UNIVERSIDADE REGIONAL DE BLUMENAU

CENTRO DE CIÊNCIAS EXATAS E NATURAIS

CURSO DE SISTEMAS DE INFORMAÇÃO – BACHARELADO

SISTEMA PARA AUDITORIA DE SEGURANÇA DE BANCO DE DADOS ORACLE

ALAN FILIPE MATTIOLLO

BLUMENAU
2012

2012/2-01

ALAN FILIPE MATTIOLLO

SISTEMA PARA AUDITORIA DE SEGURANÇA DE BANCO DE DADOS ORACLE

Trabalho de Conclusão de Curso submetido à Universidade Regional de Blumenau para a obtenção dos créditos na disciplina Trabalho de Conclusão de Curso II do curso de Sistemas de Informação — Bacharelado.

Prof. Cláudio Ratke, Mestre - Orientador

BLUMENAU
2012

2012/2-01

SISTEMA PARA AUDITORIA DE BANCO DE DADOS ORACLE

Por

ALAN FILIPE MATTIOLLO

Trabalho aprovado para obtenção dos créditos na disciplina de Trabalho de Conclusão de Curso II, pela banca examinadora formada por:

Presidente:	Prof. Cláudio Ratke, Mestre – Orientador, FURB
Membro:	Prof. Alexander Roberto Valdameri, Mestre – FURB
Membro:	Prof. Paulo Fernando da Silva, Mestre – FURB

Blumenau, 11 de dezembro de 2012.

Dedico este trabalho a todos os amigos, especialmente aqueles que me ajudaram diretamente na realização deste.

AGRADECIMENTOS

A Deus, pelo seu imenso amor e graça.

À minha família, que mesmo longe, sempre esteve presente.

Aos meus amigos, pelos empurrões e cobranças.

Ao meu orientador, Cláudio Ratke, por ter acreditado na conclusão deste trabalho.

Aos professores do Departamento de Sistemas e Computação da Universidade Regional de Blumenau por suas contribuições durante os semestres letivos.

Os bons livros fazem “sacar” para fora o que a pessoa tem de melhor dentro dela.

Lina Sotis Francesco Moratti

RESUMO

Este trabalho apresenta o desenvolvimento de um sistema que auxilia os administradores de banco de dados na tarefa de preparar um ambiente Oracle para auditoria de segurança. O sistema foi desenvolvido através do *Oracle Application Express* e do *Oracle Database 11g*, utilizando como servidor *web* o *Oracle Weblogic* em conjunto com o *Oracle Application Express Listener*. O mesmo foi implantado na empresa Teclógica e apresenta um modelo de segurança padrão que permite a alteração de várias configurações, possibilitando a adequação do sistema a diferentes níveis e necessidades de segurança. O resultado após a utilização deste sistema evidencia todas as alterações necessárias para que determinado banco de dados passe a ser mais seguro.

Palavras-chave: Banco de dados. Segurança. Auditoria. Oracle.

ABSTRACT

This paper presents the development of a system that helps database administrators in the task of preparing an Oracle environment for security audit. The system was developed over Oracle Application Express and Oracle Database 11g, using as web server the Oracle Weblogic in conjunct with Oracle Application Express Listener. The system was deployed in the enterprise Teclógica and presents a default security model and allows modification of various configurations, enabling the system's suitability to different levels and security needs. The result after the use of this system evidence all necessary changes to that particular database become safer.

Key-words: Database. Security. Audit. Oracle.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

APEX – *Application Express*

CC – *Common Criteria*

CCRA – *Common Criteria Recognition Arragement*

CEM – *Common Methodology for Information Technology Security Evaluation*

CIS – *Center for Internet Security*

CMP – *Configuration Management Pack*

DBA – *Database Administrator*

EA – *Enterprise Architect*

HTML – *HyperText Markup Language*

IEC – *International Electrotechnical Commission*

ISO – *International Organization for Standardization*

MER – Modelo de Entidade e Relacionamento

ORDBMS – *Object-Relational Database Management System*

PL/SQL – *Procedural Language/Structured Query Language*

RAC – *Real Application Clusters*

RAD – *Rapid Application Development*

RDBMS – *Relational Database Management System*

SGA – *System Global Area*

SGBD – Sistema Gerenciador de Banco de Dados

SLA – *Service-Level Agreement*

SQL – *Structured Query Language*

TCP/IP – *Transmission Control Protocol/Internet Protocol*

TI – Tecnologia da Informação

TNS – *Transparent Network Substrate*

TOE – *Target of Evaluation*

SUMÁRIO

1 INTRODUÇÃO

Segundo Date (2004), um banco de dados é basicamente um sistema computadorizado que mantém registros. O banco de dados pode ser considerado uma espécie de armário eletrônico de arquivamento, isto é, ele é um repositório ou contêiner para uma coleção computadorizada de arquivos de dados. Usuários do sistema podem realizar uma variedade de operações envolvendo estes arquivos de dados.

Os bancos de dados estão por trás dos sistemas que afetam quase todos os aspectos da vida das pessoas - contas bancárias, registros médicos, registros de emprego, registros telefônicos, compras em supermercado, taxas de impostos - quase todas as informações que possuem significado estão armazenadas em um sistema moderno de gerenciamento relacional de banco de dados. Com o aumento da utilização do comércio eletrônico e de sistemas baseados na web, os bancos de dados estão cada vez mais próximos das redes de computadores (LITCHFIELD et al., 2005).

Segundo Natan (2005), o comércio e o negócio eletrônico mudou a forma como as pessoas vivem. Os sistemas se tornaram muito integrados e muito próximos aos usuários finais. Há dez anos os bancos de dados eram acessados somente por aplicações disponíveis aos empregados, agora são acessados através de *web sites* de qualquer parte do mundo.

Estes sistemas requerem o armazenamento, processamento e oferecem acesso a informações pessoais. Os sistemas que armazenam segredos corporativos ou informações financeiras não são diferentes. Muitos dos dados armazenados são extremamente sensíveis, mas precisam estar disponíveis e serem de fácil acesso. Esta situação cria um grande desafio no campo de segurança da informação (SHAUL; INGRAM, 2007).

O Sistema Gerenciador de Banco de dados (SGBD) Oracle tem uma vasta quantidade de funções, produtos e ferramentas relacionadas à segurança. Infelizmente, o fato de estes recursos existirem não significa que são utilizados corretamente ou mesmo que são utilizados. A maioria dos usuários está familiarizada com menos de 20% dos mecanismos de segurança do Oracle. Isto leva a ambientes inseguros e/ou a utilização de ferramentas inadequadas (NATAN, 2009).

De acordo com Knox (2004), manter um banco de dados seguro pode ser a maior ação que uma organização pode tomar para pró ativamente defender-se contra ameaças. O banco de dados é o cofre que mantém os mais valiosos ativos digitais de uma organização. A exposição destes ativos pode levar a publicidade negativa, processos, perda de receita, perda

de confiança do consumidor, entre outros resultados negativos.

Em um relatório do ITRC (2011), 414 violações de segurança foram descobertas nos Estados Unidos em 2011. Isto representa mais de 22 milhões de registros com informações sensíveis de identidade ou de cartão de crédito comprometidas.

Todas as empresas deveriam possuir um manual de segurança documentando regras e procedimentos. Em segurança não há certo ou errado, há somente conformidade ou não conformidade aos procedimentos acordados. Se os administradores de banco de dados seguirem as regras e aconselharem como estas regras devem estar configuradas, então, qualquer violação de segurança não será sua falha. Seguir um manual de segurança devolve a responsabilidade aos autores deste (WATSON; RAMKLASS; BRYLA, 2010).

De acordo com Stewart, Tittel e Chapple (2005), o processo de auditoria é comumente usado para testes ou verificações de conformidade. A verificação de que um sistema está em conformidade com leis, regulamentos, normas, padrões e politicas é parte importante da tarefa de manter a segurança em qualquer ambiente. Testes de conformidade asseguram que todos os elementos necessários e requeridos de uma solução de segurança estejam propriamente implantados e funcionando conforme o esperado.

Todo final de ano, um cliente da empresa Teclógica é submetido a um processo de auditoria de segurança pela sua detentora, uma empresa internacional. Os auditores possuem uma extensa lista de requisitos que devem ser atendidos nos ambientes de banco de dados. Antes da auditoria acontecer, os administradores de banco de dados da Teclógica devem verificar todos estes requisitos e apontar os ajustes necessários para aqueles que não estiverem em conformidade com o manual de regras.

Verificar todas as configurações em vários bancos de dados é um processo bastante demorado e pode resultar em erros e incoerências. Cada recurso que necessita de ajuste demanda pesquisa e verificações para viabilizar ou não sua alteração no ambiente.

Visando automatizar e melhorar o processo de auditoria de segurança, o presente trabalho verifica o nível de segurança de um banco de dados Oracle e deve informar as alterações necessárias para adequação ao modelo de segurança escolhido.

1.1 OBJETIVOS DO TRABALHO

O principal objetivo deste trabalho é apresentar o desenvolvimento de um sistema que verifique o nível de segurança de um banco de dados Oracle, visando facilitar a análise das alterações necessárias para que o ambiente em questão se torne mais seguro.

Os objetivos específicos do trabalho proposto são:

a) desenvolver módulos que permitam o cadastro de valores para os diversos parâmetros e recursos de segurança para posterior verificação de conformidade;
b) desenvolver relatórios que informem as inconformidades de segurança da base de dados e os valores das configurações que precisam ser ajustadas para que se adequem ao modelo de segurança escolhido;
c) permitir a análise de verificações anteriores, mantendo um histórico para consulta.

1.2 ESTRUTURA DO TRABALHO

No primeiro capítulo tem-se a introdução ao tema principal deste trabalho com a apresentação da justificativa e dos objetivos.

No segundo capítulo apresenta-se a fundamentação teórica pesquisada sobre o *Common Criteria*, a auditoria, a arquitetura do banco de dados Oracle, a segurança em banco de dados Oracle, o *Oracle Listener*, a autenticação de banco de dados, a autorização, o *Oracle Application Express* (APEX), o cenário atual e os trabalhos correlatos.

O terceiro capítulo apresenta o desenvolvimento do sistema iniciando-se com o levantamento de informações, tendo na sequência as especificações, a implementação e a operacionalidade da aplicação.

No quarto capítulo têm-se as conclusões deste trabalho bem como se apresentam sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo aborda assuntos como o *Common Criteria*, auditoria, arquitetura do banco de dados Oracle, segurança em banco de dados Oracle, *Oracle Listener*, autenticação de banco de dados, autorização, *Oracle APEX*, o cenário atual e os trabalhos correlatos.

2.1 COMMON CRITERIA

O *Common Criteria for Information Technology Security Evaluation* (abreviado como *Common Criteria* ou CC) é um padrão internacional (ISO/IEC 15408) para certificação de segurança de produtos de tecnologia da informação (TI). O CC é acompanhado pelo *Common Methodology for Information Technology Security Evaluation* (CEM), os dois são a base técnica para um acordo internacional, o *Common Criteria Recognition Arrangement* (CCRA), que segundo o *Common Criteria Portal* (2012), assegura que:

a) os produtos podem ser avaliados por laboratórios independentes e licenciados, de modo a determinar o cumprimento de propriedades particulares de segurança, em certa medida ou garantia;
b) documentos de suporte são utilizados no processo de certificação do CC para definir como os critérios e métodos de avaliação são aplicados para certificar tecnologias especificas;
c) a certificação das propriedades de segurança do produto avaliado pode ser emitido por uma série de centros de certificação autorizados, com esta certificação sendo baseada no resultado de sua avaliação.

De acordo com o *Common Criteria Portal* (2012), estas certificações são reconhecidas por todos os signatários do CCRA. Os participantes deste acordo compartilham os seguintes objetivos:

a) garantir que as avaliações do produtos de TI e modelos de proteção serão realizadas com padrões elevados e consistentes, e devem contribuir significativamente para a confiança na segurança destes produtos ou modelos;
b) melhorar a disponibilidade de avaliações de produtos de TI e modelos de proteção

de segurança avançada;

c) eliminar a carga de avaliações duplicadas de produtos de TI e modelos de proteção;
d) melhorar continuamente a eficiência e eficácia dos custos de avaliação e certificação de produtos de TI e modelos de proteção.

Wallace (2003) define o *Common Criteria* como um conjunto internacional reconhecido de padrões e configurações técnicas, que permitem avaliações de segurança de produtos de TI. Um grupo individual de critérios com padrões técnicos e configurações desenvolvidas para um produto especifico ou tecnologia, é qualificado como um modelo de proteção.

O relatório de Weber (2012), mostra que o *Oracle Database 11g Release 2 Enterprise Edition* é certificado usando a CEM versão 3.1 em conformidade com o CC versão 3.1. Neste relatório são evidenciadas todas as funcionalidades de segurança que compõe o software *Oracle Database 11g Release 2 Enterprise Edition*, que é definido como um sistema gerenciador de banco de dados objeto-relacional (ORDBMS), que fornece funcionalidades avançadas de segurança em ambientes distribuídos de banco de dados:

a) identificação e autenticação de usuários, com opções de gerenciamento de senha;
b) disponibiliza controle de acesso aos objetos de banco de dados baseado na identidade de indivíduos ou grupo de indivíduos a que estes objetos pertencem, permitindo que usuários autorizados especifiquem como os objetos sob seu controle serão protegidos;
c) privilégios granulares para aplicação do conceito de privilégio mínimo;
d) atribuições configuráveis pelo usuário para gerenciamento de privilégios;
e) cotas sobre a quantidade de recursos de processamento que um usuário pode consumir durante uma sessão de banco de dados;
f) funções para auditoria que geram informações sobre todos os eventos auditáveis;
g) opções extensíveis e flexíveis de auditoria;
h) acesso seguro a bancos de dados Oracle remotos;
i) procedimentos armazenados, gatilhos e políticas de segurança para controle de acesso e auditoria.

O Quadro 1 referencia os requisitos funcionais de segurança implementados através das funcionalidades de segurança do *Target of Evaluation* (TOE) em questão, o *Oracle Database 11g Release 2*:

TOE Security Functionality	***Addressed issue***
F.IA	*Identification and Authentication*
F.LIM	*Resource Control – Database Resources*
F.DAC	*Discretionary Access Control*
F.APR	*Granting and Revoking privileges and Roles*
F.PRI	*Effective Privileges*
F.AUD	*Audit and Accountability*
F.CON	*Data Consistency*

Fonte*: Common Criteria Portal* (2012).

Quadro 1 – Funcionalidades de Segurança do *Oracle Database 11g Release 2*

2.2 AUDITORIA

A auditoria é um exame metódico ou revisão de um ambiente que tem por objetivo garantir complacência com regulamentos e detectar anomalias. A segurança de um ambiente de TI depende fortemente da auditoria. Verificações de conformidade têm por objetivo garantir que todos os elementos necessários de uma solução de segurança estejam apropriadamente implantados e funcionando conforme o esperado. Auditorias podem ser realizadas de uma das duas perspectivas: internamente ou externamente. Empregados que trabalham no ambiente de TI e conhecem as soluções de segurança, realizam auditorias internas. Auditores independentes de fora do ambiente de TI e que não estão familiarizados com as soluções de segurança, realizam auditorias externas. O objetivo das duas formas de auditoria é medir o quão efetiva é a solução de segurança implantada (STEWART; TITTEL; CHAPPLE, 2005).

Segundo Watson, Ramklass e Bryla (2010), não importam quão boas são as politicas de segurança, haverá ocasião na qual uma politica não será suficiente, será preciso aceitar que existem usuários com privilégios que podem ser perigosos. A solução é monitorar o uso destes privilégios por parte dos usuários e verificar o que está sendo feito. O Oracle disponibiliza três técnicas de auditoria:

a) a auditoria de banco de dados rastreia o uso de certos privilégios, a execução de

certos comandos, o acesso a certas tabelas e as tentativas de *logon*;

b) a auditoria baseada em valor usa gatilhos de banco de dados, sempre que uma linha é inserida, atualizada ou excluída, um bloco de código é executado para armazenar informações sobre a operação;
c) a auditoria refinada permite rastrear o acesso a tabelas de acordo com quais linhas e/ou colunas são acessadas.

