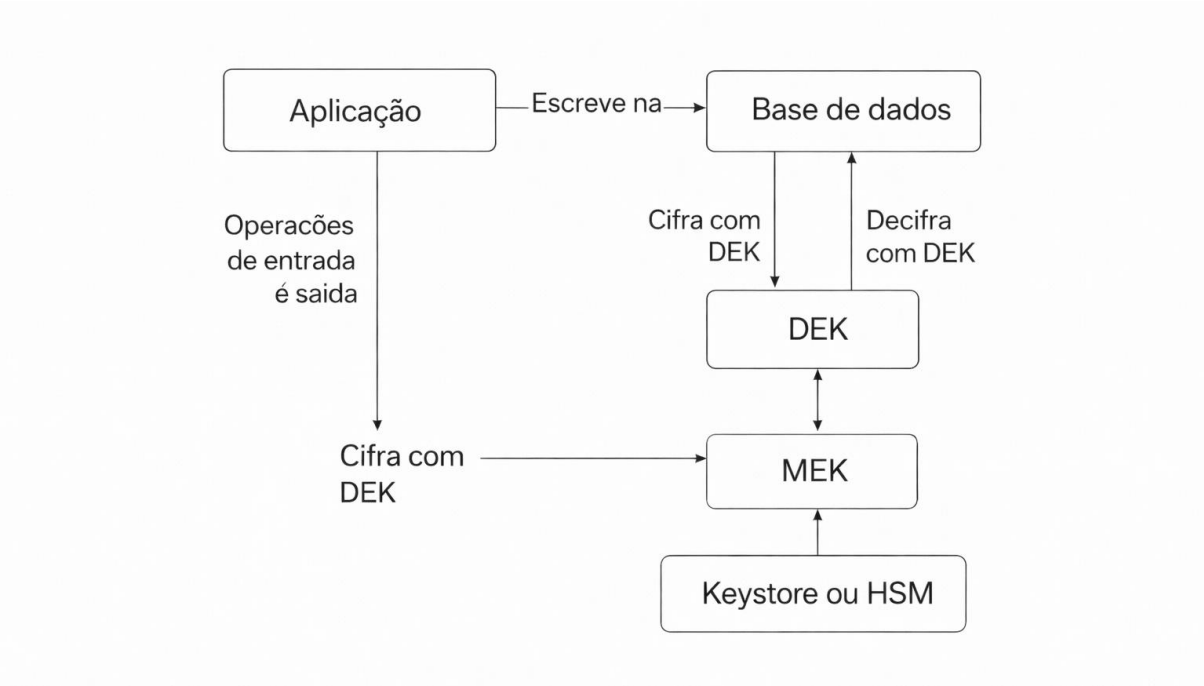
Nas secções que se seguem, esses pilares serão relacionados com os controlos de segurança oferecidos pelo Oracle *Database*, permitindo analisar de que forma a Transparent Data Encryption(TDE) contribui para a sua proteção e para o cumprimento de normas como o RGPD, a NIS 2 e a PCI-DSS.

2.2 Conceito de encriptação e relevância na proteção de dados

Existem dois modelos fundamentais de encriptação: a encriptação simétrica, que utiliza a mesma chave para cifrar e decifrar a informação, e a encriptação assimétrica, que recorre a um par de chaves pública e privada. Algoritmos simétricos como o *Advanced Encryption Standard* alcançam taxas de processamento elevadas, sobretudo quando beneficiam de aceleração por hardware, como as instruções *Intel AES NI* [15]. Já algoritmos assimétricos, como *RSA* ou criptografia baseada em curvas elípticas, permitem uma distribuição segura de chaves mas apresentam um custo computacional superior.

Os sistemas de gestão de bases de dados combinam ambos os modelos através do mecanismo designado *envelope encryption*. Neste paradigma, uma chave simétrica, conhecida como *Database Encryption Key(DEK)*, cifra os blocos de dados, sendo esta chave protegida por uma chave assimétrica armazenada numa carteira de chaves, num módulo de segurança de hardware (*Hardware Security Module*) ou num serviço de gestão de chaves (*Key Management Service*).

Figura 1 - Esquema conceptual de encriptação híbrida



Fonte: Autor

Além de salvaguardar a confidencialidade, a encriptação contribui para diversos outros objetivos de segurança e conformidade:

Integridade – funções de dispersão criptográfica (*hash functions*) e códigos de autenticação de mensagem (*Message Authentication Codes*) permitem detetar alterações não autorizadas em blocos de dados [16].

Privacidade – a combinação de pseudonimização, mascaramento dinâmico de dados e encriptação reduz significativamente a exposição de informação sensível, mesmo perante utilizadores internos com privilégios elevados.

Conformidade – normas como o *Payment Card Industry Data Security Standard* exigem a aplicação de encriptação forte a dados de titulares de cartão, tanto em repouso como em trânsito [14].

Nas bases de dados empresariais, a escolha do tipo de encriptação a adotar resulta do equilíbrio entre granularidade, impacto no desempenho e requisitos de auditoria.

A *Transparent Data Encryption*, analisada nos capítulos seguintes, posiciona-se como uma solução de cobertura total sobre os ficheiros de dados, proporcionando simplicidade operacional e um impacto moderado no desempenho quando o hardware dispõe de aceleração criptográfica.

2.3 Tipos de encriptação

A literatura especializada distingue três modelos criptográficos fundamentais, cada um com benefícios e limitações que influenciam a arquitetura de segurança das bases de dados.

A encriptação simétrica utiliza a mesma chave para cifrar e decifrar a informação. O algoritmo *Advanced Encryption Standard*, suportado por instruções de hardware como *Intel AES NI*, oferece taxas de processamento muito elevadas, o que o torna adequado à proteção de grandes volumes de dados em repouso [15]. A principal limitação reside na distribuição segura dessa chave, uma vez que a sua divulgação compromete imediatamente todo o conteúdo cifrado.

A encriptação assimétrica recorre a um par de chaves distintas, uma pública para cifrar e outra privada para decifrar. Esta separação facilita a troca segura de segredos e possibilita mecanismos adicionais como assinatura digital e não repúdio, atendendo a requisitos de auditoria regulamentar [16]. Contudo, o seu custo computacional é substancialmente superior, o que inviabiliza a sua aplicação direta a grandes blocos de dados.

A encriptação híbrida combina as duas abordagens. O sistema gera uma chave simétrica, designada *Database Encryption Key(DEK)*, para proteger os blocos de dados e cifra essa chave com uma chave mestra assimétrica armazenada numa carteira segura, num módulo de segurança de hardware (*Hardware Security Module*) ou num serviço de gestão de chaves (*Key Management Service*). Este esquema, conhecido como *envelope encryption*, alia a rapidez do *Advanced Encryption Standard* à segurança do *RSA* ou da criptografia de curvas elípticas. É o modelo adotado pela *Oracle Transparent Data Encryption*, recomendado em normas como o *Payment Card Industry Data Security Standard* e o Regulamento Geral sobre a Proteção de Dados [14][13][18].

Na prática, a escolha do esquema depende sobretudo de três fatores: a sensibilidade da informação, a exigência de desempenho e o modelo de governança de chaves da organização.

Os capítulos seguintes avaliam, de forma empírica, como a TDE, baseada em encriptação híbrida com *AES 256 GCM*, afeta o desempenho e contribui para a conformidade em ambientes *Oracle 19c*.

2.4 A importância da encriptação na proteção de dados

2.4.1 Confidencialidade e privacidade

A encriptação é o mecanismo que melhor protege a confidencialidade dos dados em repouso, pois transforma texto legível em texto cifrado, ilegível sem a chave adequada [15]. No contexto das bases de dados, a *TDE* aplica o algoritmo *AES 256 GCM* a cada bloco escrito em disco, garantindo que os ficheiros de *tablespace*, os ficheiros de registo e as cópias de segurança permanecem inacessíveis mesmo que sejam copiados ou extraviados [18].

Num enquadramento regulatório, a confidencialidade relaciona-se diretamente com o princípio da privacidade dos titulares de dados. O *RGPD* estabelece que a informação pessoal deve ser tratada de forma a assegurar uma "segurança adequada", recomendando explicitamente a utilização de salvaguardas técnicas como a encriptação e a pseudonimização [13]. Ao cifrar toda a estrutura física da base de dados, a TDE contribui para o cumprimento do princípio de *privacy by design*, evitando a exposição acidental de dados sensíveis e reduzindo o risco de reidentificação dos titulares.

Para além de impedir o acesso não autorizado, a encriptação suporta políticas internas de minimização de dados. Ficheiros de teste ou exportações antigas podem ser armazenados em ambientes de menor segurança sem violar a confidencialidade, desde que a chave de decifração permaneça devidamente segregada num módulo de segurança de hardware (*Hardware Security Module*) ou num serviço de gestão de chaves (*Key Management Service*). Esta separação entre o dado cifrado e a chave respeita os princípios de posse e controlo definidos no hexágono de Parker [5], reforçando a governança sobre cópias de segurança externas ao repositório principal.

2.4.2 Integridade dos dados

A integridade assegura que a informação permanece exata, completa e fidedigna ao longo de todo o seu ciclo de vida. Nos sistemas de gestão de bases de dados, este pilar é tradicionalmente suportado por restrições de integridade (*constraints*), transações com propriedades *ACID*, mecanismos de validação como *triggers* e modelos formais como os de *Biba* e *Clark Wilson*, que impõem separação de deveres e transações bem formadas para impedir alterações ilícitas [3][4].

A encriptação em repouso reforça estes mecanismos de três formas principais:

Modos autenticados de cifra

A *Oracle Transparent Data Encryption* utiliza o algoritmo *AES 256* no modo *Galois Counter Mode* (*GCM*), que produz simultaneamente o texto cifrado e um código de autenticação (*authentication tag*). Qualquer modificação acidental ou maliciosa num bloco cifrado invalida esse código, levando o motor da base de dados a rejeitar a leitura e a sinalizar corrupção [18]. Assim, a própria camada de encriptação atua como verificação criptográfica de integridade, sem necessidade de lógica adicional na aplicação.

Proteção de ficheiros de registo e cópias de segurança

Quando os ficheiros de registo e as cópias de segurança são cifrados, torna-se impraticável injetar comandos ou restaurar dados manipulados sem acesso à *Database Encryption Key(DEK)*. Isto protege a cadeia de custódia exigida por auditorias forenses e por normas de registo financeiro, como a *Sarbanes Oxley*, onde a imutabilidade do histórico transacional é crítica.

Deteção precoce de corrupção

Enquanto a integridade lógica só é verificada quando os dados são lidos pela aplicação, o controlo criptográfico valida cada bloco quando é decifrado na memória intermédia (*buffer cache*). Alterações de baixo nível, como as causadas por falhas de armazenamento ou por ataques que modificam diretamente partes do disco, são detetadas de imediato, permitindo ações de recuperação antes que o erro se propague.

A conjugação da encriptação autenticada com os modelos de integridade existentes cria uma dupla barreira: a camada transacional impede manipulações lógicas e a camada criptográfica impede corrupções físicas. Este alinhamento simplifica a demonstração de conformidade em auditorias de segurança, ao evidenciar controlos sobre ambos os vetores de alteração de dados.

2.4.3 Conformidade com regulamentos

A adoção de encriptação em repouso é fortemente incentivada pelos principais diplomas que regem a proteção de dados. O Regulamento Geral sobre a Proteção de Dados estabelece, no artigo 32, que os responsáveis devem aplicar medidas técnicas adequadas ao risco, referindo a encriptação como exemplo privilegiado [13]. Ao cifrar integralmente os ficheiros de dados e as cópias de segurança, a *TDE* contribui para demonstrar o cumprimento deste requisito e, em caso de violação, pode dispensar a notificação individual aos titulares prevista no artigo 34, desde que os dados permaneçam ininteligíveis.

A Diretiva *NIS 2* alarga as obrigações de ciber-resiliência a operadores de serviços essenciais e a fornecedores de serviços digitais. Entre os controlos enumerados encontram-se a gestão rigorosa de chaves e a encriptação da informação crítica [12]. A TDE satisfaz estas exigências ao isolar a chave mestra num módulo de segurança de hardware (*Hardware Security Module*) ou num serviço de gestão de chaves (*Key Management Service*) e ao garantir que os blocos físicos dos *tablespaces* ficam protegidos contra acesso não autorizado.

No setor financeiro, a norma *PCI DSS* 4.0 exige encriptação forte dos dados de titulares de cartão, tanto em bases de dados como em ficheiros temporários e cópias de segurança, conforme o requisito 3 [14]. Como a TDE cifra tabelas e ficheiros de registo de forma transparente, cumpre o objetivo técnico da norma sem exigir alterações ao código da aplicação, reduzindo custos de auditoria e de manutenção.

A *Health Insurance Portability and Accountability Act*, aplicável a entidades de saúde nos Estados Unidos, recomenda a encriptação de registos clínicos eletrónicos como salvaguarda padrão e obriga à documentação completa do ciclo de vida das chaves [19]. Ao integrar se com o *Oracle Key Vault*, a TDE permite rotação programada e controlo dual das chaves, satisfazendo os requisitos da seção §164.312 da respetiva regra de segurança.

Por fim, legislação como a *Sarbanes Oxley* impõe a retenção inviolável de registos financeiros para assegurar transparência e rastreabilidade [21]. A encriptação autenticada baseada em *AES GCM* reforça a integridade desses registos, enquanto o *Unified Audit* gera trilhas imutáveis que sustentam a prestação de contas exigida em auditorias.

Tabela 1: Correspondência entre requisitos regulamentares e controlos de segurança

Requisito regulamentar	Controlos e funcionalidades do Oracle Database
RGPD, artigo 32	*Transparent Data Encryption* para cifragem de dados em repouso
Diretiva NIS 2, artigo 21	Utilização de *Hardware Security Module* ou *Key Management Service* para gestão segura de chaves
PCI DSS, requisito 3	*Transparent Data Encryption* para cifragem de bases de dados e cópias de segurança
HIPAA, §164.312	Oracle Key Vault em conjunto com *Transparent Data Encryption* para gestão do ciclo de vida das chaves
Sarbanes Oxley, secção 404	AES 256 GCM e Unified Audit para garantir integridade e rastreabilidade

Fonte: Autor

2.4.4 Redução do impacto de ataques e violações

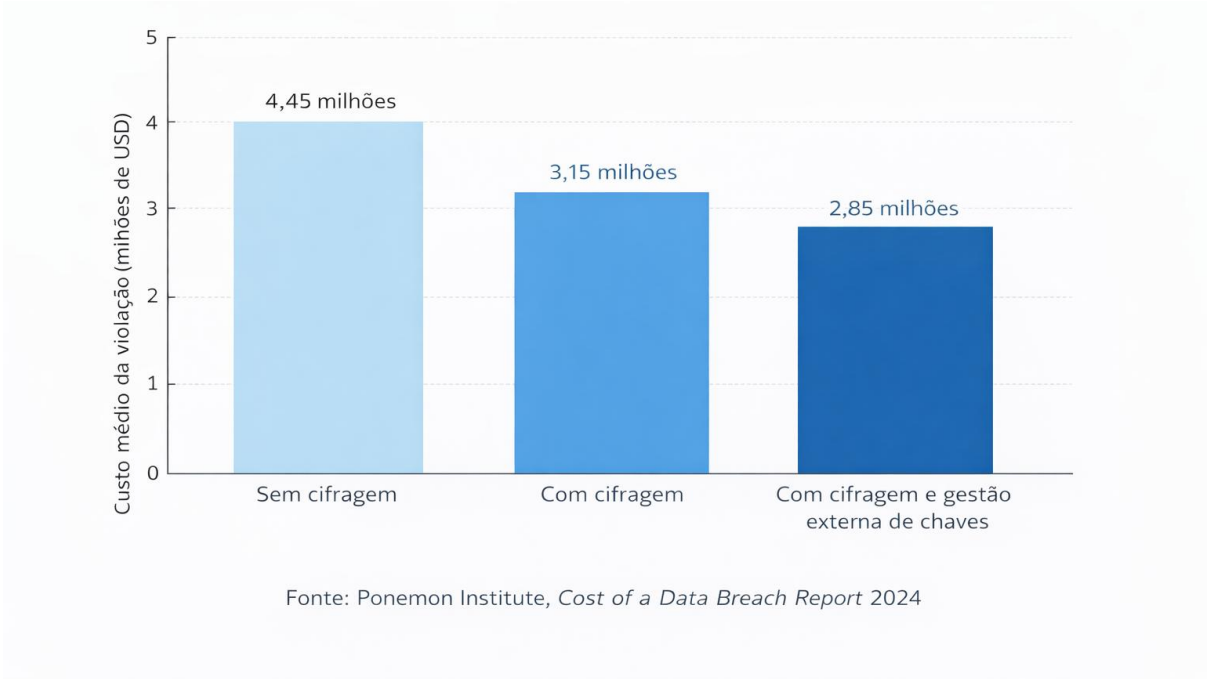
A encriptação em repouso atua como última linha de defesa quando todos os restantes controlos de segurança falham. Em situações de acesso físico não autorizado, furto de cópias de segurança ou exploração de vulnerabilidades que permitam a extração de ficheiros do *tablespace*, os dados permanecem cifrados e, portanto, inutilizáveis sem a chave de decifração. Este efeito é particularmente valioso em incidentes de grande escala, nos quais a contenção imediata dos danos nem sempre é possível.

O relatório *Ponemon 2024* demonstra que organizações que mantêm dados fortemente cifrados sofreram um custo médio de violação 49 por cento inferior ao das que não utilizavam mecanismos de encriptação em repouso [10]. Este diferencial resulta, em parte, da possibilidade de invocar a cláusula do Regulamento Geral sobre a Proteção de Dados que dispensa a notificação individual aos titulares sempre que a informação comprometida se encontre "adequadamente protegida por técnicas de encriptação" [13]. Para além de reduzir penalidades legais e custos inerentes à resposta a incidentes, esta salvaguarda contribui para

mitigar o impacto reputacional, que, segundo o mesmo estudo, representa quase metade das perdas financeiras totais.

Casos amplamente divulgados reforçam esta conclusão empírica. No incidente da *Equifax* em 2017, os registos não cifrados expuseram informação pessoal de aproximadamente 147 milhões de consumidores, resultando em multas superiores a setecentos milhões de dólares e num abalo significativo da confiança pública [16]. Em contraste, organizações que sofreram intrusões mas que armazenavam os dados em formato cifrado enfrentaram consequências jurídicas e mediáticas substancialmente menores, precisamente porque os ficheiros obtidos pelos atacantes permaneceram ininteligíveis.

Figura 2 - Impacto da encriptação no custo médio de violação de dados



Fonte: Ponemon Institute, *Cost of a Data Breach Report* 2024

A *Transparent Data Encryption* acrescenta ainda um benefício operacional relevante: impede que cópias de segurança exfiltradas em ambientes de nuvem ou em partilhas de rede possam ser restauradas noutro servidor *Oracle* sem acesso à carteira de chaves (*wallet*) ou ao módulo de segurança de hardware (*Hardware Security Module*) onde reside a chave mestra. De forma semelhante, ataques de *ransomware* que copiam ficheiros de dados para posterior tentativa de extorsão não obtêm qualquer vantagem prática, uma vez que não conseguem decifrar o conteúdo sem a chave. Tal reduz significativamente a eficácia do modelo de extorsão dupla, baseado no roubo e encriptação de informação.

2.5 Bases de dados: conceito, ameaças e mecanismos de proteção

2.5.1 Conceito de bases de dados

O conceito de base de dados evoluiu de um simples repositório de ficheiros estruturados para um ecossistema complexo de gestão de informação, essencial para a continuidade de negócio e suporte à decisão. Segundo **Deshmukh & Qureshi (2011)**, as bases de dados modernas não apenas armazenam dados, mas servem como o ativo estratégico central em organizações, onde a integridade e a disponibilidade são pilares críticos para a sobrevivência operacional face a ameaças crescentes como a exposição de backups ou acessos não autorizados por administradores privilegiados.

Tecnicamente, um Sistema de Gestão de Bases de Dados (SGBD) atua como uma camada de abstração entre o armazenamento físico e as aplicações. Esta arquitetura permite a gestão de metadados, o controlo de concorrência e a aplicação de políticas de segurança de forma centralizada e independente da lógica aplicacional. Como notado por **Natarajan & Shaik (2020)**, em sistemas de alto desempenho como o Oracle 19c, a base de dados deve garantir que os dados "em repouso" (a*t-rest*) permaneçam cifrados no nível do bloco físico, sem que isso comprometa a transparência e a agilidade das consultas. Esta "transparência" é o que define as soluções modernas de segurança de bases de dados, permitindo a proteção robusta sem a necessidade de reengenharia de software (**Deshmukh & Qureshi, 2011**).

Dentro desta arquitetura, é fundamental distinguir a natureza das operações realizadas, que se dividem predominantemente em dois perfis de utilização:

2.5.1.1 Online Transaction Processing (OLTP) O modelo OLTP

foca-se na execução de um elevado volume de transações curtas, rápidas e atómicas. Estes sistemas são orientados para a escrita e atualização constante de dados (ex: registo de vendas, operações financeiras), exigindo conformidade estrita com as propriedades **ACID** (Atomicidade, Consistência, Isolamento e Durabilidade). A fundamentação teórica de **Natarajan & Shaik (2020)** sublinha que o impacto da encriptação nestes sistemas é particularmente crítico, uma vez que a cifra ocorre em tempo real durante cada operação de entrada e saída (I/O). A otimização através de instruções de *hardware*, como as extensões **Intel**

AES-NI, é uma resposta tecnológica vital para mitigar a latência que estas transações de alta frequência poderiam introduzir na experiência do utilizador final.

2.5.1.2 Online Analytical Processing (OLAP)

Ao contrário do OLTP, os sistemas OLAP são projetados para suportar a análise de grandes volumes de dados históricos através de consultas complexas, cruzamento de tabelas massivas e agregações. Este perfil é a base de ambientes de *Business Intelligence* e *Data Warehousing*. Segundo a literatura de **Palmucci (2022)**, enquanto o OLTP gere dados "vivos" e granulares, o OLAP lida com dados consolidados que requerem alta performance em operações de leitura intensiva (*Full Table Scans*). Para estes sistemas, a encriptação transparente (TDE) ao nível do tablespace apresenta uma vantagem estratégica, pois permite que o motor da base de dados mantenha as suas otimizações de leitura em larga escala (como o *Direct Path Read*) enquanto assegura que o volume massivo de dados sensíveis armazenados para análise está protegido contra exfiltração física.

2.5.2 Importância da segurança nas bases de dados

Porque concentram informação pessoal, financeira e intelectual, as bases de dados representam um dos alvos mais valiosos para atacantes. A IBM X-Force reporta que credenciais extraídas diretamente de tabelas correspondem a mais de 70 % das divulgações em mercados clandestinos [11]. Uma violação pode acarretar perda de receitas, sanções regulatórias (RGPD, PCI-DSS) e danos reputacionais prolongados, como ilustram os casos Equifax e Capital One [16][17].

2.5.3 Principais ameaças

1. **Acesso não autorizado**: abuso de credenciais privilegiadas ou falhas de segregação de funções concedem visibilidade total a dados sensíveis.
2. **Injeção de SQL:** exploração de parâmetros de entrada inseguros que permitem a execução de comandos maliciosos no sistema de gestão de bases de dados.
3. **Roubo de cópias de segurança e de instantâneos:** ficheiros não cifrados armazenados em repositórios externos possibilitam a leitura da informação fora do ambiente controlado.
4. **Ataques de *ransomware* a bases de dados:** encriptação ou extração dos ficheiros do *tablespace* para fins de extorsão.
5. **Erros de configuração:** permissões excessivas, ausência de aplicação de atualizações e opções inseguras podem expor serviços diretamente à Internet.

2.5.4 Mecanismos de proteção

• **Controlo de acessos e princípio do menor privilégio:** perfis de utilizador bem definidos, autenticação multifator e separação de deveres reduzem significativamente a superfície de ataque.

• **Encriptação em repouso e em trânsito:** a *Transparent Data Encryption* protege ficheiros de dados e ficheiros de registo; *Transport Layer Security* assegura ligações seguras entre cliente e servidor.

• **Monitorização e auditoria:** o *Unified Audit* do *Oracle Database*, integrado num sistema de gestão de eventos de segurança (*Security Information and Event Management*), permite detetar comportamentos anómalos e manter trilhas de auditoria imutáveis.

• **Cópias de segurança seguras e testadas:** ficheiros cifrados, armazenados fora do local principal (*off site*) e sujeitos a exercícios regulares de restauração mitigam o impacto de ataques de *ransomware* e de falhas físicas.

• **Gestão de vulnerabilidades e aplicação de atualizações:** a instalação atempada das *Critical Patch Updates* corrige falhas conhecidas frequentemente exploradas em ataques automatizados.

• **Defesa em profundidade:** camadas adicionais como o *Oracle Database Vault* e firewalls de aplicação criam múltiplas barreiras antes do acesso efetivo aos dados.

