Single Sign-On: um estudo de caso em banco de dados Oracle

Cássio Tavares Brito[1]
Charles Severino[1]
José Gonçalo dos Santos[1]
Petrônio Isidoro Gonçalves[1]

Resumo: É notório que as soluções disponibilizadas pela Tecnologia da Informação (TI) trazem benefícios para áreas afins e também áreas meio. Dessa forma, aceita-se que com a evolução tecnológica os Sistemas de Gerenciamento de Banco de Dados Relacional (SGBDR) obtiveram um ganho significativo dos recursos referentes a segurança, persistência, processamento e armazenamento de dados. A junção de todos esses recursos possibilita aos administradores de banco de dados (DBA) criar, organizar e manter as diversas bases de informações de diversas organizações da forma mais efetiva possível. A esse propósito o serviço de diretório, nos bancos de dados Oracle, veio contribuir para as melhores práticas de Segurança da Informação, que integrado aos Serviços de Diretórios já existentes, tais como: Active Directory (Microsoft), eDirectory (Novell) e OpenLDAP, aumentam o leque da interoperabilidade de serviços. Assim, como resultado, tem-se o provisionamento automático de identidades dos usuários nas principais funcionalidades, tais como a criação, atualização, desativação e remoção dessas contas nos respectivos Bancos de Dados, de forma imediata, e com total transparência. Este trabalho tem como objetivo elaborar um estudo sobre o componente Oracle Internet Directory, que provisiona login e senha únicos da rede corporativa sincronizados com o serviço de diretório do banco de dados Oracle. Quando esse componente é registrado nos Bancos de Dados Oracle, otimiza o custo da troca constante das senhas dos respectivos administradores de banco de dados. Assim, fundamenta-se as bases para que o single sign-on (único ponto de entrada) nos bancos de dados Oracle possa ser implementado seguindo as melhores práticas de gestão de acesso e segurança da informação.

Palavras-chave: Lightweight directory access protocol. Oracle internet directory. Single sign-on.

Abstract: *It is clear that the solutions provided by Information Technology (IT) bring benefits to related areas and also areas between. Thus, it is accepted that with this technological evolution Relational Database Management System (RDBMS) make a gain in resources related to security, persistence, processing and data storage. The combination of all these resources enables Database Administrators (DBA) to create, organize and maintain the various databases of information from various organizations as effectively as possible. In this regard the Directory Service in Oracle Database, has contributed to best practices for Information Security, which integrates with existing directory services, such as Active Directory (Microsoft), eDirectory (Novell) and OpenLDAP, increasing the range of services interoperability. Thus, as a result we have the automatic provisioning of user identities in major features such as creating, updating, disabling and removal of these accounts in the respective databases, immediately and with full transparency. This paper aims to conduct a study on the Oracle Internet Directory component that accrues unique login and password from the corporate network synchronized with Directory Service Oracle Database. When this component is registered with Oracle Database optimizes the cost of the constant exchange of passwords in their Database Administrators. So, is based on the foundation for the Single Sign-On (Single Point of Entry) in the Oracle Database can be implemented in accordance with best practices in Access Management and Information Security.*

Keywords: *Lightweight directory access protocol. Oracle internet directory. Single sign-on.*

[1] Curso de Sistemas de Informação, UNIEURO, Campus 2 – Av. Castanheiras, 2700 – Águas Claras (DF) - Brasil
cassio.T.B@gmail.com, charles_kso@hotmail.com, jose.santos@unieuro.com.br, petronioisidoro@hotmail.com

http://dx.doi.org/10.5335/rbca.2012.2125

1 Introdução

Com o advento da tecnologia da informação (TI) foi percebido o vultoso aumento dos recursos disponíveis em processamento e armazenamento de dados. Esses recursos são usados visando criar, organizar e manter as bases de informações de diversas organizações, garantindo cada vez mais a segurança e persistência dessas informações. Para a guarda dessas existem vários sistemas de gerenciamento de banco de dados (SGBD), como Oracle, SQL Server, DB2, PostgreSQL e MySQL, mas este estudo está focado no Sistema SGDB Oracle. Oportunamente todos esses recursos vinculam-se a algum serviço e as demandas de serviço foram sendo incorporadas ao mercado que necessita de soluções para sanar dificuldades encontradas em sua trajetória, em nosso caso de trabalho é o serviço de autenticação de administradores de bancos de dados (DBA).

Em um cenário de proposta de soluções, com uma demanda de multiplicidade de bancos de dados, é desejável que exista um repositório central para autenticação dos diversos usuários desses bancos, ofertando o paradigma de centralização de informações, que pode ser vista como "uma tendência" [3]. Para os gestores da tecnologia da informação, que enfrentam vários processos descentralizados, isso é algo muito positivo devido à realidade de algumas organizações que possuem centenas de bancos de dados, com vários DBAs, que necessitam constantemente fazer logon nesses bancos e também na rede da organização, valendo-se cada um desses de um arsenal de senhas para sua autenticação.

A descentralização das informações pode ser vista como barreira pelos usuários internos ao tentar gerir bancos de dados e também as inúmeras senhas que necessitam possuir para acessá-los, o que é agravado com o uso de uma política de renovação de senhas que podem abranger períodos muito curtos (como uma quinzena, por exemplo), que tornam o crescimento do problema maior. E essas organizações ainda devem atender ao disposto [1] no que concerne à identificação e à autenticação de usuários e sistemas de gerenciamento de senha, que determina que a organização apoie seu controle seguindo o princípio, deferido pela mesma norma, que "Sistemas para gerenciamento de senhas devem ser interativos e assegurar senhas de qualidade". E boa parte dessas organizações tenta aplicar uma melhor forma de auditar quais usuários continuam a ter acesso as informações contidas nestes SGDBs, e que dependendo da corporação pode ser o seu ativo de mais préstimo.

Devido ao exposto anteriormente, este artigo apresenta uma proposta de implementação de um repositório central para proporcionar aos funcionários acesso rápido e seguro às suas aplicações, para que eles possam fazer o seu trabalho de forma eficaz. E também que a organização aumente a segurança através da aplicação do gerenciamento apropriado de senhas e, concomitantemente, reduza as chamadas ao *service desk*, eliminando problemas de senhas esquecidas. Essa solução baseia-se no single sign-on (SSO), que consiste em um único ponto de entrada para as solicitações dos usuários administradores de bancos de dados.