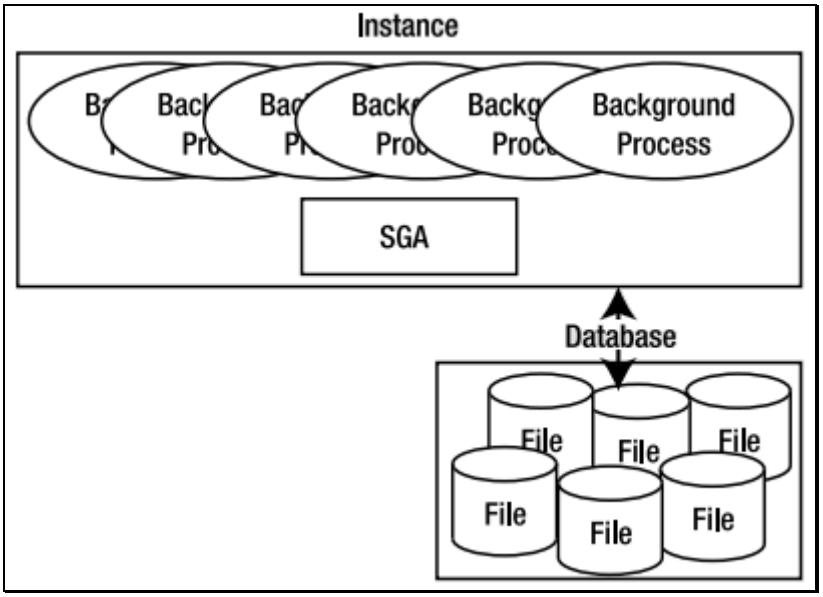
A auditoria, especialmente no ambiente produtivo, envolve uma grande quantidade de dados. Para elevar a segurança usando auditoria é preciso implantar uma solução pragmática, que permita extrair informações úteis dos dados coletados, isto significa explorar a informação para expor anomalias, erros, intrusões, más práticas e violações de politica (NATAN, 2005).

2.3 ARQUITETURA DO BANCO DE DADOS ORACLE

Um banco de dados Oracle é uma coleção de dados em um ou mais arquivos. Um banco de dados contém estruturas físicas e lógicas. Quando se está desenvolvendo uma aplicação, são criadas estruturas lógicas como tabelas e índices, para que respectivamente, armazenem linhas e agilizem suas buscas. Uma instância Oracle compreende uma área de memória chamada *System Global Area* (SGA) e processos de segundo plano, que interagem entre a SGA e os arquivos de banco de dados no disco (LONEY, 2009).

Todos os dados armazenados em um banco de dados Oracle residem em uma *tablespace*. Uma *tablespace* é uma estrutura lógica e é composta por estruturas físicas chamadas arquivos de dados. Cada *tablespace* consiste de um ou mais arquivos de dados, e cada arquivo de dado pode pertencer a somente uma *tablespace*. Quando uma tabela é criada, esta é armazenada em uma *tablespace* (GREENWALD; STACKOWIAK; STERN, 2008).

De acordo com Greenwald, Stackowiak e Stern (2008), os processos em segundo plano interagem entre eles e com o sistema operacional para gerenciar as estruturas de memória da instância. Estes processos também gerenciam o banco de dados no disco e executam uma limpeza geral para a instância. A Figura 1 mostra uma instância e um banco de dados Oracle na sua forma mais simples.

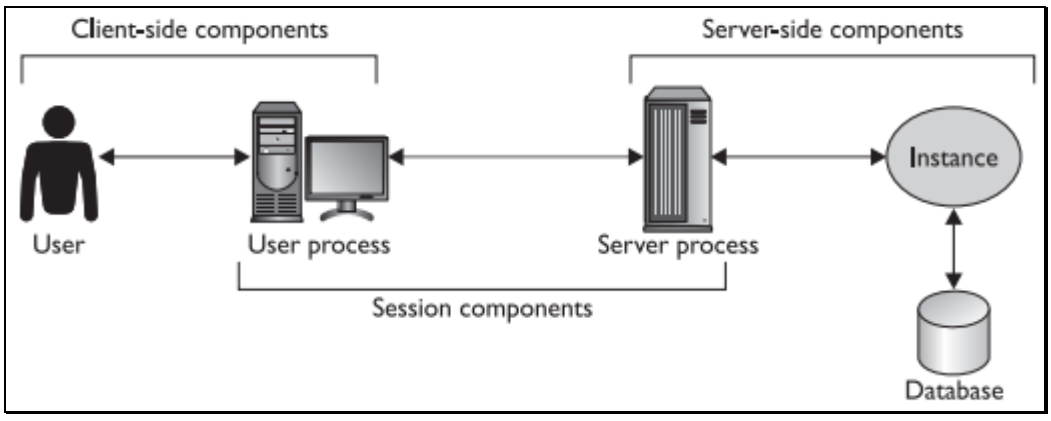


Fonte: Kyte (2010).

Figura 1 – Instância e banco de dados Oracle

De acordo com Watson (2010), a arquitetura de um banco de dados de instância única pode ser resumida pela composição de quatro componentes interagentes, representados graficamente através da Figura 2:

a) um usuário interage com um processo de usuário;
b) um processo de usuário interage com um processo de servidor;
c) um processo de servidor interage com uma instância;
d) uma instância interage com um banco de dados.



Fonte: Watson (2010).

Figura 2 – A conexão indireta entre um usuário e um banco de dados

Em um ambiente *Oracle Real Application Cluster* (RAC), o mesmo banco de dados

será usado por mais de uma instância. As instâncias que compartilham o banco de dados podem estar no mesmo servidor, mas é mais provável que elas estejam em servidores separados, conectadas por uma interconexão de alta velocidade, e que acessam um banco de dados que reside em um subsistema de disco especializado (BRYLA; LONEY, 2009).

Segundo Kyte (2010), o Oracle é projetado para ser um banco de dados bastante portátil, ele está disponível em cada plataforma de relevância, de Windows para UNIX para *mainframes*. Entretanto, a arquitetura física do Oracle é diferente nestes diferentes sistemas operacionais. No sistema operacional UNIX, o Oracle é implementado como muitos processos de sistema operacional, virtualmente um processo para cada função de maior importância. No Windows, entretanto, esta arquitetura é inapropriada e não iria funcionar muito bem (seria lenta e não escalável), assim, no Windows o Oracle é implementado como um único processo com múltiplos *threads*.

No banco de dados Oracle, o dicionário de dados é um conjunto de metadados: dados sobre dados. Ele descreve o banco de dados, tanto física quanto logicamente, e seu conteúdo. As definições de usuários, informações de segurança, restrições de integridade e informações de monitoramento de desempenho fazem parte do dicionário de dados (WATSON, 2010).

2.4 SEGURANÇA EM BANCO DE DADOS ORACLE

O banco de dados Oracle nasceu de um projeto da comunidade de inteligência dos Estados Unidos, chamado Projeto Oracle, executado pela Agência Central de Inteligência. Dado o cliente inicial, segurança era uma preocupação séria desde o primeiro dia (SHAUL; INGRAM, 2007).

De acordo com Watson (2010), o principio mais seguro a seguir quando determinar o acesso aos sistemas de computador é o do menor privilégio: ninguém pode ter acesso a qualquer coisa que esteja além do mínimo absolutamente necessário para executar seu trabalho, e qualquer coisa não especificamente permitida é proibida. O banco de dados Oracle esta de acordo com essas regras e por padrão ninguém pode fazer nada, com exceção dos usuários SYS e SYSTEM.

Os mecanismos de segurança fornecidos pela Oracle dividem-se em três categorias: autenticação, autorização e auditoria. Bryla e Loney (2009) definem autenticação e autorização da seguinte forma:

a) autenticação é um mecanismo que inclui métodos usados para identificar quem está acessando o banco de dados;
b) a autorização fornece acesso a vários objetos do banco de dados;

De acordo com Knox et al. (2010), as implicações de segurança giram em torno de duas coisas: a identificação do usuário para auditoria e prestação de contas, e o controle de acesso para permitir ou impedir os usuários de executar ações especificas, ou acessar dados específicos.

Bryla e Loney (2009) expõem a preocupação de que a segurança não depende somente da configuração dos componentes de software do banco de dados Oracle, os autores relatam a necessidade de manter seguros alguns elementos que ficam fora do banco de dados. A segurança do sistema operacional, das mídias de backup e o acesso controlado ao hardware são tópicos que devem ser considerados. Verificar o que os funcionários com acesso privilegiado – sejam eles administradores de banco de dados, auditores ou administradores de sistema operacional – estão fazendo é imprescindível. Outra necessidade é de que todos os usuários do banco de dados entendam as politicas de uso e segurança da infraestrutura de TI.

O propósito de fortalecer a segurança de um banco de dados é eliminar a maior quantidade de riscos de segurança possíveis. De acordo com Natan (2009), isto pode ser feito removendo todos os elementos não essenciais do banco de dados, selecionando opções que limitem os acessos e diminuam os riscos. Quanto maior for um sistema e as capacidades que ele utiliza, mais riscos de segurança estarão presentes. Entretanto, quanto maior a base de dados e a quantidade de funcionalidades que esta utiliza, mais importante se torna seu fortalecimento. Se algo não é utilizado pelo sistema não significa que não possa ser utilizado por algum invasor. Alguns exemplos de configurações que podem ser alteradas ou removidas se não utilizadas:

a) remover ou bloquear contas pré-definidas e alterar suas senhas;
b) remover grupos de privilégios;
c) remover componentes de software;
d) remover opções não utilizadas, como EXPROC se o sistema não utilizar procedimentos externos;
e) remover privilégios públicos.

O banco de dados Oracle possui uma grande quantidade de parâmetros. A maior parte das configurações de um banco de dados Oracle é realizada através de parâmetros de

instância, esses parâmetros são armazenados em um arquivo de texto ou em um arquivo binário, sendo este último modo o recomendado pela Oracle. De acordo com Watson (2010), alguns parâmetros são vitais para a segurança do banco de dados, e suas alterações têm por pretensão fornecer uma segurança extra.

Segundo Watson, Ramklass e Bryla (2010), para estabelecer uma conexão em uma instância do banco de dados, um usuário deve conectar-se com uma conta de usuário. A conta deve ser especificada pelo nome e autenticada por algum meio. Em algumas aplicações, cada usuário terá sua própria conta de usuário de banco de dados. Este modelo funciona bem para pequenas aplicações, mas é impraticável para sistemas maiores, onde muitos usuários se conectarão a mesma conta. Este último modelo pode tornar mais complicada a segurança e auditoria no nível de sessão.

A maior parte da atividade do banco de dados Oracle ocorre através da rede. Os clientes Oracle se conectam através de um protocolo de comunicação, como o *Transmission Control Protocol/Internet Protocol* (TCP/IP). Servidores e clientes Oracle se comunicam usando um protocolo Oracle chamado *Transparent Network Substrate* (TNS). A criação de conexões com o banco de dados é realizada pelo *TNS Listener*, ou abreviadamente, *Listener*. O *Listener* gerencia as conexões de rede e como tal, é o ponto de entrada da maioria das conexões ao banco de dados. Por esta razão o *Listener* precisa ser configurado de forma segura (NATAN, 2009).

2.5 ORACLE LISTENER

Desde o momento que a Oracle passou a oferecer conexões através da rede, ela o fez através do *Listener*. Ao longo do tempo, como quase todas as interações com o banco de dados tornaram-se baseadas em rede, o *Listener* assumiu um papel critico no controle de acesso. Segundo Shaul e Ingram (2007), o problema é que a segurança do *Listener* é com frequência completamente negligenciada pelos administradores de banco de dados. As razões para isto não são claras, mas podem estar relacionadas com a simplicidade do *Listener*, ou por este ser um componente que executa fora do banco de dados.

Apesar de sua simplicidade, o *Listener* possui poder para controlar a maioria dos acessos ao banco de dados, executar comandos de sistema operacional, executar programas e se for atacado, pode conceder controle completo ao banco de dados e ao servidor no qual ele

está em execução. De acordo com Shaul e Ingram (2007), o *Listener* é formado por dois executáveis e alguns arquivos de configuração:

a) o *tnslsnr* é o executável que provê as funcionalidades principais, é essencialmente um processo que atua como *proxy* para conexões de rede ao banco de dados Oracle;
b) o *lsnrctl* é um utilitário utilizado para configurar e controlar o *Listener*;
c) o *sqlnet.ora* é um arquivo de configuração utilizado para fornecer ao *Listener* vários parâmetros de rede. As configurações de segurança mais relevantes são utilizadas para habilitar a criptografia e a verificação de integridade das comunicações de rede, configurar modos de autenticação e fornecer uma lista de máquinas que podem (ou não) conectar-se ao banco de dados;
d) o arquivo de configuração *listener.ora* identifica o *Listener* e os bancos de dados que são 'ouvidos' por este. Essencialmente, todas as informações sobre como o *Listener* deve executar estão armazenadas no arquivo *listener.ora*.

O *Listener* é um processo altamente privilegiado e tem um importante papel envolvendo a execução de novos processos no nível do sistema operacional. A correta configuração de seus arquivos, e o acesso controlado aos seus executáveis são necessidades de segurança em um ambiente Oracle.

De acordo com Natan (2009) o primeiro e mais importante aspecto da segurança do *Listener* é limitar a habilidade de controla-lo através do utilitário *lsnrctl*. Se um invasor puder controlar o *Listener* utilizando o *lsnrctl*, este poderá desliga-lo, causando a indisponibilidade do banco de dados para novas conexões.

Com o *Listener* configurado de forma segura, o próximo passo para garantir a segurança passa pela autenticação das contas de usuário no banco de dados. O Oracle disponibiliza vários métodos para autenticar usuários. Todas as opções disponíveis permitem que se escolha a método mais apropriado para um determinado ambiente.

2.6 AUTENTICAÇÃO DE BANCO DE DADOS

Para que o banco de dados possa permitir que uma pessoa ou aplicação acesse objetos ou privilégios nele, a pessoa ou aplicação devem ser autenticadas; a identidade de quem está tentando acessar o banco de dados precisa ser validada. Em um ambiente onde a rede é

protegida com *firewalls*, e o tráfego da rede entre o servidor de banco de dados e a aplicação usa algum método de criptografia, a autenticação pelo banco de dados é o método mais comum e mais fácil de autenticar os usuários. Neste método, todas as informações necessárias para autenticar o usuário são armazenadas dentro do banco de dados (BRYLA; LONEY, 2009).

Segundo Natan (2005), se não for possível autenticar um usuário, não será possível atribuir qualquer privilégio a ele. A identificação é uma questão separada da autenticação. A identificação é algo que o usuário possui, como uma conta e senha, um certificado ou sua digital, e a autenticação é o processo pelo qual se inspeciona o que o usuário possui, e então se decide se isto prova que ele é quem diz ser.

No processo de autenticação, o método de identificação mais utilizado é o de usuário e senha. A Figura 3 mostra a importância do processo de autenticação, que é a base para qualquer modelo de segurança (NATAN, 2005).

Fonte: Natan (2005).

Figura 3 – Autenticação como base do modelo de segurança

Por ser o método de autenticação mais utilizado, assegurar o uso de senhas fortes é uma etapa importante para proteção do banco de dados. De acordo com a documentação online do banco de dados Oracle, há muitas coisas que o Oracle faz por padrão para assegurar que as senhas não sejam comprometidas, como a transmissão criptografada através da rede e o armazenamento também criptografado no banco de dados. Porém, as senhas precisam ser

protegidas durante todo seu tempo de vida.

De acordo com Loney (2009), senhas podem expirar e contas podem ser bloqueadas devido à falha em repetidas tentativas de conexão. Quando uma senha é alterada, um histórico de senhas pode ser mantido para prevenir o reuso destas senhas. O gerenciamento de senhas das contas de usuário é determinado pelo perfil associado a estas contas. Os perfis (*profiles*) podem impor:

a) o tempo de vida da senha, que determina o quão frequentemente ela precisa ser alterada;
b) o prazo após a data de expiração no qual a senha ainda pode ser alterada;
c) o número consecutivo de tentativas falhas permitidas antes que a conta seja automaticamente bloqueada;
d) o número de dias que a conta permanecerá bloqueada;
e) o número de dias que precisam passar antes que uma senha possa ser reutilizada;
f) o número de alterações de senhas que precisam ser realizadas antes que uma senha possa ser reutilizada.

O banco de dados Oracle possibilita o uso de funções customizáveis para verificação de complexidade de senha. Uma senha nova ou alterada é verificada para certificar de que é suficientemente complexa, prevenindo intrusos que tentem acessar o sistema tentando adivinhar senhas fáceis.

Após o usuário estar autenticado no banco de dados, a próxima etapa é determinar que tipos de objetos, privilégios e recursos o usuário tem permissão para acessar ou usar (BRYLA; LONEY, 2009).