2.6 Transparent Data Encryption (TDE): conceito, funcionamento e histórico

2.6.1 Conceito geral

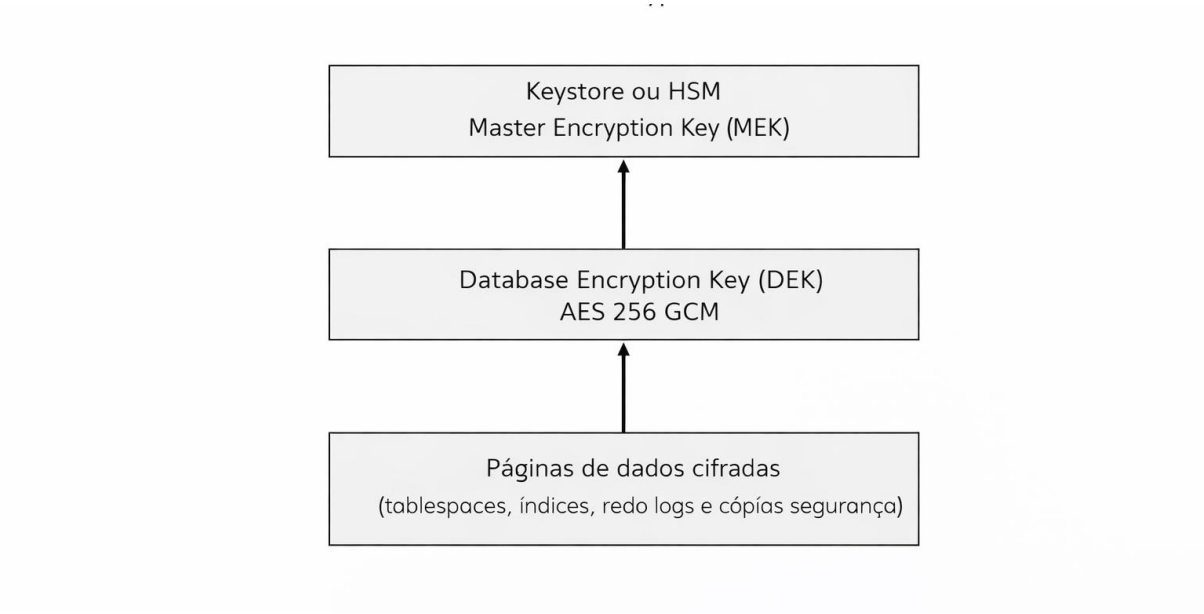
Estes mecanismos alinham-se com as recomendações da *ISO 27001*, do *ENISA Risk Management Toolkit* e da publicação *NIST SP 800 30*, formando um quadro abrangente que combina prevenção, deteção e resposta [1][12][16]. A investigação empírica desenvolvida neste trabalho centra-se na eficácia da camada de encriptação *Transparent Data Encryption* quando implementada em *Oracle 19c*, avaliando o equilíbrio entre segurança, desempenho e conformidade regulatória.

2.6.2 Arquitetura de chaves

O mecanismo segue a arquitetura de ***envelope encryption***. Existem duas chaves principais:

- **Database Encryption Key (DEK)**, simétrica, criada pelo administrador e utilizada pelo motor para cifrar e decifrar blocos de dados em tempo real.
- ***Master Encryption Key* (MEK)**, assimétrica, empregada apenas para proteger (cifrar) a DEK e armazenada separadamente numa carteira segura (Oracle *Wallet*) ou num módulo *Hardware Security Module* (HSM) externo.

Figura 3: Arquitetura hierárquica das chaves na Transparent Data Encryption



Fonte: Autor

- **MEK.** Reside na *wallet* ou num módulo HSM; nunca permanece em texto simples no disco de dados.
- **DEK.** Chave simétrica protegida pelo MEK (*envelope encryption*) e guardada no cabeçalho do *tablespace*.
- **Fluxo de E/S.**
    - Escrita: página → cifra AES → disco.
    - Leitura: disco → decifra AES → *buffer cache* → aplicação.

2.6.3 Ciclo de vida operativo

Tabela 2: Ciclo de vida operativo da Transparent Data Encryption(TDE)

Fase	Comando principal	Descrição operacional
Inicialização	ADMINISTER KEY MANAGEMENT	Cria ou abre a carteira de chaves (wallet ou keystore) e gera a *Master Encryption Key* (MEK), responsável por proteger as chaves de dados.
Ativação	ALTER SYSTEM SET ENCRYPTION KEY ALTER TABLESPACE … ENCRYPT	Ativa a encriptação e cifra os blocos de dados já existentes em segundo plano, sem necesssidade de indisponibilidade da base de dados.
Rotação	SET ENCRYPTION KEY IDENTIFIED BY …	Realiza a rotação da chave de encriptação de dados de forma online, mantendo versões anteriores para garantir a leitura de blocos cifrados com chaves→ antigas.
Cópias de segurança	RMAN BACKUP AS COMPRESSED ENCRYPTED	Gera cópias de segurança comprimidas e cifradas, assegurando que os ficheiros de backup permanecem protegidos fora da instância Oracle.
Restauração	Abrir a carteira de chaves + RESTORE DATABASE	Permite restaurar a base de dados. Sem a carteira de chaves aberta, a instância inicia, mas não consegue aceder aos *tablespaces* cifrados.

Fonte: Autor

1. **Inicialização**

   Executa-se o comando *ADMINISTER KEY MANAGEMENT*, que cria (ou abre, caso já exista) a carteira de chaves (*wallet*) onde é armazenada a *Master Encryption Key* (MEK). Nesta fase é gerada a própria MEK, que será utilizada para proteger a *Database Encryption Key* (DEK).

2. **Ativação**

   Através de *ALTER SYSTEM SET ENCRYPTION KEY* e, quando aplicável, *ALTER TABLESPACE … ENCRYPT*, o *Oracle Database* aplica a encriptação aos blocos já existentes em segundo plano. Este mecanismo garante que todo o *tablespace passe* a estar cifrado sem necessidade de desligar a base de dados ou interromper o serviço.

3. **Rotação**

   Com o comando *SET ENCRYPTION KEY IDENTIFIED BY …*, procede-se à rotação da DEK de forma totalmente online, preservando versões anteriores da chave para permitir a leitura de páginas cifradas em ciclos anteriores. Este processo é executado em modo *hot*, sem impacto significativo no funcionamento da instância.

4. **Cópias de segurança**

   Ao emitir *RMAN BACKUP AS COMPRESSED ENCRYPTED*, as cópias de segurança são produzidas já cifradas, garantindo que o ficheiro gerado não expõe dados sensíveis mesmo que seja capturado ou movido para um ambiente não confiável.

5. **Restauração**

   Para recuperar a base de dados, basta abrir novamente a carteira de chaves com *ADMINISTER KEY MANAGEMENT* (ou comando equivalente) e executar *RESTORE DATABASE*. Sem a carteira, o servidor consegue iniciar, mas não é capaz de ler os *tablespaces* cifrados, impossibilitando qualquer acesso à informação protegida.

2.6.4 Evolução histórica

Tabela 3: Evolução histórica da Transparent Data Encryption

Versão	Marco	Algoritmos suportados	Funcionalidades novas
10g R2 (2006)	TDE por coluna	3DES, AES-128	Cria ou abre a carteira de chaves (*wallet ou* keystore) e gera a *Master Encryption Key* (MEK), responsável por proteger as chaves de dados de dados.
11g (2007)	TDE por tablespace	AES-256	Ativa a encriptação e cifra os blocos de dados já existentes em segundo plano, sem necessidade de indisponibilidade da base de dados.
12c (2013)	Ambiente multitenant	AES-192/256	Comando unificado de gestão de chaves.
18c (2018)	Otimização da cache de chaves	AES-256-GCM	Aceleração AES-NI.
19c (2019)	Suporte de Key Store externo	AES-256-GCM	Auto-logout da carteira de chaves e integração com HSM.
19c (2019)	Suporte de Key Store externo	AES-256-GCM	Permite restaurar a base de dados. Sem a carteira de chaves aberta, a instância inicia, mas não consegue aceder aos *tablespaces cifrados*.

Fonte: Autor

- **10g R2 (2006)**: estreia do TDE ao nível de coluna, suportando algoritmos 3DES e AES-128, e armazenamento da *Master Encryption Key* (MEK) num simples ficheiro-*wallet*.
- **11g (2007)**: extensão para cifrar *pagespaces* inteiros (tablespaces) e introdução do AES-256, com integração nativa no RMAN para *backups* cifrados em linha.

- **12c (2013)**: adaptação ao novo ambiente *multitenant*, permitindo gerir chaves de forma unificada (tanto para PDBs como para o *container*), e alargamento para AES-192/256.
- **18c (2018)**: melhoria na eficiência através de cache otimizada de chaves e passagem ao modo autenticado AES-256-GCM, tirando partido de acelerações por *hardware* (AES-NI).
- **19c (2019)**: suporte oficial a *Key Stores* externas (HSMs ou KMS em nuvem), com AES-256-GCM, auto-logout da wallet e integração *out-of-the-box* com módulos de segurança física.

2.6.5 Vantagens da Encriptação Transparente de Dados

Cobertura integral dos ficheiros de armazenamento

A *Transparent Data Encryption* cifra automaticamente *tablespaces*, *redo logs*, ficheiros temporários e cópias de segurança geradas pelo *Recovery Manager*. Não é necessária qualquer etapa adicional no processo de cópia de segurança ou na exportação de dados para que a informação saia protegida [18]. Esta abrangência reduz o risco de existirem segmentos não cifrados, uma limitação frequente em abordagens manuais de encriptação ao nível da coluna.

Transparência para as aplicações

A ativação da TDE é realizada através de comandos *Structured Query Language* padrão e não exige alterações ao código fonte nem recompilação de objetos *Procedural Language SQL*. Esta característica simplifica projetos de adaptação em sistemas legados e reduz custos de manutenção contínua, alinhando se com o princípio da segurança por defeito recomendado pelo Regulamento Geral sobre a Proteção de Dados e pelas orientações da *European Union Agency for Cybersecurity* [13][12].

Desempenho otimizado com aceleração de hardware

Quando o processador dispõe de instruções de aceleração criptográfica, como *Advanced Encryption Standard New Instructions* em arquiteturas Intel ou *Cryptography Extensions* em arquiteturas ARM, a operação de encriptação acrescenta menos de dez por cento de sobrecarga em cargas transacionais e analíticas típicas [17][15]. A cache interna de chaves introduzida no Oracle *Database* 19c reduz a latência associada à desencriptação, tornando o impacto praticamente impercetível para os utilizadores finais.

Integração nativa com outros controlos Oracle

A TDE integra-se nativamente com outros mecanismos de segurança do Oracle Database. O *Database Vault* impede o acesso a dados aplicacionais mesmo por utilizadores com privilégios administrativos. O *Unified Audit* regista eventos de encriptação e acessos em trilhas de auditoria imutáveis, facilitando a prestação de contas exigida por normas como a *PCI DSS* e a *Sarbanes Oxley Act*. O *Oracle Key Vault* ou um módulo de segurança de hardware externo permitem alojar a chave mestra fora do sistema de gestão de bases de dados, reforçando a governação do ciclo de vida das chaves e possibilitando a aplicação de controlo dual.

Conformidade regulamentar simplificada

A cifra em repouso é exigida ou recomendada por diversos diplomas regulatórios, nomeadamente o Regulamento Geral sobre a Proteção de Dados (artigo 32), a norma *PCI DSS* 4.0 (requisito 3), a *Health Insurance Portability and Accountability Act* (secção 164.312) e a Diretiva *NIS 2* (artigo 21) [13][14][19][12].

A adoção da *Transparent Data Encryption*, validada por relatórios de auditoria, permite demonstrar conformidade com estes enquadramentos legais sem necessidade de recorrer a soluções externas adicionais.

2.6.6 Limitações e desafios

Tabela 4: Limitações da TDE e respetivas estratégias de mitigação

Área	Limitação	Mitigação
Dados em trânsito	Não cifra o tráfego de comunicação do Oracle Database	*Transport Layer Security* ou *Native Network Encryption
Ataque lógico	Administrador autenticado pode aceder a dados decifrados	*Oracle Database Vault* e separação de funções
Memória	Páginas decifradas ocupam memória adicional	Gestão de cache e nós dedicados
I/O	Operações de cifragem e decifragem em cada leitura e escrita	Processadores com AES NI* e compressão de tabelas
Gestão de chaves	Perda da carteira de chaves implica perda de acesso aos dados	Cópias de segurança seguras da carteira ou utilização *Hadwáre Module*
Gestão de chaves	Perda da carteira de chaves implica perda de acesso aos dados	Cópias de seguranca seguras da carteira ou utilização de *Hardware SecuriyM*

Fonte: Autor

2.6.7 Integração com outras funcionalidades Oracle

- ***Database Vault*** impede DBAs de aceder ao conteúdo, mantendo privilégios de administração.
- ***Data Redaction / Masking*** completa a proteção de dados *in-use*.
- ***Unified Audit*** cria trilhos imutáveis, essenciais para RGPD e NIS 2.
- ***Oracle Key Vault*** centraliza o MEK e aplica políticas de duplo controle [29].

2.6.8 Síntese crítica

A TDE apresenta-se como solução intermédia: assegurar a confidencialidade dos ficheiros em repouso com impacto de desempenho controlado e sem refatoração da aplicação. Todavia, depende de gestão de chaves robusta e de camadas adicionais contra-ataques lógicos. Estas características justificam os ensaios empíricos descritos no Capítulo 4, onde se medirá o custo-benefício da TDE em Oracle 19c.

2.7 Comparação entre Transparent Data Encryption(TDE) e outras soluções de encriptação

2.7.1 Universo de soluções analisadas

1. **TDE**: encriptação automática de ficheiros de dados e *redo/undo logs* no próprio motor (Oracle, SQL Server).
2. ***Always Encrypted*** – encriptação lato-cliente; os dados chegam cifrados ao SGBD, a chave fica na aplicação.
3. **Encriptação por coluna/campo** – *functions* do SGBD ou *middleware* que cifram atributos selecionados.
4. ***Full-Disk Encryption*** – camada de sistema operativo ou *hypervisor* que protege todo o volume físico.
5. **Encriptação ao nível da aplicação** – a lógica de negócio cifra antes do envio; o SGBD atua como *blind store*[30].

2.7.2 Quadro comparativo

Tabela 5: Comparação entre Transparent Data Encryption (TDE) e outras estratégias de encriptação.

Critério	TDE	Always Encrypted (SQL Server)	Cifra a nível de coluna	Full-Disk	Aplicação
Dados em repouso	Sim	Sim	Parcial	Sim	Sim
Dados em tránsito	Não	Não	Sim	Sim	Sim
Dados em uso	Não	Não	Não	Não	Sim
Alteração na aplicação	Nenhuma	Requerida	Geralmente requerida	Nenhuma	Elevada
Overhead típico	2-10 % CPU / IO	10-30 % CPU	5-20 %	Residual	Variável
Controlo granular	Não	Sim	Sim	Sim	Sim
Backups	Cifrados	Dependem da coluna	Cifrados	Cifrados	Cifrados
Gestão de chaves	Wallet / HSM	Cliente / KMS	DB ou aplicação	SO / TPM	Aplicação
Casos de uso	Conformidade normativa,	Dados muito sensíveis, zero-trust	*Regulamento Geal de Proteção de Dados*	Proteção física	FinTech, saúde

Fonte: Autor

2.7.3 Análise crítica dos *trade-offs*

- **Transparência versus controlo**. TDE é virtualmente invisível para a aplicação, mas não impede que um DBA autenticado leia os dados em memória. *Always Encrypted* coloca a chave fora do SGBD, oferecendo modelo *zero-trust*, à custa de perdas em *querying* (por exemplo, *LIKE, ORDER BY*).
- **Granularidade**. Se apenas duas ou três colunas contêm PII, a encriptação por campo minimiza sobrecarga; em bases densas em dados sensíveis, TDE simplifica a gestão.
- **Desempenho**. Estudos públicos apontam *overhead* inferior a dez por cento em TDE com *hardware* AES-NI, enquanto *Always Encrypted* pode exceder trinta por cento devido à encriptação no cliente e à impossibilidade de uso de índices nativos [31].
- **Gestão de chaves**. Soluções fora do SGBD transferem responsabilidade para as equipas de desenvolvimento; TDE mantém-na na esfera do DBA, o que simplifica operações mas cria dependência da *wallet* ou HSM.

- **Conformidade**. Todas as opções respondem ao RGPD se corretamente configuradas. Contudo, o modelo operacional simples da TDE é frequentemente preferido em auditorias PCI-DSS ou NIS 2, pois cobre também *backups* sem processos adicionais [32].

2.7.4 Critérios de seleção para ambientes empresariais

Tabela 6: Critérios de seleção e soluções de encriptação recomendadas

Requisito prioritário	Solução recomendada
Zero acesso do DBA a texto--claro	Always Encrypted ou encriptação ao nível da aplicação
Time-to-market mínimo	TDE ou Full-Disk
Controlo coluna-a-coluna	Encriptação por campo ou Always Encrypted
Carga de I-O elevada	TDE com AES-NI ou Full-Disk
Ambiente multitenant	TDE (suporte nativo CDB/PDB)
Sistemas legados	Full-Disk ou encriptação por coluna
Sistemas legados	Full-Disk ou encriptação por coluna

Fonte: Autor

2.8 Regulamentação aplicável à proteção de dados

A adoção de encriptação em repouso, nomeadamente através da *Transparent Data Encryption(TDE)* aliada a outros controlos Oracle, responde a obrigações impostas por vários diplomas legais e normativos. Segue-se um mapeamento sucinto entre os principais requisitos e os mecanismos descritos nas secções anteriores.

2.8.1 Regulamento Geral sobre a Proteção de Dados (RGPD)

Artigo 32.º – Segurança do tratamento
Requer a adoção de "medidas técnicas adequadas", citando explicitamente a encriptação e a pseudonimização como salvaguardas recomendadas.
Cobertura no Oracle: TDE cifra dados e cópias de segurança; *Data Redaction* e *Data Masking* aplicam minimização em tempo real.

Artigo 34.º – Notificação de violações aos titulares
Permite dispensar a notificação individual sempre que os dados comprometidos estejam "ininteligíveis" graças a encriptação forte.
Efeito prático: Se os ficheiros exfiltrados estiverem protegidos pela DEK, a organização reduz custos reputacionais e obrigações legais.

Artigo 5.º – Princípios de integridade e confidencialidade
Estabelece a exigência de rastreabilidade nas operações de tratamento de dados.
Cobertura: *Unified Audit* gera trilhas imutáveis de auditoria; *Database Vault* impede o abuso de privilégios administrativos.

2.8.2 Diretiva (UE) 2022/2555 (NIS 2)

Artigo 21.º – Medidas de gestão de risco

Impõe a existência de uma política de encriptação e gestão de chaves ajustada ao grau de criticidade da informação.

Cobertura: Oracle *Key Vault* ou HSM externo permite controlo dual, rotação documentada e segregação de funções.

Artigo 23.º – Relato de incidentes

Estabelece que violações graves devem ser comunicadas às autoridades competentes no prazo de 24 horas.

Contributo da arquitetura: A geração de *logs* unificados e a integração com sistemas SIEM aceleram a deteção e a resposta.

2.8.3 PCI-DSS 4.0 (dados de cartões)

Requisito 3 – Proteção de dados do titular em repouso

Exige a utilização de encriptação forte (como AES-256) para proteger tabelas, ficheiros temporários e cópias de segurança.

Cobertura: *Transparent Data Encryption* cifra automaticamente os *tablespaces, redo logs e backups* gerados pelo RMAN.

Requisito 10 – Registos de auditoria

Determina a existência de uma trilha imutável que registe todos os acessos e eventos relevantes.

Cobertura: *Unified Audit* e *Audit Vault* armazenam eventos assinados que garantem a integridade da auditoria.

Requisito 12 – Política de gestão de chaves

Impõe a rotação periódica das chaves e a documentação completa dos respetivos ciclos de vida.

Cobertura: O comando *ADMINISTER KEY MANAGEMENT* permite rotacionar a DEK sem interrupções; o Oracle *Key Vault* conserva o histórico completo das chaves.

2.8.4 *HIPAA Security Rule* (secção 164.312)

A *Health Insurance Portability and Accountability Act* (HIPAA), através da sua *Security Rule*, estabelece requisitos técnicos para a proteção da *Electronic Protected Health Information* (*ePHI*), exigindo a implementação de mecanismos de encriptação adequados para salvaguardar dados clínicos eletrónicos.

Neste contexto, a *Transparent Data Encryption(TDE)* assegura a encriptação dos dados em repouso utilizando o algoritmo *Advanced Encryption Standard* com chave de 256 bits no modo *Galois Counter Mode*. Adicionalmente, o *Oracle Database Vault* permite definir *realms* que segregam registos clínicos sensíveis, restringindo o acesso mesmo a utilizadores com privilégios administrativos.

A HIPAA impõe ainda requisitos de autenticação robusta e de controlo da integridade dos registos eletrónicos. Estes requisitos são suportados pelo *Oracle Database* através da integração de autenticação multifatorial e da verificação criptográfica de integridade proporcionada pelo modo *Galois Counter Mode*, que permite detetar qualquer alteração não autorizada aos dados armazenados.

2.8.5 *Sarbanes Oxley* (secção 404)

A *Sarbanes Oxley Act*, na sua secção 404, impõe a retenção inviolável de registos financeiros e a rastreabilidade completa das alterações efetuadas nos sistemas de informação. Estes requisitos visam garantir transparência, controlo interno eficaz e capacidade de auditoria sobre dados financeiros críticos.

A conformidade pode ser demonstrada através da combinação da *Transparent Data Encryption*, que impede a manipulação direta dos ficheiros físicos da base de dados, com o *Unified Audit*, que associa cada acesso ou alteração a um utilizador autenticado e gera trilhas de auditoria imutáveis. Em conjunto, estes mecanismos permitem cumprir as exigências de integridade e responsabilização definidas pela *Sarbanes Oxley*.

2.9 Integração da Transparent Data Encryption numa arquitetura de defesa em profundidade

A encriptação de dados em repouso é eficaz na mitigação de riscos associados à perda ou exfiltração de ficheiros físicos, mas não elimina outros vetores de ataque, como o abuso de privilégios ou a exposição de dados em memória. Por este motivo, a Oracle recomenda a integração da *Transparent Data Encryption* com camadas adicionais de controlo de segurança, adotando uma abordagem de defesa em profundidade.

Esta estratégia combina encriptação, auditoria, controlo de acessos privilegiados e gestão centralizada de chaves, permitindo responder simultaneamente a requisitos regulatórios de confidencialidade, rastreabilidade e governação de chaves [18].

2.9.1 Gestão centralizada de chaves com Oracle Key Vault ou HSM

O *keystore* externo separa a *Master Encryption Key* (MEK) do próprio motor de base de dados, reduzindo o risco de acesso não autorizado.

- **Controlo duplo**: a abertura ou rotação da chave exige dois administradores distintos, alinhando-se ao princípio de separação de funções exigido pelo RGPD e pela NIS 2 [13][12].
- **Rotação documentada**: registos de emissão, revogação e rotação ficam armazenados de forma imutável, facilitando auditorias de PCI-DSS (Requisito 3) [14].

2.9.2 Separação de deveres com Database Vault

O *Database Vault* cria barreiras de acesso que impedem administradores de sistema de ler dados aplicacionais enquanto ainda lhes permite executar tarefas de manutenção.

- ***Realms***: definem zonas protegidas onde apenas aplicações de negócio podem consultar tabelas sensíveis.
- ***Command Rules***: bloqueiam operações de risco fora de janelas autorizadas.

Esta camada atenua o risco interno, citado pelo IBM X-Force como fonte crescente de incidentes em bases de dados [11].

2.9.3 Monitorização e responsabilidade com Unified Audit e Audit Vault

O *Unified Audit* regista cada comando SQL, evento de encriptação ou abertura de carteira numa trilha única e imutável.

- **Integração com SIEM**: permite correlação em tempo real de tentativas de acesso indevido.
- **Cobertura PCI**: cumpre o Requisito 10 da PCI-DSS, que exige *logs* completos e invioláveis [14].

Quando integrado ao *Audit Vault*, os registos são consolidados e assinados, garantindo autenticidade para fins forenses.

2.9.4 Proteção de dados em uso: Data Redaction e Masking

Embora o TDE atue sobre dados em repouso, informações sensíveis podem aparecer no ecrã ou ser exportadas por aplicações.

- ***Data Redaction*** oculta parcial ou totalmente valores em tempo de execução, sem alterar a lógica SQL.
- ***Data Masking*** cria cópias anonimizadas, úteis em ambientes de teste, reduzindo a exposição de dados reais.

Estas técnicas implementam o princípio de minimização de dados previsto no artigo 5 do RGPD [13].

2.9.5 Controlos de perímetro no nível de base de dados

- **Oracle *Database Firewall***: inspeciona o tráfego SQL e bloqueia padrões maliciosos, complementando *firewalls* de rede tradicionais.
- ***Virtual Private Database***: aplica filtros dinâmicos a linhas e colunas, restringindo o alcance das consultas sem necessidade de visões ou tabelas auxiliares.

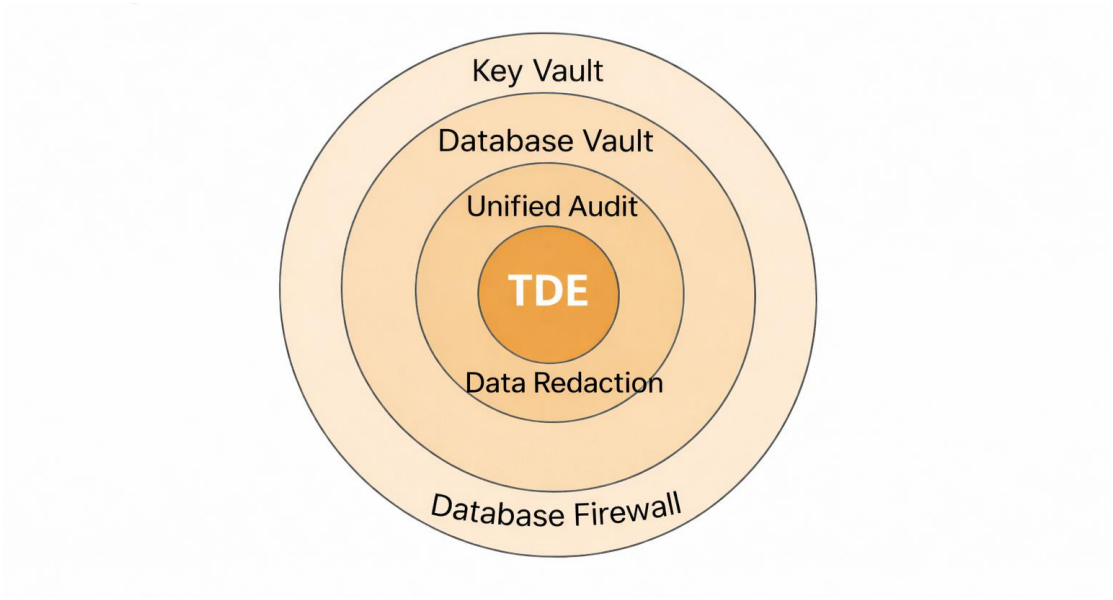
Estes controlos reduzem a probabilidade de SQL *injection* e exfiltração seletiva de dados.

