SENADO FEDERAL

Instituto Legislativo Brasileiro – ILB

Edmilson Faria Rodrigues

Identificação e Monitoramento dos Privilégios de Acesso a Dados no Âmbito do Senado Federal

Brasília

2019

Edmilson Faria Rodrigues

Identificação e Monitoramento dos Privilégios de Acesso a Dados no Âmbito do Senado Federal

Monografia apresentada ao Instituto Legislativo Brasileiro – ILB como pré-requisito para a obtenção de certificado de conclusão de Curso de Pós-Graduação Lato Sensu em Tecnologia da Informação Aplicada ao Poder Legislativo

Orientador: Dr. Lauro César Araujo

Brasília

2019

Rodrigues, Edmilson Faria.
Identificação e monitoramento dos privilégios de acesso a dados no âmbito do Senado Federal / Edmilson Faria Rodrigues. -- 2019.
47 p. : il. (algumas color.)

Orientador: Lauro César Araujo.

Trabalho de conclusão de curso (especialização) -- Curso de pós-graduação *lato sensu* em Tecnologia da Informação Aplicada ao Poder Legislativo – Instituto Legislativo Brasileiro, 2019.

1. Banco de dados, controle de acesso, Brasil. 2. Informação governamental, controle de acesso, Brasil. 3. Controle de acesso, metodologia, Brasil. 4. Brasil. Congresso Nacional. Senado Federal. I. Título.

CDD 005.83

Edmilson Faria Rodrigues

Identificação e Monitoramento dos Privilégios de Acesso a Dados no Âmbito do Senado Federal

Monografia apresentada ao Instituto Legislativo Brasileiro – ILB como pré-requisito para a obtenção de certificado de conclusão de Curso de Pós-Graduação Lato Sensu em Tecnologia da Informação Aplicada ao Poder Legislativo

Trabalho aprovado. Brasília, 11 de outubro de 2019:

Dr. Lauro César Araujo
Orientador

Me. Pabblo Cardelino Ghobad
Avaliador

Brasília
2019

Este trabalho é destinado ao nosso Luquinha,
que, com sua chegada, trouxe mais alegria e amor à minha vida.

Agradecimentos

Os agradecimentos principais são direcionados à minha equipe do Serviço de Suporte a Banco de Dados, que me ajudaram muito no presente trabalho, cada um contribuindo com seu enciclopédico conhecimento sobre o SGBD Oracle. Sem o apoio incondicional desses abnegados e competentes servidores públicos eu não teria concluído o presente trabalho. E se hoje eu me considero um DBA, devo também isso aos seus valiosos ensinamentos.

Agradecimentos especiais ao Lauro, meu orientador. Profissional e professor brilhante, foi uma honra ser orientado por ele, aprendi muito em vários aspectos e em especial no que se refere a utilização do Overleaf, da padronização ABNT para produção de textos científicos. Agradeço também ao mestre Pabblo por ter aceitado o convite para compor a banca de avaliação e pelo costumeiro apoio no nosso trabalho dentro da Coordenação de Infraestrutura (COINTI).

"Não vos amoldeis às estruturas deste mundo,
mas transformai-vos pela renovação da mente,
a fim de distinguir qual é a vontade de Deus:
o que é bom, o que Lhe é agradável, o que é perfeito."
(Bíblia Sagrada, Romanos 12, 2)

Resumo

A ausência de mecanismos de monitoramento e acompanhamento de privilégios de acesso a dados pessoais pode resultar em eventos graves de vazamento de dados e acesso não autorizado. Com o advento da Lei Geral de Proteção de Dados, o controlador de dados pode ser responsabilizado pela Autoridade Nacional de Dados por tais ocorrências. Este trabalho propõe mecanismos para identificação e monitoramento dos privilégios de acesso a dados no âmbito do Senado Federal;

Palavras-chave: LGPD. dados pessoais. banco de dados. acesso. monitoramento. auditoria.

Abstract

The lack of monitoring mechanisms and tracking of personal data access privileges can result in serious data leakage and unauthorized access events. With the advent of the General Data Protection Act, the data controller can be held responsible by the National Data Authority for such occurrences. This work propose mechanisms for identification and monitoring of data access privileges within the Federal Senate;

Keywords: LGPD. personal data. database. access. monitoring. audit.

Lista de ilustrações

Lista de abreviaturas e siglas

COINTI	Coordenação de Infraestrutura de Tecnologia da Informação
DAP	*Database Audit and Protection* (Sistema de Auditoria e Proteção de Banco de Dados
LGPD	Lei Geral de Proteção de Dados Pessoais
SGBD	Sistema Gerenciador de Banco de Dados

Sumário

1 Introdução

A Lei Geral de Proteção de Dados (CONGRESSO NACIONAL, 2018), de 14/08/2018, foi promulgada num contexto de crescente número de casos de vazamentos de dados de repercussão internacional, tais como o acesso não autorizado a documentos sobre a invasão do Afeganistão, a documentos da diplomacia dos Estados Unidos e a e-mails enviados pela então candidata a presidência da república dos Estados Unidos, Hillary Clynton. Tais informações foram divulgadas ao público pela organização internacional WikiLeaks e tiveram impacto inclusive no andamento da eleição presidencial estadunidense de 2016.

Outro evento com impacto na mesma eleição foi o acesso da organização *Cambrigde Analytics* (THE NEW YORK TIMES, 2018) aos dados pessoais e publicações dos usuários do Facebook nos Estados Unidos. A empresa foi acusada de utilizar os dados de geolocalização e, juntamente com a análise das publicações, identificar os eleitores indecisos em estados que tinham número de delegados decisivos para os destinos da referida eleição. Por meio desse cruzamento de informações, supostamente a Cambridge Analytics teria direcionado fortemente as verbas de publicidade de seu cliente, a coordenação de campanha do candidato Donald Trump, para eleitores indecisos em estados decisivos, e isso teria sido decisivo na referida eleição uma vez que Donald Trump fora eleito justamente por conseguir maior número de delegados provenientes de estados chaves, ainda que, no computo geral, tenha obtido menos votos de cidadãos estadunidenses.

Em outra situação, o plebiscito do Brexit, que decidiu sobre a saída do Reino Unido da União Européia, a Cambridge Analytics é acusada de ter operado de maneira semelhante. Outros exemplos de casos internacionalmente conhecidos são o vazamento de mais de 50 milhões de contas do Facebook[1] e do Tinder[2] em que milhares de fotos pessoais foram baixadas por um programador através de uma vulnerabilidade em uma *Application Programming Interface*[3] (API) do Tinder.

No Brasil também são notórios o caso de violações do sigilo da informação como a violação do painel do Senado (SENADO FEDERAL, 2001), o vazamento de dados pessoais do banco Inter[4], e recentemente o acesso não autorizado à transcrição de conversas do atual Ministro da Justiça, Sérgio Moro, e do chefe da Força Tarefa da operação Lava Jato, Deltan Dallagnol, dentro do aplicativo Telegram.

---

[1] Disponível em: <https://oglobo.globo.com/economia/tinder-pinterest-tentam-descobrir-se-vazamento-no-facebook-afetou-seus-usuarios-23120500>, acesso de 10.ago.2019.

[2] Disponível em: <https://blogs.uai.com.br/olhaso/2017/05/03/vazamento-de-milhares-de-fotos-de-do-tinder-foi-provocada-por-falha-de-seguranca>, acesso em 10.ago.2019.