2 Segurança da informação

O ambiente de tecnologia da informação (TI) no qual está inserido o single sign-on deve atender às disposições fundamentadas na ABNT [1] que foi desenvolvida com intuito de "prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)" [1] e sua implementação, que cobre todos os tipos de organizações, norteia um alinhamento estratégico da TI com o negócio (a organização) visando de forma transcendente a segurança o envolvimento da direção da organização com a política e implementação desse SGSI, uma vez que ela também destaca que prima por integrar o SGSI com requisitos de sistemas de gestão relacionados. No entendimento ofertado pela norma percebe-se que o SGSI tem como objetivo "assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança as partes interessadas" [1].

No tocante à abordagem organizacional de segurança da informação, que se fundamenta em processos, além do notório envolvimento da direção da organização com a segurança de TI deve-se promover o entendimento dos usuários quanto à importância de se implementar uma política de segurança, focar nos seus objetivos e requisitos e mantê-la em sua totalidade operando conforme a decisão estratégica da organização que a criou. A abordagem dos processos motivadores que culminaram na política de segurança e que envolve todos os usuários da empresa de alguma forma, deve prover operações de controle e implementação, monitoração, análise crítica e melhoria contínua com fulcro a gerenciar os riscos de TI e do negócio.

A ISO / IEC 27001:2006 [1] evidencia o envolvimento e adota o modelo "Plan-Do-Check-Act" (PDCA) que envolve processos e procedimentos do SGSI. O ciclo PDCA aborda dentro do SGSI etapas onde se deve plan (planejar), do (fazer), check (checar) e act (agir) e que envolve etapas desde o objetivo, implementação, avaliação e execução da Política de Segurança proposta pelo SGSI.

2.1 Termos e definições

Os termos e definições usados em SGSI, referenciados e determinados pela ABNT [1], e que com alguma frequência serão mencionados neste artigo são:

- aceitação de risco: decisão de aceitar um risco;
- análise de riscos: uso sistemático de informação para identificar fontes e estimar o risco;
- ativo: qualquer coisa que tenha valor para a organização;
- avaliação de riscos: processo de comparar o risco estimado com critérios predefinidos para determinar a importância do risco;
- confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
- disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;
- gestão de riscos: atividade coordenada para direcionar e controlar uma organização no que se refere a riscos;
- integridade: propriedade de salvaguarda da exatidão e completeza de ativos;
- segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação;
- sistema de gestão da segurança da informação (SGSI): a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

2.2 Segurança em recursos humanos

A abordagem de segurança da informação (SI) referida a single sign-on (SSO) também deverá implementar mecanismos que assegurem o processo de segurança em recursos humanos, que antes da contratação avalie o envolvimento desde os próprios funcionários, até fornecedores e terceiros. E que esses tenham seus papéis e responsabilidades de segurança da informação bem definidos, auxiliando e oferecendo sinergia para diminuir riscos de fraude, furto e roubo dos recursos.

A abordagem de recursos humanos leva também a pensar em proteção de ativos, visto que deve-se promover seu inventário e uso aceitável além de determinar quem são os proprietários desses ativos para delegá-los a devida responsabilidade sobre eles. Dessa forma,

> o termo proprietário identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo proprietário não significa que a pessoa realmente tenha qualquer direito de propriedade pelo ativo [1].

2.3 Controle de acesso

A implementação do SSO, necessariamente, remete a estabelecer um controle de acesso para alcançar níveis razoáveis de domínio sobre o acesso a informação. Assim, o SGSI deve prover uma política de controle de acesso, que deve ser devidamente documentada, estabelecida e mantida, independente do segmento da organização que esteja responsável por ela, que na prática pode ser feito pelo setor de recursos humanos (RH), por exemplo.

2.4 Gerenciamento de acesso e responsabilidades do usuário

O gerenciamento de acesso do usuário, que opera a partir do controle de acesso, deve naturalmente oferecer aos usuários autorizados o acesso que lhes é devido, da mesma forma aperfeiçoar o processo de negação de acesso não autorizado. Seguindo os parâmetros estabelecidos pela norma mencionada, é interessante manter registro de usuários (que conceda e revogue acesso a usuários), gerenciar privilégios e senhas dos usuários. É também recomendado que se proceda a uma análise crítica dos direitos de acesso de usuário, visto que usuários possuem mobilidade dentro da organização e podem ser realocados em outros setores dela mesma, e no pior caso estar envolvidos com atos que ferem o SGSI e por consequência terem extirpados ou cassados estes direitos de acesso. O SGSI determinará também a responsabilidade dos usuários quanto ao uso de senhas, equipamentos de usuário sem monitoração e política de mesa limpa e tela limpa, que tem por objetivo "Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação" [1].

2.5 Controle de acesso à rede

Os mecanismos de segurança presentes, nativamente, no LDAP (lightweight directory access protocol ou protocolo leve de acesso a diretório) são relevantes no processo de controle de acesso à rede e autenticação de usuários, no entanto, a organização também deve suprir com recursos previstos no SGSI a segurança à rede. Dessa forma, ela deve estabelecer uma política de uso dos serviços de rede, autenticação para conexão externa do usuário (no caso de permissão de acesso remoto), identificação de ativos de rede, segregação de redes (divisão em grupos de serviços de informação), controle de conexão de rede e controle de roteamento de redes. Todos os itens mencionados têm como objetivo manter a segurança, prevenção e tratamento de riscos que incidam sobre a segurança, disponibilidade e confidencialidade da informação.

Assim como o LDAP (lightweight directory access protocol ou protocolo leve de acesso a diretório) provê recursos nativos de segurança o Oracle Internet Directory (OID) revitaliza a segurança da informação utilizando o protocolo publick key infrastructure (PKI) abrangendo diversos componentes. Ele é implementado por meio do mecanismo secure sockets layer (SSL), que originalmente foi desenvolvido pela netscape development corporation para uso em navegadores da WEB (por volta da década de 1990), onde é baseado no conceito de chaves privadas secretas que são relacionadas às chaves públicas para facilitar as comunicações seguras entre cliente e servidor. Para fornecer serviços de identificação e autenticação, o PKI usa certificados e autoridades certificadoras (certificate authorities – CA), que são chaves públicas de uma entidade que são validadas por um terceiro confiável (uma autoridade certificadora) e ela contém informações, como o nome do usuário do certificado, a data de expiração, a chave pública etc.