2.7 AUTORIZAÇÃO

A autorização no Oracle é baseada em um modelo de privilégio, através do qual podem ser permitidos ou negados acessos a dados, ações ou processamento, e através do qual podem ser aplicados vários limites em tais ações ou acessos. Um privilégio é um direito do usuário, um direito para algum tipo de comando em *Structured Query Language* (SQL), o direito em um objeto, o direito para executar um procedimento, etc. Especificamente, existem dois tipos de privilégios que podem ser gerenciados, privilégios de objetos e privilégios de sistema

(NATAN, 2009).

Segundo Bryla e Loney (2009), um privilégio de sistema é um direito para executar uma ação em algum objeto no banco de dados, assim como outros privilégios que não envolvem nenhum objeto, mas sim procedimentos como executar *jobs* em lote, alterar os parâmetros do sistema, criar atribuições e até mesmo conectar-se ao banco de dados.

Os privilégios de objeto fornecem a habilidade de executar comandos SQL em tabelas e objetos relacionados e de executar objetos em *Procedural Language/Structured Query Language* (PL/SQL). Estes privilégios não existem para objetos que são do próprio usuário. Se um usuário possui o privilégio de sistema para criar tabelas, ele poderá executar ações nas tabelas que criou, sem a necessidade de permissões adicionais (WATSON, 2010).

De acordo com Natan (2009), muitos usuários são gerenciados em um banco de dados. Por existir tantos tipos de privilégios, tantos potenciais objetos com os quais os privilégios são definidos, e uma grande quantidade de usuários para os quais são atribuídos os direitos, gerenciar os privilégios no nível de usuário é impraticável. Nesta situação são utilizadas atribuições (*roles*). Atribuições são grupos de privilégios que são concedidos a contas de usuário ou a outras atribuições.

Watson (2010) define atribuição como um pacote de privilégios de sistema e/ou objeto que pode ser concedido ou revogado como uma unidade e, sendo concedido, pode ser temporariamente ativado ou desativado dentro da sessão.

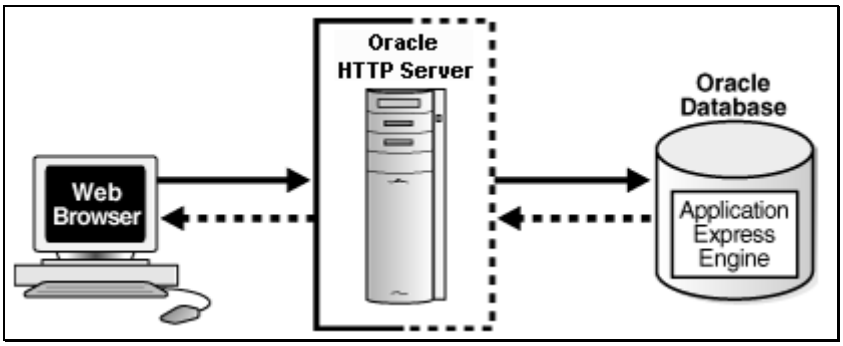
O banco de dados Oracle possui uma atribuição especial chamada *Public*. Ela é implicitamente concedida a cada usuário. Qualquer privilégio concedido a esta atribuição é concedida a todos que podem se conectar ao banco de dados. Por padrão, esta *role* tem um grande número de privilégios (WATSON; RAMKLASS; BRYLA, 2010).

Qualquer instalação do banco de dados Oracle acompanha três outras atribuições especiais. Segundo Greenwald, Stackowiak e Stern (2008), a *role* DBA inclui a maioria dos privilégios de sistema e por padrão é concedida aos usuários SYS e SYSTEM quando o banco de dados é criado. Porém, a *role* DBA não inclui tarefas administrativas básicas presentes nos privilégios de sistema SYSDBA e SYSOPER. Estes dois privilégios devem ser concedidos somente aos administradores.

2.8 ORACLE APPLICATION EXPRESS

O *Oracle Application Express* é uma ferramenta para desenvolvimento rápido de aplicações (RAD), construída sobre tecnologia Oracle. O APEX executa em uma instância de banco de dados Oracle e é uma opção gratuita que acompanha todas as versões. Ele executa inteiramente através de um navegador, e não requer a instalação de nenhum *software* na máquina cliente (GRENWALD, 2009).

A Figura 4 mostra os componentes que fazem parte de um ambiente APEX.



Fonte: *Oracle* (2012).

Figura 4 – Arquitetura do *Oracle Application Express*

O APEX não se encaixa no modelo clássico de três camadas físicas, aonde as aplicações são implantadas na camada intermediária, a camada do servidor de aplicação. As definições das aplicações são armazenadas em tabelas dentro do banco de dados Oracle. Desta forma, a camada de servidor de aplicação funciona basicamente como um *proxy* para o APEX, instalado dentro do banco de dados (HICHWA et al., 2011).

De acordo com Hichwa et al. (2011), uma das vantagens de combinar o desenvolvimento via navegador, com o armazenando das definições das aplicações como meta-dados em tabelas no banco de dados, é o tempo de projeto da aplicação. Com o Oracle APEX é possível que muitos desenvolvedores trabalhem em uma mesma aplicação, e até mesmo em uma mesma página concorrentemente. Um modelo de contenção previne que desenvolvedores sobrescrevam o trabalho de outros desenvolvedores. Outra vantagem relacionada ao modelo de meta-dados é executar as aplicações sem a necessidade de realizar implantações, após modificar a aplicação às mudanças estarão disponíveis para que o desenvolvedor teste seu trabalho.

De acordo com a documentação da Oracle (2012), este pode ser instalado de duas formas: como um ambiente de execução, que é a escolha apropriada para implantações em produção; ou como um ambiente completo de desenvolvimento. Independentemente do ambiente que for escolhido, o processo é o mesmo: o navegador envia uma requisição que é traduzida para uma chamada PL/SQL, após o banco de dados processar o PL/SQL, os resultados são enviados de volta ao navegador no formato *HyperText Markup Language* (HTML).

A bibliografia encontrada relacionada ao Oracle APEX está limitada em sua maioria a manuais de instrução de como utilizar determinada funcionalidade, não concedendo maiores detalhes sobre a arquitetura da ferramenta. A documentação da Oracle (2012) contém guias de instalação, utilização, administração e desenvolvimento.

2.9 CENÁRIO ATUAL

O sistema desenvolvido através deste trabalho será implantando em um cliente da Teclógica. A Teclógica é uma empresa que desenvolve *softwares* e oferece serviços de consultoria e suporte a sistemas e a infraestrutura.

A área de infraestrutura está subdividida em outras duas áreas, a de projetos e a de suporte. Na área de projetos são desenvolvidas e implantadas novas soluções. A área de suporte é responsável por manter os diversos itens de configuração da Teclógica e de seus clientes, buscando atingir as metas descritas nos contratos, como nível de serviço estabelecido em um contrato de acordo de nível de serviço (SLA), e o tempo de disponibilidade dos itens de configuração.

Na área de suporte de infraestrutura há uma equipe que trabalha com banco de dados e é responsável por monitora-los, mantê-los atualizados e disponíveis. Essa equipe deve atender a todas as demandas que estejam relacionadas a banco de dados, tais como: corrigir erros, aplicar melhorias, analisar o desempenho e gerar relatórios de tudo que ocorre nos ambientes.

A necessidade de verificar as configurações relacionadas à segurança é uma demanda anual de um cliente da Teclógica, que passa por uma auditoria de complacência por parte de sua detentora, uma empresa internacional. Toda a análise realizada para certificar-se de que o banco de dados alvo atende a todos os requisitos é feita manualmente, item a item. É preciso avaliar o resultado de determinado requisito no ambiente e compará-lo ao valor esperado no

documento que descreve o modelo de segurança da empresa. A grande quantidade de itens que precisam ser checados torna esta tarefa bastante demorada. O processo também é repetitivo, visto que há sempre mais de um banco de dados a ser verificado e quando o ambiente está configurado em *Real Application Clusters* (RAC), é preciso verificar cada nó, também tornando o trabalho suscetível a erros.

2.10 TRABALHOS CORRELATOS

O trabalho de conclusão de curso de Gucowski (2011), desenvolvido na Universidade Regional de Blumenau (FURB), propõe o desenvolvimento de um *middleware*, visando garantir a segurança da informação e abstração dos aspectos e conceitos dos requisitos da ISO/IEC 15.408, para os desenvolvedores de *software*. O trabalho tinha por objetivo garantir a auditoria de segurança, gerando informações sobre as ações para posterior visualização e análise. Também tratava dos assuntos de identificação e autorização do usuário, bem como o gerenciamento de acesso e de sessão entre usuário e sistema.

Por fim, visava garantir a proteção dos dados do usuário, tratando da confiabilidade e disponibilidade das informações armazenadas pelo sistema, ajudando na construção de *softwares* seguros. Para o desenvolvimento do *middleware* foi utilizada a linguagem *Java* no ambiente de desenvolvimento *Netbeans*. Para armazenamento de dados foi utilizado o banco de dados *Oracle 10g*. O sistema de gerenciamento de segurança foi desenvolvido em *Delphi 7.0.*

A monografia de Sá (2001), desenvolvida nas Faculdades Integradas de Jacarepaguá, expõe a preocupação pertinente à segurança da informação nas redes de computadores. Seu trabalho analisa e procura métodos de prevenção e defesa contra ameaças aos dados e informações disponíveis na rede.

O trabalho trata a segurança de banco dados como uma questão muito importante, contemplando áreas como a integridade dos dados, autorização e disponibilidade. Sá (2001) também cita a necessidade de se criar uma politica de privacidade e segurança. A monografia fala sobre a segurança em diferentes softwares de banco de dados, e cita que o banco de dados Oracle possui vários recursos no campo de segurança, com ferramentas avançadas para controle de autenticação e autorização, implementação de criptografia e auditoria.

O *software* correlato *Oracle Enterprise Manager Configuration Management Pack* (CMP), monitora as configurações do banco de dados para complacência em segurança e regulamentações. O CMP avalia continuamente as configurações, usando uma biblioteca de mais de 240 melhores práticas. A pontuação de complacência é calculada com base em politicas pré-definidas e configurações validadas por padrões industriais, como o *Center for Internet Security* (CIS). Os usuários também podem adicionar suas melhores práticas.

O CIS (2012) é uma organização sem fins lucrativos, focada em melhorar a segurança cibernética nos setores públicos e privados, através da colaboração dos membros e comunidades. Uma das missões do CIS é prover padrões práticos visando aumentar o nível de segurança e privacidade dos sistemas conectados a internet.

A Figura 5 mostra a página do sistema, com o resumo de pontuação por alvo, e o número de violações por alvo. O CMP é um *software* mais completo em relação ao sistema desenvolvido através deste trabalho, porém, a um custo de $12.000 por processador. O sistema desenvolvido através deste trabalho entrega uma solução semelhante, e que atende a maioria das empresas, a um custo muito menor.

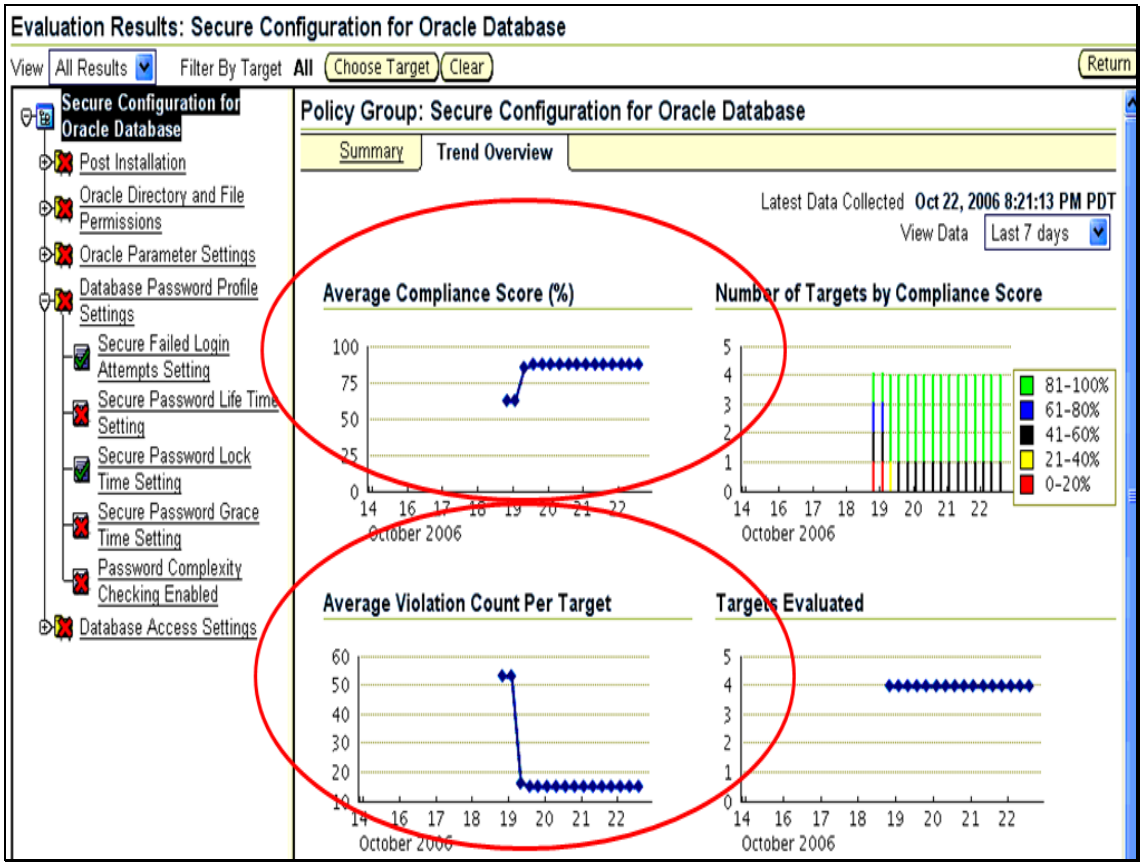


Figura 5 – CMP *Evaluation Results*

3 DESENVOLVIMENTO DO SISTEMA

Neste capitulo serão abordados os tópicos sobre o levantamento de informações, as especificações, os requisitos funcionais, os requisitos não funcionais, o diagrama de casos de uso e o modelo de entidade e relacionamento. Também será abordada a implementação, as técnicas e ferramentas utilizadas, a operacionalidade da implementação e os resultados e discussão.

3.1 LEVANTAMENTO DE INFORMAÇÕES

A base para o desenvolvimento deste trabalho utilizou informações disponibilizadas através da documentação *on-line* do banco de dados Oracle 11g. O guia de segurança possui informações de todos os recursos de segurança deste *software*, bem como, dicas para a configuração segura e eficiente destes recursos.

Também foi consultado o documento disponibilizado pelo CIS (2011), um *benchmark* que lista configurações e procedimentos necessários para operação segura do banco de dados Oracle 11g. Este documento foi criado a partir de pesquisas através da rede de tecnologia da Oracle, de vários livros publicados e diretrizes de segurança.

Por fim, foi levado em consideração o documento disponibilizado pelo cliente aonde este sistema será implantado. Este documento contém uma lista de configurações de segurança para o banco de dados Oracle 11g, e é utilizado durante o processo de auditoria de segurança, executado por auditores externos. Todas as necessidades de segurança contidas neste documento são contempladas pelo documento do CIS (2011) e extensamente descritas no guia de segurança do banco de dados Oracle.

3.2 ESPECIFICAÇÃO

Nesta seção serão apresentados os requisitos funcionais e não funcionais, os casos de uso e o Modelo de Entidade e Relacionamento (MER). O diagrama de caso de uso foi criado

utilizando a ferramenta *Enterprise Architect* (EA). O MER foi criado através do *software DBDesigner*.

3.2.1 Requisitos funcionais

O Quadro 2 apresenta os requisitos funcionais do sistema e sua vinculação com os casos de uso.

Requisitos Funcionais	**Caso de Uso**
RF01: O sistema deverá permitir manter configurações de *profiles* de contas de usuário.	UC01
RF02: O sistema deverá permitir manter exceções para os *profiles*.	UC02
RF03: O sistema deverá permitir manter configurações de grupos de privilégios (*roles*).	UC03
RF04: O sistema deverá permitir manter exceções para grupos de privilégio.	UC04
RF05: O sistema deverá permitir manter configurações de privilégios de sistema.	UC05
RF06: O sistema deverá permitir manter configurações de privilégios a objetos.	UC06
RF07: O sistema deverá permitir manter configurações de comandos auditáveis.	UC07
RF08: O sistema deverá permitir manter configurações de parâmetros do Oracle *SQLNet.*	UC08
RF09: O sistema deverá permitir manter configurações de parâmetros de instância.	UC09
RF10: O sistema deverá permitir manter configurações de parâmetros do Oracle *Listener*.	UC10
RF11: O sistema deverá permitir manter exceções para contas de usuário.	UC11
RF12: O sistema deverá permitir a criação de modelos de segurança.	UC12
RF13: O sistema deverá permitir a exclusão de um modelo de segurança.	UC13
RF14: O sistema deverá permitir a verificação do banco de dados alvo utilizando o modelo de segurança escolhido.	UC14

RF15: O sistema deverá permitir a visualização dos resultados da verificação através de relatórios detalhados.	UC15
RF16: O sistema deverá apresentar um resumo dos itens verificados.	UC16
RF17: O sistema deverá permitir o usuário efetuar *login* no sistema.	UC17

Quadro 2 – Requisitos funcionais

3.2.2 Requisitos não funcionais

O Quadro 3 mostra os requisitos não funcionais previstos para o sistema.