[3] Biblioteca de software utilizada para comunicação entre sistemas computacionais.

[4] Disponível em <https://www.tecmundo.com.br/seguranca/129811-exclusivo-vazam-dados-400-mil-clientes-banco-inter.htm>, acesso em 10.09.2019

Com o intuito de evitar situações como essa e de sobretudo proteger a intimidade e a vida privada dos cidadãos, a Lei Geral de Proteção de dados estabelece que "o titular (dos dados) tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso", facultando ao cidadão inclusive a revogação da permissão de acesso a dados pessoais já mantidos, mesmo que coletados anteriormente a promulgação da lei. Também estabelece responsabilidades das pessoas jurídicas de direito público no que se refere à guarda e compartilhamento das informações pessoais, inclusive vedando expressamente seu compartilhamento a pessoas jurídicas de direito privado, com exceção das hipóteses previstas em lei, e delegando a Autoridade Nacional de Proteção de Dados a aplicação de sanções aos gestores públicos que derem margem a tal infração.

1.1 A LGPD e os Normativos do Senado Federal

A partir da promulgação da Lei Geral de Proteção de Proteção de Dados , as pessoas jurídicas de direito público devem revisar e reforçar suas práticas para garantia da integridade, confiabilidade e confidencialidade das informações armazenadas por meio de seus sistemas computacionais. Tais esforços devem ter como balizadores os princípios elencados na Lei Geral de Proteção de Dados em seu artigo 6º, com ênfase especial dada no presente trabalho para os incisos V a X:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> ...
>
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Nesse sentido o Senado Federal instituiu a Política Corporativa de Segurança da Informação do Senado Federal, que tem o seguinte objetivo:

> estabelecer princípios, diretrizes estratégicas, responsabilidades, competências e subsídios para a implantação do sistema de gestão de segurança da informação, a fim de viabilizar e assegurar a disponibilidade, a integridade, a autenticidade e a confidencialidade das informações recebidas, produzidas, processadas, armazenadas e transmitidas pelo Senado Federal(CONGRESSO NACIONAL, 2018, cap. IV)

De forma complementar o Ato da Comissão Diretora 6/2017, institui o Manual de Transparência e Classificação de Informações do Senado Federal (SENADO FEDERAL, 2017b), onde fica estabelecido o que é informação pessoal:

> A informação pessoal é aquela relacionada à pessoa natural identificada ou identificável. São consideradas informações pessoais as relativas à intimidade, à vida privada, à honra e à imagem, dentre outras:
>
> Nomes de cônjuge, ou companheiro, e parentes até o 4º grau, endereço de residência e número de telefone, número de CPF e de documentos de identidade, exceto quando constarem de documentos comprobatórios de despesas indenizáveis pelo Senado;
>
> Número identificador de contrato firmado pelo senador com companhia telefônica e de outros contratos de telecomunicações passíveis de reembolso de despesas pelo Senado;
>
> Prontuários, Laudos, Exames, Perícias, Relatórios médicos;
>
> No caso de reembolso de despesas médico-hospitalares: qualquer elemento identificador do prestador de serviço ou a identificação ou descrição do procedimento realizado;
>
> Discriminação de quaisquer descontos facultativos, ou decorrentes de ação judicial, incidentes sobre remuneração, proventos, subsídios, gratificações e vantagens.

Também estabelece o referido Ato os mecanimos de controle e credenciamento de acesso a documentos que contenham informações pessoais e faz referência a Comissão Permanente de Acesso a Dados, Informações e Documentos, que possui, dentre outras atribuições, a responsabilidade de assessorar a alta direção na regulamentação do acesso e da salvaguarda de dados, informações e documentos sigilosos do Senado Federal.

Para controle e fiscalização da aplicação do disposto na LGPD, esta estabelece a figura do controlador, a quem competem as decisões referentes ao tratamento de dados pessoais. Em cada órgão público exercem o papel de controlador os gestores das unidades que são responsáveis pela coleta e manipulação das informações para atingimento dos objetivos do referido órgão, uma vez que são essas unidades que determinam como a informação será usada e quem deverá ter acesso a ela, dentro da organização, para cumprir ou contribuir no cumprimento das diversas etapas dos processos administrativos públicos finalísticos.

Já as unidades de assessoramento técnico são aquelas cujo resultado do seu trabalho não representam a finalidade do órgão público, mas sim são provedoras de recursos e serviços para que outras unidades forneçam serviços de interesse público. Como exemplo desse tipo de serviço pode ser citado o fornecimento de material gráfico, de serviço de gerenciamento de recursos humanos, serviço de segurança institucional e fiscalização do patrimônio público e, com especial destaque para o presente trabalho, o serviço de processamento de dados.

No caso específico do Senado Federal, a unidade de assessoramento técnico responsável pelo fornecimento do serviço de processamento de dados, é o PRODASEN, cujas atribuições estão elencadas no Regulamento Administrativo do Senado Federal:

> À Secretaria de Tecnologia da Informação (Prodasen) compete prover, por meio de recursos próprios ou de terceiros, serviços, soluções, suporte e infraestrutura de tecnologia da informação; gerir a tecnologia da informação do Senado Federal; implementar a estratégia de tecnologia da informação; propor inovações nos processos finalísticos e de apoio do Senado, com uso de tecnologia da informação; propor padrões, normas, métodos e processos para uso da tecnologia da informação e monitorar sua aplicação; integrar iniciativas de adoção de novas soluções de tecnologia da informação por outras unidades da Casa; gerir a segurança da informação do Senado no âmbito da tecnologia da informação; gerenciar os riscos operacionais do Senado com origem em tecnologia da informação; e executar outras atividades correlatas. (SENADO FEDERAL, 2018, p. 116)

A Lei Geral de Proteção de Dados também determina perfis e suas responsabilidades:

> Art. 5º Para os fins desta Lei, considera-se:
>
> ...
>
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
>
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; Congresso Nacional (2018)

Desta forma, pela conciliação das informações dispostas Manual de Transparência e Classificação de Informações do Senado Federal (SENADO FEDERAL, 2017b) e nas competências elencadas no Regulamento Administrativo do Senado Federal (SENADO FEDERAL, 2018, p. 116), bem como pela análise das definições apresentadas pela Lei Geral de Proteção de Dados, como acima exposto, o PRODASEN não detem o papel de controlador dos dados.

O PRODASEN, bem como seu corpo técnico, encaixam-se na definição de operador, uma vez que não é responsável por definir os critérios de compartilhamento dos dados, mas sim de prover e manter operantes os recursos tecnológicos capazes de servir como ferramentas para o atingimento dos critérios de compartilhamento definidos pelo controlador de modo a garantir integridade, interoperabilidade (art. 25) e confidencialidade da informação.

O PRODASEN também é responsável por aplicar boas práticas para o tratamento de dados pessoais, podendo ser solicitado pela autoridade nacional a informar acerca dos procedimentos e políticas utilizados para o tratamento das informações pessoais.

Dessa forma, é de responsabilidade do órgão técnico prover os recursos tecnológicos para que seja realizado um mapeamento completo dos processos que envolvem o tratamento dos dados; identificar eventuais vulnerabilidades; definir os mecanismos de controle mais eficientes, fornecendo inclusive suporte a criptografia dos dados, quando aplicável; fazer o monitoramento contínuo dos incidentes e participar da criação e aplicação de uma política de segurança da informação na instituição.