2.6 Oracle application server (OAS)

O oracle application server é um conjunto de ferramentas que a Oracle disponibiliza de forma a prover o acesso single sign-on, e entender como esses componentes se completam é necessário para absorver por completo o SSO, dentre essa composição de ferramentas destacam-se [4],[7],[8],[9] e [10]:

O Oracle Identity Management (OIM) é um componente do Oracle application server 10g e 11g que fornece um framework completo, de ponta a ponta, para gerenciar centralmente as contas de usuários dos diversos bancos de dados Oracle existentes, desde a criação de suas contas, autorização de acesso aos recursos do banco de dados, até a sua exclusão. Ele centraliza o gerenciamento das contas de usuários, aplicações, serviços Web ou qualquer outra entidade de rede que usa autenticação e autorização.

O Oracle Identity Management economiza tempo e recursos financeiros, pois gera menos custos de provisionamento das contas dos usuários uma vez que, como as contas e os recursos estão centralizados, a administração é a mesma independente da aplicação que está sendo mantida, melhorando a segurança da empresa. Os usuários utilizam somente uma identificação e uma única senha para acessar todos os recursos da organização, sendo menos propensos a escrevê-las em meios e locais inapropriados, e, no pior caso, esquecê-las. Quando um usuário deixa a empresa todos os acessos às aplicações e aos serviços são removidos rapidamente e facilmente de um único repositório.

Uma abordagem prática sobre o gerenciamento de acesso dos usuários, provido pelo OIM, deve ser feita apropriadamente neste ponto, visto que, embora a TI provisione os recursos e mecanismos para conceber

(abrindo um chamado para o gestor da área onde o funcionário será alocado) e eliminar (no momento da saída deste funcionário da empresa) privilégios de usuários DBA, nem sempre ela mesma é a responsável por mantê-lo. Ocorre que muitas organizações podem optar por confiar esse serviço ao RH, por exemplo, à medida que no processo de admissão e demissão de funcionários, todos devem ser atendidos de forma criteriosa por esse setor da empresa. No entanto, é notório que são eliminados, na saída do funcionário, os privilégios e não os registros de Log. Uma vez que é necessário mantê-los para enriquecer os mecanismos de segurança da empresa, como a auditoria, por exemplo.

O Oracle Internet Directory (OID) é um importante componente da ferramenta Oracle Application Server, responsável por melhorar o gerenciamento das aplicações e serviços de armazenamento e o acesso das informações, tais como credenciais dos usuários e privilégios de acesso e aos metadados das aplicações, oferecendo um serviço aberto baseado na confiabilidade, disponibilidade e escalabilidade. Para que isso seja possível, o LDAP também está integrado ao pacote de ferramentas do Oracle Server Application, garantindo a interoperabilidade entre os diversos aplicativos com interfaces de programa padronizados que se adequam ao serviço de diretório.

O serviço de diretório é projetado para fornecer uma grande variedade de informações sobre usuários, aplicativos, serviços de rede e outros objetos, dentre os quais destacam-se:

- serviço de armazenamento extensível – serviço de diretório projetado para uma grande variedade de informações relacionadas com os recursos utilizados. Algumas dessas informações podem ser padronizadas, enquanto outros tipos de informações podem ser específicos para um determinado diretório;
- serviço de ampla acessibilidade - serviço de diretório projetado para fornecer dados para múltiplas aplicações. Este tipo de diretório em geral é chamado de diretório corporativo, que armazena os atributos mais utilizados por quase todos os aplicativos, compreendendo os dados de usuários e suas respectivas senhas.
- serviço de acesso distribuído - serviço de diretório projetado a partir de uma base de dados de apoio à gestão distribuída e recuperação da informação. Muitos serviços de diretório são distribuídos em regiões, cidades, países diferentes de forma a garantir a disponibilidade do serviço sem nenhuma interrupção ou impacto em caso de qualquer evento da natureza.

A escalabilidade de um serviço de diretório pode ser avaliada sob dois aspectos: quanto ao número de entradas, ou objetos de diretório que podem ser suportados em uma única instância de servidor, ou quanto ao número de acessos de clientes simultâneos suportados pelo servidor.

A experiência demonstra que os aspectos de escalabilidade são de especial interesse para a prestação de serviços principalmente em organizações de grande porte e em ambientes de extranet, pois determinam em grande medida o número de nós de diretório de servidor necessários para suportar uma árvore de informações. Com o OID, isso traduz a capacidade de armazenar mais de meio bilhão de entradas reais de um diretório em um único servidor.

2.7 LDAP

O lightweight directory access protocol ou protocolo leve de acesso a diretório é um protocolo fundamental no contexto abordado de SSO, pois possibilita a consulta de informações existentes em um único diretório simples (com foco em leitura) que pode ser acessado por clientes LDAP, partindo de outros fornecedores, o que envolve uma alta compatibilidade com outros produtos e também atende a requisitos de segurança como a criptografia de autenticação. Para entender melhor o que é o LDAP, é necessário entender como ele surgiu e a que fins pretendia atender.

Conforme apresentado em Microsoft [3], o LDAP unifica redes permitindo interação entre servidor LDAP com outros servidores em rede. O que remete também a interoperabilidade, ou seja, a comunicação entre esses servidores. Ele minimiza esses problemas, pois suas características principais estão padronizadas. Importante também é mencionar a integração de diretório que significa habilitar o aplicativo do cliente a acessar dados em um diretório LDAP. Ainda, por ser tão performático, atua resolvendo nomes, entretanto, não é uma substituição ao DNS (sistema de nomes e domínios), mas pode-se usar como um sistema de armazenamento de backend para arquivos de zona de DNS, ou seja, mover dados de zona de DNS para um diretório LDAP.

Ao se falar em LDAP deve-se ter em mente o quanto é importante a estrutura de árvore de pesquisa, o modelo com o qual é feita a guarda e consulta das informações, e onde dificilmente é realizada uma atualização, o que otimiza respostas a um grande número de pesquisas com alto nível de segurança, conforme mostra a Figura 3, Estrutura de Árvore do LDAP, é estruturado conforme Figura 1.