2.9.6 Benefícios combinados da arquitetura em camadas

Ao integrar a TDE com os módulos acima, obtém-se:

1. **Confidencialidade física** com cifra em repouso.
2. **Confidencialidade lógica** com filtros VPD e *realms* do *Database Vault*.
3. **Responsabilidade e rastreabilidade** através de *Unified Audit* e registos de chave no Key Vault.
4. **Redução de superfície de ataque** por meio de *firewall* SQL e minimização de dados exibidos.

Figura 4: Defesa em profundidade no Oracle *Database* 19c



Fonte: Autor

Esta arquitetura endereça simultaneamente os requisitos de confidencialidade, integridade, disponibilidade e responsabilidade estabelecidos pelas normas ISO 27000, pelo RGPD, pela NIS 2 e pela PCI-DSS, fornecendo uma base robusta para ambientes que processam dados críticos.

2.10 Lacunas identificadas na literatura

A revisão sistemática evidencia uma produção académica e técnica consolidada em torno dos modelos de segurança, fundamentos da encriptação e enquadramento regulamentar. No entanto, identificam-se lacunas significativas, sobretudo no que respeita à aplicação prática desses conceitos na versão 19c do Oracle *Database*, atualmente predominante em ambientes empresariais [9].

Medição empírica de desempenho em Oracle 19c

A maior parte dos estudos de *benchmark* concentra-se em versões anteriores ou noutros SGBD, como SQL *Server* (Madyatmadja et al., 2021) [17]. Dados robustos sobre a sobrecarga real do AES-256-GCM na 19c, considerando cargas mistas OLTP/OLAP, permanecem escassos.

Integração de TDE com serviços externos de gestão de chaves

Embora a literatura descreva boas práticas associadas à utilização de módulos de segurança de hardware e serviços de gestão de chaves, faltam análises quantitativas sobre a latência adicional, os custos operacionais e os riscos de falhas de sincronização de carteiras em cenários que envolvem *Oracle Data Guard* ou *Real Application Clusters* distribuídos por múltiplas zonas de disponibilidade.

Impacto em ambientes de computação em nuvem híbridos e bases de dados como serviço

Relatórios produzidos por fornecedores abordam a utilização da *Transparent Data Encryption* na *Oracle Cloud Infrastructure*, contudo são escassos os estudos independentes que comparem ambientes locais, infraestruturas como serviço e bases de dados como serviço utilizando métricas homogéneas. Questões como a partilha de responsabilidades na gestão da carteira de chaves e a migração segura de chaves entre diferentes provedores de nuvem permanecem insuficientemente documentadas.

Avaliação do custo benefício regulatório

Diversos autores referem que a TDE contribui para o cumprimento de enquadramentos como o Regulamento Geral sobre a Proteção de Dados, a norma *PCI DSS* e a Diretiva *NIS 2*. No entanto, não existem métricas consolidadas que quantifiquem de forma objetiva a redução do esforço de auditoria, em termos de tempo e recursos, ou a diminuição dos custos associados à resposta a incidentes quando a encriptação está ativa.

Gestão operacional pós incidente

A literatura reporta casos de perda irrecuperável de dados resultante da corrupção ou perda da carteira de chaves, mas carece de estudos aprofundados sobre procedimentos operacionais robustos. Em particular, faltam análises relativas a estratégias de cópia de segurança da carteira, testes regulares de restauração e mecanismos de custódia de chaves em contextos que envolvem múltiplas equipas administrativas.

Interação entre a TDE e otimizações avançadas de desempenho

Existem poucos trabalhos que avaliem de forma sistemática a compatibilidade da encriptação em repouso com funcionalidades avançadas de otimização de desempenho, como o *Automatic Indexing*, o *In Memory Column Store* ou o *Exadata Smart Scan*, especialmente no que respeita ao impacto combinado em latência e consumo de recursos.

3. Metodologia

Esta investigação adota a ***Design Research Methodology*** **(DRM)** como estrutura macro, integrando um **desenho quase-experimental** para a fase de avaliação técnica. Esta combinação permite não só desenhar um procedimento de *benchmarking* rigoroso, mas também validar a sua eficácia através de ensaios práticos num ambiente controlado.

O projeto organiza-se nas seguintes fases:

Enquadramento Metodológico

A escolha da DRM justifica-se pela natureza técnica desta dissertação, que visa resolver um problema identificado: a escassez de métricas empíricas atualizadas para a versão 19c do Oracle *Database*. Seguindo os princípios de Peffers et al. (2007), o trabalho foca-se no desenvolvimento de um artefacto (neste caso, um *framework* de testes de performance) e na sua subsequente avaliação.

Fase 1: Estudo da Literatura e Levantamento de Requisitos

Nesta fase inicial, procedeu-se à revisão de *white papers*, documentação de fornecedores (Oracle, Microsoft) e artigos de investigação. O objetivo foi compreender a arquitetura interna da TDE e identificar os *benchmarks* e algoritmos (como o AES-256-GCM) que servem de base ao estado da arte.

Fase 2: Desenho do Framework de Benchmarking

Com base na literatura, estabeleceu-se o modelo de avaliação que responde às lacunas identificadas. O *framework* define a utilização do *workload* **TPC-C** (através do HammerDB) e a seleção de métricas críticas de sistema (CPU, I/O e RAM), garantindo que o procedimento de teste é replicável e cientificamente válido.

Fase 3: Avaliação (Desenho Quase-Experimental)

A validação do *framework* foi realizada através de um **desenho quase-experimental aplicado num ambiente laboratorial controlado**. O objetivo central foi quantificar o impacto da *Transparent Data Encryption* (TDE) no desempenho da base de dados Oracle 19c *Enterprise Edition.*

A abordagem combina a comparação "antes e depois", executando os testes em dois cenários distintos:

1. **Cenário Baseline:** Instância operando sem encriptação para estabelecer o desempenho de referência.
2. **Cenário Experimental:** A mesma instância após a ativação da TDE, mantendo todas as outras variáveis de hardware e configuração rigorosamente constantes.

Este desenho metodológico permite isolar o efeito da encriptação e extrair evidência empírica sobre o seu impacto real, respondendo diretamente aos objetivos traçados no Capítulo 1.

3.1 Ambiente Experimental

Os testes foram realizados numa máquina virtual dedicada, garantindo isolamento e repetibilidade. Todo o *software* necessário foi instalado de raiz para assegurar consistência entre execuções.

O ambiente de testes inclui:

• Máquina virtual com 2 vCPUs, 6.6 GB de RAM e armazenamento dividido entre o sistema operativo e o diretório de dados Oracle.
• Oracle Linux 8.9 com kernel UEK 6.
• Oracle Database 19c Enterprise Edition, configurado como Container Database (CDB) com uma PDB dedicada ao estudo.
• Ferramentas de monitorização de baixo nível (vmstat e iostat).
• AWR (Automatic Workload Repository) com snapshots a cada 15 minutos.
• HammerDB 4.3 com *workload* TPC-C para simulação de transações OLTP.

A configuração foi mantida rigorosamente constante ao longo de todos os testes. Qualquer diferença observada entre cenários resulta exclusivamente da ativação da TDE.

3.2 Preparação dos Dados e Estrutura da Base de Dados

Para suportar os testes foi criado um *tablespace* dedicado (TBS_BENCH), inicialmente não encriptado. Este *tablespace* foi posteriormente encriptado com AES-256 durante a fase experimental.

O *schema* TPC-C foi carregado com aproximadamente 4 GB de dados distribuídos pelas principais tabelas do *benchmark* (*CUSTOMER, ORDERS, ORDER_LINE, STOCK* e *WAREHOUSE*), representando uma carga transacional realista. O *workload* TPC-C foi configurado com 50 *warehouses* e 32 virtual users, permitindo gerar transações em volume suficiente para medir diferenças de desempenho entre cenários.

3.3 Procedimento de Testes

Os testes foram organizados em quatro fases independentes.

Fase 0 – Preparação

Incluiu:

• Instalação do sistema operativo
• Instalação do Oracle 19c
• Criação da CDB e da PDB
• Configuração do AWR
• Criação do *tablespace* TBS_BENCH
• Instalação do HammerDB
• Carga completa dos dados TPC-C

Esta fase estabeleceu um ambiente limpo e reprodutível.

Fase 1 – Testes *Baseline* (sem TDE)

A base de dados operou sem qualquer encriptação. Para cada execução:

1. Foi limpo o *page cache* do sistema
2. Criou-se um *snapshot* AWR inicial
3. Iniciou-se monitorização contínua (vmstat, iostat)
4. Executou-se o *workload* TPC-C durante 30 minutos
5. Criou-se um *snapshot* AWR final
6. Foram recolhidas métricas de CPU, I/O e *wait event*s

Esta fase estabeleceu o desempenho de referência.

Fase 2 – Ativação da TDE

A ativação da TDE incluiu:

• Configuração dos parâmetros *wallet_root* e *tde_configuration*
• Criação do *keystore* baseado em ficheiros
• Geração da chave-mestra (AES-256)
• Encriptação online do *tablespace* TBS_BENCH
• Reinício controlado da instância

Fase 3 – Testes com TDE Ativada

Após a encriptação do *tablespace*, todo o procedimento da Fase 1 foi repetido de forma idêntica, permitindo comparação direta entre cenários.

Fase 4 – Testes de Segurança

Foram realizados dois testes adicionais:

• Criação de um *backup* RMAN encriptado e verificação da sua integridade
• Simulação de ataque físico, copiando o *datafile* encriptado para fora do ambiente Oracle e tentando extrair texto em claro através do utilitário *strings.*

Estes testes avaliaram a eficácia da TDE como medida de proteção de dados em repouso.

3.4 Métricas Recolhidas

As métricas foram recolhidas de três fontes:

• HammerDB: *throughput* (NOPM e TPM), quando disponível
• vmstat/iostat: CPU *user, system, wait I/O, idle*, utilização de memória, *context switches,* leituras e escritas por segundo
• AWR: *wait events, logical reads, physical reads*, CPU *time* e *DB time*

As métricas foram selecionadas de modo a permitir uma análise detalhada do impacto da TDE no desempenho da carga transacional.

4.0 Trabalho Prático e Resultados

4.1 Introdução aos Resultados

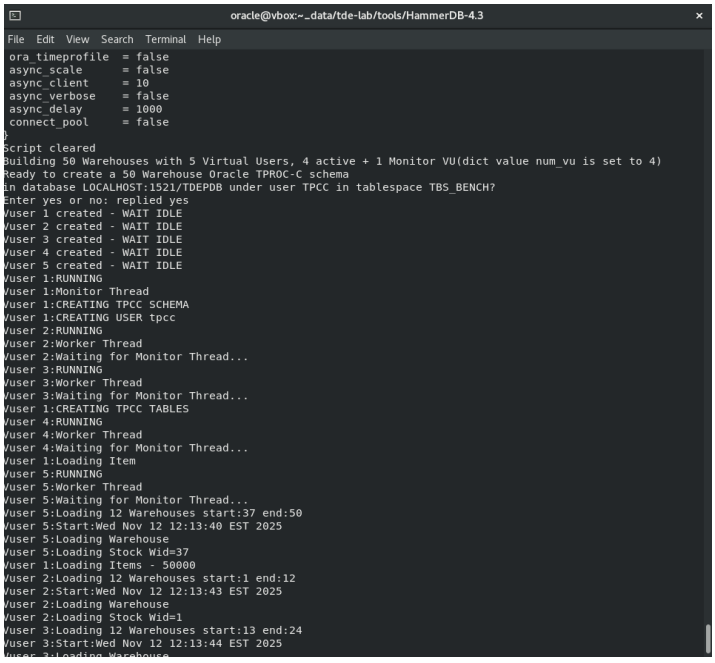
Este capítulo apresenta os resultados obtidos nos ensaios experimentais realizados sobre o Oracle Database 19c, nos cenários sem TDE (baseline) e com TDE ativada. Os resultados incluem métricas de desempenho (CPU, I/O, waits), throughput transacional (TPC-C via HammerDB), efeitos da encriptação no consumo de recursos e validação da eficácia da TDE enquanto mecanismo de proteção dos dados em repouso.
Os detalhes completos de configuração e todos os registos visuais encontram-se organizados nos Anexos A a C.

4.2 Resultados Baseline (Sem *Transparent Data Encryption*)

4.2.1 Execução do *Benchmark* TPC-C

O *benchmark* TPC-C foi executado durante 30 minutos, com 32 utilizadores virtuais. A Figura 5 apresenta o ecrã inicial do HammerDB no momento do arranque da carga.

Figura 5 - Execução do *Benchmark* TPC-C



Fonte: Autor

Todos os restantes passos operacionais – construção do *schema, snapshots* iniciais, criação de dados e resultados intermédios – encontram-se no **Anexo B**.

Os valores reportados pelo HammerDB foram:

```
NOPM: 825

TPM: 1659

Estado: SUCCESS
```

4.2.2 Utilização de CPU

Durante o ensaio sem TDE, o consumo médio de CPU foi:

```
User:        6.64%

System:     23.76%

Wait I/O:   36.18%

Idle:       24.79%

Total Used: 66.59%
```

4.2.3 Principais *Wait Events*

O relatório AWR identificou:

- *db file sequential read* – 38%
- *log file sync* – 37%
- *free buffer waits* – 7%

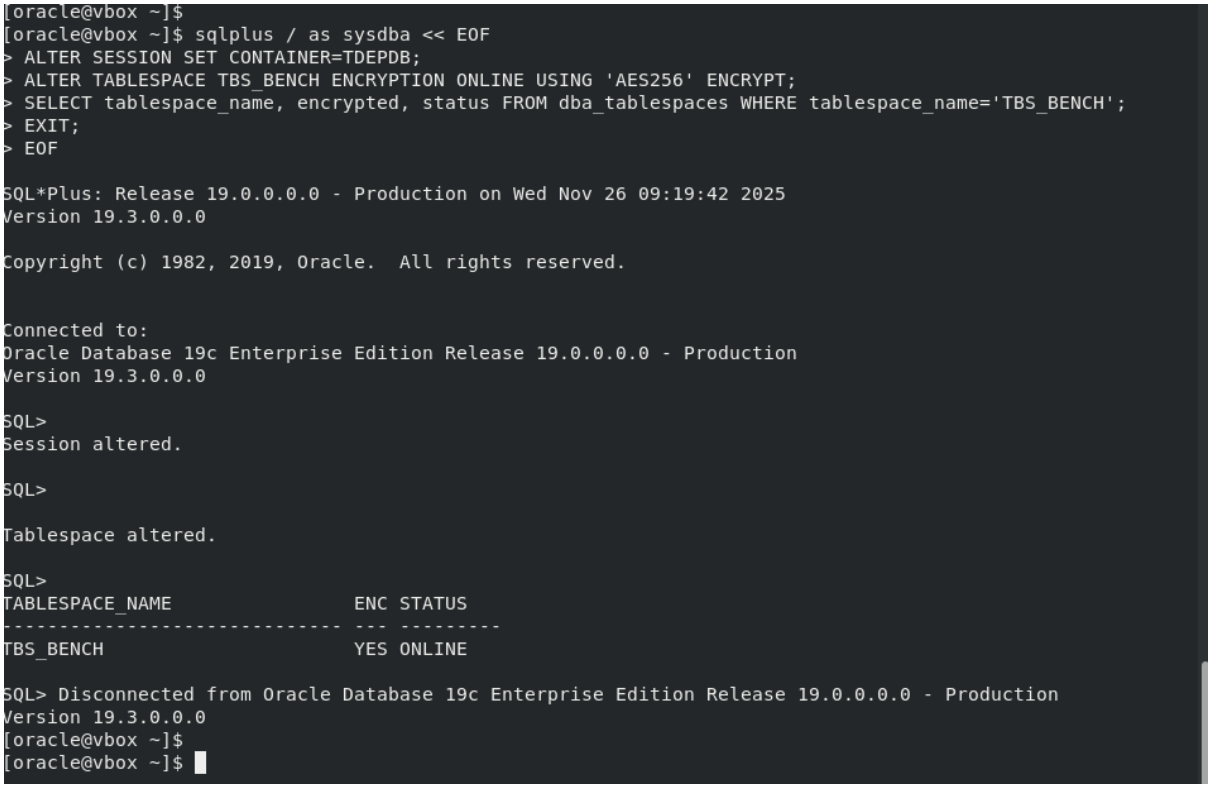
  Os *snapshots* e relatório AWR completos estão no **Anexo B**.

4.3 Resultados com TDE Ativada

4.3.1 Prova da Encriptação do *Tablespace*

A Figura 6 apresenta o momento em que o *tablespace* TBS_BENCH foi totalmente encriptado com AES-256

Figura 6 – Encriptação online do *tablespace* TBS_BENCH após ativação da TDE.



Fonte: Autor

Outros *screenshots* como:

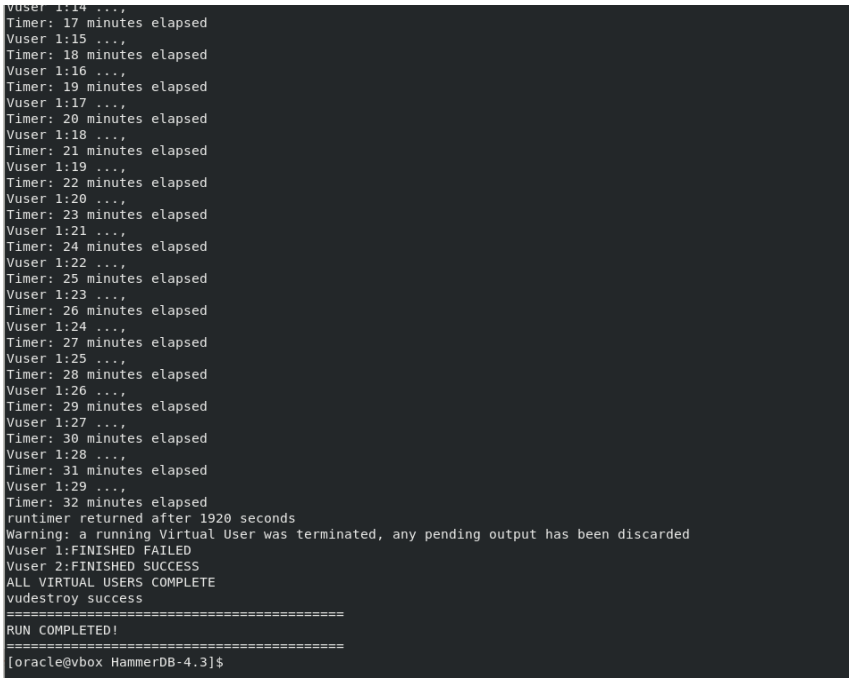
- Configuração do *keystore*
- *Keystore* aberto
- Parâmetros *Transparent Data Encryption*

  → ficam todos nos **Anexos.**.

4.3.2 Execução do *Benchmark* TPC-C com TDE

A Figura 7 mostra o momento de execução da carga após ativação da TDE.

Figura 7 – Execução do *workload* TPC-C com TDE ativa.



Fonte: Autor

Resultados combinados com duas execuções:

```
CPU Total Média: 73.07%

CPU User:        15.33%

CPU System:      28.72%

CPU Wait I/O:    29.02%

Idle:            18.28%
```

4.4 Comparação *Baseline* vs TDE

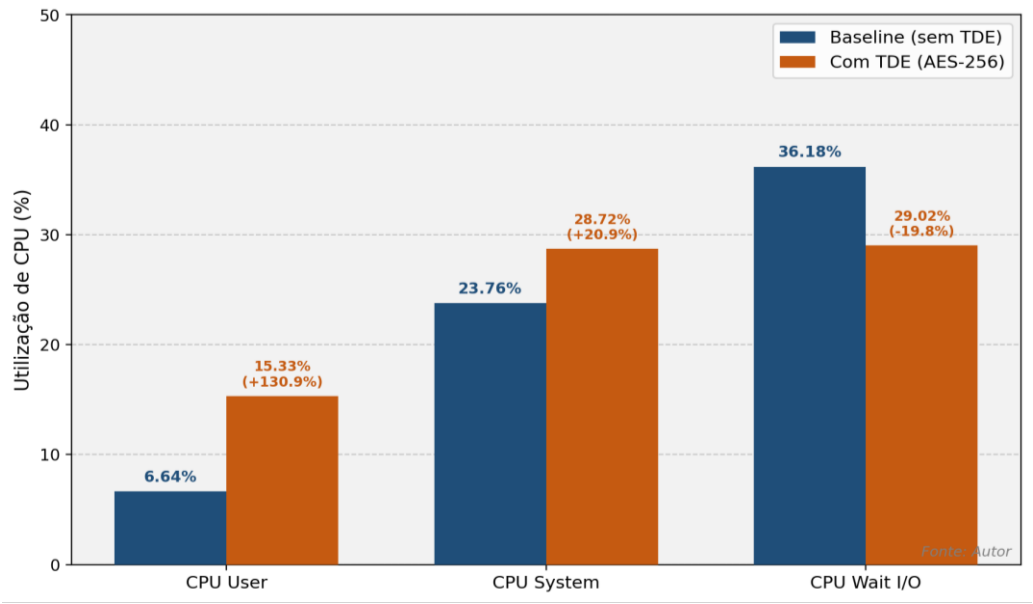
4.4.1 Tabela Comparativa

Tabela 7 – Comparação de métricas de CPU entre cenário baseline e Transparent Data Encryption(TDE)

Métrica	Baseline (%)	TDE (%)	Overhead (%)
CPU total	66,59	73,07	+9,7%
CPU em modo utilizador	6,64	15,33	+130,9%
CPU em modo sistema	23,76	28,72	+20,9%
CPU em espera (I/O)	36,18	29,02	−19,8%
CPU ociosa	24,79	18,28	−26,3%

Fonte: Autor

Figura 10 – Comparação de métricas de CPU: Baseline vs TDE (Oracle Database 19c *Enterprise Edition – Workload* TPC-C)



Fonte: Autor

4.4.2 Cálculo do *Overhead*

```
Overhead = ((73.07 - 66.59) / 66.59) × 100 = 9.73%
```

4.5 Testes de Segurança

4.5.1 *Backup* Encriptado com RMAN

A Figura 8 mostra a conclusão do *backup* RMAN encriptado.

Figura 8 – *Backup* RMAN encriptado concluído.

```
SQL>
Tablespace altered.

SQL>
TABLESPACE_NAME                STATUS
------------------------------ ---------
TBS_BENCH                      ONLINE

SQL> Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
[oracle@vbox backup]$ rman target sys/Oracle123@localhost:1521/TDEPDB << EOF
> LIST BACKUP OF TABLESPACE TBS_BENCH;
> EXIT;
> EOF

Recovery Manager: Release 19.0.0.0.0 - Production on Wed Nov 26 12:03:44 2025
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates.  All rights reserved.

connected to target database: TDELAB:TDEPDB (DBID=2065190859)

RMAN>
using target database control file instead of recovery catalog

List of Backup Sets
===================


BS Key  Type LV Size       Device Type Elapsed Time Completion Time
------- ---- -- ---------- ----------- ------------ ---------------
1       Full    2.38G      DISK        00:05:20     26-NOV-25
        BP Key: 1   Status: AVAILABLE  Compressed: YES  Tag: TAG20251126T115151
        Piece Name: /home/oracle_data/tde-lab/results/security/backup/0349ocqn_1_1
  List of Datafiles in backup set 1
  File LV Type Ckp SCN    Ckp Time  Abs Fuz SCN Sparse Name
  ---- -- ---- ---------- --------- ----------- ------ ----
  13      Full 4509753    26-NOV-25              NO    /u02/TDELAB/TDEPDB/tbs_bench01.dbf

RMAN>

Recovery Manager complete.
[oracle@vbox backup]$
```

Fonte: Autor

Resultados:

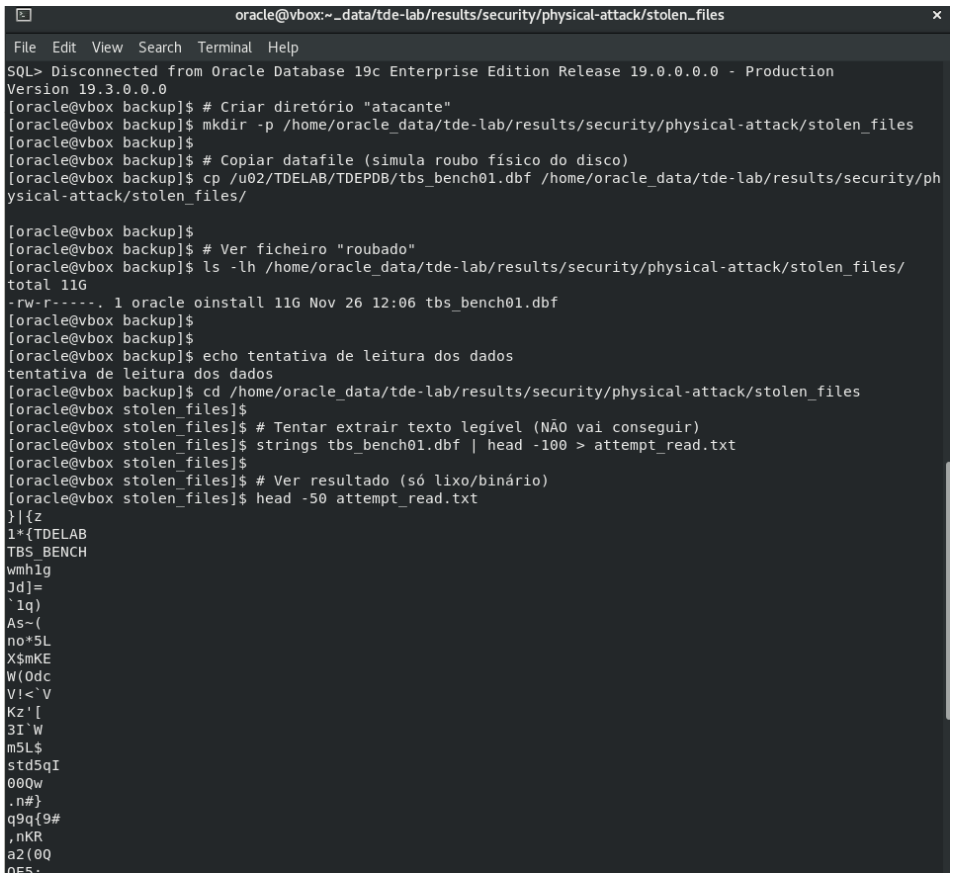
• Tamanho final: 2.38 GB
• Compressão: 78.79%
• Encriptação AES-256 aplicada corretamente

Todos os comandos e *logs* completos → **Anexo C**.