1.2 Problema

Conforme apresentado na seção anterior, a ausência de ferramentas de monitoramento e controle de privilégios aumenta o risco de vazamento de dados. A situação de violação do painel do próprio (SENADO FEDERAL, 2001) demonstra que essas violações podem ocorrer por modificações de programas que acessam o banco de dados. Podem ainda ocorrer por acesso direto ao banco de dados por usuários privilegiados.

Assim, a ausência de monitoramento de privilégios é uma das falhas que aumentam as chances de vazamento ou até mesmo destruição dos dados. Outro problema comum é o registro de demandas de concessão de privilégios sem o corresponde pedido de revogação dos referidos privilégios quando estes já não são mais necessarios, o que permite que usuário que já estejam em outros departamentos ou até mesmo já não pertençam ao corpo funcional da organização continue tendo tais privilégios.

1.3 Justificativa

Com intuito de contribuir no atendimento dessa responsabilidade do órgão técnico o presente trabalho apresenta o desenvolvimento de um conjunto de rotinas capazes de fornecer às unidades finalísticas informações dos privilégios que cada usuário ou perfil tem dentro do banco de dados corporativo do Senado Federal, bem como apresentar um relatório constantemente atualizado com informações acerca dos privilégios de acesso à

registros no banco de dados que não estão sendo utilizados, a fim de que tais ferramentas possibilitem um trabalho proativo para evitar o acesso não autorizado aos dados.

O relatório intitulado Controles Críticos de Segurança para a efetiva defesa cibernétcia do Centro para Segurança na Internet é uma publicação das diretrizes de melhores práticas para segurança de computadores. A publicação foi inicialmente desenvolvida pelo Instituto SANS e é também conhecido como SANS Top 20. As diretrizes consistem em 20 ações-chave, chamadas de controles de segurança críticos, que as organizações devem tomar para bloquear ou mitigar ataques conhecidos.[5]

> 1.4.2.4. implante mecanismos de proteção dos registros de auditoria (logs) contra modificações e exclusões não autorizadas, em especial por parte de usuários administradores, bem como contra problemas operacionais, observando as recomendações do item 10.10.3 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;
>
> 1.4.2.5. implante procedimentos que possibilitem o monitoramento proativo do uso dos recursos de infraestrutura de TI que dão suporte ao [Sistema], observando as recomendações do item 10.10.2 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;
>
> 1.4.2.6. implante controle formal (motivação, aprovação e documentação), registros de auditoria (logs), monitoramento e análise crítica regular das atividades de usuários administradores, observando as recomendações do item 10.10.4 da Norma Técnica ABNT NBR ISO/IEC 27002:2005, ou implante controles compensatórios para monitorar as atividades realizadas por estes usuários; Congresso Nacional (2018)

A Consultoria Gartner (PERALLIS, 2018) recomenda que uma boa solução de proteção de banco de dados deve tratar adequadamente 9 dessas 20 diretrizes, diretamente relacionadas a banco de dados:

Esta pesquisa pretende definir mecanismos para atender a 2 dessas 9 recomendações do Instituto Gartner, a saber:

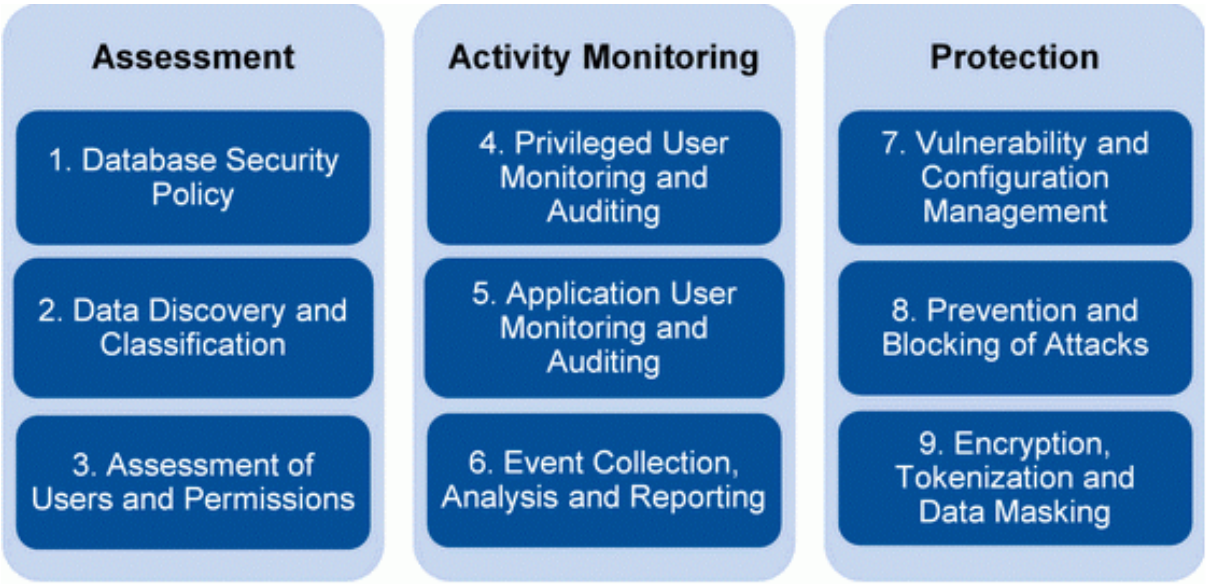
a) avaliar, monitorar e gerenciar as permissões de usuários, administradores e desenvolvedores de segurança através de sua capacidade de acessar cada SGBD. Aplicar ao menos uma política de privilégio para minimizar os direitos de acesso concedidos as pessoas físicas;

b) monitorar as atividades do usuário altamente privilegiado com alertas em tempo real e relatórios em curso para identificar alterações de configuração inadequadas de SGBDs, acesso a dados, alterações ou conceções de permissões.

Ou seja, em outras palavras, as recomendações 4 e 5 indicadas na Figura 1. Com relação as demais ações indicadas na referida figura, embora igualmente importantes, estão além do escopo desta pesquisa.

[5] Disponível em: <https://en.wikipedia.org/wiki/The_CIS_Critical_Security_Controls_for_Effective_Cyber_Defense>, acesso em 10.ago.2019.

Figura 1 – Funcionalidades críticas de uma solução de proteção de banco de dados



Fonte: (PERALLIS, 2018)

Segundo a Consultoria Gartner (2014), a identificação do grau de criticidade e confidencialidade das informações é uma tarefa desafiadora para a maioria das organizações. Desafio maior ainda é a capacidade de rastrear modificações feitas a esses dados. Muitas organizações utilizam ferramentas de gerenciamento de dados para tal fim, no entanto essas ferramentas não fornecem uma interface adequada para fins de segurança de dados. Nesse contexto, recomenda a utilização de ferramentas *Database Audit and Protection* (DAP) que permitem que o monitoramento de atividades do banco (auditoria) possa ser usado em conjunto com o gerenciamento de privilégios de usuário, para atendimento das alíneas a e b, acima indicadas como escopo desta pesquisa e que fazem parte integrante do relatório SANS Top 20 (SAANS, 2018).