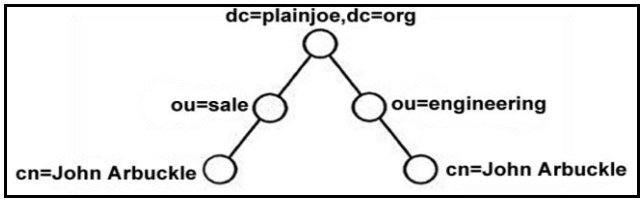


Figura 1: Estrutura de Árvore LDAP ([3])

A Figura 1 consiste em uma árvore de pesquisa, na qual o início apresenta um nó raiz dc (Domain Container) = plainjoe, dc = org, os dois nós filhos abaixo ou (objeto Organization) = sales e ou = engineering são containers usados para armazenar informações de grupos dos usuários (atributos da unidade organizacional, departamentos) e os nós folhas com Common Name ou Nomes comuns (cn) cn = John Arbuckle e cn = John Arbuckle são referências de distinção entre estes nomes, evitando-se conflito entre eles.

Essa terminologia envolve um conjunto de atributos como o Distinguished Names (DN), ou Nomes Distintos, que são usados para identificar uma entrada unicamente. Eles são formados por um conjunto de Relative Distinguished Names (RDN), ou Nomes Distintos Relativos. E cada RDN corresponde a um Directory Information Tree (DIT), composto por listas de informações da árvore, desde a raiz (nó folha da árvore) até a entrada a qual o DN faz referência.

Trata-se também de uma forma de reduzir o número de entradas que tem o mesmo nó pai (departamentos) o que facilita bastante a busca no diretório. Dessa forma, infere-se com clareza que mesmo tendo os mesmos nomes comuns (cn), John Arbuckle, eles não são os mesmos objetos, pois estão em departamentos diferentes, vendas e engenharia, o que é relevante no critério de busca de usuários quando se depara com usuários de mesmos nomes.

O serviço de autenticação do LDAP abrange também vínculos de logon da plataforma Windows usando o Active Directory (AD), que é um serviço de diretório proprietário da Microsoft [7].

Sobre o Active Directory,é salutar descrever que é usado em recursos de integração de outras plataformas e redes com recursos oriundos da Microsoft, desde que usem o protocolo Kerberos na versão 5, além disso:

> O Active Directory pode ser descrito como um serviço de diretório de sistema operacional de rede (NOS) que utiliza LDAPv3 como seu protocolo de acesso primário e é, juntamente com o Kerberos 5, a peça mais importante do maior modelo de infra-estrutura de domínio da Microsoft [3].

2.7.1 Segurança em LDAP

A abordagem desta seção será fundamentada nos conceitos apresentados em Microsoft [3], segundo quem a segurança deve ser abordada além do contexto do OID, visto que é crucial que o protocolo LDAP, que autentica os usuários envolvidos nos grupos, também apresente de forma robusta mecanismos e recursos de segurança próprios. Quando se abrange a autenticação de usuários, envolvemos as diversas informações que foram colocadas no diretório, que, dentre outras funcionalidades, controla os usuários que podem fazer logon nas máquinas da rede e bancos de dados.

No diretório podem, além das senhas, ficar hospedadas muitas outras informações, tais como: informações de recursos humanos da empresa, nomes de usuários, dados pessoais de usuários e, inclusive, informações confidencias. Dessa forma, será necessário detalhar o nível de segurança desejado e as informações que são protegidas. Para tal, pode-se fazer uso de recursos de segurança tratados em LDAP avaliando como o módulo PAM (módulos plugáveis de autenticação) se vincula ao LDAP e SASL (simple authentication and security layer) que suporta métodos seguros de autenticação como Kerberos 5 e MD 5 no tratamento de proteção

de senhas e outros recursos pra proteção de outras informações. Com fulcro em manter um ambiente seguro, deve-se também se perguntar qual o nível de segurança que se pretende implementar e quais informações, efetivamente, se deseja proteger. Para respostas que são esperadas nesse contexto, soluções já apontadas como o Kerberos 5 da Microsoft são boas opções, eis que consiste, este, no principal protocolo de segurança para autenticação em um domínio. O Kerberos 5 verifica, ainda, a identidade do usuário que solicita a autenticação e o servidor que fornece a autenticação solicitada. Aliado a este se tem o MD 5 que aborda a criptografia das credenciais, devendo-se verificar com qual algoritmo de criptografia o servidor em questão (da organização) é compatível.

Como o LDAP possui uma maturidade em nível de segurança, pode-se também optar por negociar uma camada de transporte segura que abrangerá informações envolvidas no acesso, na vinculação (autenticação em nível de LDAP) e autorização.

Para garantir o acesso aos recursos de segurança que são aplicados no cliente e no servidor e implementados pelo software Open SSL, pode-se usar o comando Start TLS, que é disponibilizado pelo SLDAP através do transport layer security - segurança da camada de transporte (TLS), que é semelhante à secure sockets layer (SSL), que, por sua vez, é um sistema de codificação para proporcionar a máxima confidencialidade na troca de dados pela internet (os dados passam a ser cifrados no envio e decifrados no destino), no entanto, o TLS usa uma tecnologia diferente do SSL, mas o papel de ambos é garantir a segurança das informações trocadas na rede. O SLDAP, sendo um serviço LDAP autônomo, de um produto específico que negocia essa camada, segura e "escuta" as portas definidas (que nesses casos passam a escutar a porta 636 ao invés da 389, inclusive nos serviços de provimento de mensagens como Windows Live Mail), realiza esse processo antes da vinculação ao servidor. No contexto do serviço de correio é importante mencionar o agente de transferência de correio (MTA) que envolve servidor simple mail transfer protocol e servidores de correio em geral. O SLDAP é configurado através do ficheiro sladp.conf, onde é possível adaptá-lo e configurá-lo a fim de atender aos serviços do sistema.

A autenticação sugere a conferência da identidade validando um cliente no serviço, o LDAP suporta, nesse quesito, o simple authentication and security layer, que viabiliza um acordo entre cliente e servidor para estabelecer um método seguro de autenticação.

A autorização tem por objetivo conceder ou negar direitos ou funcionalidades aos clientes. Os recursos também podem se estender, até se dizer "quem" deve ter acesso a "que" tipo de informação, para isso, conta-se com as listas de controle de acesso do diretório. Uma forma mais simples de controle de acesso é definir um nível padrão de autenticação. A definição de "quem" corresponde aos usuários conectados (que se considera ter realizado o processo de autenticação de forma bem sucedida), sendo que os níveis mais altos possuem todos os recursos presentes nos níveis mais baixos. E a "que" é definida uma entrada e os atributos aos quais a lista deve se aplicar. Ademais, uma ACL pode ser usada para determinar as unidades básicas de informação (entradas do diretório) e o cliente pode visualizar que alterações possui permissão para realizar. Outros mecanismos de provimento de segurança serão oportunamente descritos, à medida que o processo de vinculação do LDAP venha a ser implementado junto ao OAS da Oracle.