4.5.2 Simulação de Ataque Físico

A tentativa de leitura do *datafile* roubado é mostrada na Figura 9.

Figura 9 – Tentativa de leitura de *datafile* encriptado mostra apenas dados ilegíveis.



Fonte: Autor

O ficheiro apresenta conteúdo não interpretável, demonstrando que:

- sem o *keystore* aberto.
- sem a *Database Encryption Key(DEK).*
- não existe forma prática de recuperar o *plaintext.*

4.6 Síntese dos Resultados

• TDE adiciona *overhead* de **cerca de 9.7% na CPU**
• O impacto não impede execução normal do *workload* OLTP
• O uso de CPU *user* aumenta devido ao processo de encriptação de páginas
• *Backups* permanecem totalmente protegidos
• *Datafiles* extraídos não revelam dados sensíveis
• TDE cumpre eficazmente o objetivo de proteger dados em repouso

5.0 Discussão

5.1 Interpretação geral dos resultados

Os ensaios demonstraram que a ativação da *Transparent Data Encryption* (TDE) no Oracle 19c introduz um impacto mensurável no desempenho da base de dados. O efeito mais evidente foi o aumento da utilização da CPU (Unidade Central de Processamento), que subiu aproximadamente 9,7 por cento em comparação com o cenário sem encriptação. Apesar deste acréscimo, a base de dados manteve a capacidade de executar operações de Processamento de Transações Online (OLTP), o que indica que a TDE é compatível com cargas transacionais de intensidade moderada.

Este comportamento está de acordo com o esperado para mecanismos de encriptação ao nível do *tablespace*. A cifra AES-256 exige operações adicionais de cálculo durante a leitura e escrita de blocos, aumentando o processamento necessário em cada transação.

5.2 Comparação com estudos relacionados

Os resultados obtidos mostram coerência com conclusões de trabalhos anteriores. Estudos recentes reportam que a TDE tende a introduzir entre 2 e 15 por cento de impacto no desempenho, dependendo da carga e do hardware utilizado. O valor de aproximadamente 10 por cento verificado neste estudo encontra-se dentro desse intervalo.

Além disso, verificou-se um aumento significativo da utilização da CPU em modo de utilizador, fenómeno também descrito em estudos de desempenho da Oracle. Isto ocorre porque o processo de cifra e decifra é executado ao nível da aplicação e não do *kernel* do sistema operativo.

Outro aspeto relevante foi a diminuição do tempo em operações de Entrada/Saída (I/O). Quando a CPU passa a assumir mais trabalho devido à encriptação, o sistema pode apresentar menor dependência do armazenamento, reduzindo o tempo de espera associado ao subsistema de disco. Este comportamento também foi identificado em benchmarks publicados por especialistas Oracle.

5.3 Implicações para ambientes OLTP

5.3.1 Viabilidade operacional

Os resultados demonstram que a TDE é tecnicamente viável para ambientes OLTP com carga moderada. A degradação no desempenho é previsível e estável, o que facilita o planeamento de capacidade.

5.3.2 Necessidade de capacidade de processamento adequada

Em cenários onde a CPU já opera próxima do limite, a ativação da TDE deve ser analisada com cuidado. Processadores com suporte a instruções AES-NI, ou servidores com maior paralelismo, tendem a mitigar a maior parte do impacto observado.

5.3.3 Considerações sobre virtualização

O ambiente experimental utilizou uma máquina virtual, sem aceleração de *hardware*. Em ambientes físicos com unidades NVMe e AES-NI ativo, é provável que o impacto real seja inferior ao observado neste estudo.

5.4 Impacto na segurança dos dados em repouso

5.4.1 Resistência a ataques físicos

Os testes de segurança mostraram que, mesmo quando um ficheiro de dados é extraído manualmente do servidor, não é possível recuperar informação em texto legível. Ferramentas como o utilitário *strings* devolvem apenas dados aleatórios. A tentativa de anexar o ficheiro noutra instância Oracle falha por ausência da chave de encriptação. Isto confirma que a TDE cumpre o objetivo de proteger dados em repouso, mesmo em caso de acesso não autorizado ao armazenamento.

5.4.2 Proteção de cópias de segurança

O teste ao mecanismo de cópias de segurança mostrou que o *RMAN* produz conjuntos de cópias encriptadas que permanecem inacessíveis sem o *keystore* correspondente. Este comportamento demonstra conformidade com boas práticas de segurança e com recomendações de normas internacionais.

5.5 Relação com o quadro regulatório

5.5.1 RGPD

O Regulamento Geral sobre a Proteção de Dados indica a encriptação como medida técnica adequada para reduzir riscos. Os resultados obtidos demonstram que, mesmo em caso de fuga física de um ficheiro, não é possível aceder a dados pessoais, o que reduz substancialmente o impacto de um incidente.

5.5.2 PCI-DSS

A norma PCI-DSS exige a proteção criptográfica forte de dados de titulares de cartão. A aplicação da TDE cumpre diretamente esta exigência, garantindo que dados armazenados e cópias de segurança permanecem cifrados.

5.5.3 NIS 2

A diretiva NIS 2 reforça a importância da resiliência e proteção de ativos críticos. Os testes realizados demonstram que a TDE contribui para estes requisitos, preservando a confidencialidade dos dados mesmo em cenários adversos.

5.6 Limitações do estudo

O estudo apresenta algumas limitações que devem ser consideradas. O ambiente experimental é reduzido e não representa sistemas empresariais de grande escala. O *workload* utilizado segue o modelo TPC-C, adequado para OLTP, mas não cobre cenários analíticos. Não foi testada a integração com módulos de segurança de *hardware* (HSM) ou com o Oracle *Key Vault,* que poderiam influenciar os resultados. Por fim, o ambiente virtual não tira partido da aceleração dedicada de cifra, o que pode amplificar o impacto observado.

5.7 Considerações finais

Os resultados indicam que a TDE introduz um impacto previsível no desempenho, mas oferece uma proteção robusta dos dados em repouso. A solução revela-se especialmente adequada em ambientes onde a segurança e a conformidade são prioridades. A relação custo-benefício é favorável: o aumento de utilização de CPU é compensado pela capacidade de prevenir acessos indevidos e cumprir requisitos legais e normativos.

6. Conclusões e Trabalho Futuro

6.1 Síntese do Trabalho Realizado

O presente estudo teve como objetivo avaliar o impacto da T*ransparent Data Encryption* (TDE) no desempenho de bases de dados Oracle 19c, bem como analisar a sua eficácia enquanto mecanismo de proteção de dados em repouso e o seu contributo para a conformidade regulatória. Para isso, foi construído um ambiente laboratorial controlado, onde foram efetuados testes antes e depois da ativação da encriptação transparente.

A metodologia incluiu a criação de um cenário de referência sem encriptação, seguido da ativação da TDE com algoritmo AES-256 e repetição integral dos mesmos ensaios. Foram analisadas métricas de utilização de processador, tempos de espera associados a operações de entrada e saída, métricas do sistema recolhidas por ferramentas de baixo nível e relatórios AWR. Adicionalmente, foram realizados testes de segurança, incluindo a criação de cópias de segurança encriptadas e a simulação de um ataque físico ao ficheiro de dados.

Os resultados demonstram que a TDE introduz um acréscimo moderado de utilização de processador, tendo sido registado um aumento aproximado de 9.7 por cento na média de consumo total. Os testes de segurança confirmaram que os dados encriptados permanecem **ilegíveis** fora do contexto da base de dados e que interpretações forçadas do ficheiro físico não permitem extrair qualquer informação sensível. Do ponto de vista regulatório, verificou-se que a TDE contribui de forma significativa para o cumprimento de requisitos como os do Regulamento Geral sobre a Proteção de Dados, da diretiva NIS 2 e do PCI-DSS.

6.2 Conclusões Gerais

Os resultados obtidos permitem tirar as seguintes conclusões:

1. **A ativação da TDE implica um custo de desempenho aceitável**
   A subida de aproximadamente 9.7 por cento na utilização média do processador encontra-se dentro do intervalo comumente referido na literatura e não compromete o funcionamento normal de cargas transacionais moderadas.

2. **A TDE demonstra elevada eficácia na proteção de dados em repouso**
   A simulação de exfiltração de ficheiros e a análise fora da base de dados confirmaram que o conteúdo permanece totalmente inacessível sem a chave criptográfica, reforçando a utilidade da TDE como medida de proteção estrutural.

3. **A TDE facilita o cumprimento de obrigações legais e normativas**
   A encriptação automática de ficheiros de dados e de cópias de segurança constitui um controlo técnico diretamente alinhado com requisitos de segurança previstos no RGPD, na NIS 2 e no PCI-DSS, reduzindo riscos e potenciais custos associados a incidentes de segurança.

4. **O impacto na experiência operacional é reduzido**
   A configuração e gestão da TDE, incluindo o processo de encriptação do espaço de tabelas, demonstraram ser operações estáveis, previsíveis e totalmente integradas com o ecossistema Oracle.

6.3 Limitações do Estudo

Embora o estudo tenha sido realizado de forma estruturada e controlada, existem limitações naturais que devem ser consideradas:

1. **Recursos de hardware limitados**
   O ambiente de testes foi executado numa máquina virtual com recursos modestos, o que pode amplificar ou reduzir determinados comportamentos quando comparado com servidores empresariais de grande capacidade.

2. **Número reduzido de execuções totais**
   Por motivos de tempo, foi possível executar apenas duas execuções completas por cenário, o que limita a profundidade estatística mas não compromete a identificação de tendências claras.

3. **Tipo de carga de trabalho**
   Apenas foi testado um cenário transacional (TPC-C). Cargas analíticas ou misturadas

podem evidenciar comportamentos diferentes.

4. **AWR com dados incompletos em alguns momentos**
   Determinadas lacunas nos relatórios limitaram a análise de alguns eventos de espera.

5. **Escopo focado exclusivamente em encriptação transparente**
   Outras opções de segurança, como encriptação em movimento ou tokenização, não foram avaliadas.

6.4 Trabalho Futuro

Com base nas limitações identificadas e nos resultados obtidos, sugerem-se as seguintes linhas de investigação futura:

1. **Avaliar o impacto da TDE em *hardware* com suporte avançado de instruções criptográficas**, incluindo processadores modernos com otimizações específicas que podem reduzir ainda mais o custo da encriptação.

2. **Repetir os testes com volumes de dados superiores e com cargas mistas ou analíticas**, nomeadamente cenários equivalentes ao TPC-DS, para avaliar o comportamento em ambientes de análise intensiva.

3. **Integrar e testar soluções de gestão de chaves externas**, como o Oracle *Key Vault,* módulos de segurança de hardware e cofres na nuvem, comparando tempos de resposta e impacto no desempenho.

4. **Avaliar a interação da TDE com soluções de alta disponibilidade**, tais como Oracle *Data Guard, Real Application Clusters* ou replicação *GoldenGate*, medindo o efeito da encriptação em processos de sincronização.

5. **Medir de forma mais detalhada o impacto da TDE em operações de cópia de segurança incrementais**, restaurações e recuperação após falhas.

Referências

[1] ISO/IEC. (2018). *ISO/IEC 27000:2018 — Information technology — Security techniques — Information security management systems — Overview and vocabulary*. International Organization for Standardization.

[2] Bell, D. E., & LaPadula, L. J. (1975). *Secure computer systems: Mathematical foundations*. MITRE Corporation.

[3] Biba, K. J. (1977). *Integrity considerations for secure computer systems* (Tech. Rep. MTR-3153). MITRE.

[4] Clark, D. D., & Wilson, D. R. (1987). A comparison of commercial and military computer security policies. *Proceedings of the IEEE Symposium on Security and Privacy*, 184-194. https://doi.org/10.1109/SP.1987.10032

[5] Parker, D. B. (2002). *Fighting computer crime: A new framework for protecting information*. John Wiley & Sons.

[6] International Data Corporation. (2024). *IDC Global Datasphere Forecast 2023-2027*.

[7] Gartner. (2023). *Market Guide for DBMS Platforms*. Gartner Research.

[8] IBM Security X-Force. (2024). *Threat Intelligence Index 2024*.

[9] Madyatmadja, E. D., Hakim, A. N., & Sembiring, D. J. M. (2021). Performance testing on Transparent Data Encryption for SQL Server's reliability and efficiency.
Journal of Big Data, 8(134), 1-14. https://doi.org/10.1186/s40537-021-00520-z

[10] Ponemon Institute. (2024). *Cost of a Data Breach Report 2024*.

[11] Statista. (2024). *Worldwide database management systems market share in 2023*.

[12] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016 (Regulamento Geral sobre a Proteção de Dados).Diretiva (UE)

2022/2555 (NIS 2).

[13] PCI Security Standards Council. (2022). *Payment Card Industry Data Security Standard version 4.0*.

[14] U.S. Congress. (2002). *Sarbanes-Oxley Act of 2002*.

[15] U.S. Department of Health and Human Services. (2013). *HIPAA Security Rule* (45 CFR § 164).

[16] Parlamento Australiano. (2024). *Cyber Security Act 2024*.

[17] United Nations. (2024). *UN Convention on Cybercrime* (draft adopted 2024).

[18] Equifax. (2018). *Equifax cybersecurity incident 2017: Post-mortem report*.

[19] U.S. Senate Committee on Homeland Security and Governmental Affairs. (2020). *How the 2019 Capital One breach happened* (Hearings S.Hrg. 116-580).

[20] Oracle Corporation. (2023). *Oracle® Database 19c Security Guide* (F22306-12).

[21] Oracle Corporation. (2023). *ADMINISTER KEY MANAGEMENT syntax — Oracle 19c SQL Reference* (F22427-09).

[22] Intel. (2022). *Intel® Advanced Encryption Standard New Instructions (AES-NI) white paper*.

[23] Percona. (2020, Maio 7). *Transparent Data Encryption (TDE)* [Blog post]. https://www.percona.com/blog/transparent-data-encryption-tde/

[24] Skillz Cafe. (2021, Julho 14). *Transparent Data Encryption vs Always Encrypted in SQL Server*. https://www.skillzcafe.com/blog/microsoft/sql-server/transparent-data-encryption-and-always-encrypted

[25] European Union Agency for Cybersecurity. (2021). *ENISA Risk Management Toolkit*.National Institute of Standards and Technology. (2012).

NIST SP 800-30 rev. 1: Guide for conducting risk assessments.

[26] Intel, AMD, & Arm. (2023). *State of confidential computing 2023* (Industry white paper).

[27] CRYSTALS-Kyber team. (2023). *CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM* (Submission to NIST post-quantum standardisation, round 4).

[28] Kubernetes Security Special Interest Group. (2022). *Secrets management patterns in Kubernetes*.

[29] Oracle Corporation. (2023). *Advanced Security with Oracle Database 19c: White Paper*. Disponível em: https://www.oracle.com/a/tech/docs/dbsec/aso/advanced-security-wp-19c.pdf (Natarajan & Shaik, 2020).

[30] Deshmukh, A. P. A. G., & Qureshi, R. (2011). *Transparent Data Encryption- Solution for Security of Database Contents*. International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 2, No. 3.

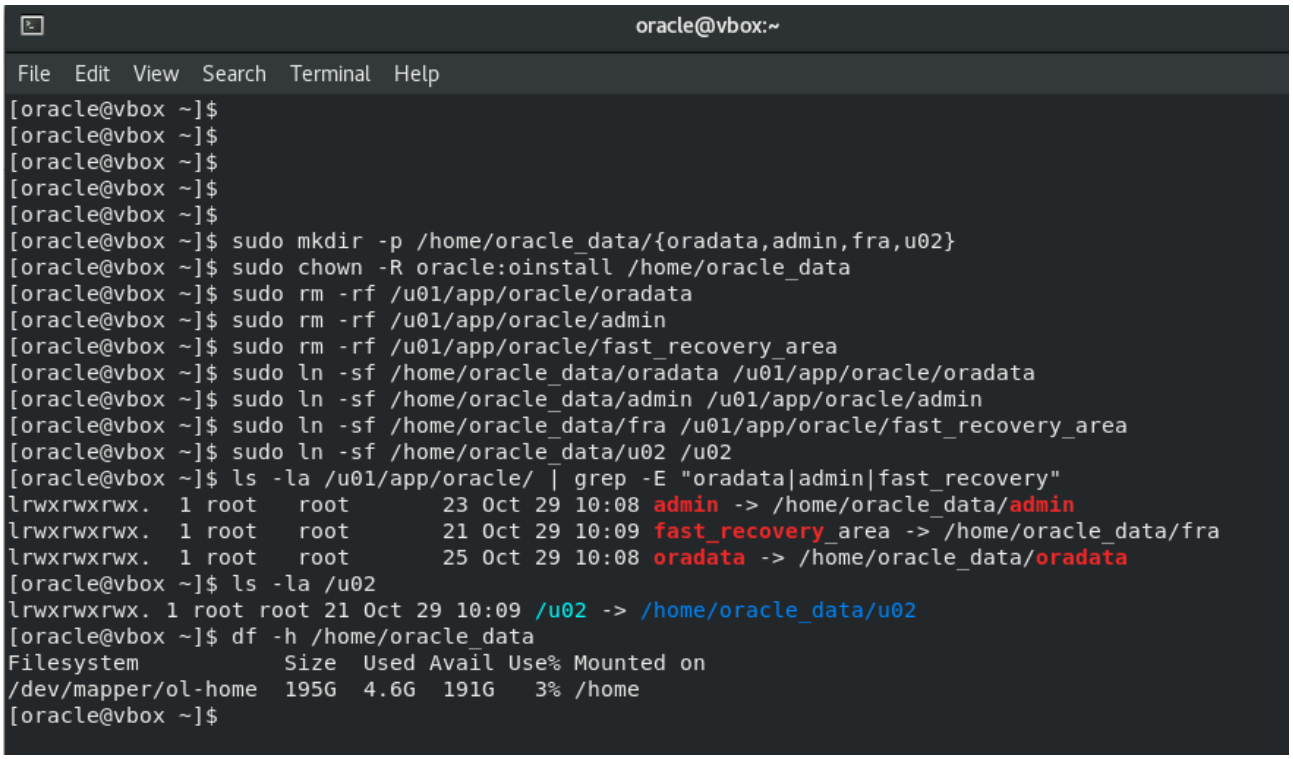
[31] Palmucci, M. (2022). *Securing databases using Attribute Based Encryption and Shamir's Secret Sharing*. Master Thesis, Università degli Studi di Perugia.

[32] Oracle Corporation. (2023). *Oracle Database 19c Security Guide (F22306-12)*.

ANEXOS

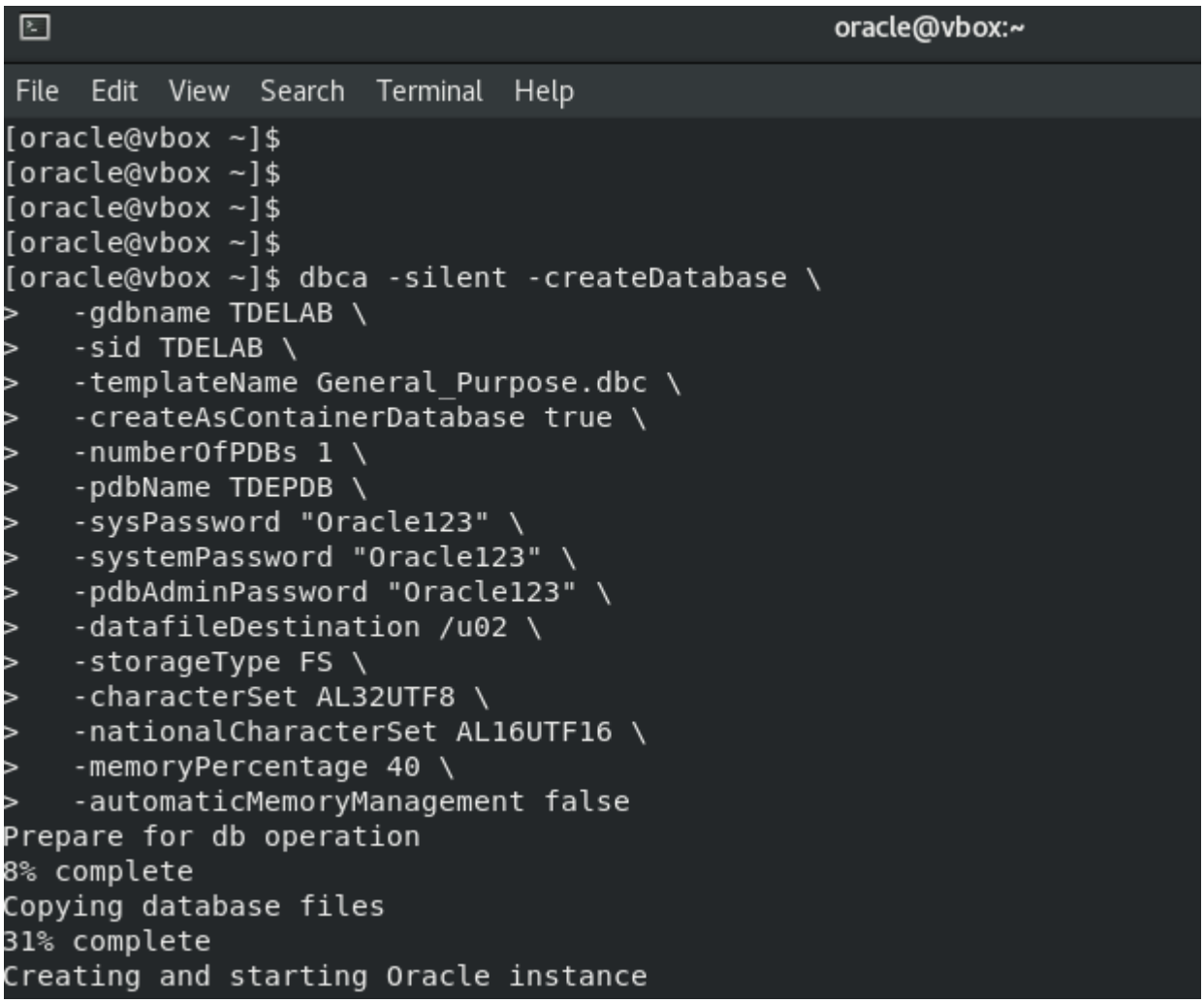
ANEXO A: AMBIENTE EXPERIMENTAL E CONFIGURAÇÃO INICIAL