Assim, feita a classificação da informação com o apoio da área finalística, é possível identificar quais privilégios existem, mas não estão sendo utilizados e, portanto, podem ser revogados, bem como identificar quais papéis (roles) estão associadas a dados sensíveis. O Infosphere Guardium[6] é a solução DAP utilizada pelo Senado Federal para segurança de dados multiplataforma, cujas características incluem descoberta de dados e classificação, monitoramento de atividade de dados, mascaramento on-line de dados (*data redaction*), automação da implementação de políticas de conformidade como as definidas na norma ISO 27002 (ABNT, 2018), avaliação de vulnerabilidade, relatórios de privilégios de usuários, um sistema de auditoria de configuração para servidores de banco de dados e criptografia de dados para as comunicações entre agentes (software instalado na instância de banco de dados para fazer a captura dos comandos) e coletores (software que recebe os comandos capturados e faz a consolidação e organização dos mesmos). Os relatórios podem ser

[6] <http://www.ibm.com/Guardium>, acesso de 10.ago.2019.

gerenciados por meio de um ciclo de atestação, submetendo os mesmos a apreciação e ateste de auditores da área finalística credenciados na ferramenta.

No Capítulo 2 é explorado em detalhe os procedimentos utilizados para extrair informações de privilégios de usuários e permitir seu acompanhamento pela área finalística em uma interface intuitiva fornecida pela nossa solução DAP, bem como o cruzamento dessas informações com o registro de auditoria dos privilégios efetivamente em uso pelo usuário.

1.4 Objetivo Geral

Criar uma metodologia e propor mecanismos para identificação e monitoramento dos privilégios de acesso a dados no âmbito do Senado Federal.

1.5 Objetivos Específicos

1. Definir forma de verificação dos privilégios pelo controlador, sem necessidade de acesso privilegiado às ferramentas de administração da instância de banco de dados;

2. Construir método de monitoramento de utilização de privilégios de acesso por controladores de dados;

3. Indicar orientações para tratamento de fluxos de quarentena e revogação de privilégios concedidos e não utilizados.

1.6 Metodologia

Esta pesquisa é classificada como explicativa com propostas de implementação de protótipos. São construídos modelos e prototipagem de soluções

1.7 Referencial Teórico

Os sistemas computacionais atualmente estão presentes em todas as áreas de negócio e o núcleo do seu funcionamento consiste em receber informações, fazer algum tipo de processamento ou transformação com essa informação e devolver um resultado ao usuário. Nesse sentido, todo sistema computacional precisa do suporte de um sistema específico para armazenar e garantir a integridade e consistência desses dados. Daí a necessidade dos Sistemas Gerenciadores de Bancos de Dados.

De acordo com (BRYLA BOB; LONEY, 2009) um banco de dados:

> é uma coleção de dados em um ou mais arquivos no discso de um servidor que coleta e mantém informações relacionadas. O banco de dados consiste em várias estruturas físicas e lógicas, sendo a tabela a estrutura lógica mais importante. Uma tabela é composta de linhas e colunas que contêm dados relacionados", ou seja, quando atemos uma coleção de dados em um repositório de informação relacionadas, estruturada logicamente em tabelas, podemos dizer que temos um baco de dados.

Já de acordo com (SILBERSCHATZ ABRAHAM.; KORTH, 2001) um Sistema gerenciador de banco de dados é "constituído por um conjunto de dados associados a um conjunto de programas para acesso a esses dados. O conjunto de dados, comumente chamado banco de dados, contém informações particulares a uma empresa"

Uma instância de banco de dados corresponde ao conjunto de programas que são executados em um servidor (computador de grande porte) e é responsável pela recuperação e atualização dos dados no banco de dados localizados em dispositivos de armazenamento.

Quando um acesso é solicitado a uma determinada tabela, o SGBD verifica se o usuário que está solicitando o acesso tem os privilégios necessários para tal. O acesso pode ser, dentre outros:

- *Select*: faz a leitura de uma linha (registro) em uma tabela
- *Delete*: remove um registro de uma tabela
- *Update*: faz uma atualização em um registro existente
- *Insert*: faz uma inserção de um registro

No SGBD Oracle cada usuário é também um *container* de seus objetos (como tabelas, por exemplo), ou seja, um objeto necessariamente pertence a um usuário ou esquema, que são termos equivalentes dentro do SGBD Oracle.

O usuário sempre pode fazer acesso a objetos pertencentes ao seu esquema, mas, para fazer acesso a objetos de outros esquemas eles precisa possuir os privilégios. Um privilégio pode ser, por exemplo, de realizar um *Select*, *Update*, *Delete* ou *Insert* em uma tabela de outro esquema.

Os privilégios podem ser concedidos e, naturalmente, podem ser igualmente revogados. Para melhorar a atribuição ou revogação de privilégios eles podem ser agrupados em *roles*, de modo que a atribuição de uma role a um usuário concede a este todos os privilégios que estão agrupados naquela *role*.

Esse conjunto de usuários e seus respectivos privilégios estão armazenados no próprio SGBD em tabelas que são gerenciadas somente pelo próprio SGBD, e são comumente chamadas de tabelas do dicionário de dados.

Diante da necessidade de monitoramento desses privilégios conforme exposto na seção 1.3 muitas organizações utilizam ferramentas dos próprios SGBDs para tal fim. No entanto essas ferramentas não fornecem uma interface adequada para fins de segurança de dados. As ferramentas de auditoria e proteção de banco de dados (DAP- do inglês *Database Audit and Protection*) fornecem um amplo espectro de recursos de segurança para sistemas de gerenciamento de banco de dados relacional (SGBDs). Além dos recursos básicos de monitoramento, em resposta aos requisitos adicionais dos clientes, os fornecedores desse tipo de solução adicionaram recursos como descoberta e classificação de dados, gerenciamento de ameaças e vulnerabilidades, análise em nível de aplicação, prevenção de intrusões e bloqueio de atividades e análise de gerenciamento de identidade e acesso.

As ferramentas DAP possuem recursos de descoberta de informações críticas, seja por meio da aplicação de padrões conhecidos contra os dados existentes no banco de dados ou pela pesquisa dos tipos e nomes de colunas e seus relacionamentos. Uma vez que os dados estejam classificados, as ferramentas DAP podem gerar alertas de segurança com o fim de identificar rapidamente um processo de negócio ou de TI que está acessando ou armazenando informações confidenciais ou críticas indevidamente.

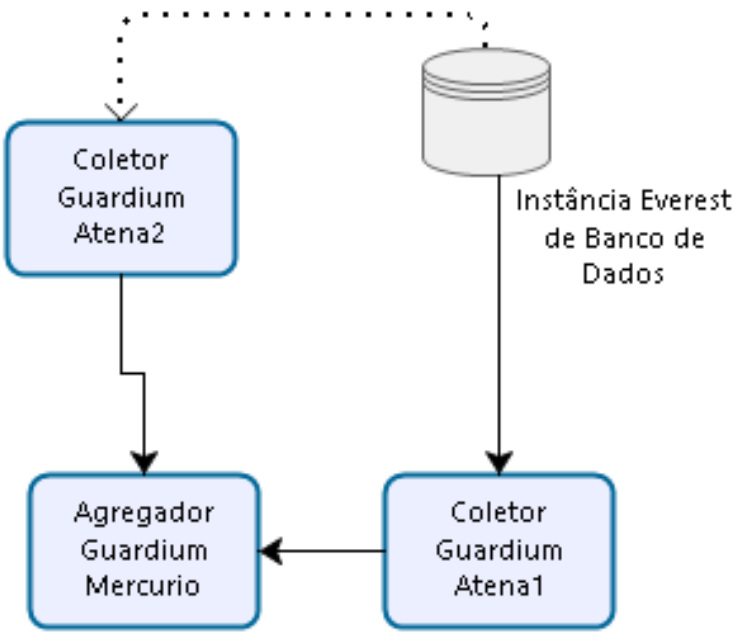
As ferramentas DAP permitem ainda que o monitoramento de atividades do banco (auditoria) possa ser usado em conjunto com o gerenciamento de privilégios de usuário. Assim, feita a classificação da informação mencionada nos parágrafos anteriores, é possível identificar quais privilégios existem, mas não estão sendo utilizados e, portanto, podem ser revogados, bem como identificar quais papéis (*roles*) estão associadas a dados sensíveis. Embora os Sistemas Gerenciadores de Bancos de Dados (SGBDs) possuam mecanismos para identificação de privilégios de usuários e de papéis de usuários, não é possível obter de maneira rápida e direta toda a cadeia de privilégios relacionando-a ao histórico de utilização dos dados