2.8 Enterprise user security (EUS)

Enterprise User Security é uma funcionalidade do banco de dados através da qual os usuários passam a ser autenticados em um serviço de diretório. Atualmente somente o Oracle internet directory suporta essa autenticação.

Uma vez tendo sua credencial criada no OID, o usuário pode acessar, de acordo com seus privilégios (roles), todos os bancos de dados que estejam configurados para autenticar os usuários no serviço LDAP provido pelo OID e que foram mapeados nas roles dadas aos usuários. A Figura 2 mostra um exemplo do uso do EUS.

O EUS provê suporte a dois tipos de schemas de banco de dados: private e shared.

No schema private, cada enterprise user pode ter seus próprios objetos lógicos de banco de dados (tabelas, índices, packages, etc). Já a credencial do usuário, ainda precisa ser criada no Banco de Dados, a única diferença é que no momento da autenticação o servidor de banco utiliza os serviços de LDAP para fazer a autenticação do usuário.

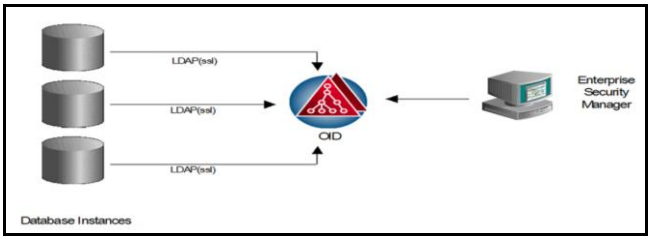


Figura 2: Autenticação dos usuários LDAP no OID

No schema shared, cada enterprise user pode ser mapeado para um "sharedschema" em cada um dos bancos de dados de um enterprise domain. Um "sharedschema" é um usuário dono de objetos de banco (tabelas, índices etc) que não consegue se conectar no Banco de Dados.

O enterprise user security que integra o Oracle application server possui como sua principal funcionalidade a consolidação das diversas contas existentes nos diversos bancos de dados e aplicações existentes na empresa com o Oracle internet directory, de forma a executar uma autenticação externa dos usuários, em schemas privados ou compartilhados, cadastrados no banco de dados do OID.

Para desabilitar o acesso a todos os sistemas e bancos quando um empregado sai da empresa, o administrador faz uma única alteração no serviço de diretórios da empresa e o acesso é revogado automaticamente de todos os ambientes registrados no OID, sendo, dessa forma, esse empregado movido para um contêiner de inativos em uma árvore LDAP específica dentro do servidor.

Abaixo são descritas as etapas do processo de autenticação de usuário ao banco de dados utilizando o Oracle internet directory.

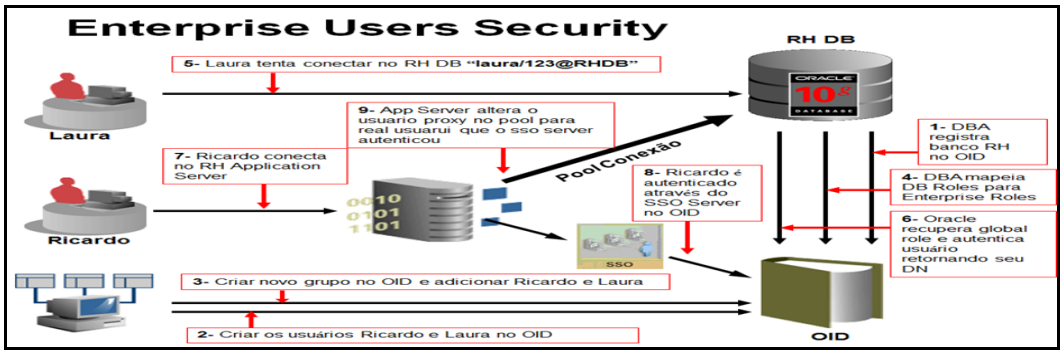


Figura 3: Etapas da autenticação de um usuário utilizando o OID

A autenticação de um usuário no Oracle internet directory poderá ser realizada através de schemas individuais ou schemas compartilhados. A necessidade do projeto define a melhor forma de configuração do processo de autenticação. Os schemas compartilhados possibilitam que diversos usuários cadastrados no Oracle internet directory se conectem em um banco de dados Oracle utilizando somente uma única conta, do tipo shared. Já no que concerne aos schemas individuais, existe, para cada conta existente no serviço de diretório, uma conta associada ao banco de dados [2].

3 Estudo de caso

O estudo de caso realizado consiste em um delineamento de pesquisa que permite a descrição e o aprofundamento sobre o conhecimento bibliográfico do single sign-on em banco de dados Oracle.

A empresa Log Telecomunicações, que é objeto de estudo neste trabalho, atua no ramo de telecomunicações na cidade de Brasília, Distrito Federal, e foi escolhida para o estudo de caso por possuir um cenário com uma grande quantidade de bancos de dados Oracle e, consequentemente, vários DBA, gerenciando-os, mas também por não possuir um mecanismo central de autenticação para os usuários, o que se torna um problema para gestão de controle da grande quantidade de senhas necessárias para acesso, autenticação e autorização aos bancos de dados, o que ocorre pela necessidade de cada DBA possuir usuário e senha para cada

banco específico. Esse ambiente propicia a apresentação de proposta de centralização dos processos de autenticação desses usuários (DBA).

3.1 Cenário atual

O cenário atual retrata a dificuldade dos administradores de banco de dados (DBA) em memorizar cada uma das senhas que compõem o parque de databases da organização conforme exposto na Figura 4. Como se pode observar, para cada banco de dados existe uma política de senha individual.

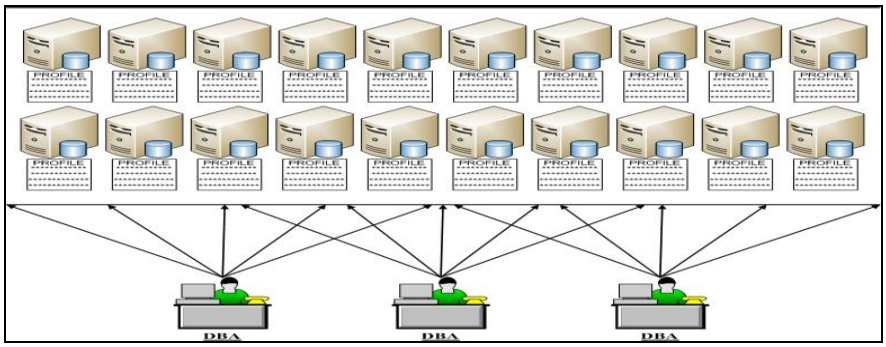


Figura 4: Política de senha individual para cada banco de dados

Para proposição do novo cenário, as seguintes etapas foram seguidas: formulação do problema; coleta dos dados e resultados.