Requisitos Não Funcionais
RNF01: O sistema deverá utilizar banco de dados Oracle 11g (portabilidade).
RNF02: O sistema será desenvolvido em PL/SQL (implementação).
RNF03: As páginas e relatórios serão desenvolvidos através do Oracle APEX (implementação).
RNF04: O sistema poderá ser acessado através de qualquer navegador (portabilidade).

Quadro 3 – Requisitos não funcionais

3.2.3 Diagrama de caso de uso

A Figura 6 apresenta o digrama de caso de uso. Para melhor entendimento do projeto, o detalhamento dos principais casos de uso encontra-se no Apêndice A.

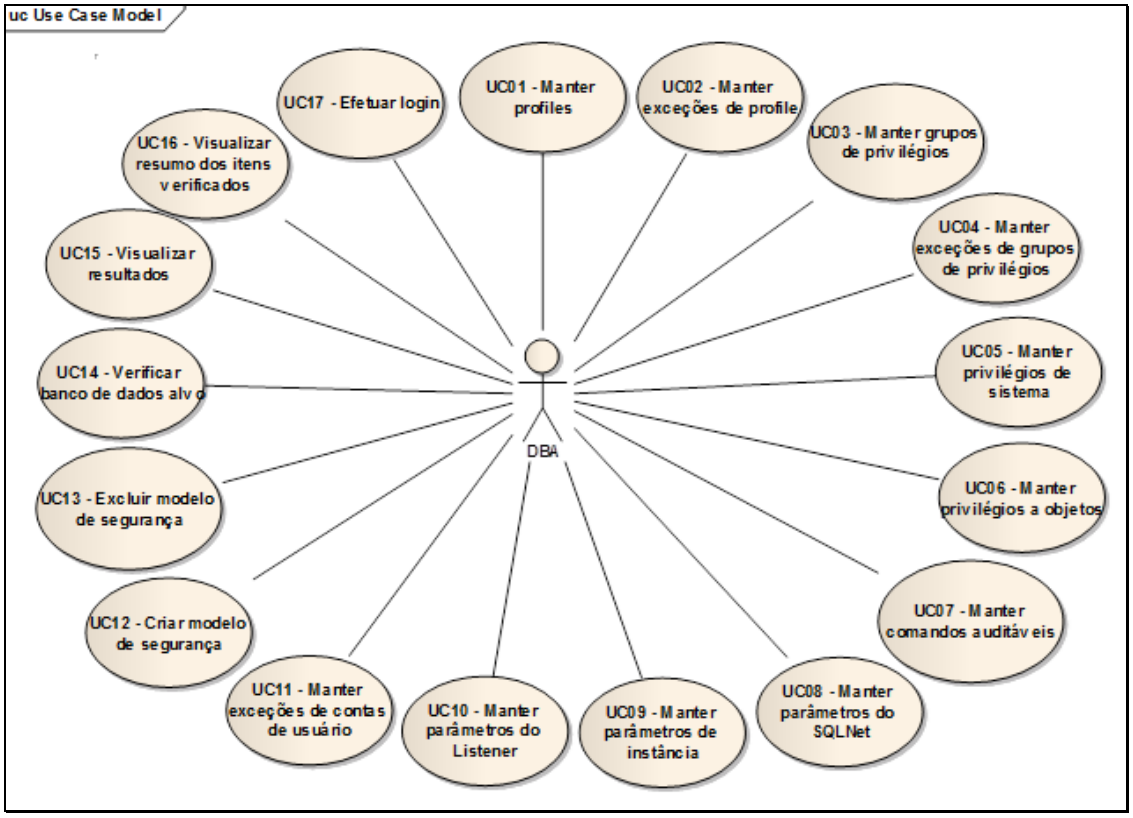


Figura 6 – Diagrama de caso de uso do sistema

3.2.4 Modelo de Entidade e Relacionamento

A Figura 7 mostra o Modelo de Entidade e Relacionamento (MER). O dicionário de dados desenvolvido para especificar o sistema é apresentado no apêndice B. O MER não está totalmente normalizado em função do Oracle *Application Express*. As páginas tabulares criadas através do APEX não permitem a utilização de *joins* e são completamente baseadas em uma tabela específica, visando à utilização das funcionalidades disponibilizadas por este tipo de página (que são alterar, incluir ou excluir uma ou várias linhas), optou-se pela não normalização de algumas tabelas.

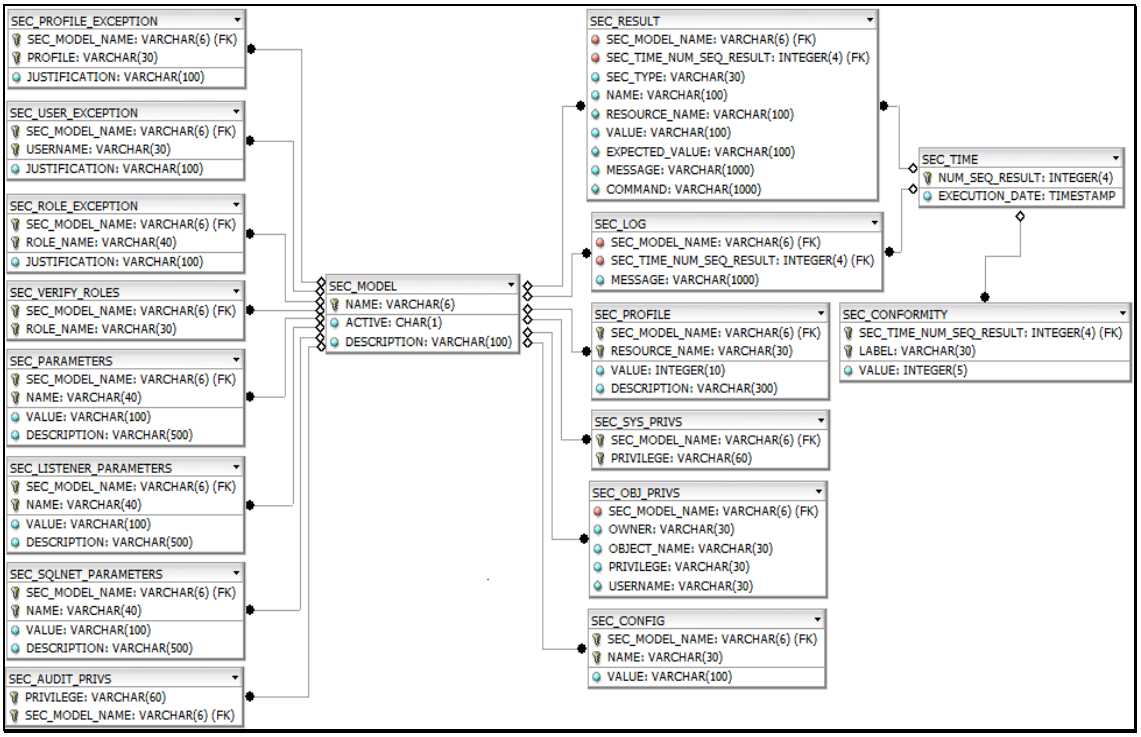


Figura 7 – Modelo de Entidade e Relacionamento

3.3 IMPLEMENTAÇÃO

A seguir são mostradas as técnicas e ferramentas utilizadas e a operacionalidade da implementação.

3.3.1 Técnicas e ferramentas utilizadas

Para desenvolvimento deste trabalho foram utilizadas duas ferramentas da Oracle, o *SQL Developer*, para desenvolvimento e criação de objetos no banco de dados, e o *Applicaton Builder* do *Oracle Application Express*, para desenvolvimento de páginas e relatórios. Para armazenamento dos dados foi utilizado o banco de dados *Oracle 11g*.

O sistema traz um modelo de segurança padrão, que possui configurações pré-definidas que atendem ao documento do CIS (2011) e estão de acordo com as recomendações da Oracle.

As rotinas que verificam o banco de dados alvo foram implementadas como

procedimentos, dentro de um pacote de banco de dados. A Figura 8 mostra parte do código do procedimento que verifica os parâmetros de instância.

```
145         else
146           -- Se os diretórios forem iguais, valida se o diretório existe e se o Oracle tem permissão de escrita no mesmo
147           begin
148             -- Monta comando para criar diretório
149             wrk_create_directory := 'create or replace directory ' || wrk_directory || ' as ' || '''' || wrk_value || '''';
150             -- Cria diretório executando SQL dinâmico
151             execute immediate wrk_create_directory;
152             -- Realiza teste tentando criar um arquivo no diretório
153               begin
154                 test_file := utl_file.fopen(wrk_directory, wrk_file_name, 'w');
155                 utl_file.fclose_all;
156                 utl_file.fremove(wrk_directory, wrk_file_name);
157               exception
158                 -- Se o diretório não existir ou não tiver privilégio para escrever
159                 when utl_file.invalid_operation then
160                   -- Monta comando de ajuste
161                   wrk_command := 'alter system set ' || rl.name || '=' || rl.value || ' scope=both;';
162                   sec_oracle.insert_result(
163                     check_parameters.model_name,
164                     check_parameters.sec_time_num_seq_result,
165                     'Parameter',
166                     rl.name,
167                     rl.name,
168                     wrk_value,
169                     rl.value,
170                     'Invalid directory or no privilege.' || rl.description,
171                     wrk_command);
172
173                 when others then
174                   ecode := sqlcode;
175                   emesg := sqlerrm;
```

Figura 8 – Parte da implementação do procedimento de parâmetros de instância

O sistema busca informações em dois arquivos que ficam fora do banco de dados Oracle. Os arquivos *listener.ora* e *sqlnet.ora* são utilizados para configurar o banco de dados Oracle em rede. A Figura 9 mostra parte do código do procedimento que abre um arquivo, busca a informação de determinado parâmetro e o retorna para o procedimento que o chamou. São realizadas todas as validações necessárias, verificando, por exemplo, se o parâmetro existe e se não está comentado.

A verificação do banco de dados é bastante rápida. Por estar armazenado no próprio banco de dados, não há trafego de rede entre a execução dos diversos comandos, como ocorreria em um sistema desenvolvido em outra linguagem. Para desenvolvimento de algumas funcionalidades, foram utilizados vários pacotes e procedimentos disponibilizados por qualquer banco de dados Oracle, com versão superior a 10g.

```
677             -- Retorna o valor do parâmetro se não estiver comentado
678             elsif(wrk_exists > 0) then
679              -- Se estiver comentado (no inicio)
680              if(substr(trim(wrk_text),1,1) = '#') then
681                utl_file.fclose_all;
682                return '#' || trim(substr(wrk_text,(instr(wrk_text,'=')+1)));
683              else
684                -- Se estiver comentado no final (após o valor), remove comentário e só retorna o valor
685                if(instr(trim(wrk_text),'#',1) > 1) then
686                  wrk_text := trim(replace(wrk_text,trim(substr(wrk_text,(instr(wrk_text,'#')))),''));
687                end if;
688                -- Retorna o valor
689                utl_file.fclose_all;
690                return trim(substr(wrk_text,(instr(wrk_text,'=')+1)));
691              end if;
692            end if;
693          exception
694            -- Se o parâmetro não for encontrado, retorna nulo
695            when no_data_found then
696              utl_file.fclose_all;
697              return 'NULL';
698          end;
699        end loop;
700      exception
701        -- Se o diretório não existir ou não tiver privilégio de leitura
702        when utl_file.invalid_operation then
703          -- Monta comando
704          wrk_command := 'Directory' || wrk_dir || 'wrong or insufficient privileges!';
705          -- Insere no resultado (para relatório)
706          sec_oracle.insert_result(
707            get_parameter_value.model_name,
```

Figura 9 – Parte do código do procedimento *get_parameter_value*

No *Applicaton Builder* foram criadas as páginas e relatórios. A página que permite a configuração de privilégios a objetos possui algumas validações. O usuário pode especificar um nome de objeto utilizando os caracteres de percentual e sublinhado, estes são caracteres especiais de substituição utilizados no comando *like* da linguagem SQL. A Figura 10 mostra a validação criada para verificar se o objeto informado existe debaixo de determinada conta, no banco de dados alvo.

Com exceção das páginas de parâmetros do *SQLNet* e parâmetros do *Listener*, todas as outras páginas possuem validações em todos os campos aplicáveis. Para validar os nomes destes parâmetros seria necessário abrir os respectivos arquivos, *sqlnet.ora* e *listener.ora*. Existe a possibilidade do parâmetro não estar definido no arquivo, o que impediria seu cadastro, fazendo com que a validação falha-se. Desta forma, se um parâmetro destes dois tipos de configuração for definido incorretamente, o mesmo aparecerá no relatório como um item em não conformidade, pois não será encontrado no arquivo de configuração.

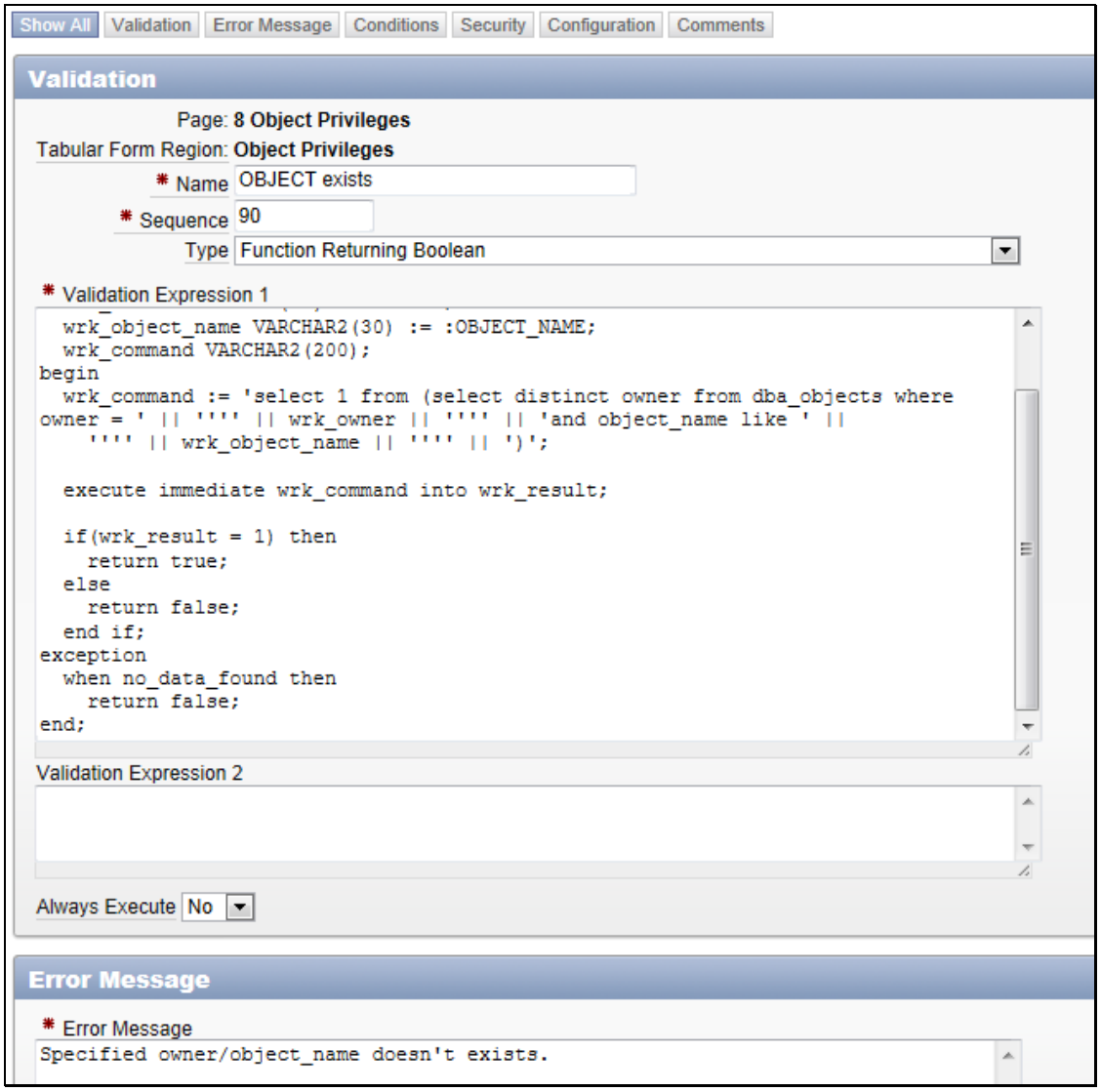


Figura 10 – Validação de objeto no Oracle APEX

Os resultados da verificação do banco de dados são armazenados em uma tabela de resultado. Todos os relatórios consultam esta tabela. A Figura 11 mostra a consulta utilizada para criar o relatório que mostra os parâmetros do *Listener* que não estiverem em conformidade.