2 Desenvolvimento

Conforme descrito na seção 1.3, a primeira recomendação do SANS Top 20, objeto do presente trabalho, é "avaliar, monitorar e gerenciar as permissões de usuários, administradores e desenvolvedores de segurança através de sua capacidade de acessar cada SGBD". Para tal implantaremos na solução DAP InphoSphere Guardium o relatório de privilégios (do inglês, *Entitlements Report*), conforme descrito na seção 2.2.

De posse dessas informações, é feito o cruzamento com os logs de auditoria, utilizando rotinas de exportação, transformação e carga dos registros de logs para a instância Oracle, uma vez que a ferramenta DAP não possui recursos nativos para implementar tal funcionalidade. Esse procedimento é descrito na seção 2.1.

Figura 2 – Instância de Banco de Dados e Coletores Guardium



Fonte: Os autores

A Figura 2 mostra a arquitetura na qual foi feito o desenvolvimento dos protótipos de solução apresentados na presente pesquisa: [1] um agente da solução DAP Guardium captura, a nível de sistema operacional, as requisições que chegam na instância de Banco de Dados Everest e os envia para o Coletor Guardium Atena1, em caso de falha desse coletor, o coletor Guardium Atena2 assume esse papel. Já o Agregador Guardium Mercurio

[1] Nomes das instâncias de SGBD e appliances Guardium foram trocados para fins de sigilo.

é reponsável pela consolidação desses dados, gerenciamento e monitoramento dos demais componentes e comunicação com os sistemas de armazenamento de longo período para envio e recuperação de trilhas de auditoria de períodos superiores a 60 dias.

2.1 Relatório de privilégios para a área finalística

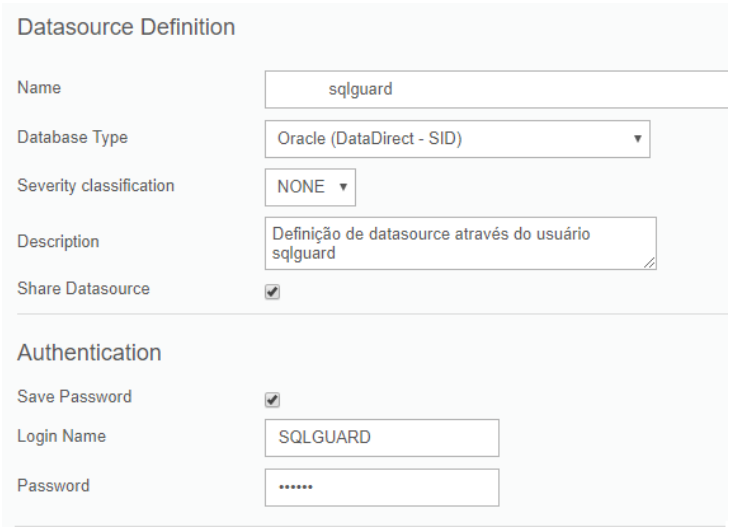
O recurso de *Entitlements Report* (Relatórios de Titularidade) ou Relatório de Privilégios do Guardium foi configurado de modo a possibilitar que o controlador, segundo o conceito definido em Congresso Nacional (2018), seja capaz de verificar os perfis existentes e seus privilégios no banco de dados.

O processo de revisão de titularidade, executado por controladores ou ainda por auditores internos ou externos, consiste em validar e assegurar que os usuários tem somente os privilégios necessários para fazer as suas atividades.

Em todo SGBD, além de autenticar os usuários, é recomendável que o acesso ao SBGD seja baseado em *roles*. Além disso, conforme definido em Perallis (2018), é necessária uma revisão periódica dos privilégios de acesso.

Entretanto, conhecer toda a cadeia de milhares de privilégios concedidos, muitos deles concedidos de maneira recursiva, por meio de *roles* atribuídas a outra *roles*, não é tarefa simples para o usuário com perfil controlador, uma vez que esse tem o conhecimento da área finalística e não propriamente dos mecanimos de funcionamento do SGBD e da obtenção de relatórios de privilégios por meio de acesso ao dicionário de dados do SGBD.

Figura 3 – Definição de *Data Source* para popular as *custom tables*



Fonte: Os autores

Assim, nesta seção, a solução DAP Guardium é utilizada como interface web para fácil extração dos privilégios de dados. A Figura 3 mostra a definição de um *Data Source*

que consiste na configuração de uma conexão ao SGBD por meio do usuario `sqlguard`, criado especificamente para esse fim, e a quem foi atribuído a *role* GDENT que possui os privilégios necessários para consultar o dicionário de dados do SGBD Oracle e assim popular as *custom tables* que serão utilizadas para apresentar relatórios web na interface da ferramenta DAP.

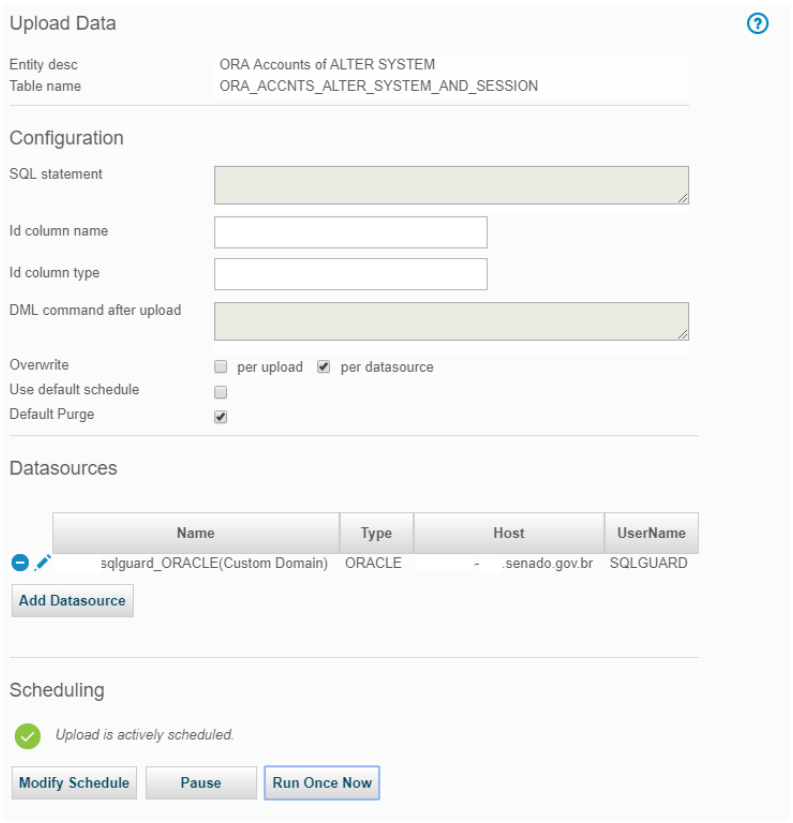
As *Custom Tables* são tabelas que existem somente dentro do escopo de uma conexão de dados definida dentro do *Guardium*, ou seja, o *Guardium*, por meio de uma definição de uma fonte de dados (*Data Source*), obtem informações existentes nessa fonte, que, no presente caso, corresponde aos usuários e seus privilégios armazenados nas tabelas dos dicionários de dados do SGBD Oracle