Imagem 1 – Criação da estrutura de diretórios



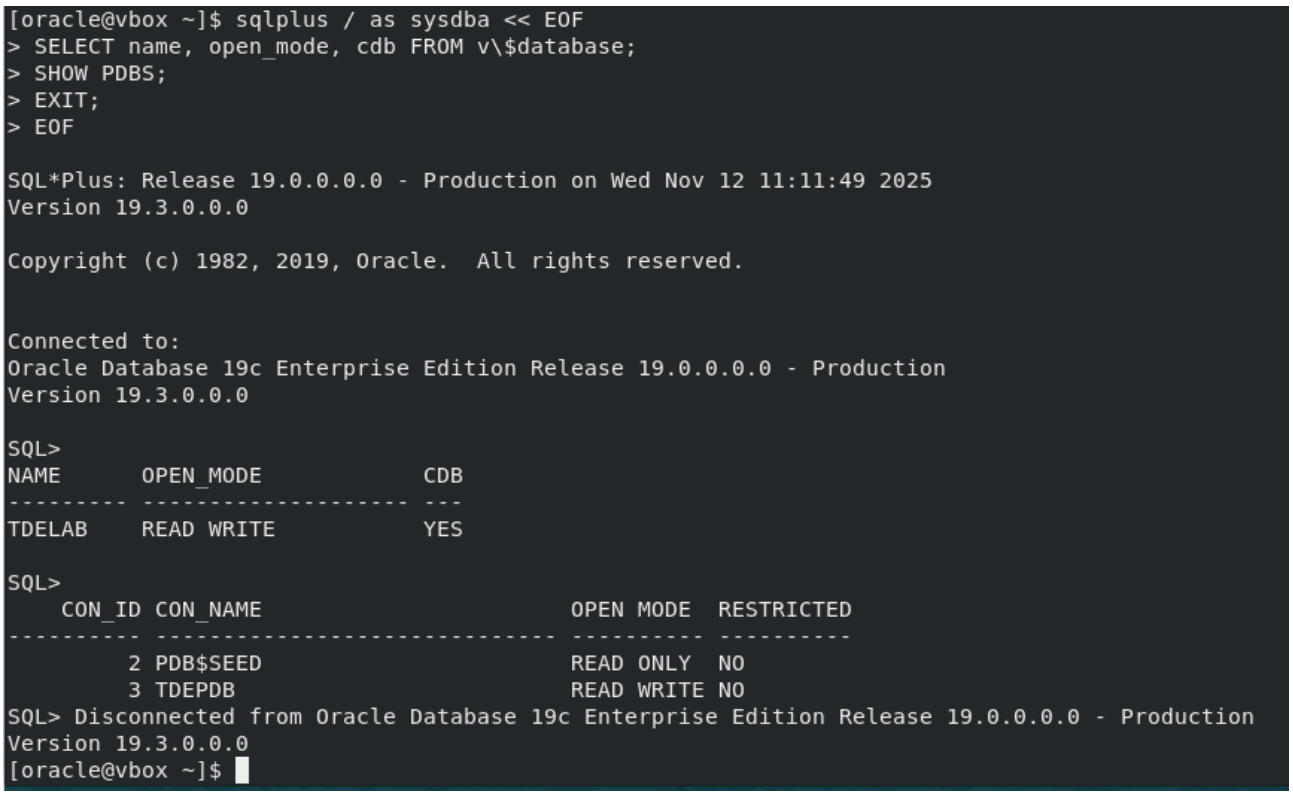
Fonte: Autor

Imagem 2 – Base de dados TDELAB



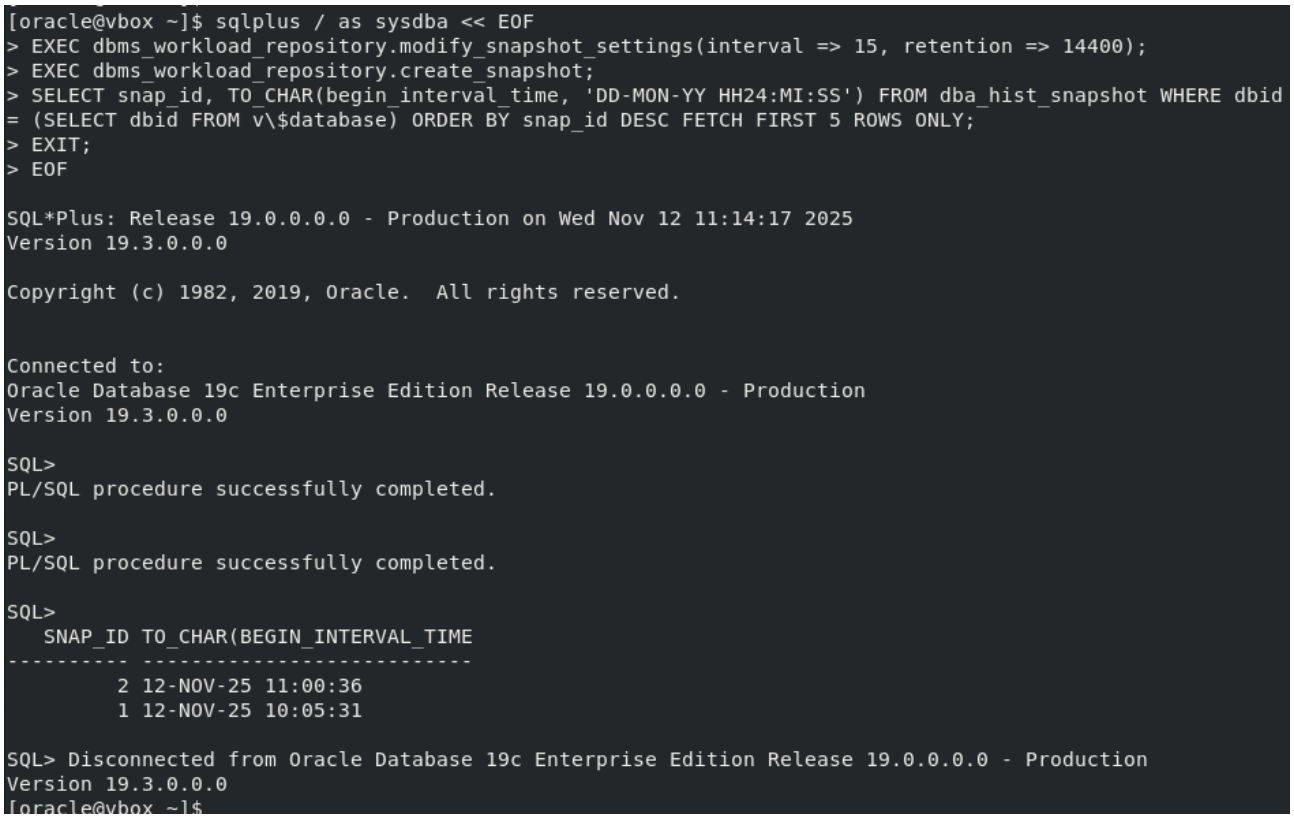
Fonte: Autor

Imagem 3 – Base de dados operacional



Fonte: Autor

Imagem 4 – Configuração do *Automatic Workload Repository* (AWR)



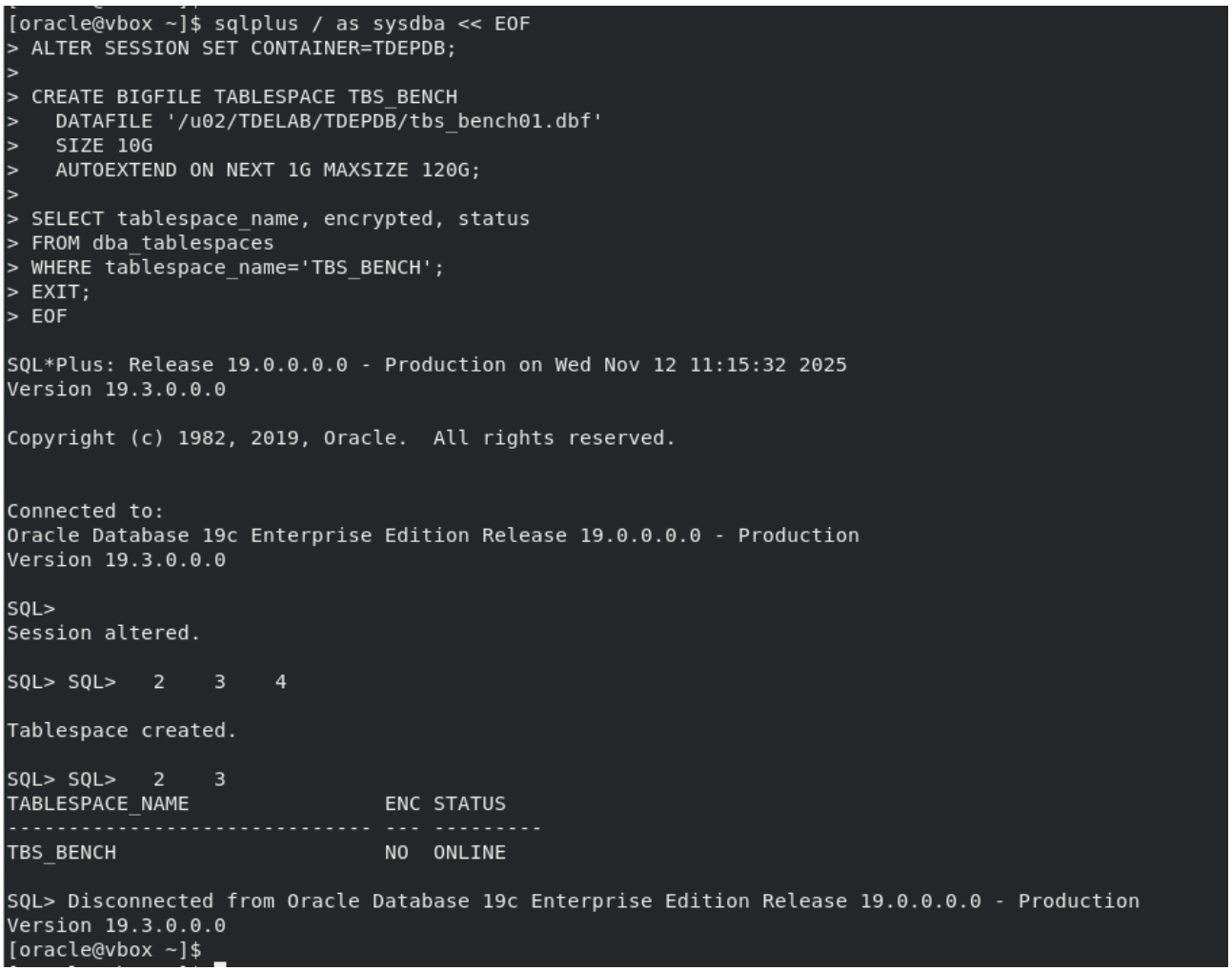
Fonte: Autor

Imagem 5 – Criação do *tablespace* sem encriptação

```
SQL> ALTER SESSION SET CONTAINER=TDEPDB;

Session altered.

SQL> CREATE BIGFILE TABLESPACE TBS_BENCH
  DATAFILE '/u02/oradata/TDELAB/TDEPDB/tbs_bench01.dbf'
  SIZE 10G
  AUTOEXTEND ON NEXT 1G MAXSIZE 120G;  2    3    4

Tablespace created.
```

Fonte: Autor

Imagem 6 – *Tablespace* TBS_BENCH criado sem *Transparent Data Encryption*(TDE)

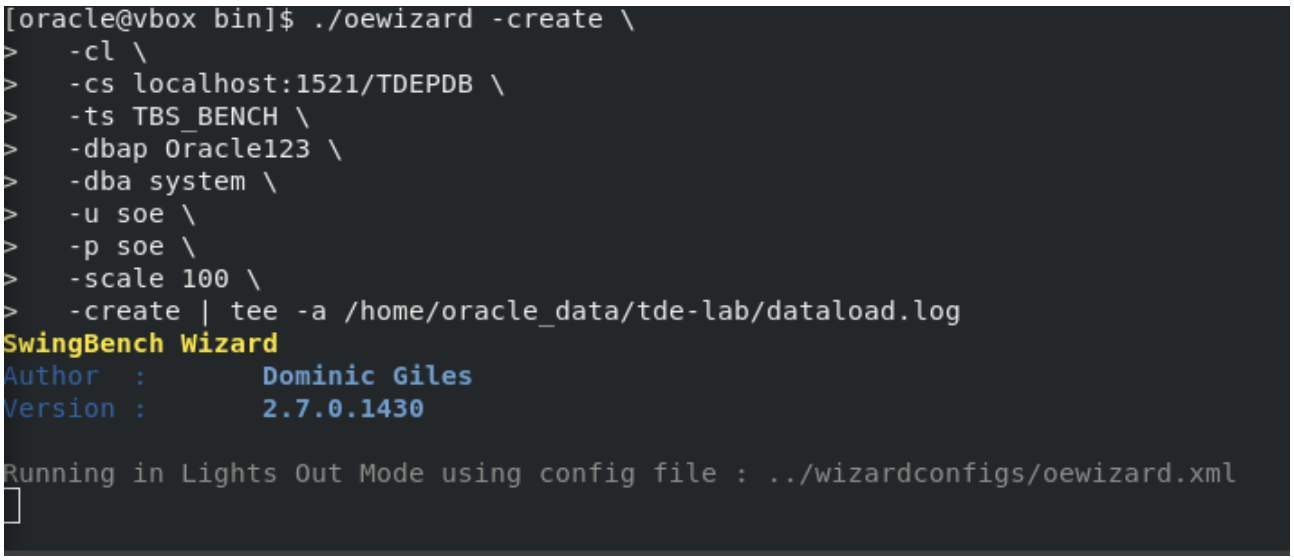


Fonte: Autor

Imagem 7 – Instalação do HammerDB

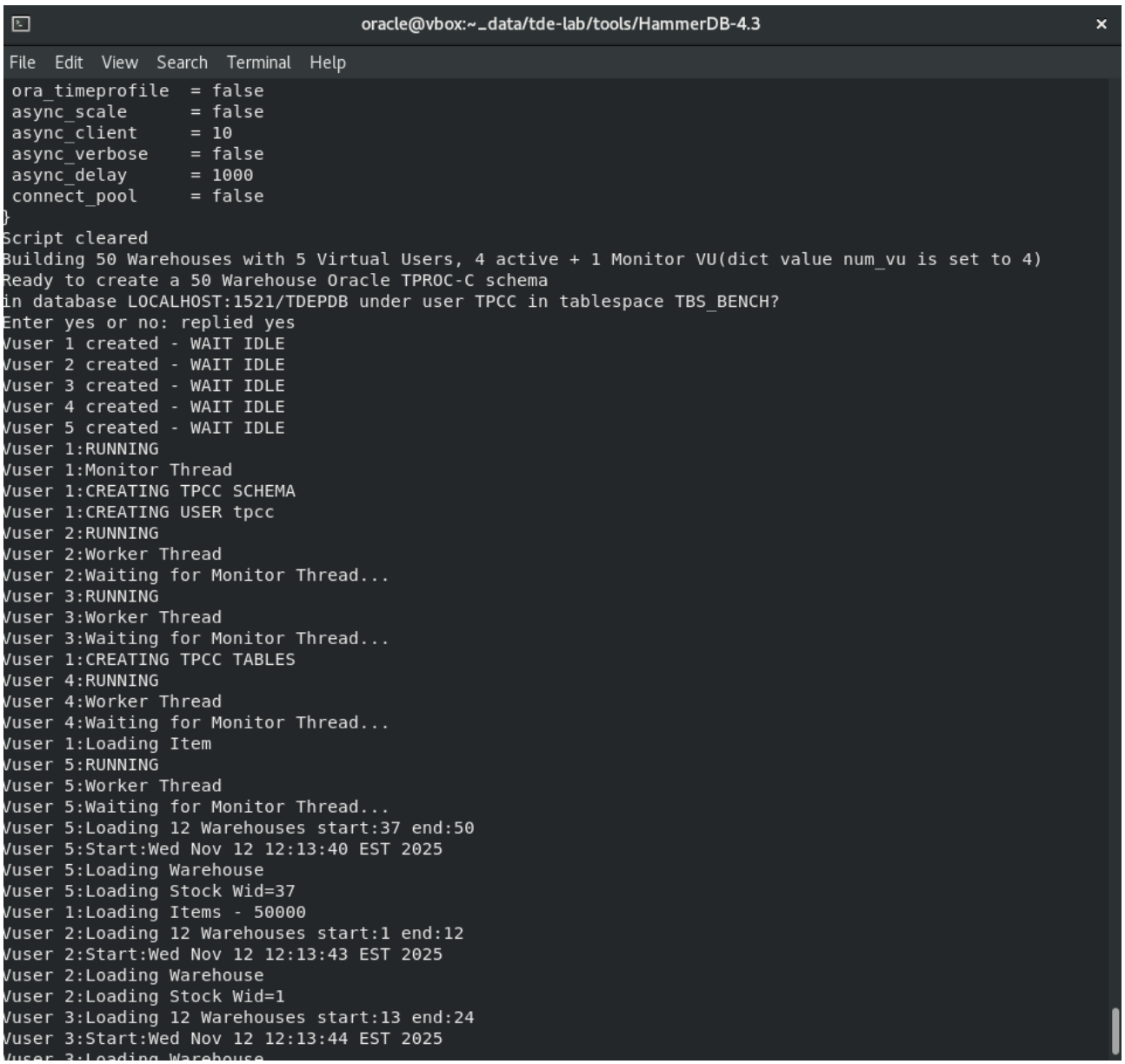
Fonte: Autor

Imagem 8 – Início da carga de dados TPC-C



Fonte: Autor

Imagem 9 – Processo de carga de dados



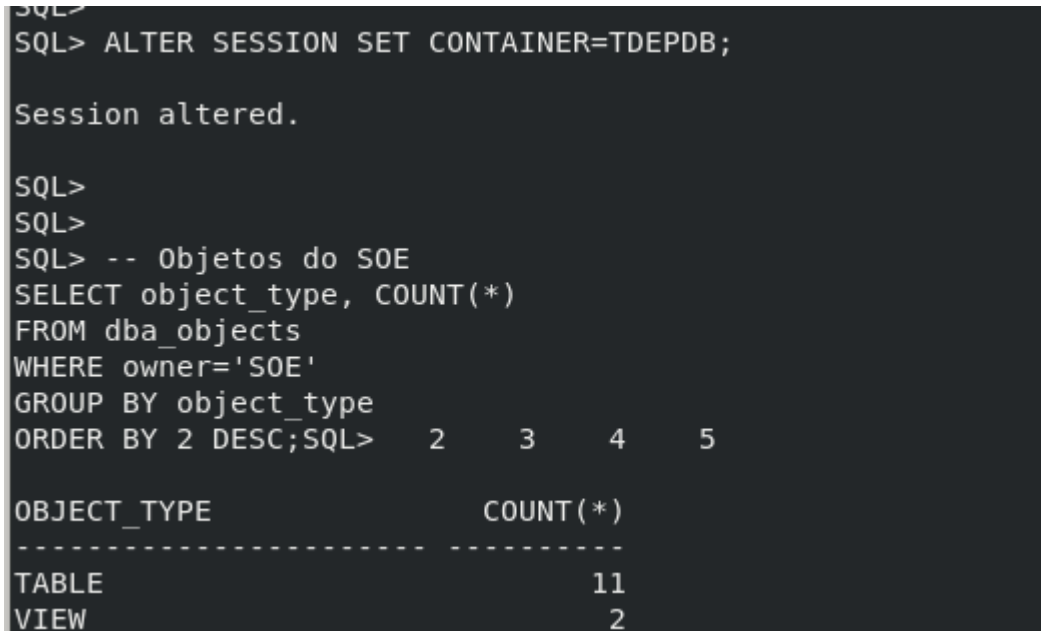
Fonte: Autor

Imagem 10 – Conclusão da carga de dados

```
Vuser 5:Loading Orders for D=6 W=50
Vuser 5:Orders Done
Vuser 5:Loading Orders for D=7 W=50
Vuser 5:Orders Done
Vuser 5:Loading Orders for D=8 W=50
Vuser 5:Orders Done
Vuser 5:Loading Orders for D=9 W=50
Vuser 5:Orders Done
Vuser 5:Loading Orders for D=10 W=50
Vuser 5:Orders Done
Vuser 5:End:Wed Nov 12 12:33:24 EST 2025
Vuser 5:FINISHED SUCCESS
Vuser 1:Workers: 0 Active 4 Done
Vuser 1:CREATING TPCC INDEXES
Vuser 1:CREATING TPCC STORED PROCEDURES
Vuser 1:GATHERING SCHEMA STATISTICS
Vuser 1:TPCC SCHEMA COMPLETE
Vuser 1:FINISHED SUCCESS
ALL VIRTUAL USERS COMPLETE
waittocomplete called script exit
[oracle@vbox HammerDB-4.3]$
```

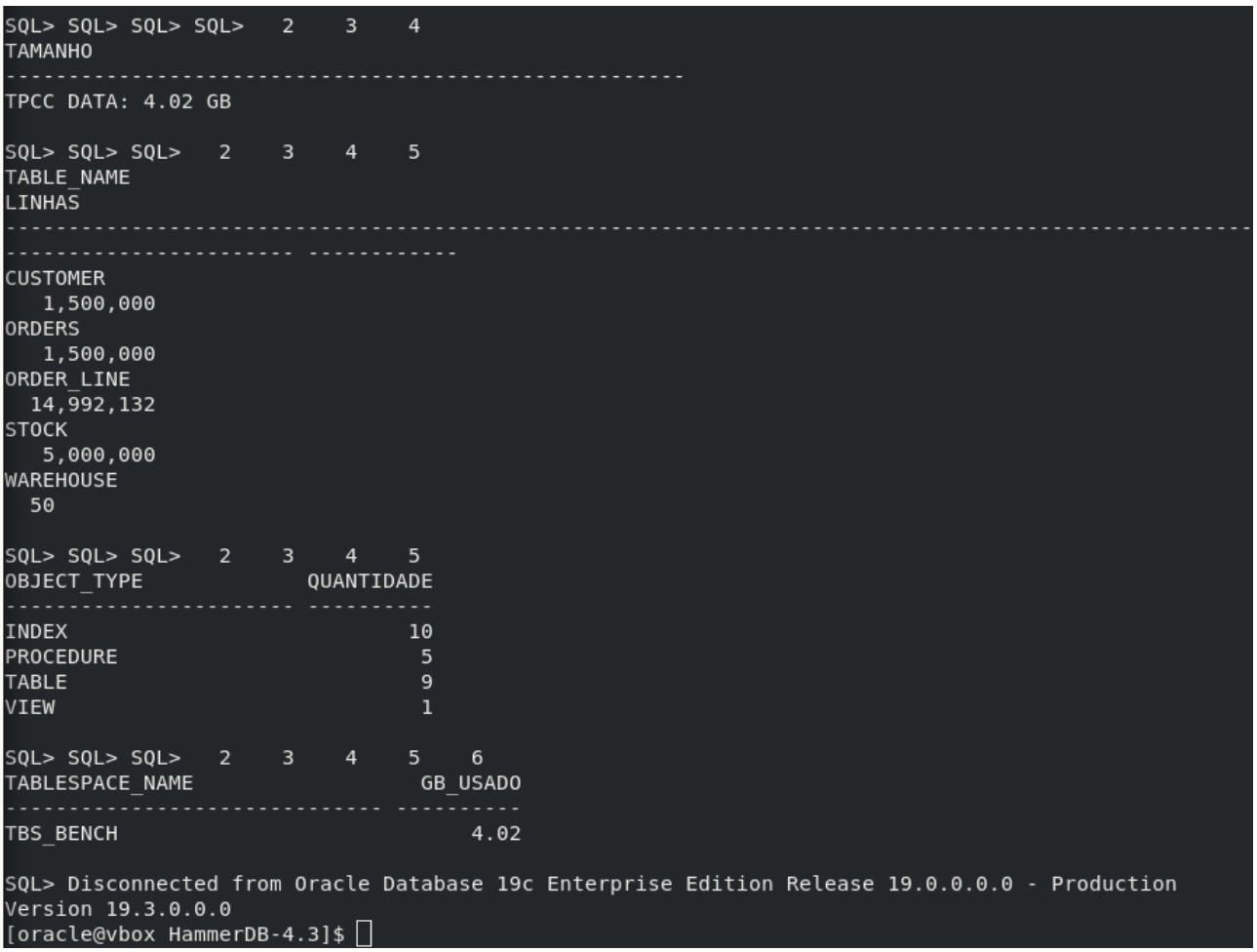
Fonte: Autor

Imagem 11 – Verificação do tamanho dos dados



Fonte: Autor

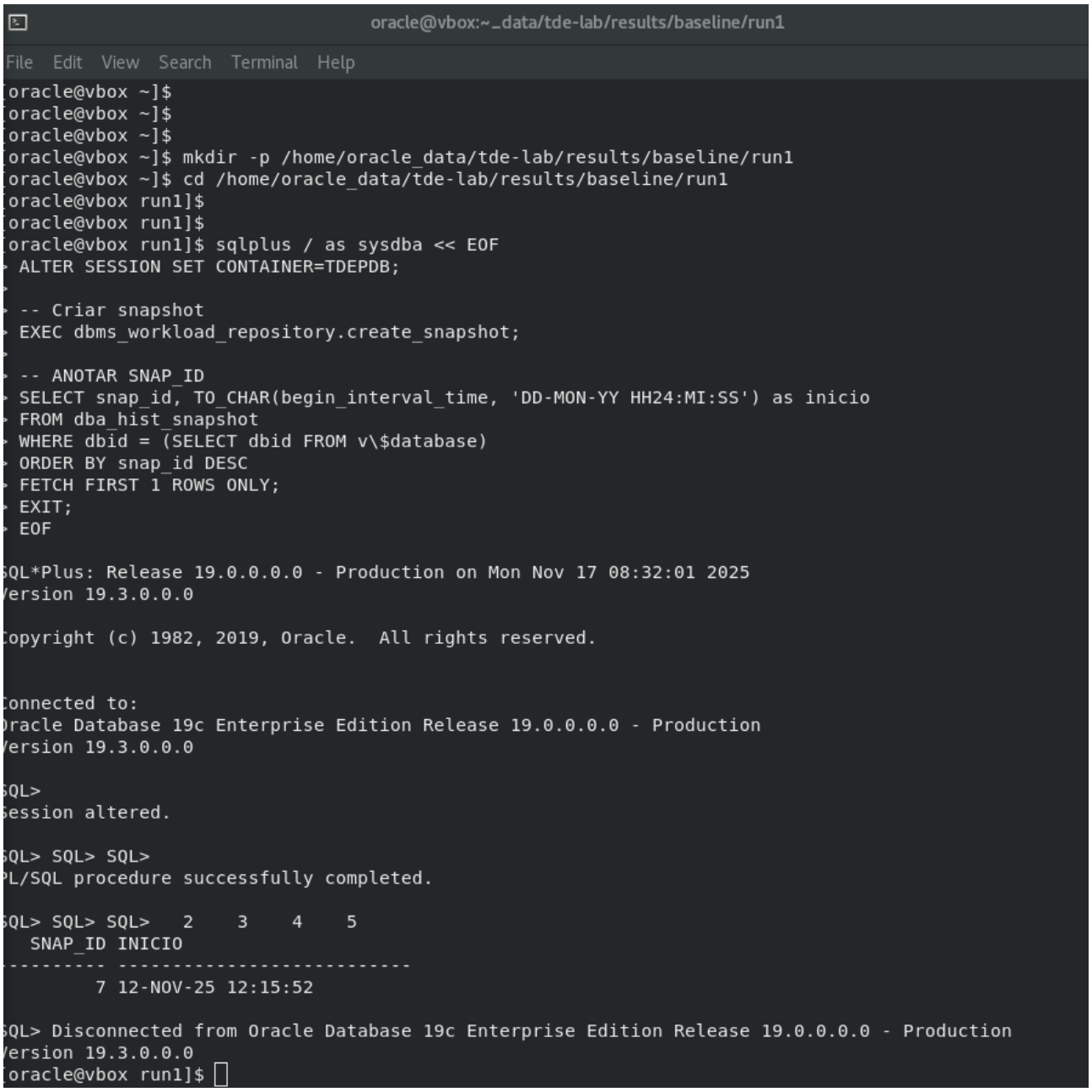
Imagem 12 – Confirmação dos dados carregados