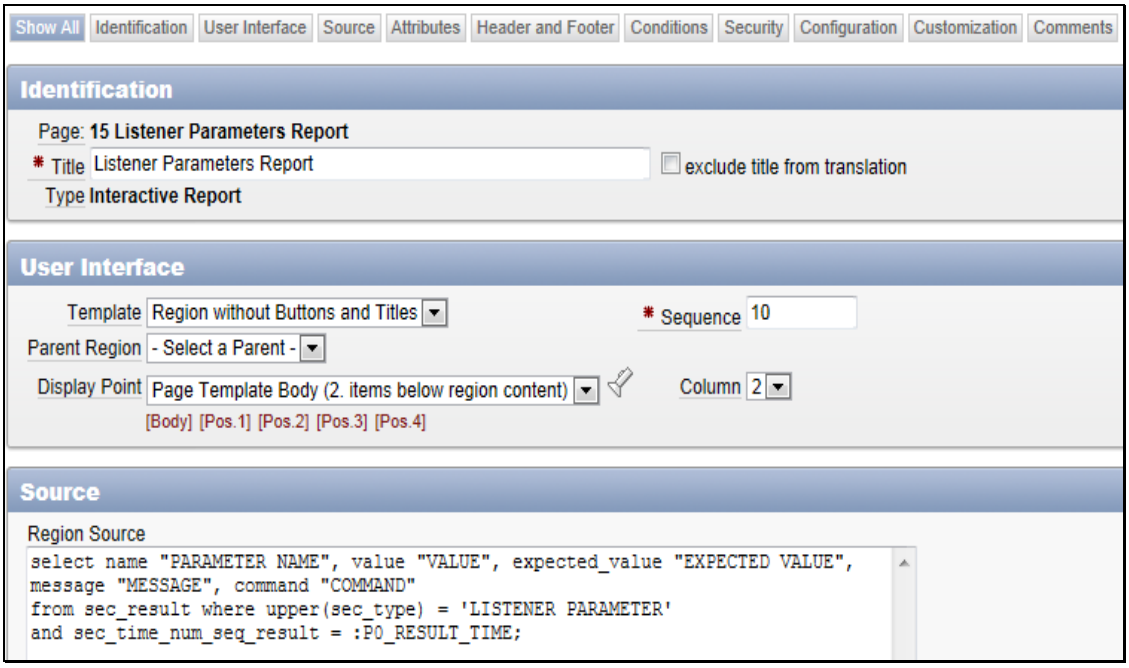


Figura 11 – Consulta no relatório de parâmetros do *Listener*

3.3.2 Operacionalidade da implementação

Nesta subseção será apresentada a sequência de páginas e operações para correta utilização do sistema. Após realizar o *login* no sistema, a página inicial é apresentada. A Figura 12 mostra a página inicial, que possui uma lista dos modelos de segurança cadastrados. O campo *active* indica qual é o modelo de segurança ativo, este será utilizado durante a avaliação do banco de dados.

Ainda na página inicial é possível selecionar outro modelo e ativa-lo. O modelo ativo é utilizado nas abas configuração e relatório, para filtrar respectivamente as configurações dos recursos e os resultados das verificações já executadas.

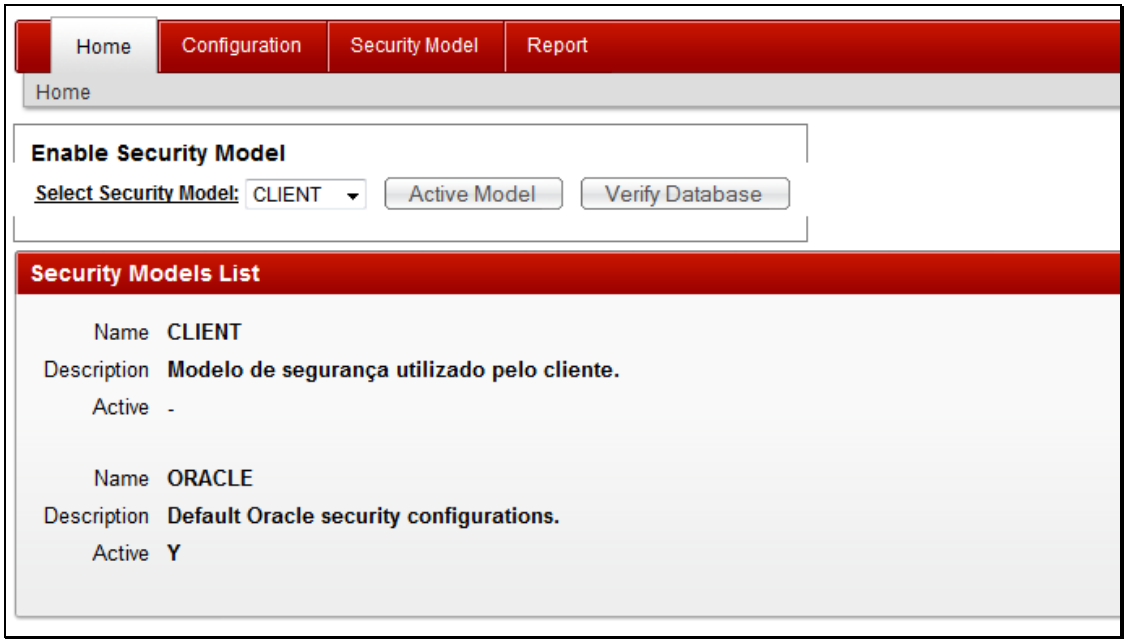


Figura 12 – Página inicial do sistema

A aba *Security Model* permite a criação de um novo modelo de segurança, baseado em um modelo previamente cadastrado. Por padrão o sistema possui um modelo de segurança, denominado Oracle. A Figura 13 mostra a criação de um modelo de segurança, que irá copiar as configurações do *template* selecionado.

Na mesma página é possível excluir um modelo já cadastrado. O sistema não permite a exclusão do modelo padrão (Oracle) ou do modelo que estiver ativo. A exclusão de um modelo resultará na perda de todo seu histórico de verificações.

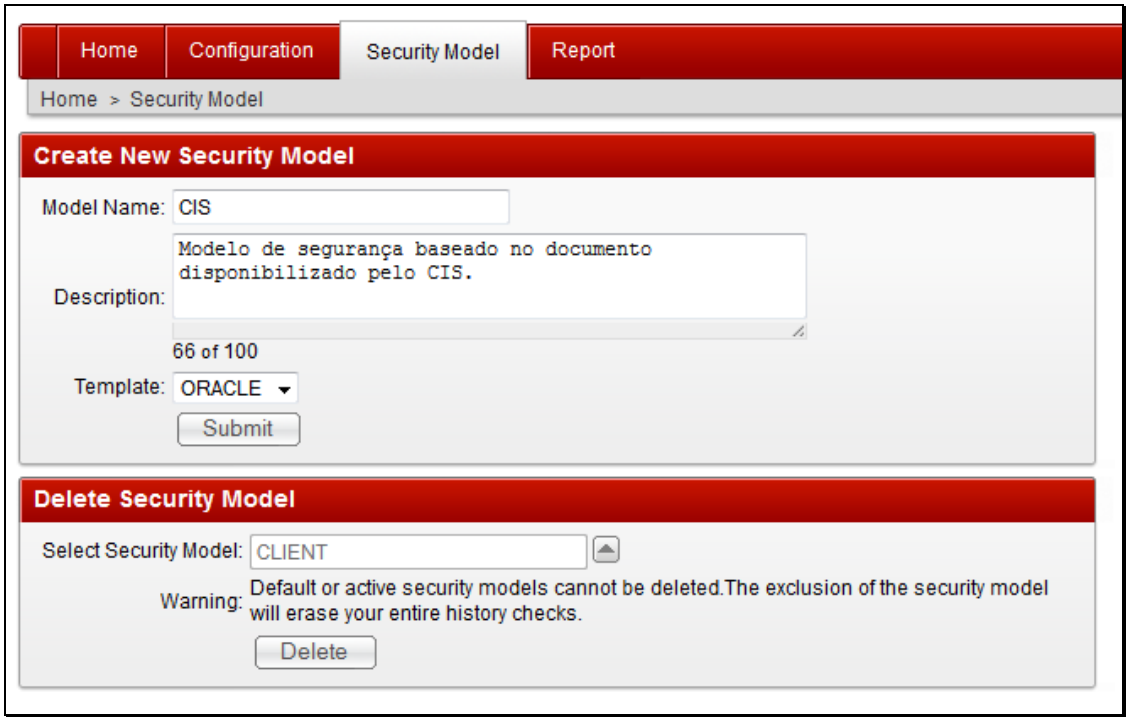


Figura 13 – Criação e exclusão de um modelo de segurança

A aba *Configuration* permite o ajuste em vários recursos avaliados pelo sistema. A configuração da estrutura do Oracle *Listener* é necessária para que o sistema encontre os arquivos *listener.ora* e *sqlnet.ora* para posterior avaliação. A Figura 14 mostra a página principal de configuração. Nesta página é possível configurar os usuários que serão desconsiderados durante as avaliações de privilégios.

A lista de opções na parte esquerda da página disponibiliza acesso a todas as outras páginas de configurações, que são separadas por funcionalidades de segurança. Logo abaixo das abas, o sistema mantém um caminho, visando facilitar a navegação e a localização do usuário entre as páginas.

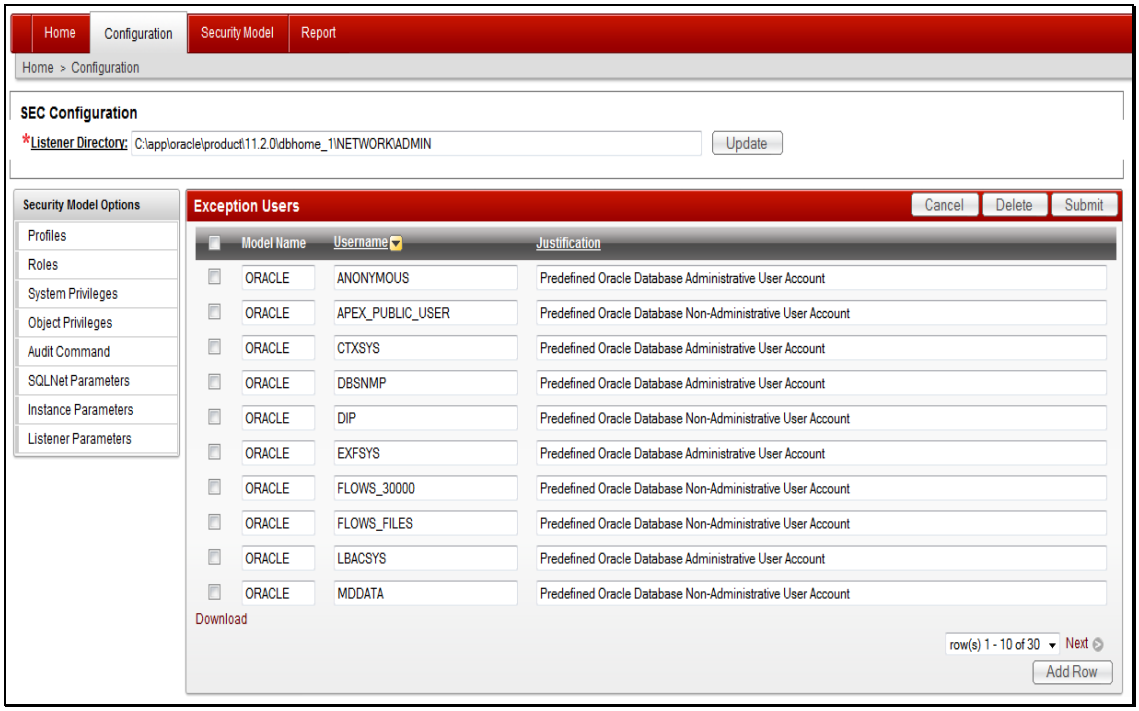


Figura 14 – Página principal de configuração

A Figura 15 mostra a página para configuração dos *profiles* de conta de usuário. Através desta página é possível adicionar *profiles* que não serão levados em consideração durante a verificação do banco de dados. Ao selecionar a opção visualizar *profiles* de exceção o usuário será direcionado para a página da Figura 16. A página *profiles* de exceção mostra todos os *profiles* de exceção cadastrados para o modelo ativo.

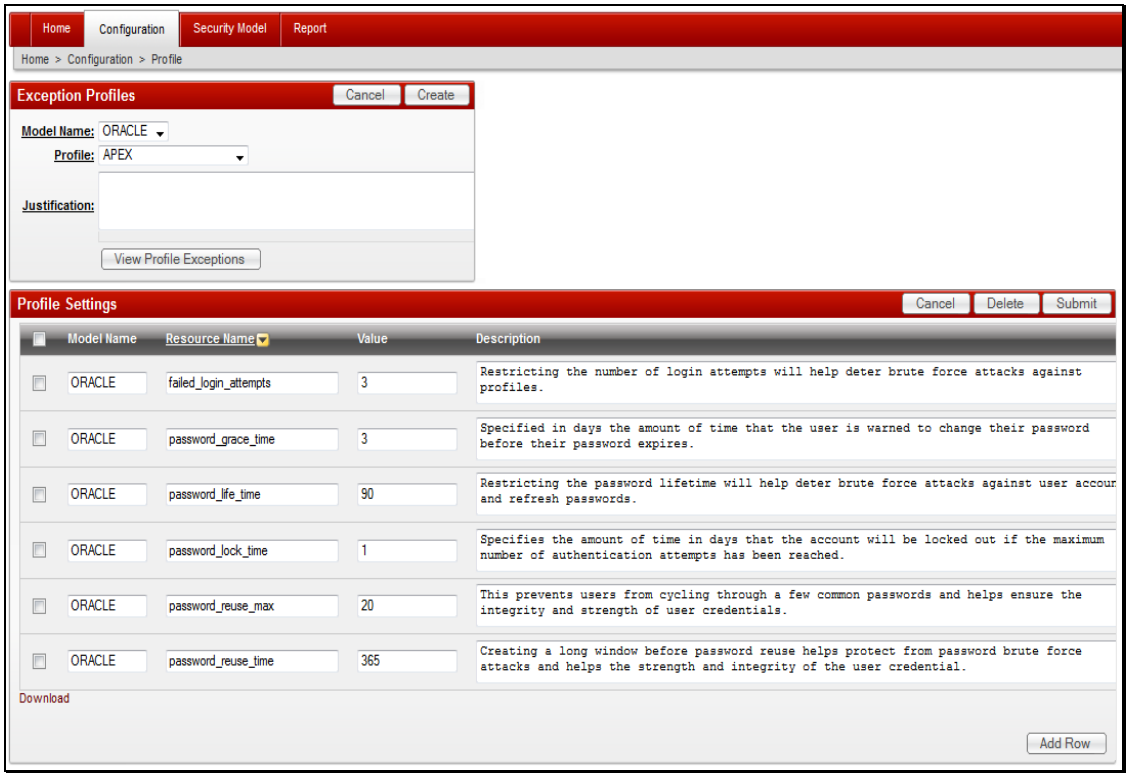


Figura 15 – Configuração de *profiles* de conta de usuário

Figura 16 – *Profiles* cadastrados como exceção

A Figura 17 mostra a página de configurações de *roles*. Nesta página é possível adicionar as *roles* exceção, estas serão desconsideradas nas verificações de privilégios realizadas pelo sistema. Na mesma página é possível cadastrar as *roles* que deverão ser avaliadas, ou seja, nenhum usuário ou *role* exceto os usuários e *roles* exceções devem possuir estas atribuições. A Figura 18 mostra a lista de atribuições cadastradas como exceções.