O código SQL a seguir apresenta os privilégios da role GDENT criada para esse fim:

```
1  CREATE ROLE GDENT NOT IDENTIFIED;
2
3  -- Object privileges granted to GDENT
4  GRANT SELECT ON DBA_COL_PRIVS TO GDENT;
5  GRANT SELECT ON DBA_DEPENDENCIES TO GDENT;
6  GRANT SELECT ON DBA_OBJECTS TO GDENT;
7  GRANT SELECT ON DBA_ROLE_PRIVS TO GDENT;
8  GRANT SELECT ON DBA_ROLES TO GDENT;
9  GRANT SELECT ON DBA_SYS_PRIVS TO GDENT;
10 GRANT SELECT ON DBA_TAB_PRIVS TO GDENT;
11 GRANT SELECT ON DBA_USERS TO GDENT;
12 GRANT SELECT ON OBJ$ TO GDENT;
13 GRANT SELECT ON OBJAUTH$ TO GDENT;
14 GRANT SELECT ON TABLE_PRIVILEGE_MAP TO GDENT;
15 GRANT SELECT ON USER$ TO GDENT;
16 GRANT SELECT ON V_$PWFILE_USERS TO GDENT;
17 GRANT SELECT ON SQLPLUS_PRODUCT_PROFILE TO GDENT;
18
19 -- Roles atribuidas a GDENT
20 GRANT CONNECT TO GDENT;
21
22 -- Usuarios com a role  GDENT
23 GRANT GDENT TO SQLGUARD;
24 GRANT GDENT TO SYS WITH ADMIN OPTION;
```

A Figura 4 mostra as definições para a carga da *custom table ORA Accounts of Alter System*, que utiliza a conexão SqlGuard.

Figura 4 – Carga das *custom tables*



Fonte: Os autores

A Figura 5[2] mostra um dos relatórios para acompanhamento dos privilégios de acesso em bancos de dados pelo controlador ou auditor. Neste relatório a coluna *Grantee* indica o usuário que recebeu o privilégio, a coluna *Privilege* indica o privilégio recebido, a coluna *Table Name* indica o nome da tabela no qual o usuário possui o referido privilégio, a coluna *Owner* indica o esquema que contém essa tabela, a coluna *Grantor* indica o usuário que concedeu aquele privilégio e a coluna *Grantable* indica se o usuário que recebeu o privilégio pode concedê-lo a um terceiro.

2.2 Monitoramento de privilégios utilizados

Para fazer o monitoramento dos acessos aos registros no banco de dados Everest foi definida uma consulta no coletor Athena1 do Guardium, conforme Figura 6.

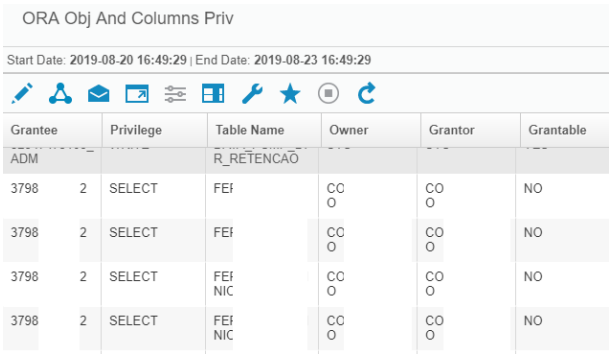
Essa consulta foi definida para rodar como um processo de auditoria com periodicidade mensal, conforme Figura 7.

A execução desse processo de auditoria resultou no relatório da Figura 8.

Esses dados são exportados no formato `csv` pelo Guardium, o qual será utilizado

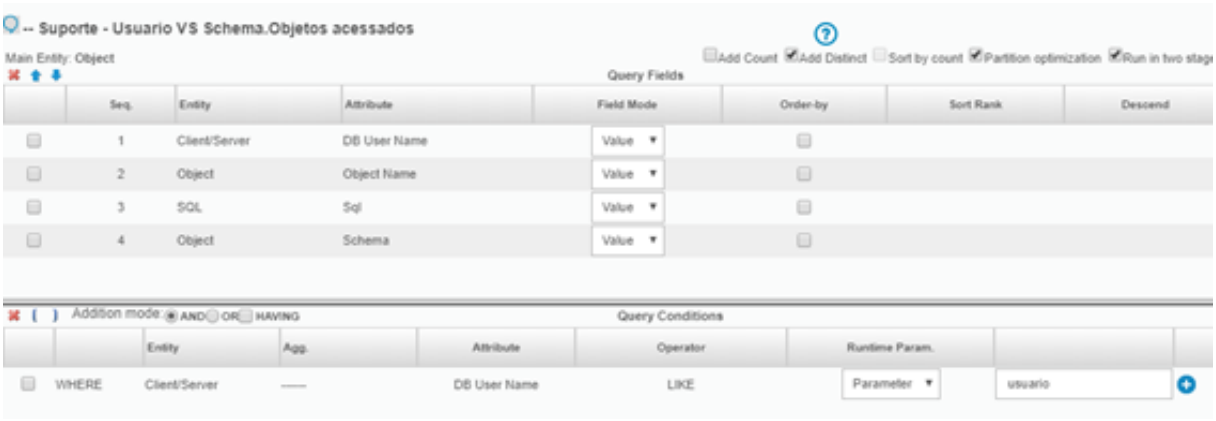
[2] A figura foi modificada para fins de sigilo referente ao ambiente computacional do Senado Federal.

Figura 5 – Relatório de privilégios



Fonte: Os autores

Figura 6 – Consulta para recuperação do log de acesso ao banco de dados



Fonte: Os autores

pelo SQL Loader para importação na área de *staging*[3], da instância Everest.

O SQL Loader é um aplicativo de importação que acompanha o SGBD Oracle, tendo como diferencial a flexibilidade na configuração, pois utiliza uma linguagem de scripts, definida no seu arquivo de controle, para importar os dados. O conteúdo do arquivo de controle, para a carga no banco de Dados dos acessos coletados pelo Coletor Atena1, está descrito no Apêndice A:

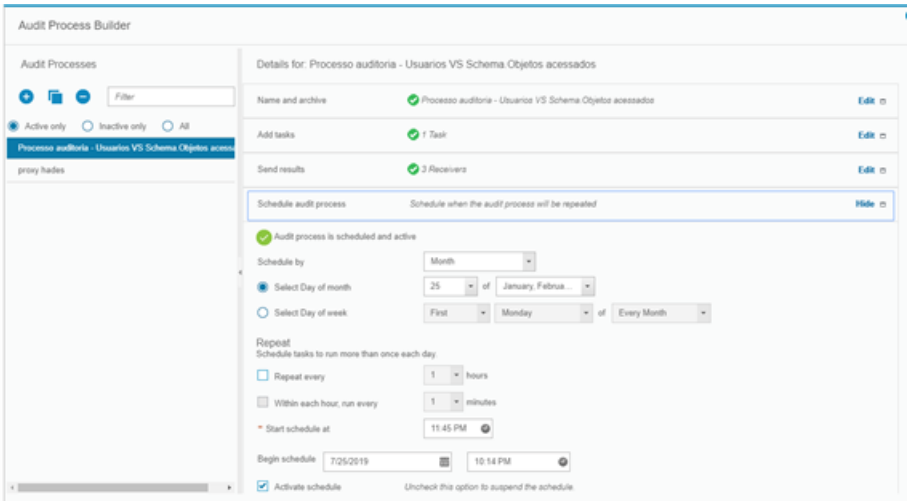
A Figura 9 mostra o resultado dessa carga de dados. Os dados importados do arquivo CSV incluem um série de caracteres especiais. Assim, será necessário, nas rotinas de transformação que seja feita uma limpeza desses dados.