3.1.1 Formulação do problema

Conhecer a identificação e descrição do problema, que envolve desde vulnerabilidades, ameaças técnicas, produtos ou procedimentos que podem ser usados na organização para prover desempenho e eficácia a algum serviço ou processo, é o passo inicial para se determinar a apresentação de uma proposta de solução. Conhecê-lo e descrevê-lo é fundamental para oferecer possíveis mecanismos e aplicações que viabilizem um novo processo para tratar e resolver este problema, além de apresentar resultados da eficácia dessas medições comprovando a existência do problema.

A empresa Log Telecomunicações usa banco de dados Oracle e possui vários funcionários ocupantes do cargo de administrador de banco de dados, esses se autenticam na rede Windows, pelo serviço de diretório AD para usar aplicações, e também nos bancos de dados para executarem suas tarefas afins, no entanto, foi percebido que cada DBA possui uma senha para se autenticar na rede e uma senha específica para acessar cada banco de dados, é conhecido que cada DBA é responsável por dezenas de bancos de dados e cada um destes possui um usuário e senha próprios, e ainda que a empresa possui uma política de renovação de senhas, com fulcro a fortalecer o processo da política de segurança como um todo, que compulsoriamente faz com que os usuários renovem suas senhas a cada 45 dias, via portal de senhas da empresa.

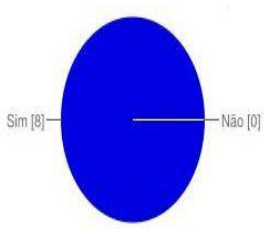
O problema fica determinado à falta de um mecanismo central para fortalecer o processo de autenticação desses usuários na rede e nos bancos de dados e também prover, simultaneamente, uma melhor segurança para a empresa, visto que os DBAs podem valer-se de qualquer recurso para recordarem das inúmeras senhas que possuem e que devem ser ainda renovadas. O que vai muito além da decisão de aceitação do risco proposto na ABNT [1], uma vez que não foram tomados os devidos cuidados para prover uma política de segurança que atenda de fato a referida norma e proteja os ativos dessa organização.

3.1.2 Coleta dos dados resultados

Essa etapa do processo consiste em visitas à empresa Log Telecomunicações para, in loco, proceder entrevistas e aplicar questionários aos DBAs, que trabalham em equipes de oito funcionários por turno, e se necessário a seus gerentes e aos líderes envolvidos com processos afins (como exemplo, os envolvidos com o

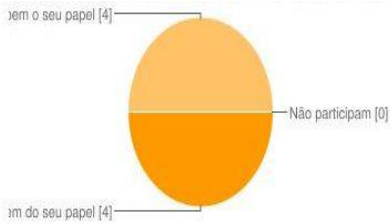
serviço de identidade digital da empresa) para que esses respondam as questões de forma a se avaliar o cenário atual da empresa a partir dos seguintes pontos:

1. Os usuários sabem da existência de uma política de segurança na empresa?



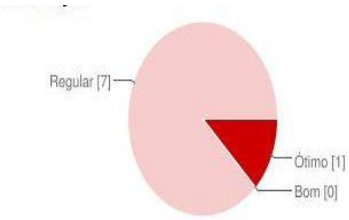
Sim	8	100%
Não	0	0%

2. Em caso positivo, eles participam desta e sabem qual é o seu papel neste contexto?



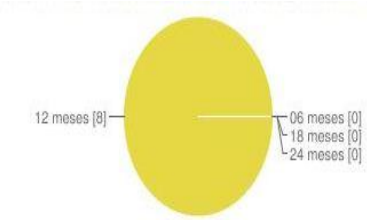
Sim, participam e sabem do seu papel	4	50%
Sim, participam mas não sabem o seu papel	4	50%
Não participam	0	0%

3. Como pode ser qualificado o atual serviço de autenticação de usuários a rede e aos bancos de dados dentro dos critérios de segurança aplicados a atual política da organização?



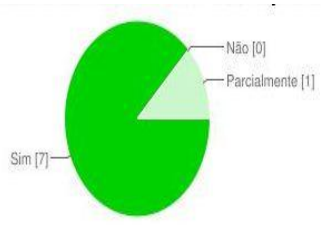
Ótimo	1	13%
Bom	0	0%
Regular	7	88%

4. Qual o período em que a empresa é auditada internamente para quantificar o número de DBAs ativos e os que contam com permissão para manipulação dos bancos de dados?



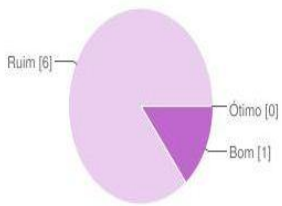
06 meses	0	0%
12 meses	8	100%
18 meses	0	0%
24 meses	0	0%

5. Os usuários conhecem o funcionamento do serviço de acesso, autenticação e autorização para bancos de dados?



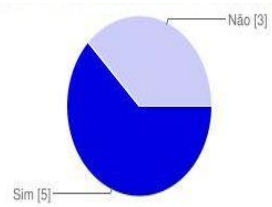
Sim	7	88%
Não	0	0%
Parcialmente	1	13%

6. Em caso positivo, como os usuários avaliam este serviço?



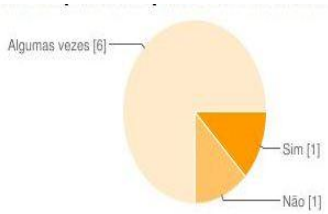
Ótimo	0	0%
Bom	1	13%
Ruim	6	75%

7. Os usuários conhecem alguma ferramenta que ofereça uma otimização para este serviço de autenticação em bancos de dados Oracle?



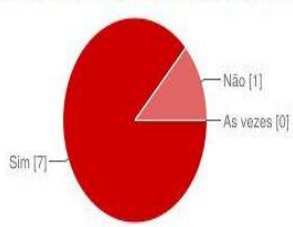
Sim	5	63%
Não	3	38%

8. A empresa preocupa-se em ouvir seus funcionários visando a implementar melhoria de processos de segurança e novas tecnologias que provisionem um melhor acesso, autenticação e autorização dos recursos de banco de dados?