Fonte: Autor

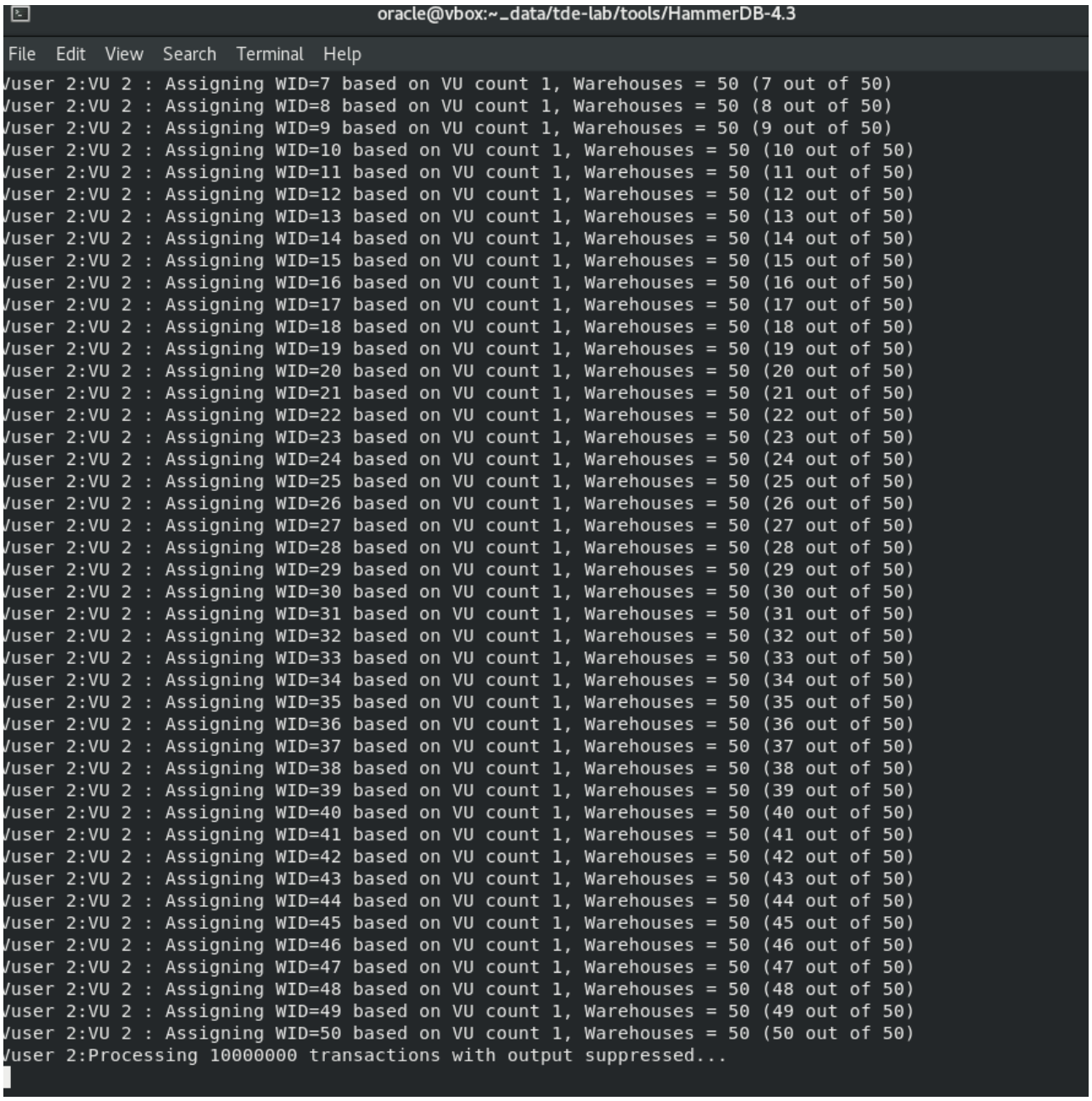
ANEXO B: TESTES DE PERFORMANCE

Imagem 13 – *Snapshot Automatic Workload Repository* (AWR) inicial do teste *baseline*



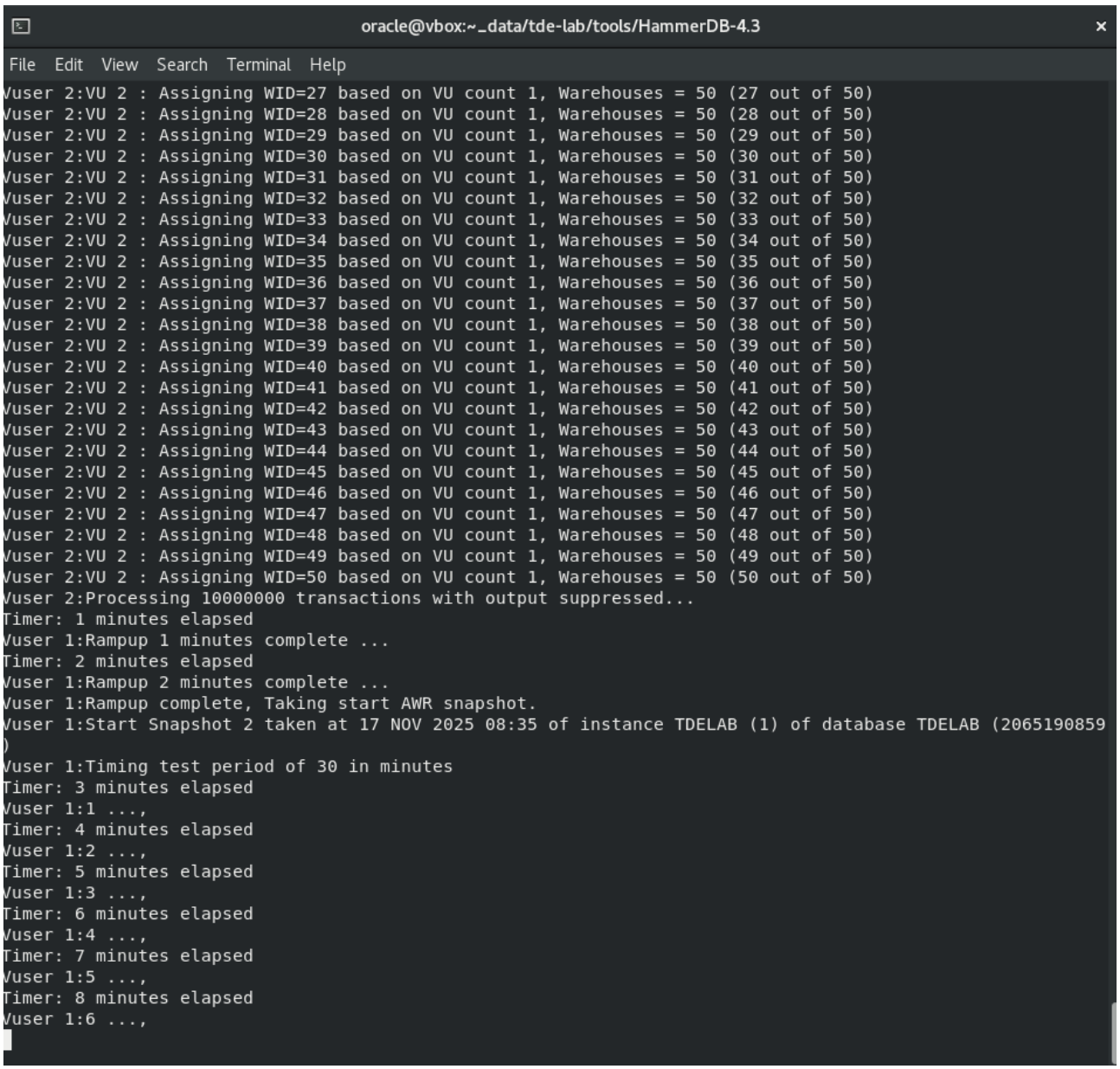
Fonte: Autor

Imagem 14 – Teste baseline em execução (2 minutos)



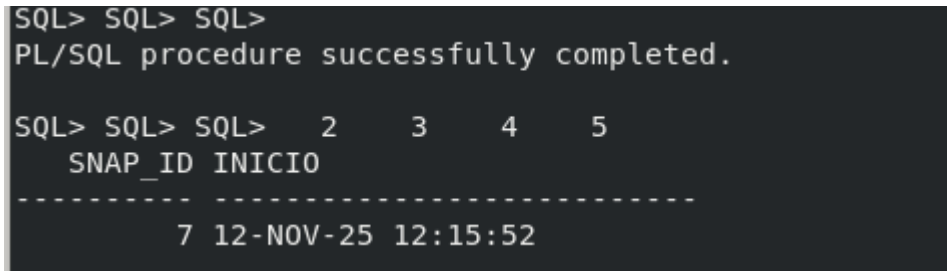
Fonte: Autor

Imagem 15 – Progresso do teste *baseline* (8 minutos)