A Figura 10 apresenta a definição de um modelo de dados para as tabelas onde ficarão armazenados os registros de acesso de cada usuário a cada um dos objetos do banco Everest.

Para mapeamento dos usuário e seus privilégios no banco de dados, foi preparada

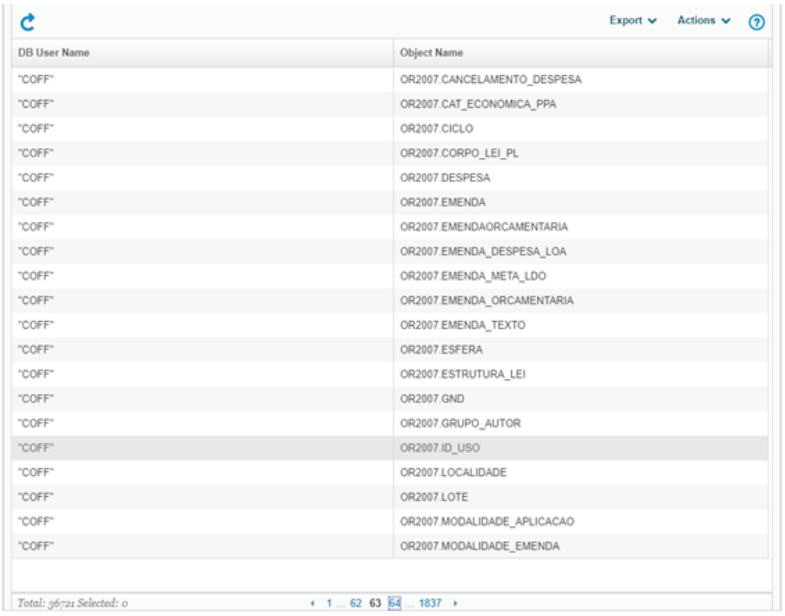
[3] Staging é uma área de intermediária de armazenamento utilizada durante o processo de extração, transformação e carga em Bancos de Dados

Figura 7 – Tela para construção do processo de auditoria



Fonte: Os autores

Figura 8 – Saída web do relatório Guardium



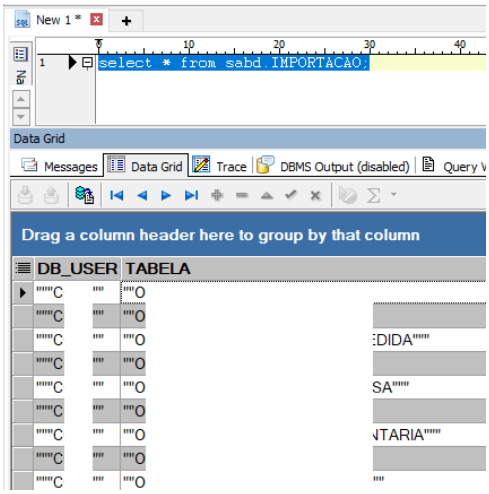
Fonte: Os autores

uma rotina recursiva para identificar de maneira hierárquica os privilégios de acesso dos usuários (seja acesso direto ou acesso por meio de cadeia de *roles*). O código SQL dessa rotina recursiva é apresentado no Apêndice B.

A seguir é feita a limpeza e transformação dos dados importados para a tabela de *staging*. O código SQL tal rotina é apresentado no Apêndice C.

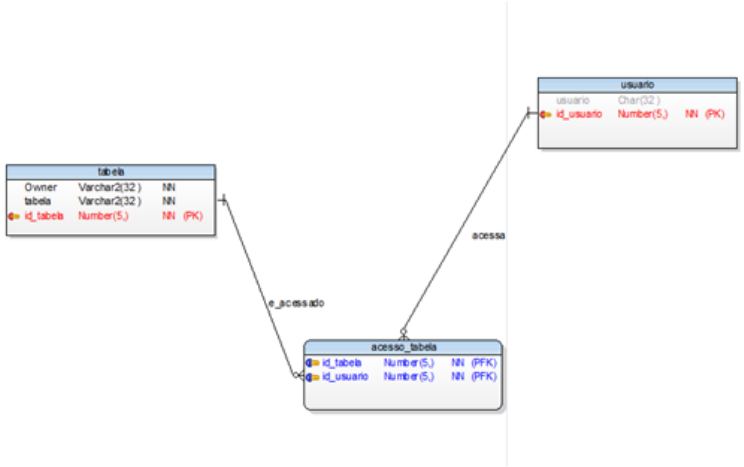
O cruzamento das informações resultantes das duas últimas listagens nos dá a informação de quais privilégios foram atribuídos mas não foram utilizados no período de captura de logs de acesso no Guardium. Estando tanto a consolidação dos privilégios

Figura 9 – Dados carregados a partir do relatório do Guardium para a tabela de staging



Fonte: Os autores

Figura 10 – Modelo de dados para registros dos acessos às tabelas



Fonte: Os autores

quanto os logs de acesso carregados no banco de dados, a verificação de privilégios não utilizados ocorre por meio de uma subconsulta utilizando uma cláusula `EXISTS`. Entretanto, a execução de tal consulta estava durando mais de 20 minutos sem que houvesse retorno da informação. Assim foi criada uma *materialized view* para promover uma denormalização dos dados e acelerar o processo de verificação dos privilégios:

```
1 CREATE MATERIALIZED VIEW ACESSOS_CONSOLIDADOS
2 (
3     USUARIO,
4     TABELA,
5     OWNER
6 )
```

```
7  AS
8     SELECT U.USUARIO, t.TABELA, t.OWNER
9       FROM usuario u, tabela t, acesso_tabela at
10     WHERE u.ID_USUARIO = at.ID_USUARIO
11     AND at.ID_TABELA = t.ID_TABELA;
```

A partir da view materializada, pode-se fazer a subconsulta correlacionada para encontrar os privilégios não utilizados no último mês na instância Everest.

```
1  SELECT *
2    FROM tab_user_privs tup
3   WHERE
4   NOT EXISTS
5                (SELECT 1
6                   FROM acessos_consolidados ac
7                  WHERE     AC.USUARIO= TUP.GRANTEE
8                        AND AC.OWNER= UPPER(TUP.OWN)
9                        AND AC.TABELA=TUP.TAB);
```

2.3 Fluxos de Quarentena de Privilégios de Acesso

No âmbito do presente trabalho verificou-se, com as ferramentas desenvolvidas na seção 2.2, que de um total de 84.319 privilégios concedidos direta ou indiretamente, cerca de 82.298 não aparecem nos registros de auditoria, o que sugere alguns encaminhamentos para a definição de um fluxo de auditoria de privilégios em bancos de dados:

a) o período de captura dos logs de acesso deve ocorrer por período superior a um mês, antes de se encaminhar um privilégio para a situação de quarentena;

b) deve ser feita uma análise sobre a quantidade de privilégios necessários para que procedimentos, *triggers*, funções, *materialized views* possam executar satisfatoriamente. Os passos para execução de tais procedimentos ocorre internamente ao mesmo e portanto invisível a solução DAP que captura os comandos que chegam ao listener do SGBD, por meio de monitoramento a nível de sistema operacional;

c) a própria solução DAP pode ser usada para monitorar exceções resultantes de falhas decorrentes da eliminação de privilégios de acesso que expiraram seu período de quarentena.