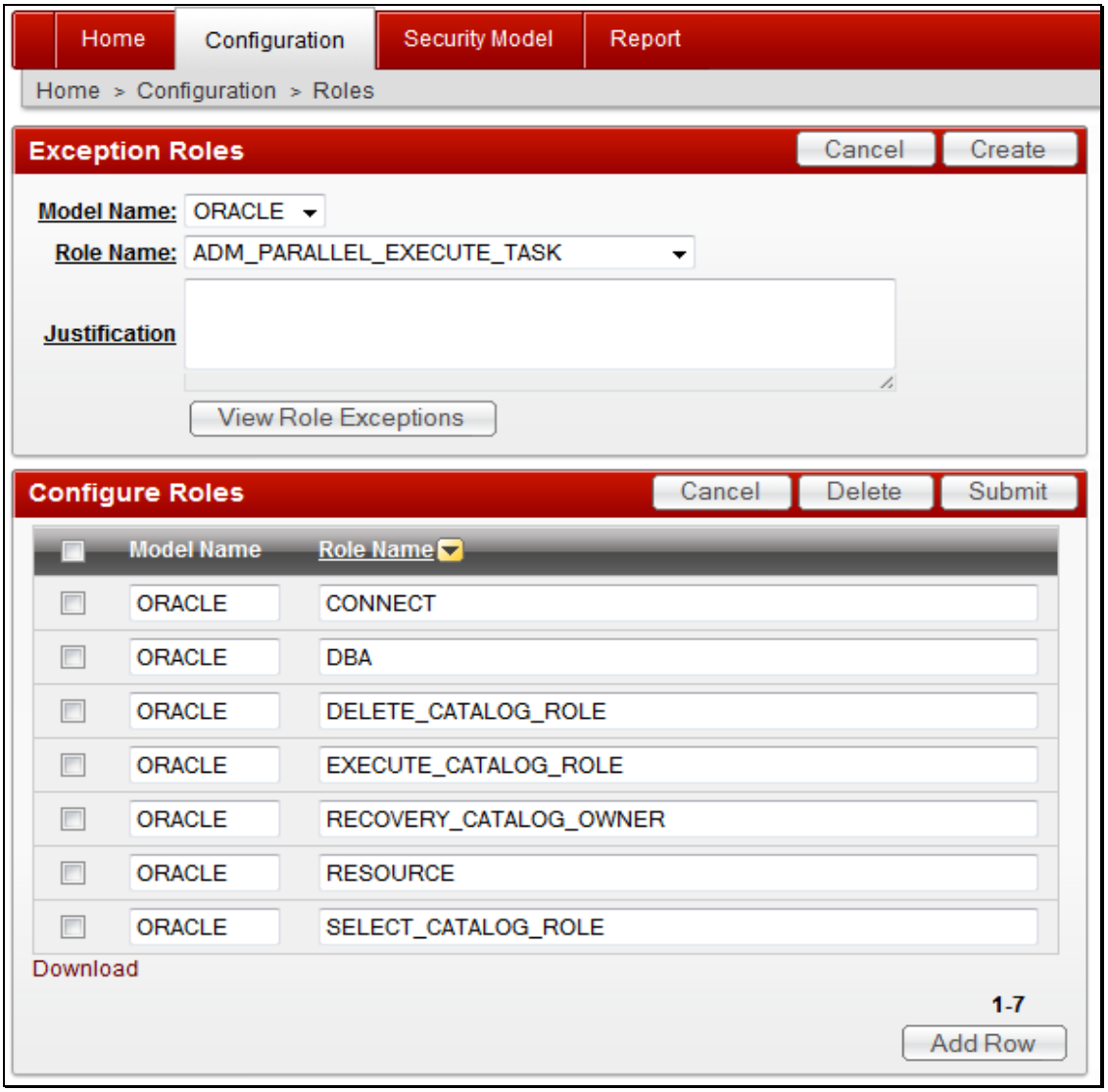


Figura 17 – Configuração de *roles*

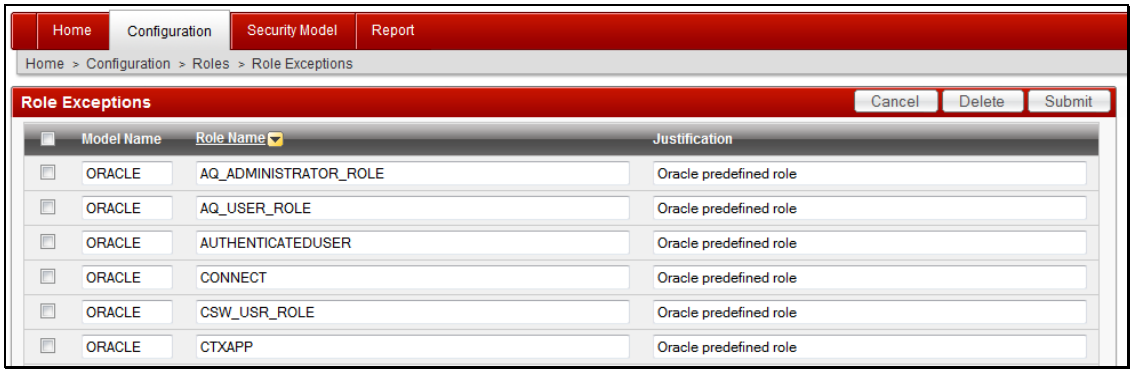


Figura 18 – *Roles* cadastradas como exceção

A Figura 19 mostra a página para configuração de privilégios de sistemas. Estes privilégios serão verificados e, nenhuma conta de usuário ou atribuição poderá possuir algum

destes privilégios, exceto usuários e atribuições cadastrados como exceção.

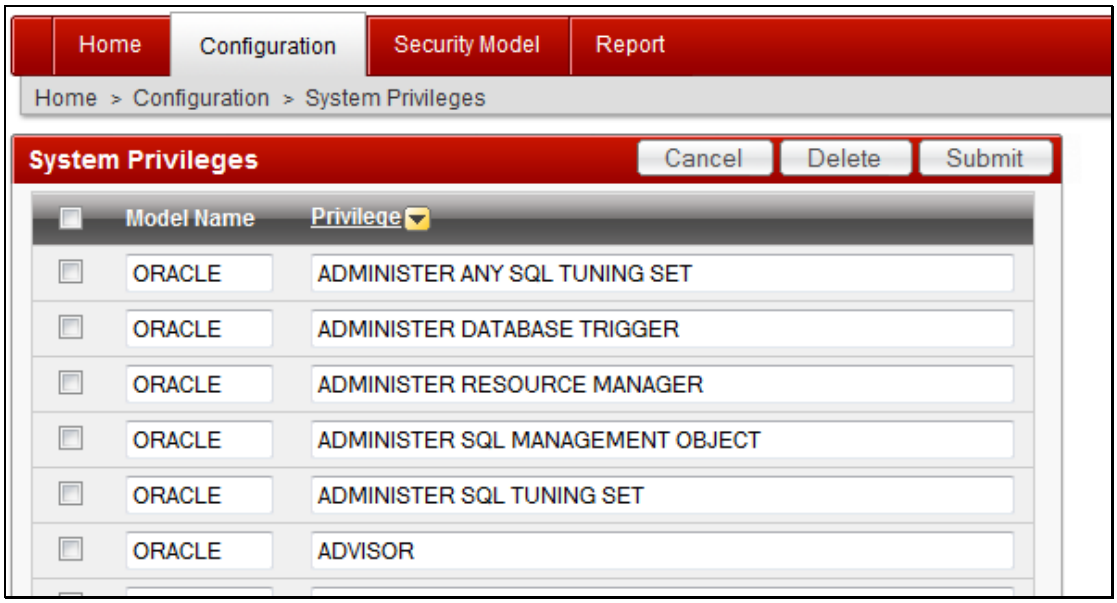


Figura 19 – Configuração de privilégios de sistema

O sistema permite que o usuário configure privilégios a determinados objetos, objetos que podem conter informações sensíveis. A Figura 20 mostra a página de configuração de privilégios a objetos. Nesta página é possível especificar qual é o nome do objeto, ou parte do nome, através da utilização dos caracteres de percentual e sublinhado, estes são caracteres especiais de substituição utilizados no comando *like* da linguagem SQL. É preciso informar quem é o dono do objeto (ou objetos) e, qual privilégio não pode ser concedido, ou todos (*all*). Pode-se especificar também uma conta de usuário em especifico, ou todas, se o campo for deixado em branco.

Todas as validações necessárias são realizadas diretamente na página, se o objeto informado, o privilégio ou o usuário não existir, uma mensagem de erro será exibida e a linha ou linhas com problema serão destacadas.

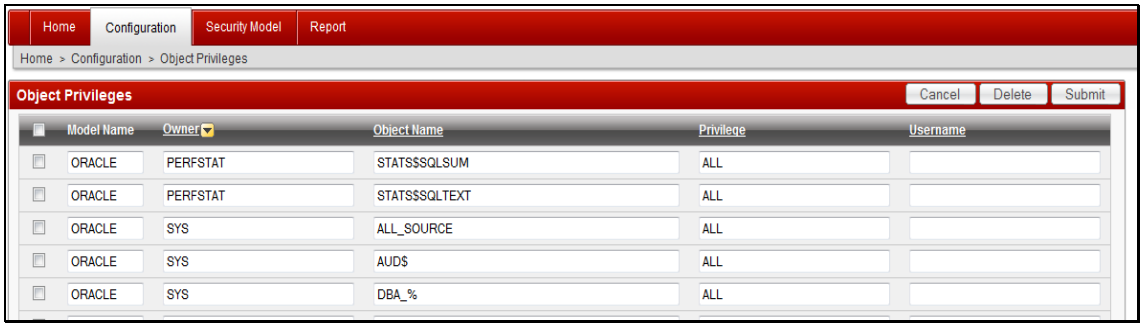


Figura 20 – Configuração de privilégios a objetos

Alguns privilégios de sistema são poderosos, e por este motivo seu uso precisa ser auditado. A Figura 21 mostra a página que permite configurar os privilégios de sistema que devem ser auditados. O sistema irá verificar se os comandos especificados nesta página estão sendo auditados pelo banco de dados alvo.

Figura 21 – Auditoria de privilégios de sistema

As Figuras 22, 23 e 24 mostram respectivamente a configuração dos parâmetros de instância, do Oracle *Listener* e do Oracle *SQLNet*.

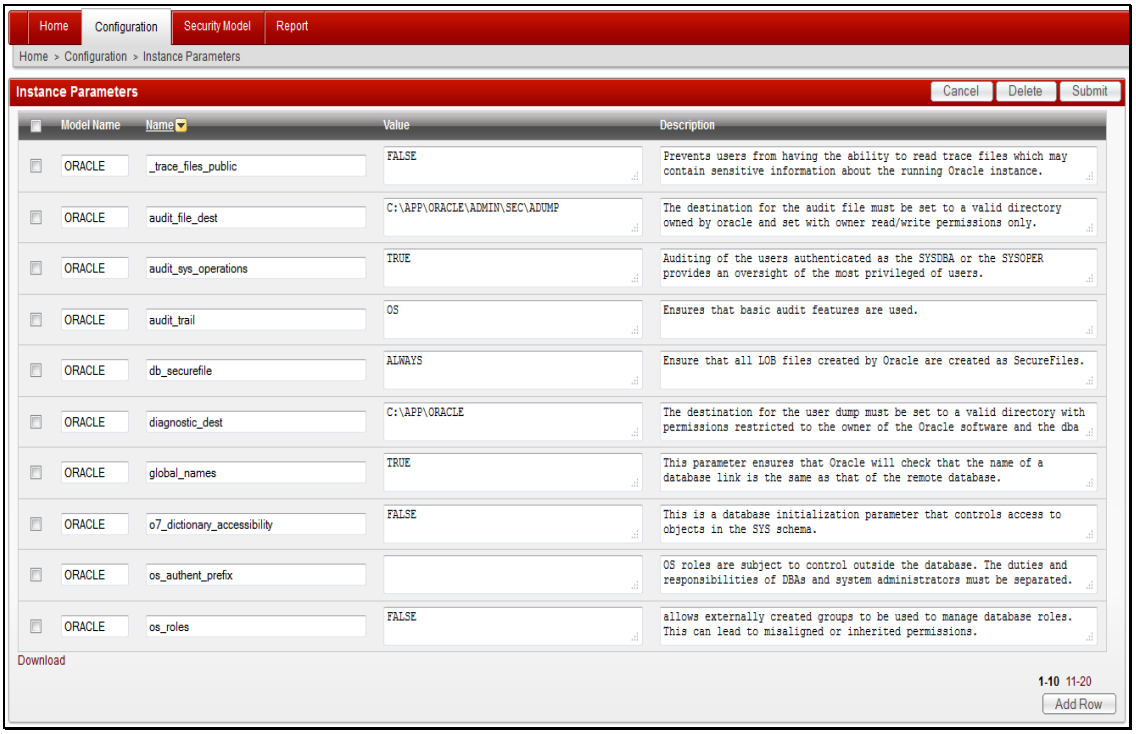


Figura 22 – Configuração de parâmetros de instância

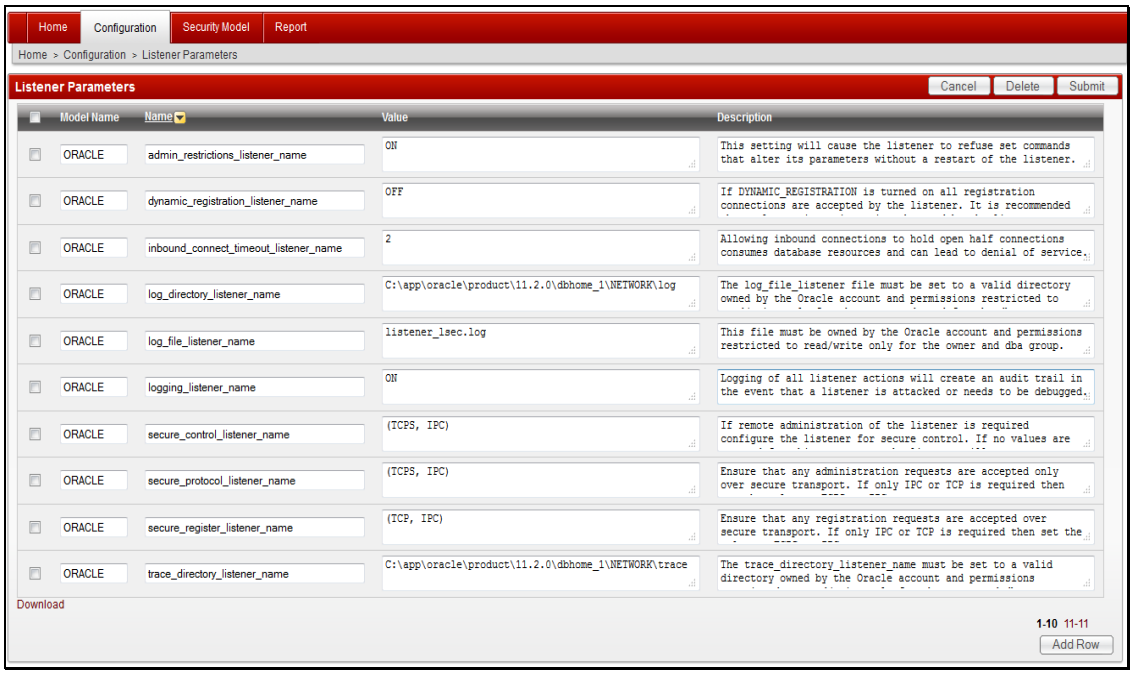


Figura 23 – Configuração de parâmetros do Oracle *Listener*

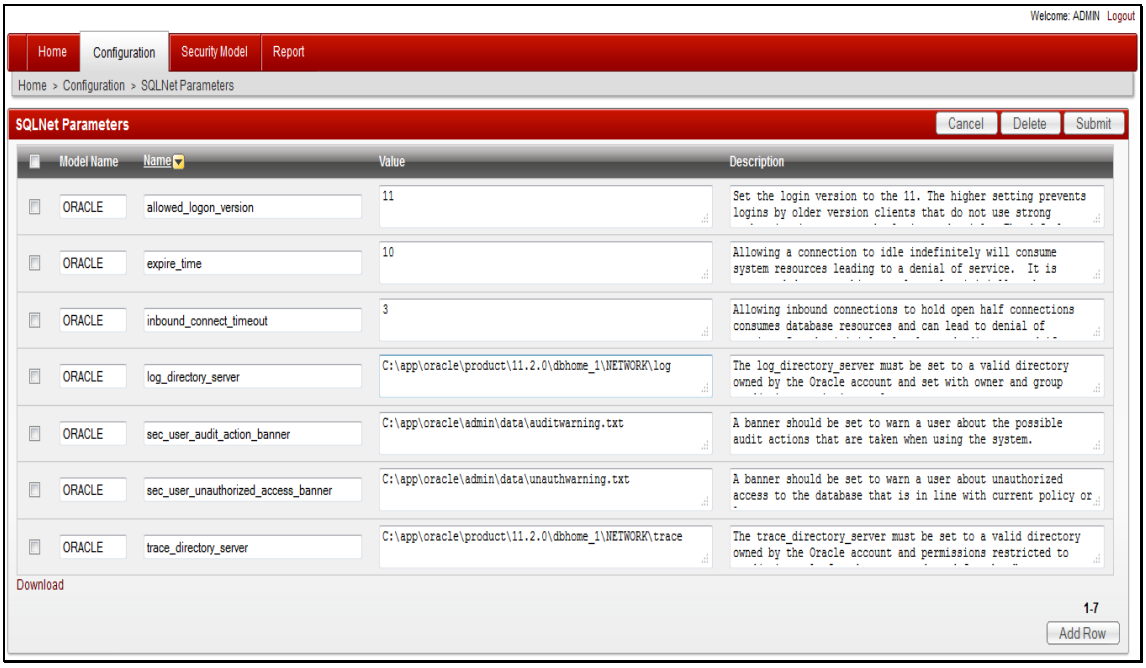


Figura 24 – Configuração de parâmetros do Oracle *SQLNet*

Após terem sido realizadas as configurações necessárias, a verificação do banco de dados poderá ser disparada através da página inicial. O botão verificar banco de dados irá chamar um procedimento de banco de dados, que por sua vez irá chamar todos os procedimentos necessários para realizar a verificação completa do banco de dados. As configurações do modelo de segurança que estiver ativo serão utilizadas. Os resultados serão armazenados em uma tabela.