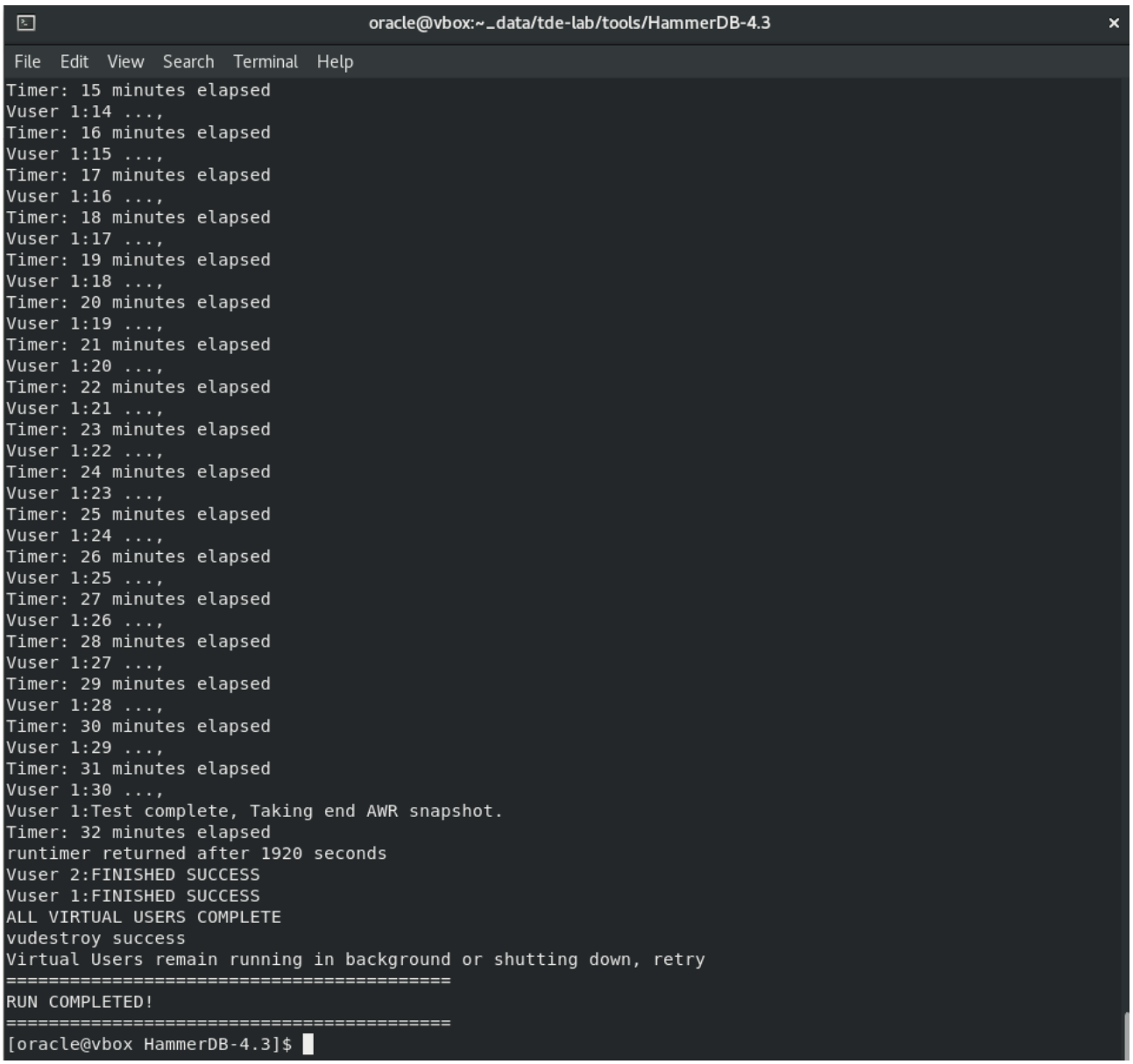
Fonte: Autor

Imagem 16 – *Snapshot* ID durante teste



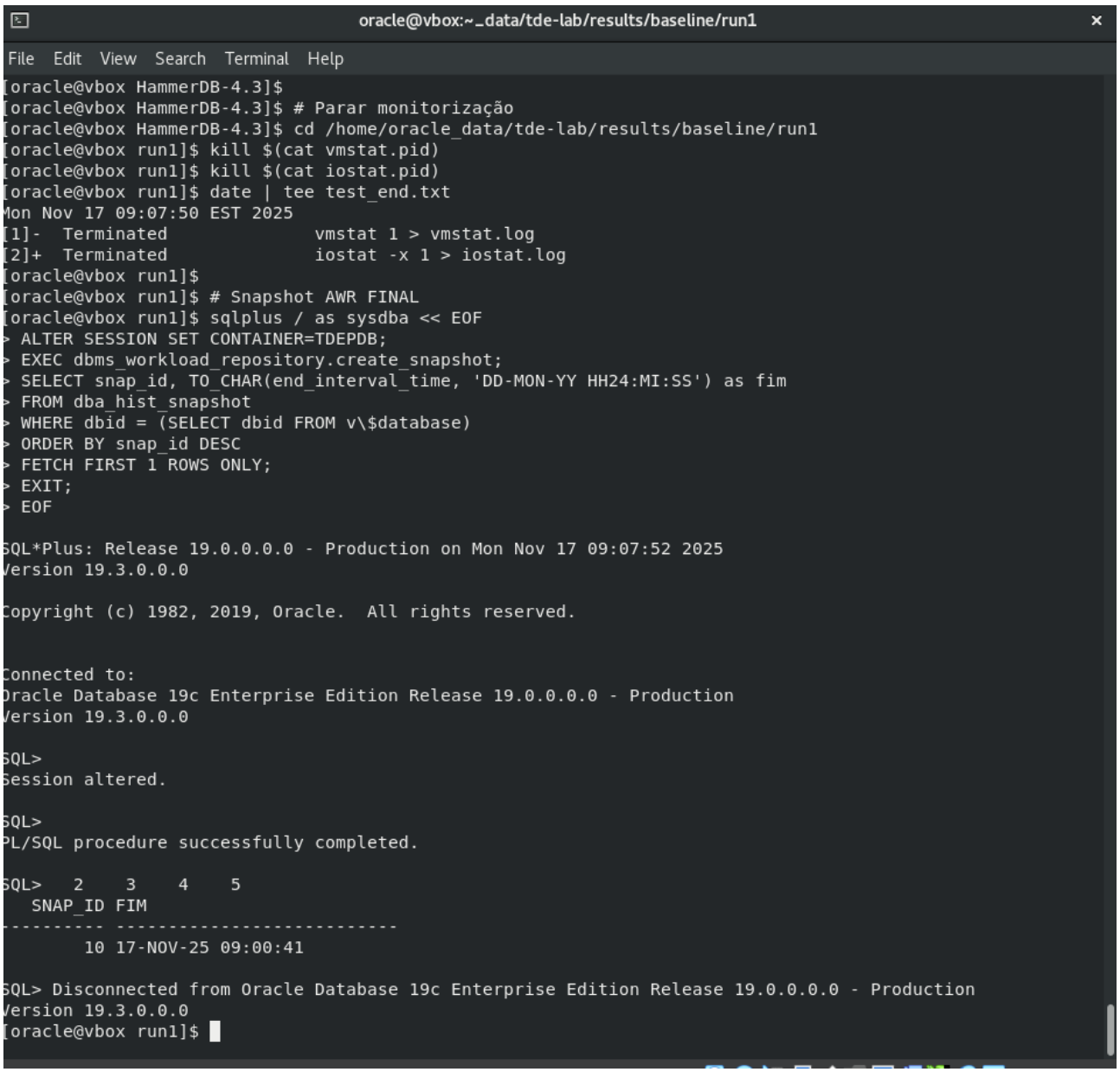
Fonte: Autor

Imagem 17 – Conclusão do teste *baseline*



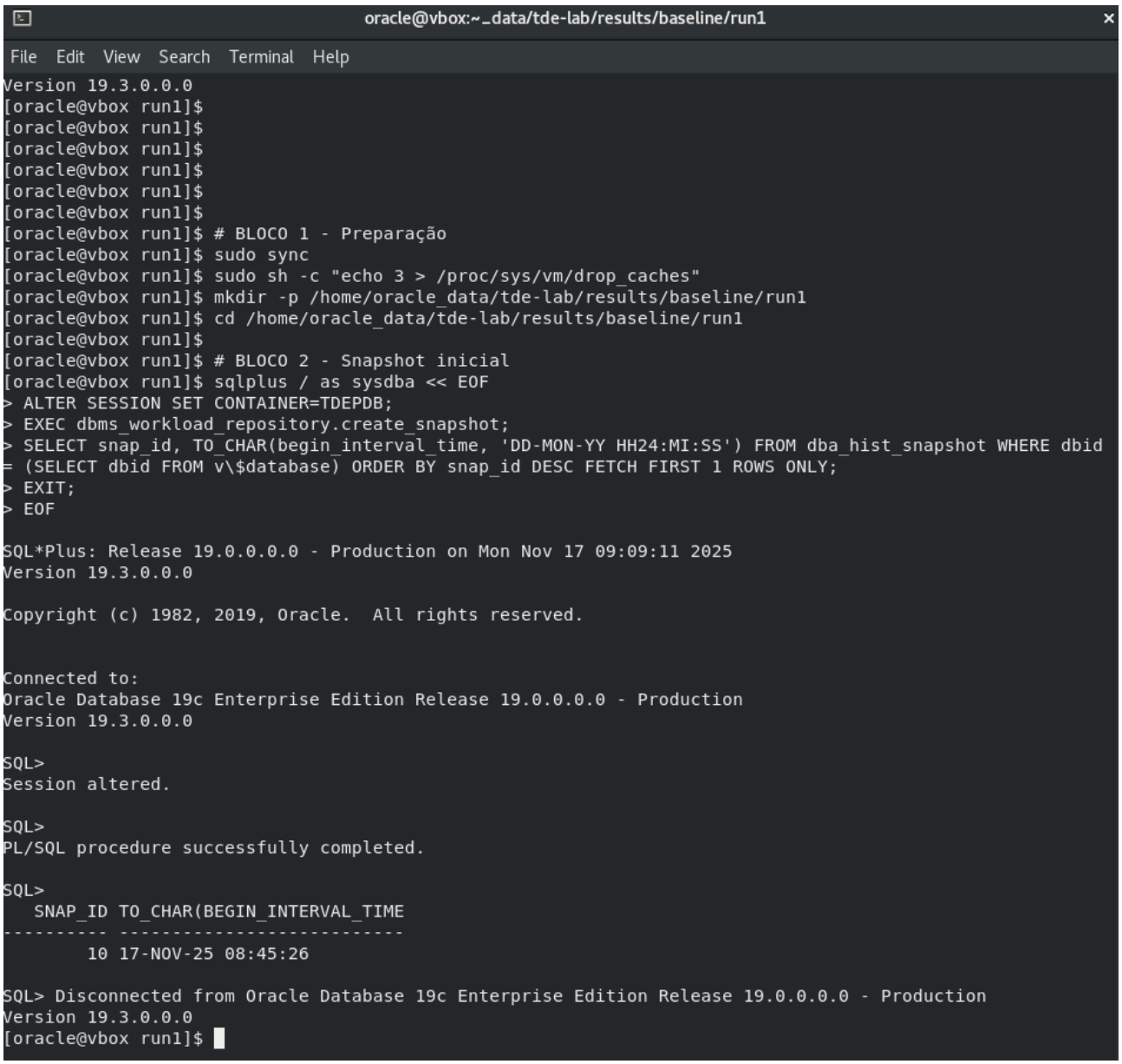
Fonte: Autor

Imagem 18 – *Snapshot* final do *baseline*



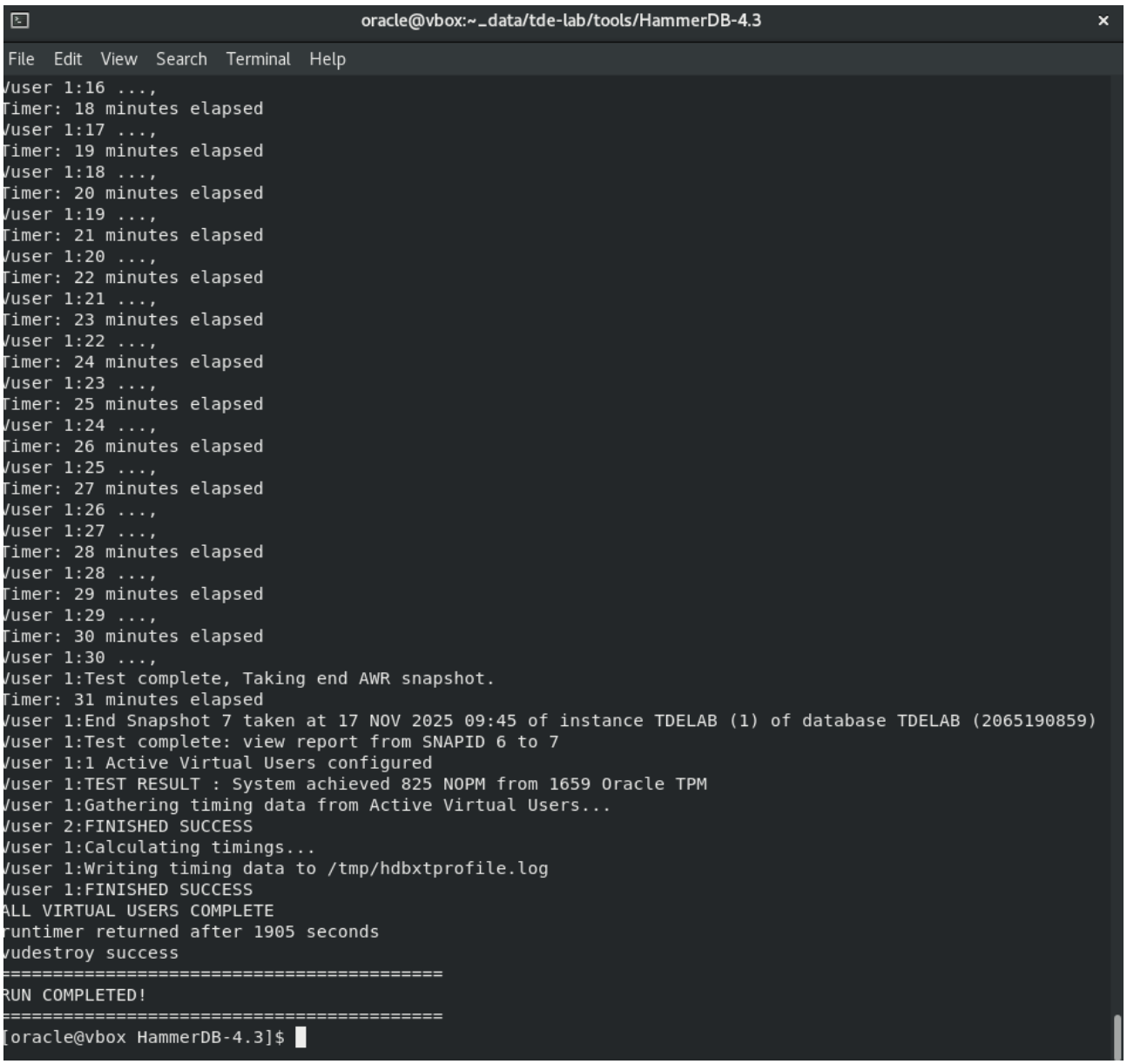
Fonte: Autor

Imagem 19 – *Snapshot* inicial do segundo teste



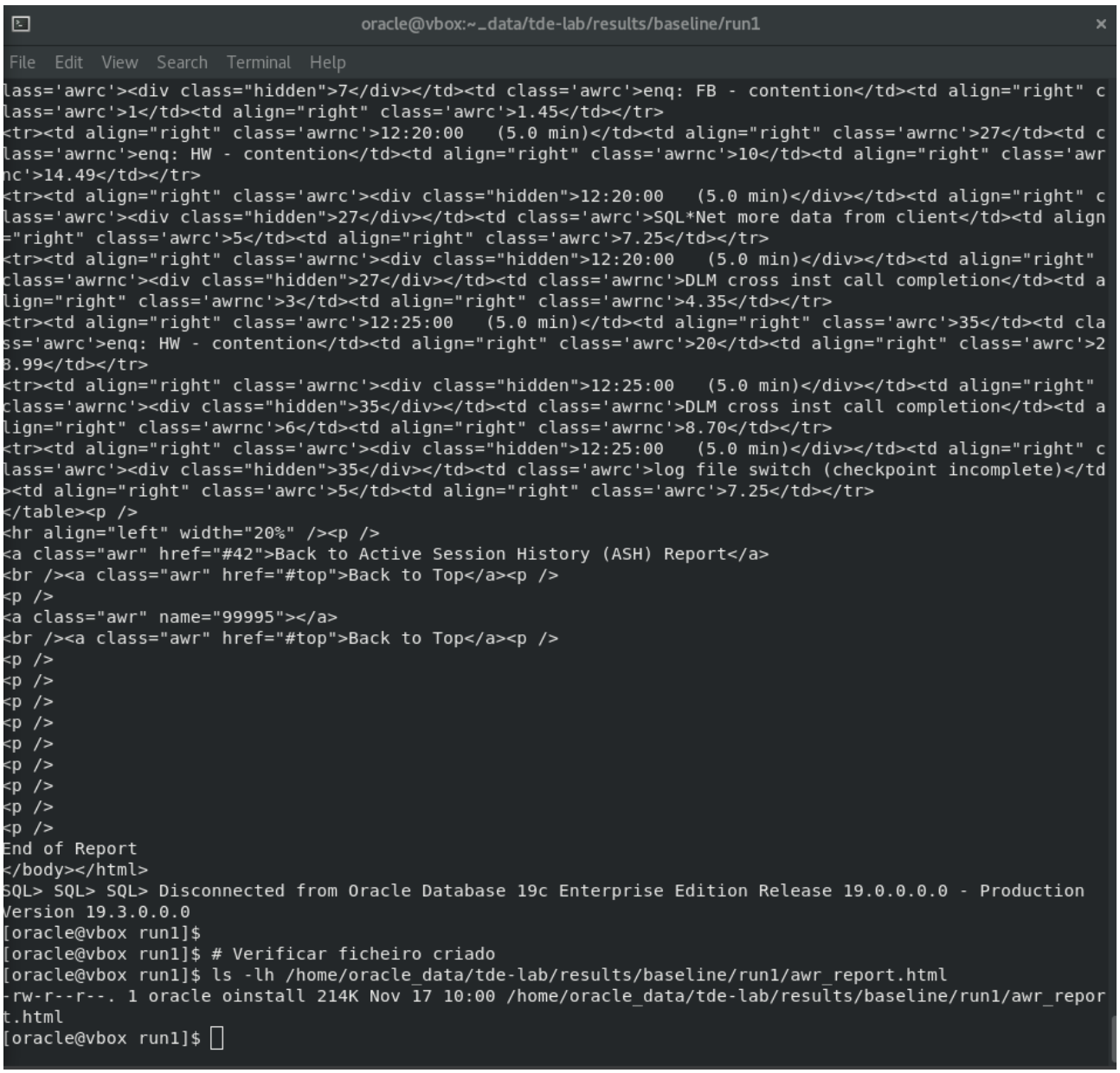
Fonte: Autor

Imagem 20 – Resultados finais do teste *baseline*



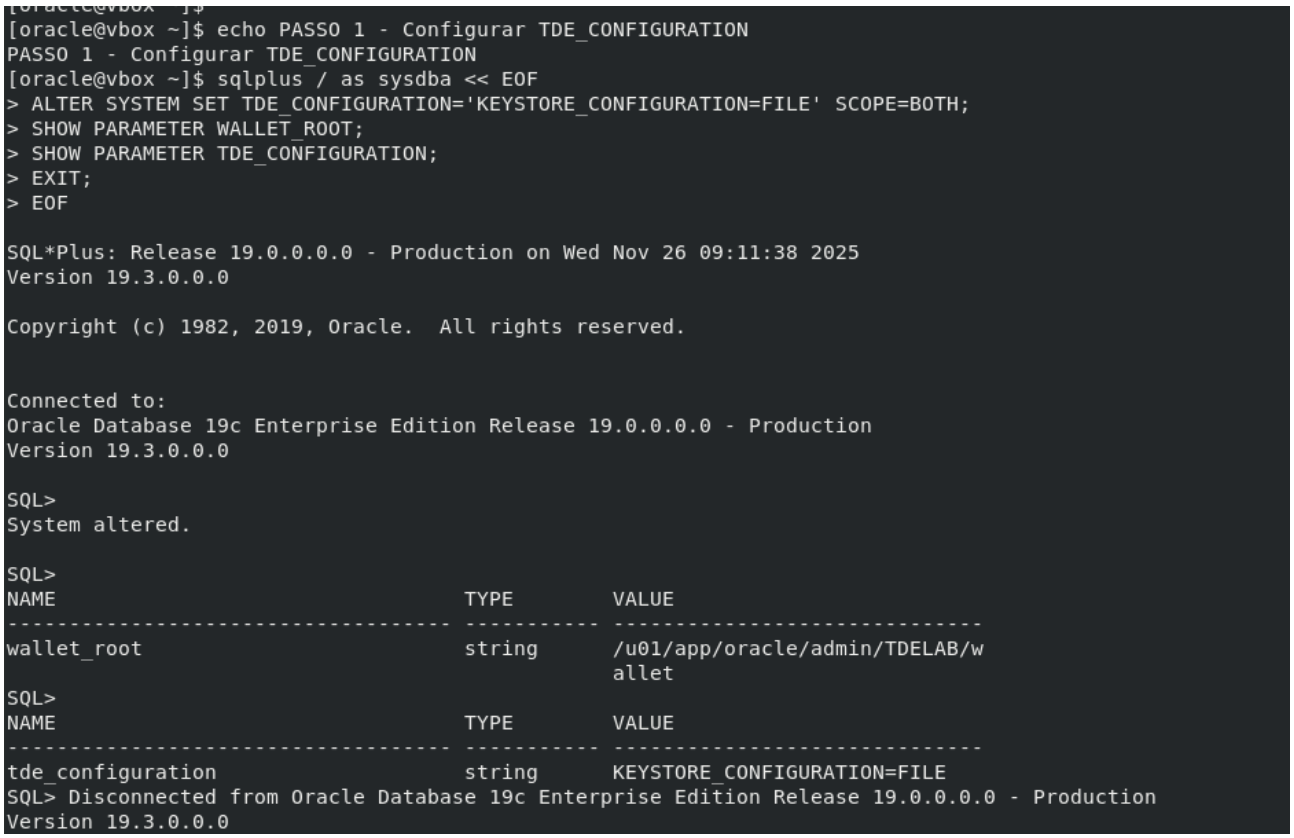
Fonte: Autor

Imagem 21 – Relatório A*utomatic Workload Repository* (AWR) gerado



Fonte: Autor

Imagem 22 – Configuração de parâmetros *Transparent Data Encryption*(TDE)



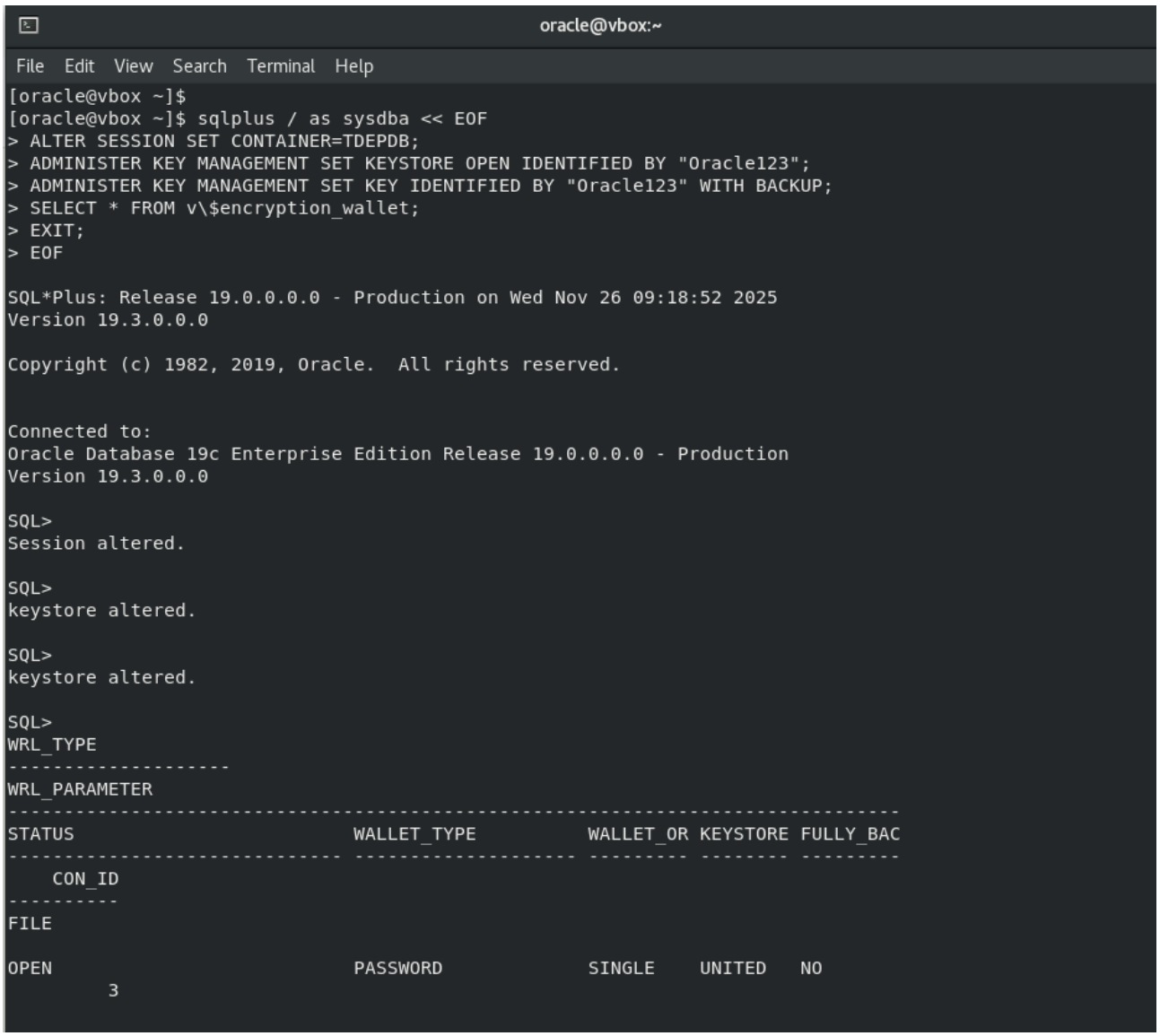
Fonte: Autor

Imagem 23 – *Keystore* com Transparent Data Encryption(TDE) criado

```
[oracle@vbox ~]$ sqlplus / as sysdba << EOF
> ADMINISTER KEY MANAGEMENT CREATE KEYSTORE IDENTIFIED BY "Oracle123";
> ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY "Oracle123";
> ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY "Oracle123" WITH BACKUP;
> SELECT * FROM v\$encryption_wallet;
> EXIT;
> EOF

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Nov 26 09:18:18 2025
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL>
keystore altered.

SQL>
keystore altered.

SQL>
keystore altered.

SQL>
WRL_TYPE
--------------------
WRL_PARAMETER
--------------------------------------------------------------------------------
STATUS                         WALLET_TYPE          WALLET_OR KEYSTORE FULLY_BAC
------------------------------ -------------------- --------- -------- ---------
    CON_ID
----------
FILE
/u01/app/oracle/admin/TDELAB/wallet/tde/
OPEN                           PASSWORD             SINGLE    NONE     NO
```

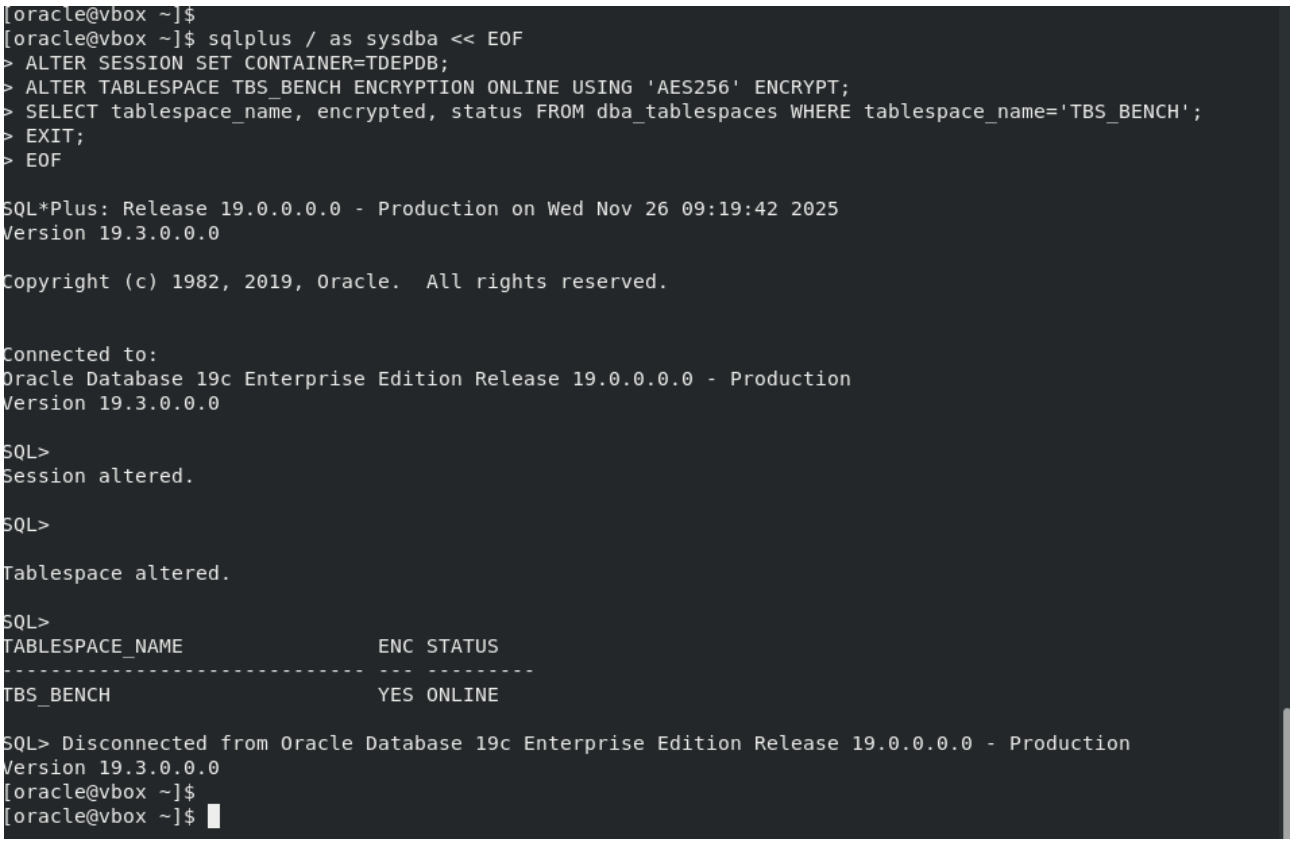
Fonte: Autor

Imagem 24 – *Keystore* aberto



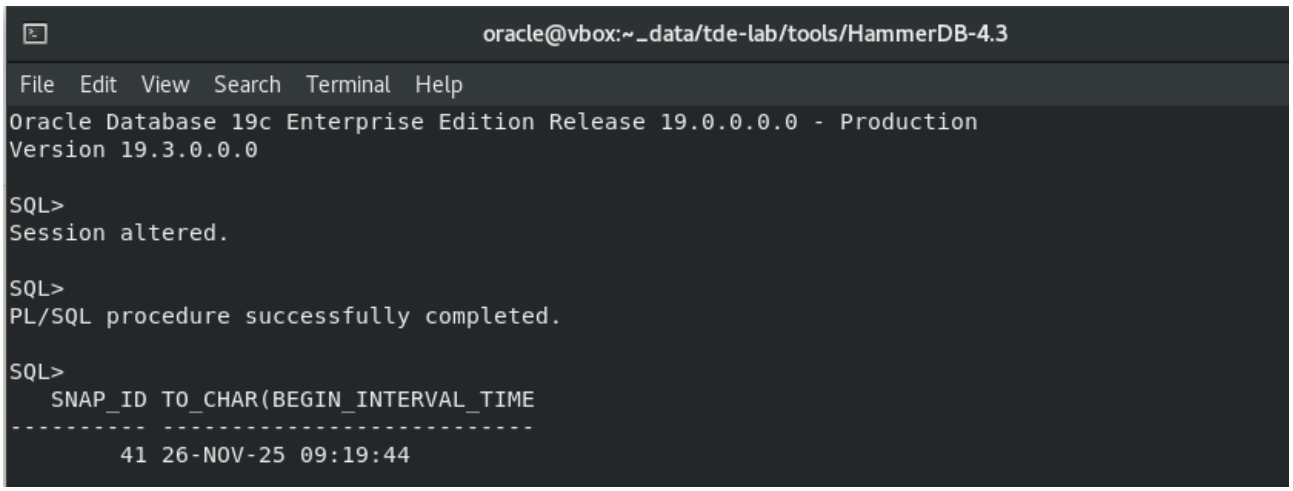
Fonte: Autor

Imagem 25 – *Tablespace* encriptado com *Transparent Data Encryption*(TDE)



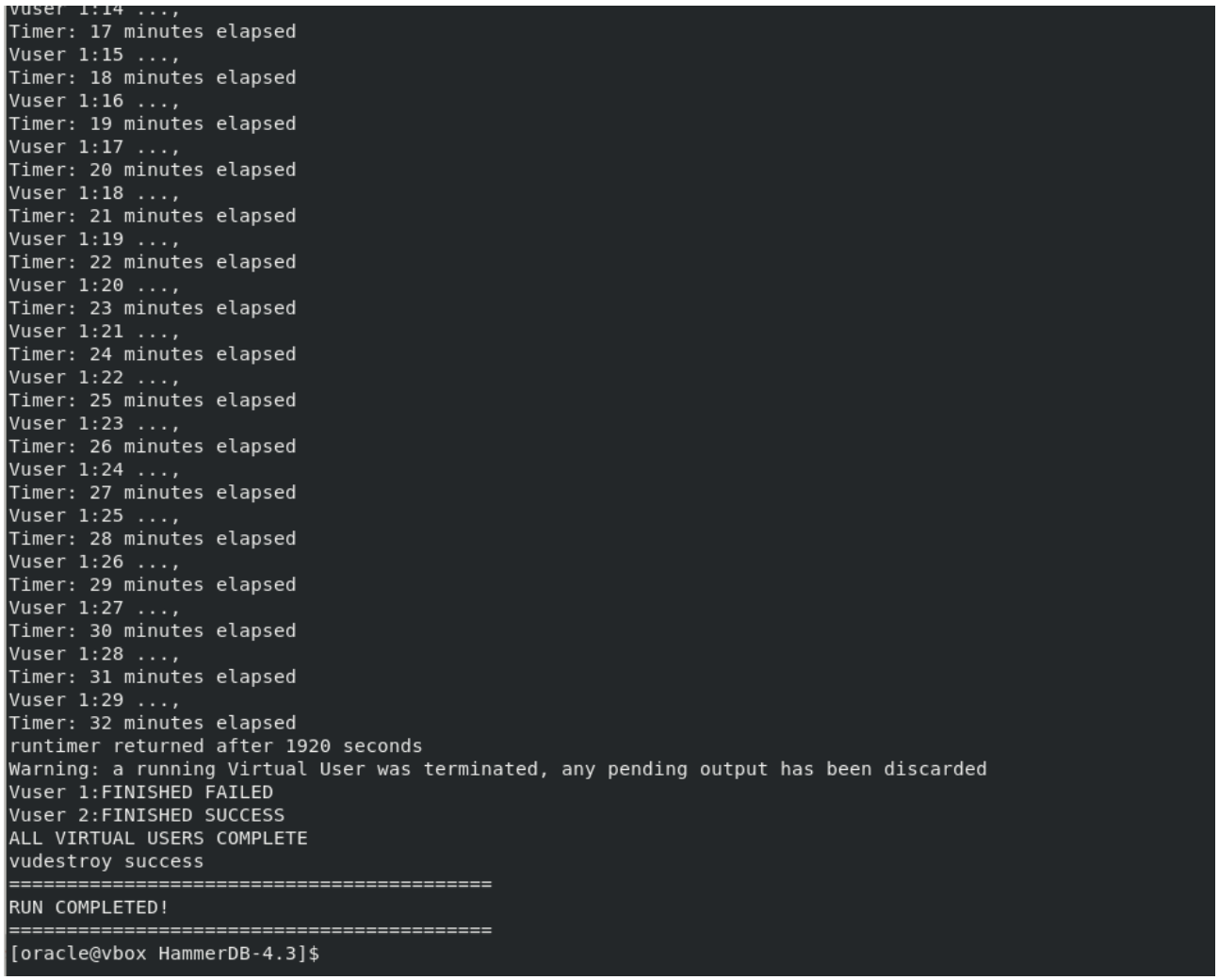
Fonte: Autor

Imagem 26 – *Snapshot* inicial do teste *Transparent Data Encryption(*TDE)



Fonte: Autor

Imagem 27 – Resultados do primeiro teste com *Transparent Data Encryption*(TDE)

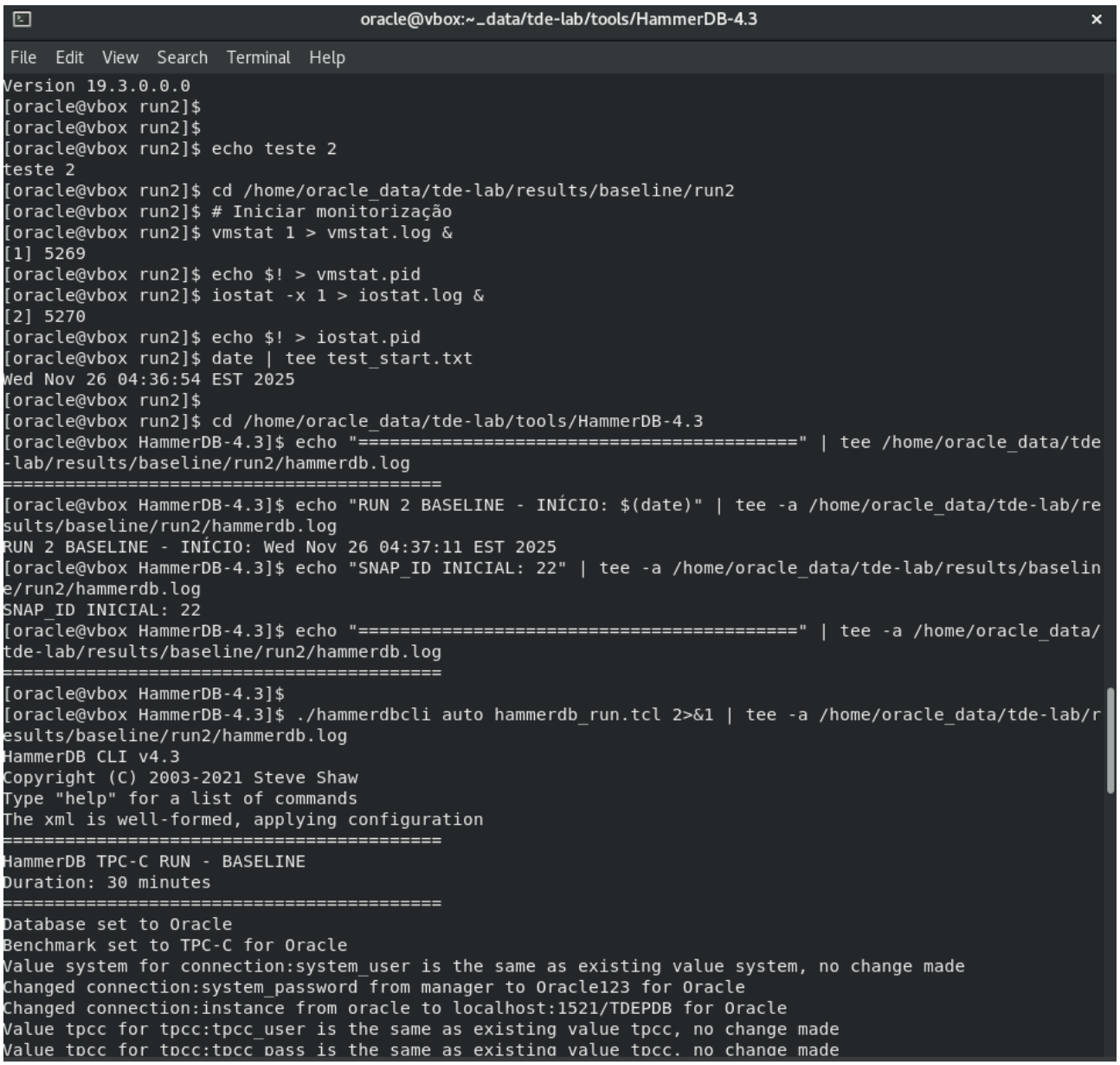


Fonte: Autor

Imagem 28 – *Snapshot* inicial do segundo teste *Transparent Data Encryption*(TDE)

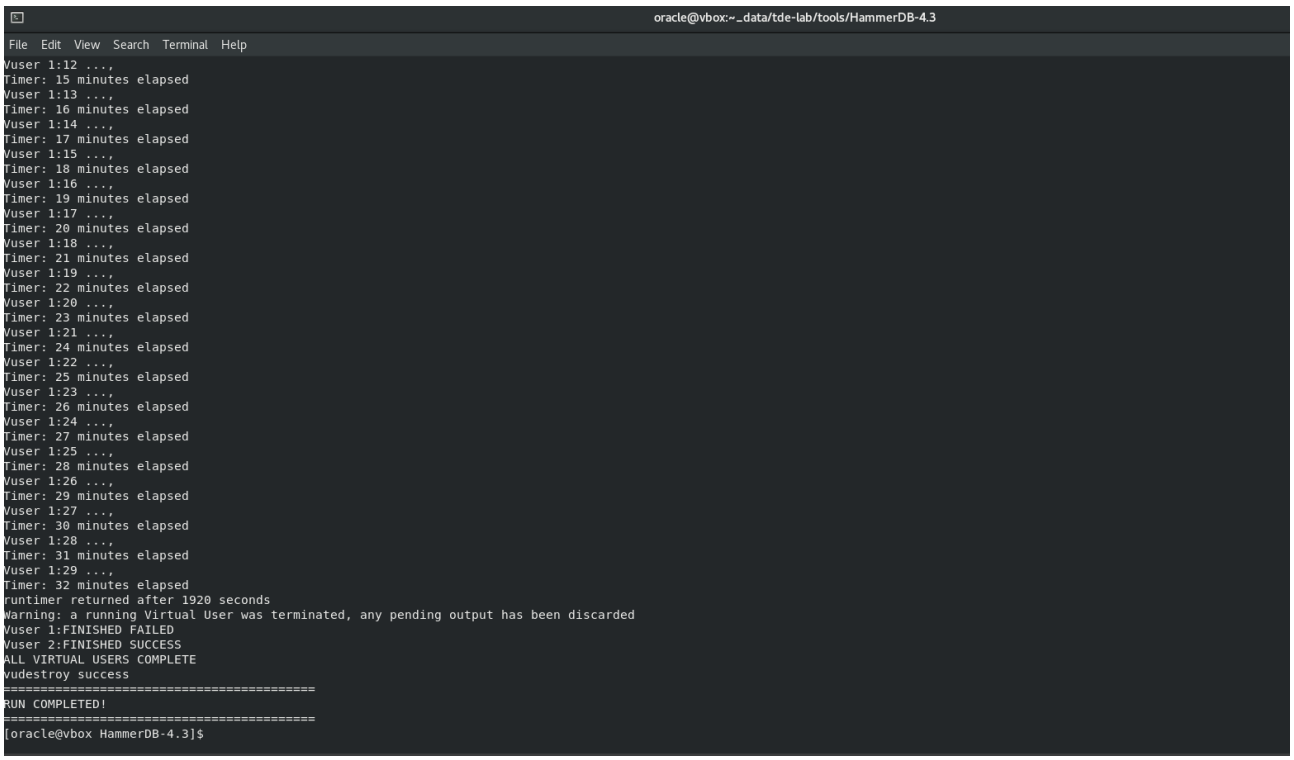
```
[oracle@vbox run1]$ echo run2 TDE
run2 TDE
[oracle@vbox run1]$ sudo sync
[oracle@vbox run1]$ sudo sh -c "echo 3 > /proc/sys/vm/drop_caches"
[oracle@vbox run1]$ mkdir -p /home/oracle_data/tde-lab/results/tde-file/run2
[oracle@vbox run1]$ cd /home/oracle_data/tde-lab/results/tde-file/run2
[oracle@vbox run2]$ sqlplus / as sysdba << EOF
> ALTER SESSION SET CONTAINER=TDEPDB;
> EXEC dbms_workload_repository.create_snapshot;
> SELECT snap_id, TO_CHAR(begin_interval_time, 'DD-MON-YY HH24:MI:SS') FROM dba_hist_snapshot WHERE dbid
= (SELECT dbid FROM v\$database) ORDER BY snap_id DESC FETCH FIRST 1 ROWS ONLY;
> EXIT;
> EOF

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Nov 26 10:23:56 2025
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL>
Session altered.

SQL>
PL/SQL procedure successfully completed.

SQL>
   SNAP_ID TO_CHAR(BEGIN_INTERVAL_TIME
---------- --------------------------
        44 26-NOV-25 10:00:56

SQL> Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
[oracle@vbox run2]$
```