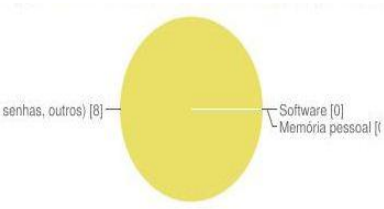
Sim	1	13%
Não	1	13%
Algumas vezes	6	75%

9. Os usuários percebem alguma queda de produtividade devido ao atual procedimento de autenticação deles mesmos nos bancos de dados?



Sim	7	88%
Não	1	13%
As vezes	0	0%

10. Quais recursos são comumente usados para que os usuários se recordem das dezenas de senhas de acesso para todos os bancos que são responsáveis?



Software	0	0%
Meios fisicos (papel, cartão de senhas, outros)	8	100%
Memória pessoal	0	0%

Com base nas respostas obtidas acima, nos problemas apresentados no cenário atual e nos conhecimentos do grupo a respeito do tema, foi proposta uma solução centralizada de acesso, autenticação e autorização a empresa, visto que, ao realizar esse processo de questionário aliado a entrevistas, foi possível conhecer o cenário real e atual que esses DBA possuem na empresa e a partir dessas primeiras informações coletadas propor soluções que realmente atendam as necessidades da organização e se necessário customizá-las para que os componentes envolvidos no processo interajam de forma harmônica, o que proporciona uma ampla compatibilidade entre os produtos e plataformas envolvidos. O conceito de diretório ativo que é implementado firma-se sobre o protocolo LDAP que provisiona a autenticação centralizada e integrada, o que independe do produto.

3.2 Cenário proposto

O cenário proposto retrata a facilidade que os administradores de banco de dados (DBA) obtêm quando o parque de todo os databases estiverem sincronizados no serviço do Oracle internet directory que garantirá o sincronismo do mesmo logon e senha de rede para todos os bancos registrados no serviço.

Na proposição de uma solução ao ambiente anterior, apresenta-se o ambiente centralizado, como demonstra a Figura 5, que aborda a grande vantagem que os DBAs têm em realizar suas atividades administrativas, conectando-se em diversas databases existentes através de uma única senha, passando pelo processo de autenticação via OID.

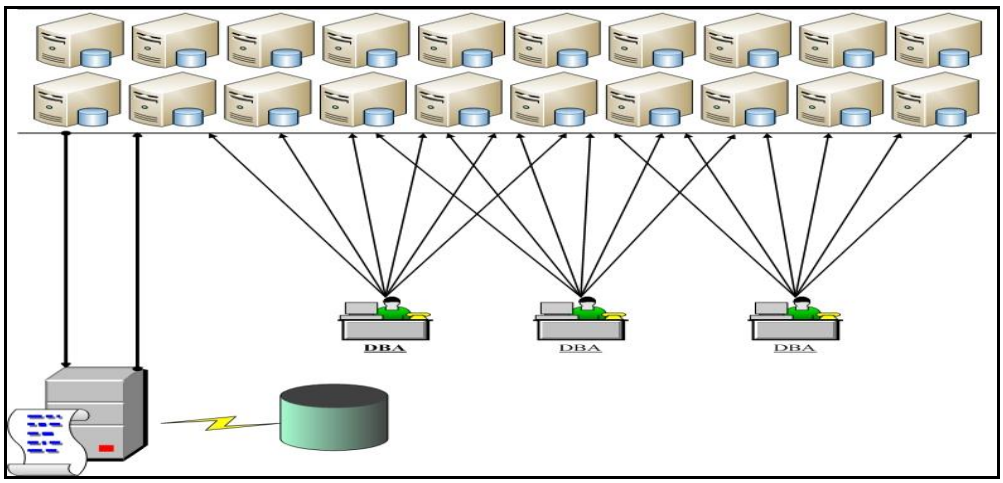


Figura 5: Política de senha centralizada no OID

3.3 Pesquisa de satisfação com a implantação do single sign-on

Foi realizada uma coleta de dados junto aos DBA da empresa antes da implementação do single sign-on. Dessa forma, após a ferramenta já instalada e disponibilizada para uso, foram coletadas novas informações, geradas e disponibilizadas por aplicação Web aos funcionários da empresa. Com base nas nove perguntas respondidas, conforme mostrado na tabela abaixo, onde P1 refere-se à pergunta um e assim por diante. A participação de 60 % (sessenta por cento) dos DBAs da empresa viabilizou mensurar a qualidade do serviço single sign-on já implantado, como mostra a Figura 6, fundamentado nas perguntas encontradas na Tabela 1.

Tabela 1: Perguntas sobre o desempenho do single sign-on (SSO)

Pergunta	Descrição
P1	A agilidade do acesso aos bancos de dados demonstra a eficiência do OID?
P2	O usuário e senha do Login de rede são os mesmos utilizados para acessar os banco de dados?
P3	A renovação da senha do usuário DBA, periodicamente a cada 45 dias, é automática nos bancos de dados uma vez que realizada no portal de senhas da empresa?

P4	A rastreabilidade do acesso ao banco de dados é mantida?
P5	A conta do DBA ao ser bloqueada ou removida no OID, automaticamente, impossibilita o acesso, autenticação e autorização nos Bancos de Dados?
P6	A integridade referencial do produto OID, permite que um usuário DBA removido do diretório também seja removido do grupo ao qual ele pertence?
P7	O serviço de OID gerou alguma indisponibilidade que prejudicou o acesso aos bancos de dados?
P8	O usuário DBA concorda que o OID retira o GAP de contas de DBA desligados da empresa, existentes nos Bancos de Dados?
P9	O usuário DBA recomenda a utilização do OID para outras empresas que primam pelas melhores práticas de Segurança, como a Lei Sox?

Com base nas respostas obtidas em cada uma das perguntas da Tabela 1 foi gerado o gráfico da Figura 6. Como pode ser observado, a maioria dos DBAs concorda que a implantação do serviço de OID é vantajoso, como pode ser visto nas respostas da maioria das perguntas. Cabe ainda dizer que o número de respondentes que concordam que a implantação do OID gerou alguma indisponibilidade que prejudicou o acesso aos bancos de dados ser igual ao número de discordantes, se deve ao fato de que a implantação de novas ferramentas, apesar do planejamento sempre gera algum tipo de inconveniente, que no caso pode ser superado por outras vantagens como as mostradas na pesquisa de satisfação, conforme Tabela 2 e ilustrada pelo gráfico da Figura 6.