A Figura 25 mostra a aba relatório. A página permite selecionar a data e hora no qual ocorreu a verificação do banco de dados alvo, e todo o histórico de verificações irá aparecer nesta lista, permitindo a análise de execuções anteriores. A lista de relatórios que fica no lado esquerdo da página dá acesso aos relatórios detalhados de cada recurso de segurança do Oracle. A Figura 25 também mostra um dos relatórios, com o resultado da verificação dos parâmetros de instância.

Através do botão ações, logo acima do relatório, é possível criar filtros, selecionar colunas, escolher as colunas que devem ser exibidas, configurar a quantidade de linhas a serem exibidas, salvar o relatório em arquivo, entre outras funcionalidades.

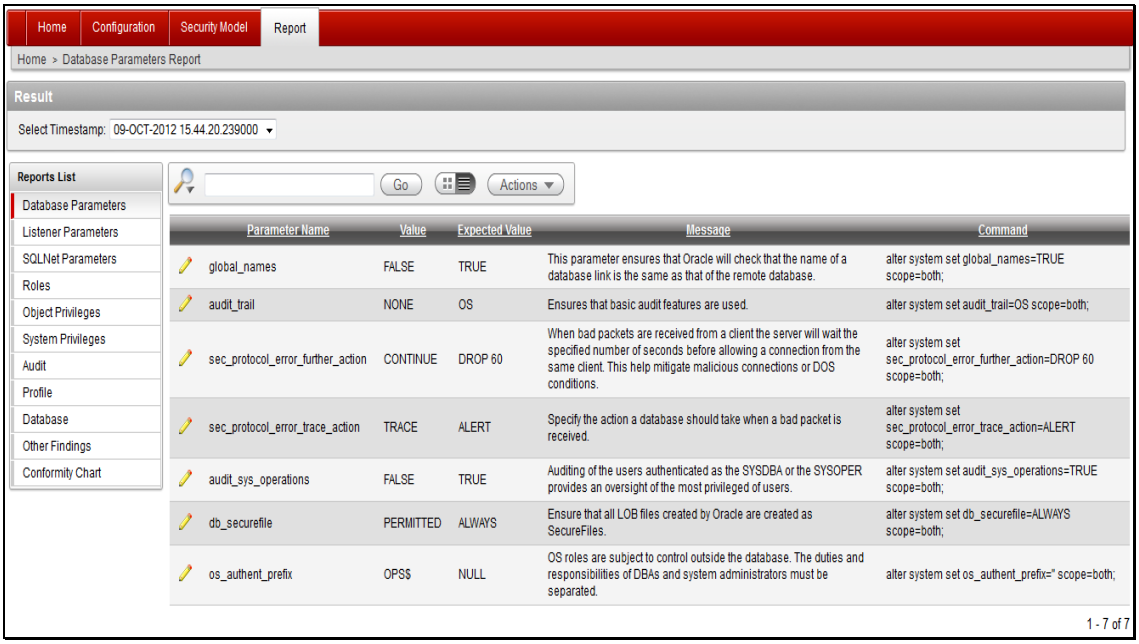


Figura 25 – Relatórios detalham os resultados da verificação do banco de dados

A Figura 26 exibe o gráfico de conformidade. Nele é apresentado um resumo da verificação realizada no banco de dados alvo. O relatório mostra a quantidade de itens em conformidade e a quantidade de itens em não conformidade. Logo abaixo do gráfico é exibido um resumo que explica como os itens são calculados.

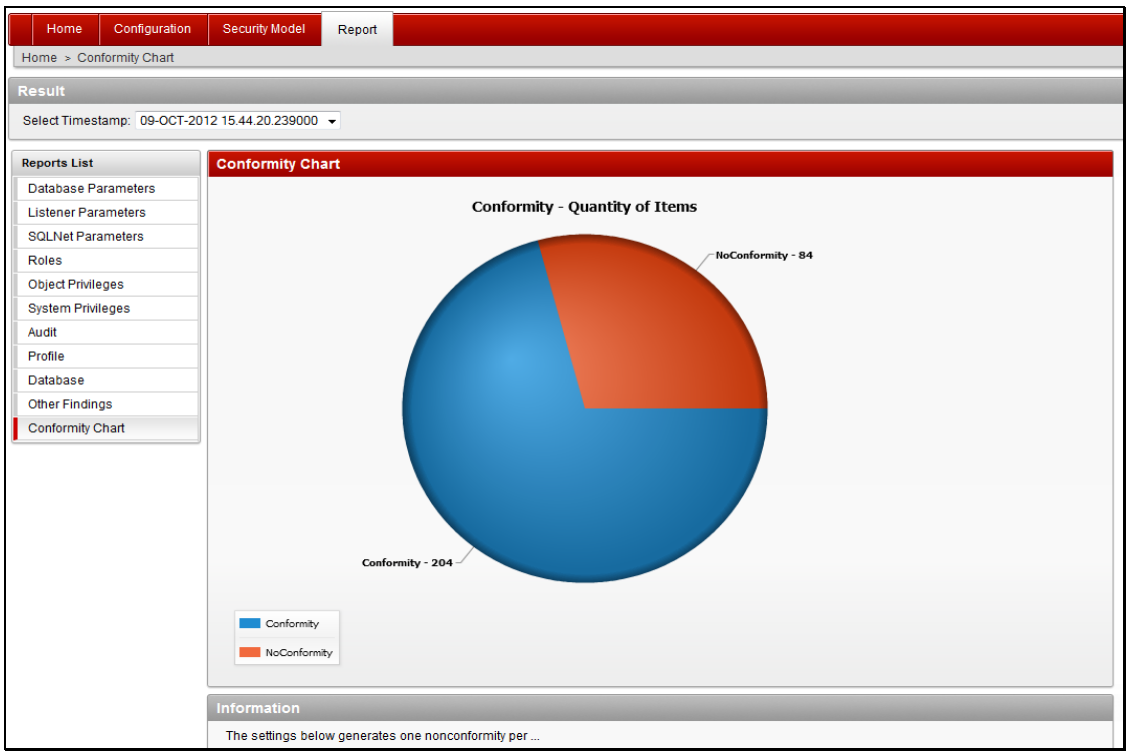


Figura 26 – Gráfico de conformidade

3.4 RESULTADOS E DISCUSSÃO

O principal objetivo deste trabalho foi desenvolver um sistema pra apoiar os administradores de banco de dados na tarefa de avaliar questões pertinentes à segurança em um banco de dados Oracle. O sistema desenvolvido permite organizar melhor as configurações ideais de segurança e automatiza a avaliação de um banco de dados, economizando tempo e extinguindo a ocorrência de falhas que podem ocorrer em uma avaliação manual, resultando em uma análise de melhor qualidade.

Os trabalhos correlatos citados, assim como este, visam garantir a segurança da informação. Para isto, utilizam técnicas e expõe a necessidade de tratar questões como autorização e identificação, confiabilidade, integridade dos dados, privacidade e disponibilidade. Também tratam da necessidade de utilização de recursos para auditoria de informação. A preocupação com a segurança dos dados, com a criação de diretrizes e procedimentos no campo de segurança é observada nos três trabalhos.

O *software* da Oracle apresentado nos trabalhos correlatos tem a mesma proposta do sistema desenvolvido através deste trabalho. O objetivo de ambos é monitorar e avaliar o banco de dados para garantir que o mesmo esteja em complacência com as melhores práticas definidas. Porém, o sistema da Oracle é mais robusto, traz mais funcionalidades e a possibilidade de avaliar mais configurações, como as ligadas a segurança do sistema operacional no qual o banco de dados reside. O custo do sistema é bastante alto, sendo inviável para uma grande quantidade de empresas, o que não quer dizer que a segurança não precise ser avaliada nestas empresas. O sistema desenvolvido através deste trabalho visa atender também a este cenário.

Para avaliar o sistema desenvolvido, foram realizados testes por três administradores de banco de dados da Teclógica. Um dos administradores trabalha na área de suporte, os outros dois fazem parte da equipe de projetos. A avaliação ocorreu nos dias 30 e 31 de Outubro de 2012. A Figura 27 apresenta o resumo do questionário aplicado (presente no Apêndice C). A avaliação foi baseada na média aritmética simples das opções escolhidas pelos avaliadores. O resultado demonstra o potencial do sistema e a melhoria que ele deve trazer ao processo de avaliação de segurança de um banco de dados Oracle.

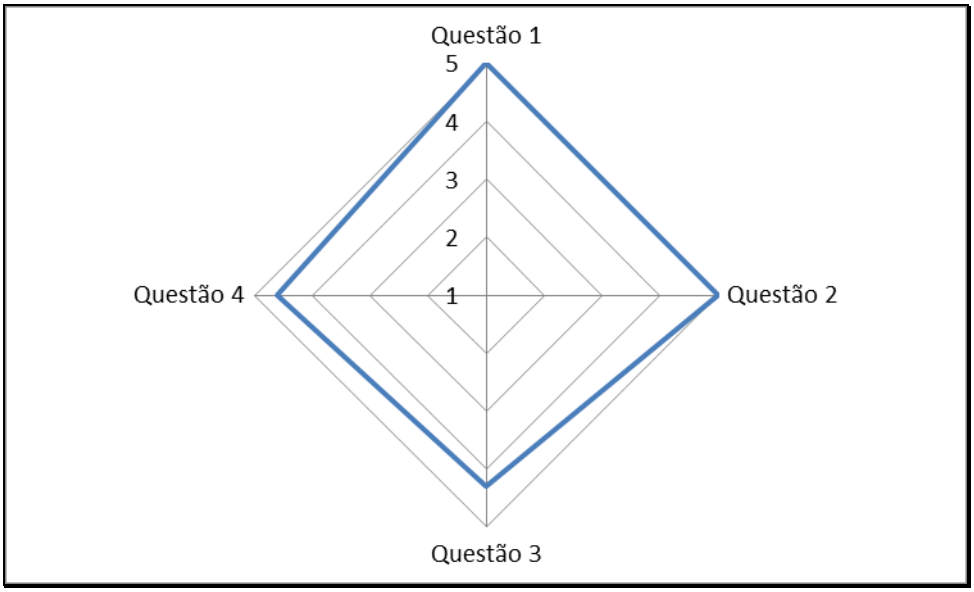


Figura 27 – Resultado da avaliação da ferramenta

4 CONCLUSÕES

Pode-se observar através da bibliografia e da opinião de pessoas e empresas especializadas, que o atual cenário dos sistemas ligados à internet evidência a necessidade de se garantir a confidencialidade das informações que transitam pela rede, e que estão armazenadas nos bancos de dados.

Analisando os objetivos deste trabalho, conclui-se que todos foram atingidos. O sistema desenvolvido auxilia os administradores de banco de dados na avaliação de segurança de um banco de dados Oracle, permitindo a análise de verificações atuais e anteriores. A ferramenta para desenvolvimento rápido de aplicações utilizada neste trabalho, o *Oracle APEX*, até então desconhecida pela equipe de projetos de infraestrutura da Teclógica, foi apresentada através de trabalho. Pode-se avaliar o potencial da ferramenta, que é gratuita e tem uma excelente integração com o banco de dados Oracle.

A apresentação do sistema foi realizada, tendo como plateia a equipe de administradores de banco de dados e o gerente de projetos da área de infraestrutura da Teclógica. O sistema superou as expectativas, entregando a solução necessária para a implantação imediata no cliente. Para implantar o sistema será preciso enviar uma requisição de mudança, instalando-o primeiramente no ambiente de homologação, para depois, passa-lo para o ambiente produtivo.

Levando em consideração o atual ambiente do cliente, que conta com uma grande quantidade de bancos de dados Oracle, e que possui um procedimento de avaliação manual para auditoria de segurança, o sistema desenvolvido através deste trabalho atende as necessidades e é bastante flexível no que diz respeito a customizações futuras.

Durante o desenvolvimento deste sistema foi observada à impossibilidade de avaliar a segurança do sistema operacional aonde o banco de dados alvo reside. Os documentos de recomendações da Oracle, o documento do CIS e o modelo de segurança do cliente também tratam de pontos que precisam ser avaliados no sistema operacional. Esta recomendação será comentada nas extensões.

4.1 EXTENSÕES

Desenvolver um sistema para avaliar a segurança do sistema operacional aonde o banco de dados reside. O sistema deve comtemplar alguns sistemas operacionais, como os mais utilizados Linux e Windows. Algumas das avaliações que podem ser feitas:

a) permissões em arquivos e diretórios;
b) avaliação de parâmetros de núcleo do Linux;
c) avaliação de configurações no registro do Windows;
d) avaliação da configuração das interfaces de rede.

Adicionar funcionalidades a este sistema:

a) bancos de dados como itens de configuração, possibilitando avaliar um ou mais de um banco de dados por vez;
b) níveis de configuração, informando que determinado item pode ser alterado por qualquer pessoa que tenha o mínimo de conhecimento técnico; outro item pode requerer conhecimento do ambiente e dos sistemas, bem como maior conhecimento técnico;
c) níveis de pontuação, avaliando qual é o grau de inconformidade de determinado item, ou seja, o item pode estar próximo do ideal, fazendo com que sua alteração não tenha tanto impacto.

Através da implementação das funcionalidades citadas acima, poderiam ser gerados relatórios a nível gerencial, contendo, por exemplo, o resultado de complacência por alvo avaliado. Também poderiam ser gerados relatórios contendo os resultados separados por configurações de níveis diferentes, ou itens com mais ou menos impacto.

REFERÊNCIAS

BRYLA, Bob; LONEY, Kevin. **Oracle database 11g manual do dba**. Tradução Altair Caldas Dias de Moraes. Porto Alegre: Bookman, 2009.

CIS. **Mission and Overview**. [East Greenbush, NY], 2012. Disponível em: <http://www.cisecurity.org/about/index.cfm>. Acesso em: 12 dez. 2012.

CIS. **Security benchmark for Oracle database server 11g**. [East Greenbush, NY], 2011. Disponível em: <http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.oracle11g.100>. Acesso em: 16 out. 2012.

COMMON CRITERIA PORTAL. **About the common criteria**. [Ft. George Meade, MD], 2012. Disponível em: <http://www.commoncriteriaportal.org/ccra/>. Acesso em: 16 out. 2012.

DATE, C. J. **An introduction to database systems, 8th edition**. Boston, MA: Pearson Education, 2004.

GREENWALD, Rick; STACKOWIAK, Robert; STERN, Jonathan. **Oracle essentials: Oracle database 11g 4th edition**. Sebastopol, CA: O'Reilly, 2008.

GREENWALD, Rick. **Beginning Oracle application express**. Indianapolis, IN: Wiley, 2009.