Imagem 29 – Início do segundo teste *Transparent Data Encryption*(TDE)



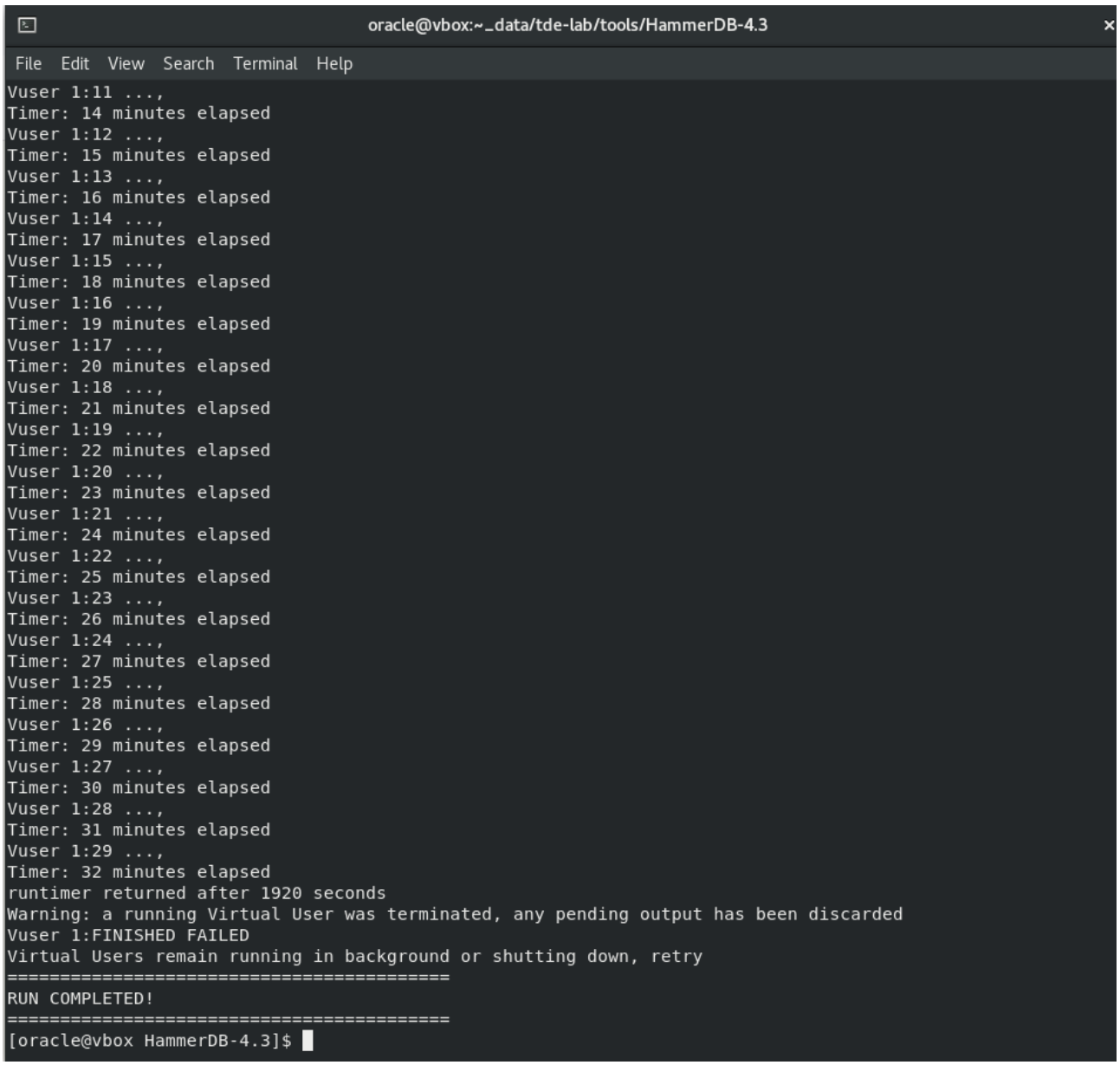
Fonte: Autor

Imagem 30 – Conclusão do segundo teste *Transparent Data Encryption*(TDE)



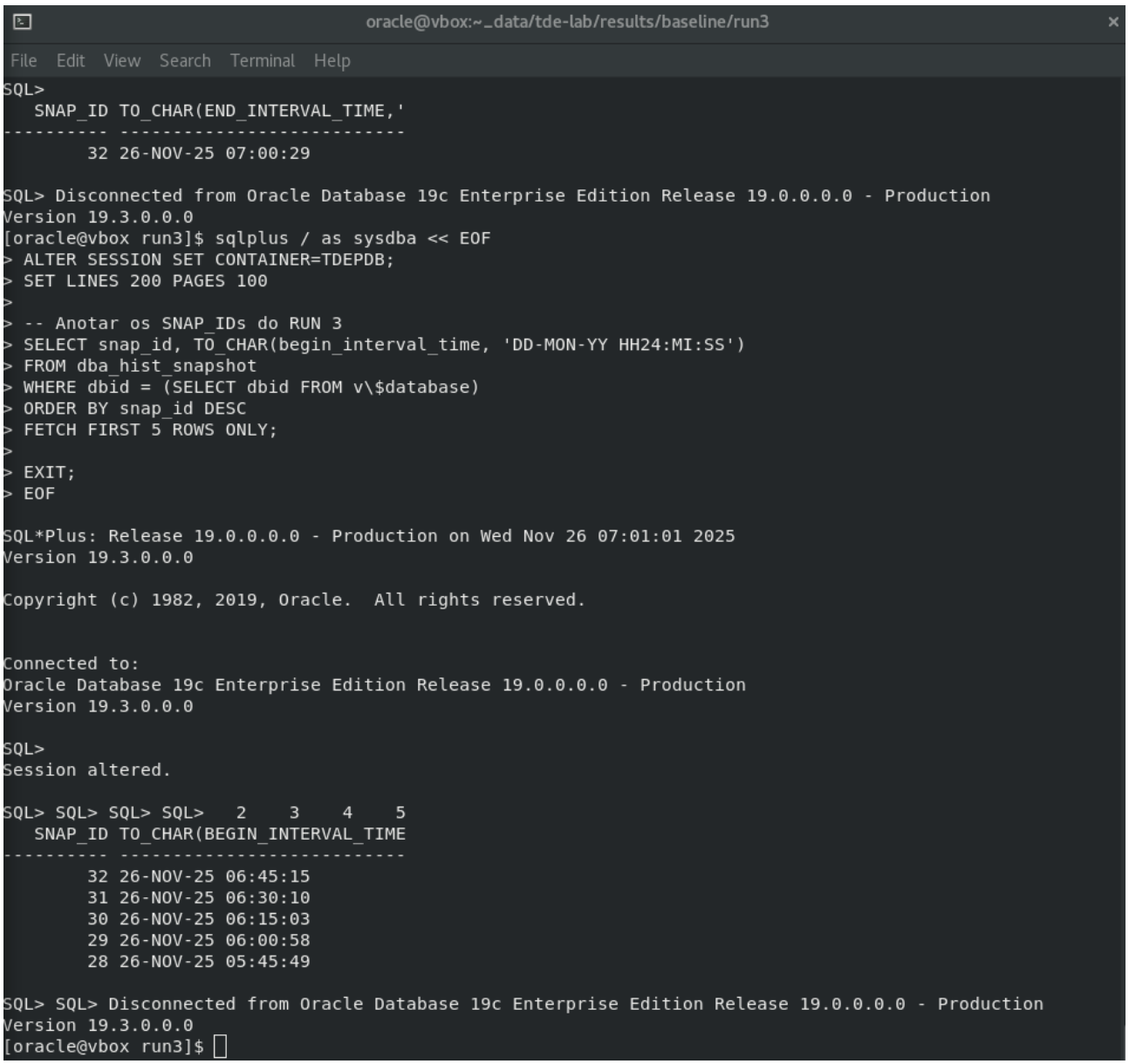
Fonte: Autor

Imagem 31 – Comparação de resultados (Execução 2)



Fonte: Autor

Imagem 32 – *Timeline* de *snapshots* AWR (Execução 3)



Fonte: Autor

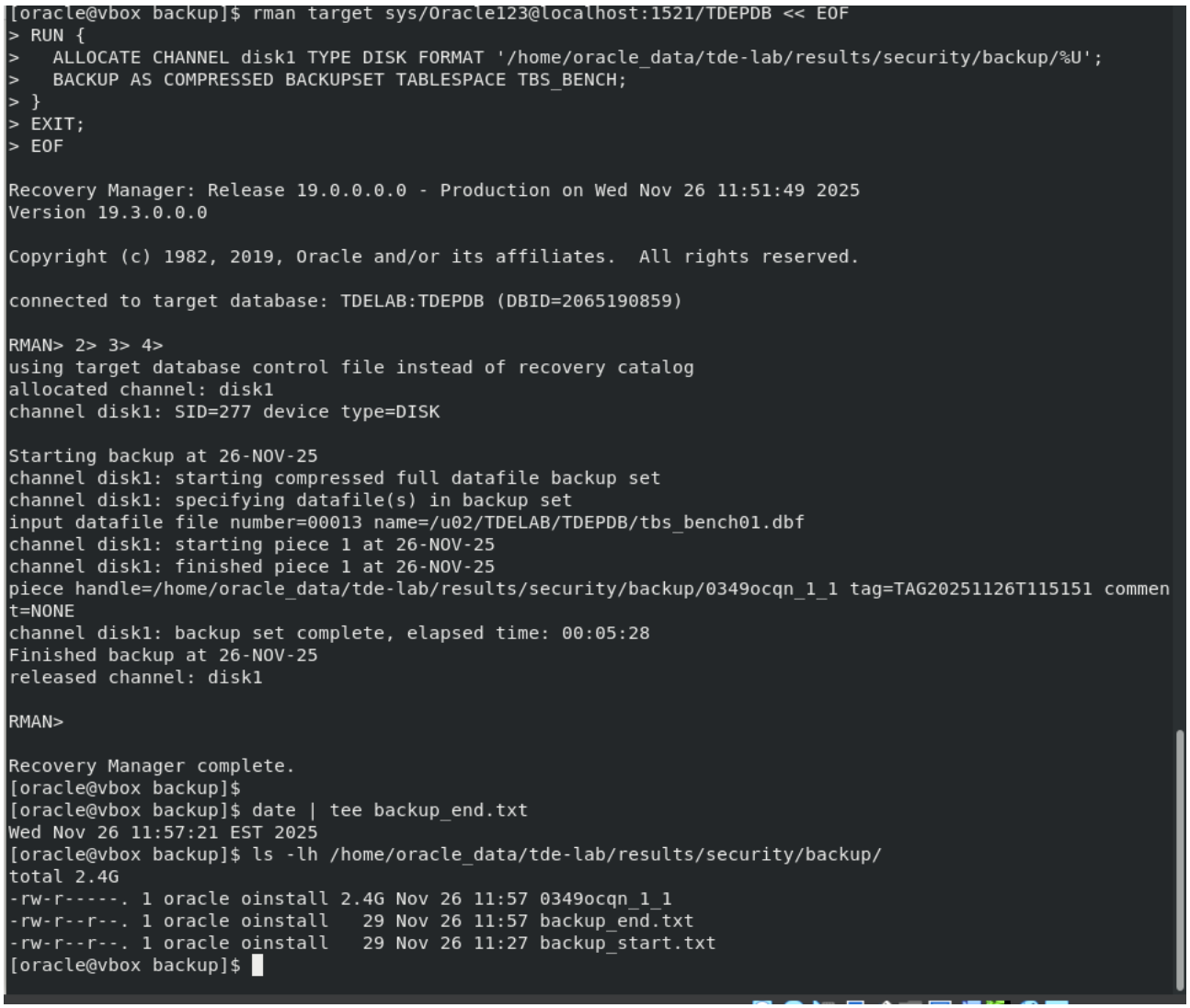
ANEXO C: TESTES DE SEGURANÇA E RESULTADOS

Imagem 33 – Configuração de encriptação no RMAN

```
[oracle@vbox run1]$
[oracle@vbox run1]$
[oracle@vbox run1]$
[oracle@vbox run1]$
[oracle@vbox run1]$ # Criar estrutura para testes de segurança
[oracle@vbox run1]$ mkdir -p /home/oracle_data/tde-lab/results/security/{backup,physical-attack}
[oracle@vbox run1]$ mkdir -p /home/oracle_data/tde-lab/screenshots/phase4_security
[oracle@vbox run1]$
[oracle@vbox run1]$
[oracle@vbox run1]$ rman target / << EOF
> CONFIGURE ENCRYPTION FOR DATABASE ON;
> CONFIGURE ENCRYPTION ALGORITHM 'AES256';
> EXIT;
> EOF

Recovery Manager: Release 19.0.0.0.0 - Production on Wed Nov 26 11:25:37 2025
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates.  All rights reserved.

connected to target database: TDELAB (DBID=2066362831)

RMAN>
using target database control file instead of recovery catalog
new RMAN configuration parameters:
CONFIGURE ENCRYPTION FOR DATABASE ON;
new RMAN configuration parameters are successfully stored

RMAN>
new RMAN configuration parameters:
CONFIGURE ENCRYPTION ALGORITHM 'AES256';
new RMAN configuration parameters are successfully stored

RMAN>

Recovery Manager complete.
[oracle@vbox run1]$
```

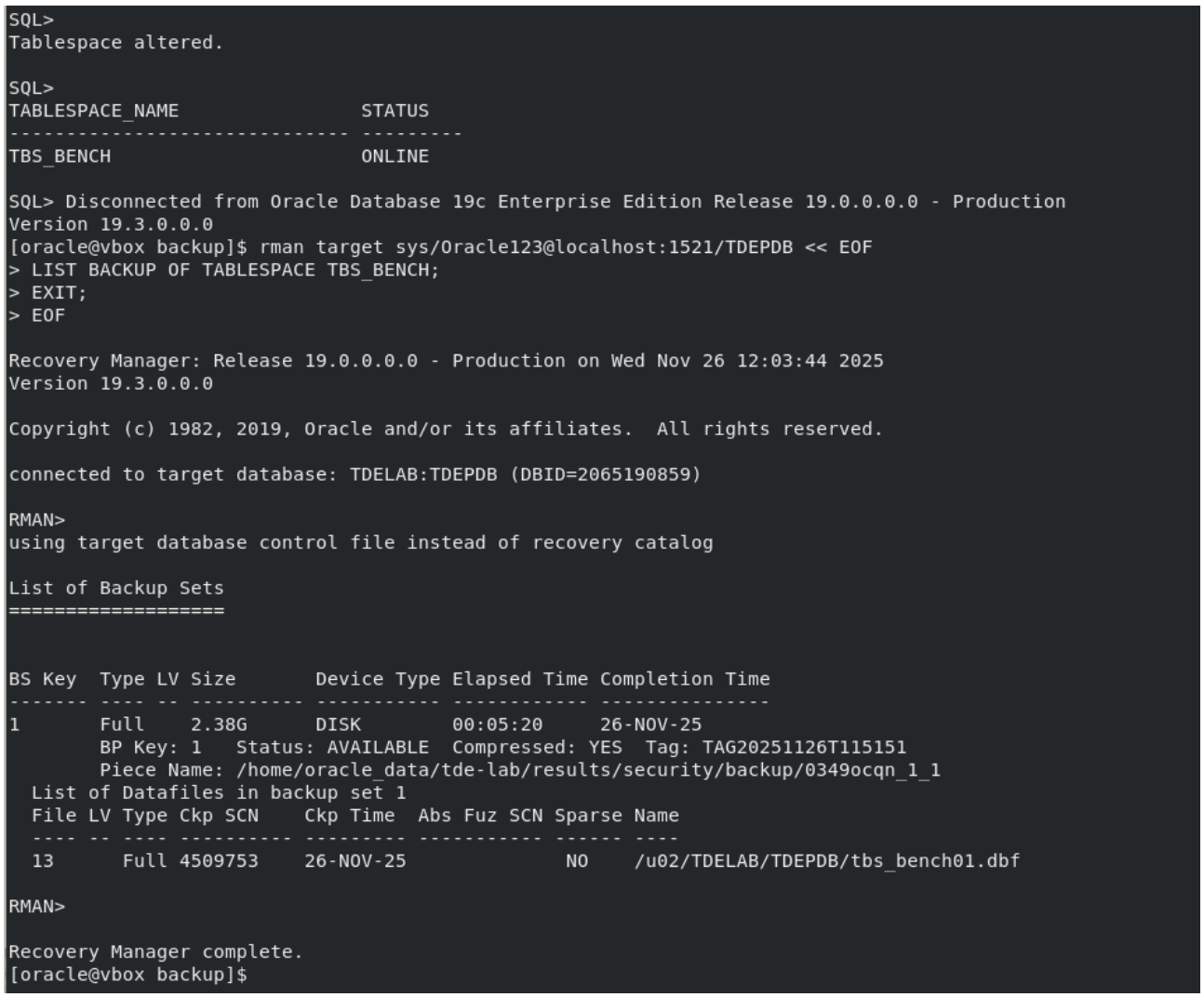
Fonte: Autor

Imagem 34 – *Backup* RMAN concluído



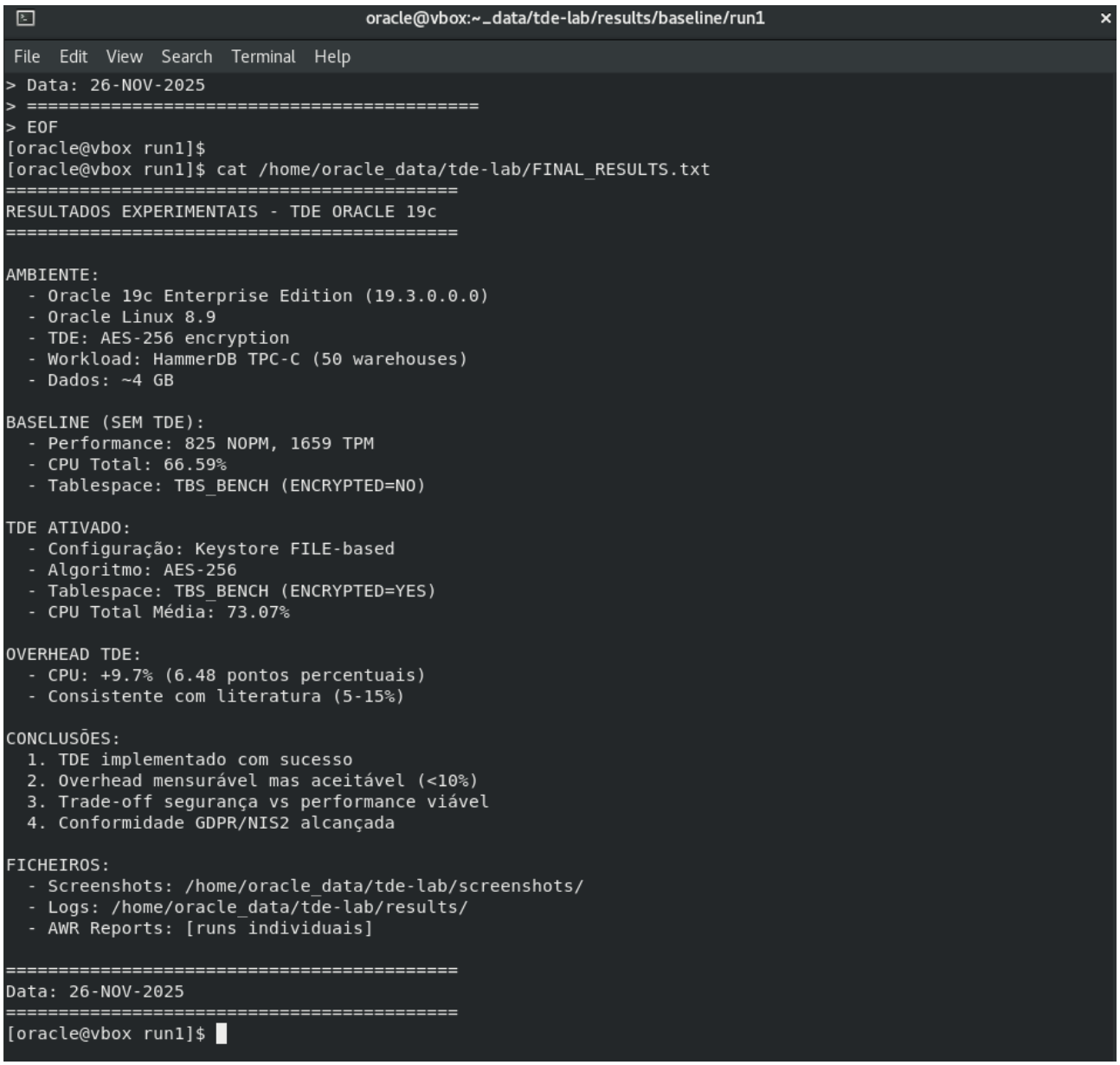
Fonte: Autor

Imagem 35 – Verificação do *backup* encriptado



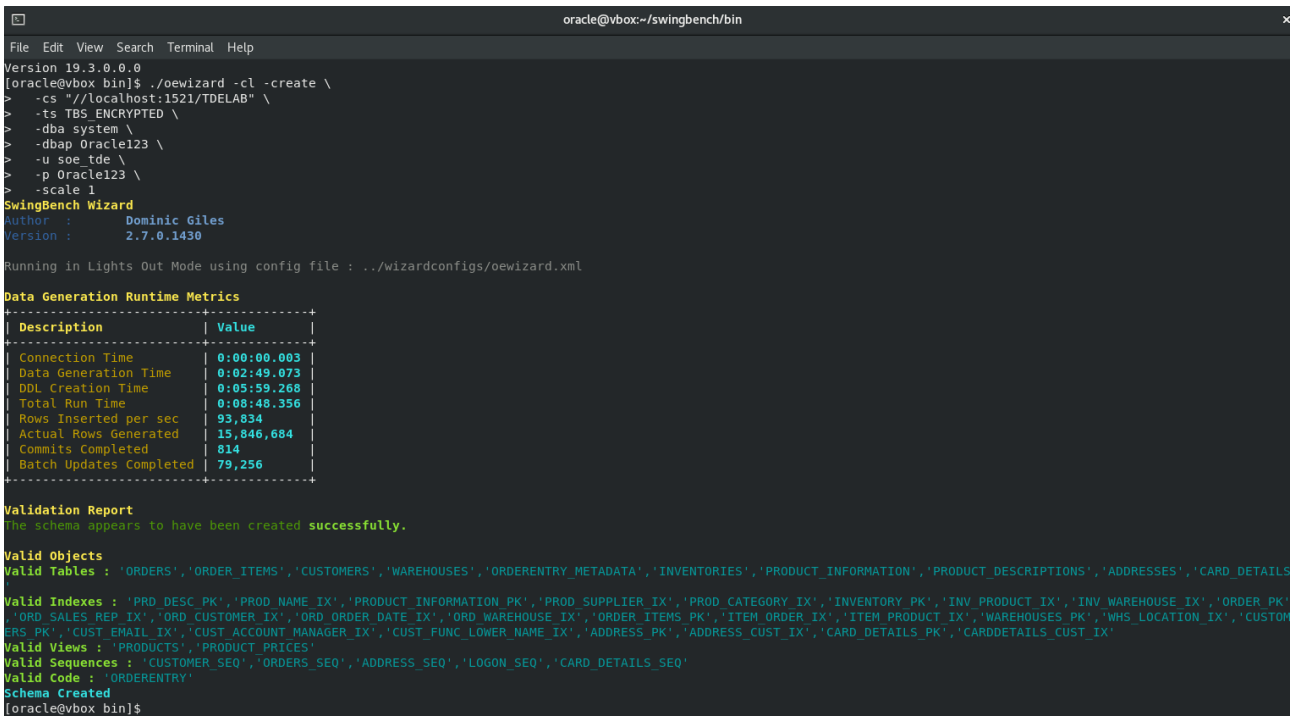
Fonte: Autor

Imagem 36 – Resultados consolidados finais



Fonte: Autor

Imagem 37 – *Schema* TDE SOE cifrado



Fonte: Autor