Tabela 2: Respostas às perguntas da Tabela 1

Pergunta	Concorda	Concorda parcialmente	Não concorda
P1	7 (88%)	1 (12%)	0 (0%)
P2	7 (88%)	1 (12%)	0 (0%)
P3	7 (88%)	1 (12%)	0 (0%)
P4	7 (88%)	1 (12%)	0 (0%)
P5	8 (100%)	0 (0%)	0 (0%)
P6	8 (100%)	0 (0%)	0 (0%)
P7	3 (38%)	2 (24%)	3 (38%)
P8	7 (88%)	1 (12%)	0 (0%)
P9	7 (88%)	1 (12%)	0 (0%)

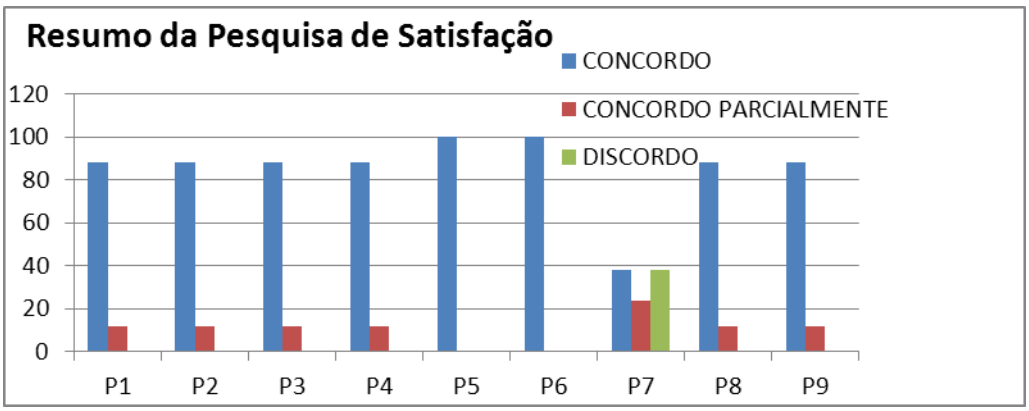


Figura 6: Pesquisa de Satisfação

4 Conclusões

A solução disponibilizada pelo single sign-on oferta uma infraestrutura em alta disponibilidade, em ambientes de aplicação e banco de dados redundantes. Dessa forma, percebemos, através das pesquisas

realizadas, que é imprescindível a monitoração dos serviços aqui disponibilizados, pois esse procedimento visa garantir que qualquer desvio do comportamento habitual, tanto da aplicação quanto do banco de dados, possa ser corrigido antes que venha prejudicar a disponibilidade do serviço.

De modo geral acreditamos que a solução single sign-on em bancos de dados Oracle corrobora para uma gestão mais eficaz e eficiente da administração do acesso irrestrito aos bancos de dados, haja vista que elimina o GAP retratado quando determinado administrador de banco de dados deixava a organização e sua conta ainda permanecia ativa nos sistemas de gerenciamento de banco de dados (SGBD), o que poderia acarretar em fraudes e manipulações imensuráveis à organização.

A interoperabilidade do Oracle internet directory com os serviços de diretórios (AD e NDS) existentes é mais uma peça fundamental na escolha dessa solução, pois reforça as melhores práticas de segurança da informação em concordância com a lei Sarbanes-Oxley, de modo a mitigar riscos aos negócios e certificar às organizações a legibilidade das operações financeiras no exterior, visto que essa solução destina-se a organizações de grande porte.

Efetivamente, através de um único login e senha cada administrador de banco de dados pode ter acesso ao domínio da empresa e aos diversos bancos de dados Oracle, refletindo em redução da carga administrativa na gestão e troca periódica das senhas, o que otimiza mensuravelmente esse processo, deixando o serviço disponibilizado pelo portal de senhas mais performático.

Em face dos argumentos expendidos, mesmo tratando-se de uma ferramenta proprietária da Oracle Corporation, com custos condizentes aos melhores produtos de segurança do mercado, trata-se de uma solução direcionada às grandes organizações que zelam pelo bem maior do seu negócio, que é a informação, na qual são incluídos os dados confidenciais. Nesse sentido, por tudo que foi exposto neste estudo de caso e com todos os pontos positivos encontrados, afirmamos que, após estudo de viabilidade, que deve ser feito por cada organização, essa solução atingiu o objetivo esperado e é recomendada por trazer benefícios tangíveis ao dia a dia das organizações e atuar preventivamente, evitando a indisponibilidade do serviço de autenticação de administradores de banco de dados Oracle.

Referências

[1] ABNT. NBR ISO/IEC 27001:2006. Disponível em: <http://www.abnt.org.br/ISOIEC27001.pdf>. Acesso em: 19 mai. 2011.

[2] BRYLA, B.; LONEY, K.. *Oracle Database 11g*: manual do DBA. Porto Alegre: Bookman, 2009.

[3] CARTER, Gerald. *LDAP Administração de Sistemas*. Rio de Janeiro: Alta Books, 2009.

[4] DATE, C. J. *Introdução a sistemas de bancos de dados*. 8. ed. Rio de Janeiro: Campus, 2004.

[5] JOSUTTIS, Nicolai M. *SOA na Prática*: A arte da Modelagem de Sistemas Distribuídos. Rio de Janeiro: Alta Books, 2008.

[6] MICROSOFT. Active Directory. Disponível em: <http://www.microsoft.com.br>. Acesso em: 17 jun. 2011.

[7] ORACLE. Oracle Advanced Security Administrator's. Disponível em: <http://download-east.oracle.com/docs/cd/B10501_01/network.920/a96573/toc.htm>. Acesso em: 18 mai. 2011.

[8] ORACLE. Enterprise User Security. Disponível em: <http://download-east.oracle.com/docs/cd/B19306_01/network.102/b14269/toc.htm>. Acesso em: 16 mai. 2011.

[9] ORACLE. Identity Management. Disponível em: <http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index-082035.html>. Acesso em: 12 mai. 2011.

[10] ORACLE. Oracle Internet Directory. Disponível em: <http://download-uk.oracle.com/docs/cd/B28196_01/idmanage.1014/b15991/toc.htm>. Acesso em: 14 mai. 2011.