GUCOWSKI, Bruno Castellani. **Middleware para fornecimento de serviço de segurança em conformidade com a ISO/IEC 15.408**. 2011. 75 f. Trabalho de Conclusão de Curso (Bacharelado) – Curso de graduação de Ciência da Computação, Universidade Regional de Blumenau, Blumenau.

HICHWA, Michael; SCOTT, John; AUST, Dietmar; D'SOUZA, Martin; GAULT, Doug; GIELIS, Dimitri; HARTMAN,Roel; KENNEDY, Sharon; KUBICEK, Denes; MATTAMAL, Raj; MCGHAN, Dan; MIGNAULT, Francis; NIELSEN, Anton. **Expert Oracle application express**. New York, NY: Apress, 2011.

ITRC. **2011 data breach stats**. [San Diego, CA], 2011. Disponível em: <http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202011.pdf>. Acesso em: 16 out. 2012.

KNOX, David; GAETJEN, Scott; JAHANGIR, Hamza; MUTH, Tyler; SACK, Patrick; WARK, Richard; WISE, Bryan. **Applied Oracle security: developing secure database and middleware environments**. New York, NY: McGraw-Hill, 2010.

KNOX, David. **Effective Oracle database 10g security by design**. New York, NY: Oracle Press, 2004.

KYTE, Thomas. **Expert Oracle database architecture, 2nd edition**. New York, NY: Apress, 2010.

LITCHFIELD, David; ANLEY, Chris; HEASMAN, John; GRINDLAY, Bill. **The database hacker's handbook**. Indianapolis, IN: Wiley, 2005.

LONEY, Kevin. **Oracle database 11g the complete reference**. New York, NY: McGraw-Hill, 2009.

NATAN, Ron Ben. **HOWTO secure and audit Oracle 10g and 11g**. Boca Raton, FL: CRC Press, 2009.

NATAN, Ron Ben. **Implementing database security and auditing**. Burlington, MA: Elsevier, 2005.

ORACLE. **Oracle application express 4.2 documentation**. [Redwood City, CA], 2012. Disponível em: <http://www.oracle.com/technetwork/developer-tools/apex/documentation/index.html>. Acesso em: 12 dez. 2012.

SÁ, Patricia Vargas Rocha dos Santos. **Segurança de dados**. 2001. 84 f. Monografia (Especialização em Análise e Gerência de Sistemas) – Curso de Pós-graduação "Lato Sensu", Faculdades Integradas de Jacarepaguá, Rio de Janeiro.

SHAUL, Josh; INGRAM, Aaron. **Practical Oracle security**. Rockland, MA: Syngress, 2007.

STEWART, James Michael; TITTEL Ed; CHAPPLE Mike. **CISSP: certified information systems security professional study guide 3rd edition**. Alameda, CA: Sybex, 2005.

WALLACE, Kathryn. **Common criteria and protection profiles: how to evaluate information technology security**. [Bethesda, MD], 2003. Disponível em: <http://www.sans.org/reading_room/whitepapers/standards/common-criteria-protection-profiles-evaluate-information_1078>. Acesso em: 16 out. 2012.

WATSON, John; RAMKLASS, Roopesh; BRYLA, Bob**. OCA/OCP Oracle database 11g all-in-one exam guide**. New York, NY: McGraw-Hill, 2010.

WATSON, John. **OCA Oracle database 11g administração I**. Tradução Altair Caldas Dias de Moraes. Porto Alegre: Bookman, 2010.

WEBER, Joachim. **Certification report for Oracle database 11g release 2 enterprise edition from Oracle Corporation**. [Bonn], 2012. Disponível em: <http://www.commoncriteriaportal.org/files/epfiles/0766a_pdf.pdf>. Acesso em: 16 out. 2012.

APÊNDICE A – Descrição dos Casos de Uso

Este Apêndice apresenta a descrição dos principais casos de uso do sistema. O Quadro 4 apresenta o detalhamento do caso de uso "Manter *profiles*".

Caso de uso – Manter *profiles*
Ator: Administrador de banco de dados (DBA)
Objetivo: Configurar recursos relacionados aos *profiles* de contas de usuário.
Pré-Condições: Usuário deve estar autenticado no sistema.
Pós-Condições: Novas configurações salvas no banco de dados.

Cenário Principal:
1. Usuário acessa a página de configuração de *profiles*.
2. Usuário opta por alterar/cadastrar as configurações de *profiles.*
3. Usuário adiciona linha(s).
4. Usuário altera linha(s).
5. Usuário submete as inclusões e/ou alterações realizadas.
6. Sistema valida o nome do modelo de segurança.
7. Sistema valida o nome da configuração de *profile*.
8. Sistema insere e/ou atualiza as informações.
9. Usuário seleciona a opção cancelar.
10. Usuário seleciona a opção visualizar *profiles* exceção.

Cenário Alternativo:
No passo 2, caso o usuário opte por cadastrar um *profile* como exceção:
1.1. Usuário seleciona o nome do modelo de segurança.
1.2. Usuário seleciona o nome do *profile*.
1.3. Usuário informa uma justificativa.
1.4. Usuário seleciona criar.
1.5. Sistema insere o *profile* como exceção.
1.6. Usuário seleciona cancelar.

Cenário Alternativo:
No passo 2, caso o usuário opte por excluir uma ou mais configurações de *profile*:
2.1. Usuário seleciona linha(s).
2.2. Usuário seleciona a opção excluir.
2.3. Sistema exclui a(s) linha(s) selecionada(s).

Cenário Alternativo:
No passo 10, o usuário é direcionado para a página que contém a lista de *profiles* que são exceção.

Cenário Alternativo:
Nos passos 1.6 e 9, o usuário é direcionado para a página inicial de configurações.

Quadro 4 – Descrição do caso de uso Manter *profiles*

O Quadro 5 apresenta o detalhamento do caso de uso "Manter privilégios a objetos".

Caso de uso – Manter privilégios a objetos
Ator: Administrador de banco de dados (DBA)
Objetivo: Configurar privilégios a determinados objetos do banco de dados alvo para posterior verificação.
Pré-Condições: Usuário deve estar autenticado no sistema.
Pós-Condições: Novas configurações salvas no banco de dados.

Cenário Principal:
1. Usuário acessa a página de configuração de privilégios a objetos.
2. Usuário opta por cadastrar/alterar as configurações de privilégios a objetos.
3. Usuário adiciona linha(s).
4. Usuário altera linha(s).
5. Usuário submete alterações e/ou inclusões realizadas.
6. Sistema valida o nome do modelo de segurança.
7. Sistema valida o dono do objeto.
8. Sistema valida o nome do objeto.
9. Sistema valida se o privilégio especificado existe.
10. Sistema valida o nome do usuário que não deve possuir o acesso.
11. Sistema insere e/ou atualiza as informações no banco de dados.
12. Usuário seleciona a opção cancelar.

Cenário Alternativo:
No passo 2, o usuário opta por excluir configurações de privilégios a objetos:
1.1. Usuário seleciona linha(s).
1.2. Usuário seleciona a opção excluir.
1.3. Sistema exclui a(s) linha(s) selecionada(s).

Cenário Alternativo:
No passo 12, o usuário é direcionado para a página inicial de configurações.

Quadro 5 – Descrição do caso de uso Manter privilégios a objetos

O Quadro 6 apresenta o detalhamento do caso de uso Criar modelo de segurança.

Caso de uso – Criar modelo de segurança
Ator: Administrador de banco de dados (DBA)
Objetivo: Criar um novo modelo de segurança.
Pré-Condições: Usuário deve estar autenticado no sistema.
Pós-Condições: Modelo de segurança criado no banco de dados.

Cenário Principal:

1. Usuário acessa a página de modelo de segurança.
2. Usuário opta por criar um novo modelo de segurança.
3. Usuário informa o nome e a descrição do novo modelo.
4. Usuário seleciona o modelo de segurança do qual serão copiadas as configurações.
5. Usuário seleciona a opção submeter.
6. Sistema cria o modelo de segurança com base nas configurações do modelo de segurança selecionado.

Quadro 6 – Descrição do caso de uso Criar modelo de segurança

O Quadro 7 apresenta o detalhamento do caso de uso Verificar banco de dados alvo.

Caso de uso – Verificar banco de dados alvo
Ator: Administrador de banco de dados (DBA)
Objetivo: Verificar o banco de dados
Pré-Condições: Usuário deve estar autenticado no sistema.
Pós-Condições: Resultados da verificação disponíveis para visualização.

Cenário Principal:

1. Usuário acessa a página inicial do sistema.
2. Usuário seleciona o modelo de segurança que será utilizado na verificação.
3. Usuário seleciona a opção ativar modelo.
4. Usuário seleciona a opção verificar banco de dados.
5. Sistema verifica o banco de dados alvo.

Quadro 7 – Descrição do caso de uso Verificar banco de dados alvo

O Quadro 8 apresenta o detalhamento do caso de uso Visualizar resultados.

Caso de uso – Visualizar resultados
Ator: Administrador de banco de dados (DBA)
Objetivo: Visualizar os resultados gerados pela verificação do banco de dados
Pré-Condições: Usuário deve estar autenticado no sistema.

Cenário Principal:

1. Usuário acessa a página de relatórios.
2. Usuário seleciona a data e hora da verificação a ser visualizada.
3. Usuário seleciona um dos relatórios presentes na lista de relatórios.
4. Sistema monta o relatório buscando as informações do banco de dados.

Quadro 8 – Descrição do caso de uso Visualizar resultados

APÊNDICE B – Dicionário de dados

Este Apêndice apresenta o dicionário de dados das tabelas do sistema através dos Quadros 9 a 25. Os tipos de dados estão associados a formatos específicos de armazenamento e aceitam diferentes séries de valores:

a) *varchar2*: armazena caracteres alfanuméricos de tamanho variável;
b) *char*: armazena caracteres alfanuméricos de tamanho fixo;
c) *number*: armazena números fixos e de ponto flutuante.
d) *timestamp*: armazena valores temporais (data e tempo). Armazena o ano (incluindo o século), o mês, o dia, as horas, os minutos, os segundos e as frações de segundo.

SEC_AUDIT_PRIVS – Armazena os privilégios de sistema que devem ser auditados.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Privilege	Privilégio de sistema	Varchar2	60	Sim
Sec_model_name	Nome do modelo de segurança.	Varchar2	6	Sim

Quadro 9 – Tabela Sec_audit_privs

SEC_CONFIG – Armazena os parâmetros do sistema.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança.	Varchar2	6	Sim
Name	Nome do parâmetro	Varchar2	30	Sim
Value	Valor do parâmetro	Varchar2	100	Não

Quadro 10 – Tabela Sec_config

SEC_CONFORMITY – Armazena o resumo do resultado da verificação do banco de dados, com a quantidade de itens em conformidade e não conformidade.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_time_num_seq_result	Id do resultado	Number	4	Sim

Label	Nome do resultado	Varchar2	30	Sim
Value	Valor do resultado	Number	5	Não

Quadro 11 – Tabela Sec_conformity

SEC_LISTENER_PARAMETERS – Armazena as configurações dos parâmetros do *Oracle Listener*.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança	Varchar2	6	Sim
Name	Nome do parâmetro	Varchar2	40	Sim
Value	Valor do parâmetro	Varchar2	100	Não
Description	Descrição do parâmetro	Varchar2	500	Não

Quadro 12 – Tabela Sec_listener_parameters

SEC_LOG – Armazena as mensagens de exceção geradas durante a verificação do banco de dados.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança	Varchar2	6	Não
Sec_time_num_seq_result	Id do resultado	Number	4	Não
Message	Descrição da exceção	Varchar2	1000	Não

Quadro 13 – Tabela Sec_log

SEC_MODEL – Armazena os modelos de segurança cadastrados.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Name	Nome do modelo de segurança	Varchar2	6	Sim
Active	Modelo de segurança ativo	Char	1	Não
Description	Descrição do modelo de segurança	Varchar2	100	Não

Quadro 14 – Tabela Sec_model

SEC_OBJ_PRIVS – Armazena as configurações de privilégios a objetos.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança	Varchar2	6	Não
Owner	Dono do objeto	Varchar2	30	Não
Object_name	Nome do objeto	Varchar2	30	Não
Privilege	Privilégio ao objeto	Varchar2	30	Não
Username	Nome do usuário	Varchar2	30	Não

Quadro 15 – Tabela Sec_obj_privs

SEC_PARAMETERS – Armazena os valores dos parâmetros de instância.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança	Varchar2	6	Sim
Name	Nome do parâmetro	Varchar2	40	Sim
Value	Valor do parâmetro	Varchar2	100	Não
Description	Descrição do parâmetro	Varchar2	500	Não

Quadro 16 – Tabela Sec_parameters

SEC_PROFILE – Armazena as configurações dos *profiles* de usuário.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança	Varchar2	6	Sim
Resource_name	Nome da configuração	Varchar2	30	Sim
Value	Valor da configuração	Number	10	Não
Description	Descrição da configuração	Varchar2	300	Não

Quadro 17 – Tabela Sec_profile

SEC_PROFILE_EXCEPTION – Armazena os *profiles* que são exceção.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança	Varchar2	6	Sim
Profile	Nome do *profile*	Varchar2	30	Sim
Justification	Justificativa da exceção	Varchar2	100	Não

Quadro 18 – Tabela Sec_profile_exception

SEC_RESULT – Armazena o resultado da verificação do banco de dados alvo.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança	Varchar2	6	Não
Sec_time_num_seq_result	Id o resultado	Number	4	Não
Sec_type	Tipo do resultado	Varchar2	30	Não
Name	Nome do parâmetro	Varchar2	100	Não
Resource_name	Nome da configuração	Varchar2	100	Não
Value	Valor da configuração	Varchar2	100	Não
Expected_value	Valor esperado para a configuração	Varchar2	100	Não
Message	Informação sobre a configuração	Varchar2	1000	Não
Command	Comando para ajuste	Varchar2	1000	Não

Quadro 19 – Tabela Sec_result

SEC_ROLE_EXCEPTION – Armazena as *roles* que são exceções.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança	Varchar2	6	Sim
Role_name	Nome da *role*	Varchar2	40	Sim
Justification	Justificativa da exceção	Varchar2	100	Não

Quadro 20 – Tabela Sec_role_exception

SEC_SQLNET_PARAMETERS – Armazena as configurações dos parâmetros do *Oracle SQLNet*.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança	Varchar2	6	Sim
Name	Nome do parâmetro	Varchar2	40	Sim
Value	Valor do parâmetro	Varchar2	100	Não
Description	Descrição do parâmetro	Varchar2	500	Não

Quadro 21 – Tabela Sec_sqlnet_parameters

SEC_SYS_PRIVS – Armazena as configurações dos privilégios de sistema.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança	Varchar2	6	Sim
Privilege	Privilégio de sistema	Varchar2	60	Sim

Quadro 22 – Tabela Sec_sys_privs

SEC_TIME – Armazena informações sobre a verificação do banco de dados alvo.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Num_seq_result	Id da execução	Number	4	Sim
Excecution_date	Data da verificação	Timestamp		Não

Quadro 23 – Tabela Sec_time

SEC_USER_EXCEPTION – Armazena as contas de usuário que são exceção.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança	Varchar2	6	Sim
Username	Nome da conta de usuário	Varchar2	30	Sim
Justification	Justificativa da exceção	Varchar2	100	Não

Quadro 24 – Tabela Sec_user_exception

SEC_VERIFY_ROLES – Armazena as *roles* que devem ser verificadas.				
Campo	**Descrição**	**Tipo**	**Tamanho**	**Chave Primária**
Sec_model_name	Nome do modelo de segurança	Varchar2	6	Sim
Role_name	Nome da *role*	Varchar2	30	Sim

Quadro 25 – Tabela Sec_verify_roles

APÊNDICE C – Questionário utilizado na avaliação do sistema

No Quadro 26 é apresentado o questionário que foi aplicado aos Administradores de Banco de Dados da Teclógica para avaliação do sistema desenvolvido.

1. Como ficou o processo de auditoria de segurança em banco de dados Oracle em comparação ao processo atual? 1. Muito ruim 2. Ruim 3. Igual 4. Bom 5. Muito bom 2. Como você qualifica a utilização deste sistema para análise de segurança em um banco de dados Oracle? 1. Muito ruim 2. Ruim 3. Igual 4. Bom 5. Muito bom 3. Como você avalia as configurações disponibilizadas pelo sistema? 1. Muito ruim 2. Ruim 3. Igual 4. Bom 5. Muito bom 4. As informações disponibilizadas pelos relatórios são suficientes para entendimento dos itens em não conformidade? 1. Muito ruim 2. Ruim 3. Igual 4. Bom 5. Muito bom

Quadro 26 – Questionário utilizado na avaliação do sistema