A escolha do período de monitoramento dos acessos e do período de quarentena deve ser feita de maneira empírica. Assim temos algumas situações a considerar nesses testes:

a) períodos muito pequenos de monitoramento: tendem a capturar poucos registros de acesso e assim pode indicar num falso positivo, ou seja, um privilégio de acesso que fora concedido mas que não foi utilizado durante o período de monitoramento, mas que será necessário no futuro;

b) períodos muito grandes de monitoramento: além de provocar um atraso na avaliação dos resultados do monitoramento, ainda podem resultar numa carga de trabalho excessiva para manipulação pelas rotinas de ETL apresentadas no presente trabalho.

Durante o período de quarentena o privilégio não acessado estará revogado, mas as tentativas de utilização desses privilégios serão objeto de monitoramento. Por outro lado, o registro de privilégios que foram removidos, de modo a permitir que sejam reaplicados, não demanda esforço computacional considerável, trata-se apenas de uma tabela no banco de dados a armazenar alguns milhares de registros. Ademais, o monitoramento de exceções por tentativas de acesso não sucedidas é recurso disponível na solução DAP Guardium, de modo que nem o registro nem o monitoramento de privilégio em quarentena demanda esforço computacional ou humano considerável.

De tal forma que se prepõe, como ponto de partida, um monitoramento cíclico onde as rotinas demonstradas na seção 2.2 são executadas todo final de semana, considerando a janela de análise correspondente aos últimos 60 dias. Já para a definição do período de quarentena, pelos motivos expostos acima, propõe-se uma abordagem mais conservadora, onde os privilégios revogados durante todo o último ano sejam objeto de registro e monitoramento.

3 Conclusão

O presente trabalho foi uma oportunidade de implementar uma demanda já existente no Serviço de Suporte a Banco de Dados do Senado Federal, e o desenvolvimento da solução para controle de privilégios não utilizados foi aplicado a uma instância de produção do SGBD Oracle, e os resultados apresentados na seção anterior motivaram um aprofundamento do debate acerca do controle de concessão e monitoramento de privilégios, inclusive com a intenção de ampliar o foro desse debate para incluir outras unidades do Prodasen bem como a área finalística, responsável por exercer o papel de controlador, segundo a Lei Geral de Proteção de Dados Pessoais (CONGRESSO NACIONAL, 2018).

A seção 2.1 demonstrou o atingimento do objetivo específico 1 por meio da construção e apresentação de relatórios customizáveis para identificação de privilégios de acesso a dados no SGBD. A geração e consulta de tal relatório não demanda conhecimento específico do dicionário de dados do SGBD Oracle e tampouco requer privilégios de acesso direto ao SGBD.

A seção 2.2 demonstrou o atingimento do objetivo específico 2 por meio da bem sucedida captura dos logs de auditoria, carga dos mesmos para o SGBD, limpeza e transformação dos dados e cruzamento destes com os registros de privilégios direta e indiretamente concedidos.

A seção 2.3 demonstrou o atingimento do objetivo específico 3 por meio da proposição de um fluxo de Quarentena que considerou os resultados obtidos e a grande quantidade de privilégios concedidos que não apareceram nos logs de auditoria. Tal situação apresenta uma oportunidade dos seguintes trabalhos futuros:

a) Identificar os privilégios necessários para a execução de *procedures* ou *functions* no banco de dados. Para que uma *procedure* possa executar, seu *container* precisa de privilégio direto de acesso aos objetos aos quais essa *procedure* faz referência;

b) Avaliar alternativas de ferramentas de código aberto para atingimento dos objetivos aqui propostos, bem como da recém lançada funcionalidade de *Entitlements Optimization* da própria solução DAP *InfoSphere Guardium*;

c) Definição de um normativo que venha a complementar a Política de Segurança da Informação do Senado Federal (SENADO FEDERAL, 2017a), especificamente no que tange à auditoria e monitoramento de privilégios de acesso a dados pessoais.

Em especial no que se refere à alinea C do parágrafo anterior é importante obser-

var que a necessidade de conciliação entre as iniciativas de classificação da informação, existentes atualmente no Senado Federal conforme determina o artigo Sétimo da Política de Segurança da Informação do Senado Federal com a identificação dos objetos de bancos de dados que armazenam essas informações.

Assim, o perfil de auditor, que terá a responsabilidade de auditar os relatórios gerados conforme detalhado na seção 2.1 deverá incluir competências que permita, com o apoio da área de tecnologia, identificar os objetos sensíveis em banco de dados de modo a pemitir o seus monitoramento.

Não fez parte do escopo do presente trabalho apresentar uma metologia para identificação de objetos sensíveis, mas sim demonstrar que, uma vez feita essa identificação, as ferramentas aqui apresentadas são necessárias e suficientes para identificar os perfis que tem privilégio de acesso a esses objetos a utilização desses perfis ao longo do tempo, de modo a identificar perfis não utilizados e que possam ser revogados.

Referências

ABNT. *NBR ISO 27002- Código de Prática para a Gestão da Segurança da Informação*. [S.l.], 2018. Disponível em: <http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf>. Acesso em: 21/08/2019. Citado na página 27.

BRYLA BOB; LONEY, K. *Oracle database 11g Manual do DBA: Administre um banco de dados corporativo Oracle escalável e seguro*. 1. ed. [S.l.]: Bookman, 2009. Acesso em: 10 outubro 2019. Citado na página 28.

CONGRESSO NACIONAL. *Lei Geral de Proteção de Dados Pessoais*. 2018. Online. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 10/08/2019. Citado 6 vezes nas páginas 21, 23, 24, 26, 32 e 41.

PERALLIS. *O que a Gartner pensa sobre Segurança de Banco de Dados*. 2018. Online. Disponível em: <https://www.perallis.com/news/o-que-a-gartner-pensa-sobre-seguranca-de-banco-de-dados>. Acesso em: 10/08/2019. Citado 3 vezes nas páginas 26, 27 e 32.

SAANS. *The CIS Critical Security Controls for Effective Cyber Defense*. [S.l.], 2018. Disponível em: <https://www.sans.org/critical-security-controls>. Acesso em: 10/08/2019. Citado na página 27.

SENADO FEDERAL. *Técnicos contam como foi a violação do painel*. [S.l.], 2001. Disponível em: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/498268/2001-04-25.pdf?sequence=1>. Acesso em: 21/08/2019. Citado 2 vezes nas páginas 21 e 25.

SENADO FEDERAL. *ATO DA COMISSÃO DIRETORA Nº 9, DE 2017- Institui a Política Corporativa de Segurança da Informação do Senado Federal - PCSI*. [S.l.], 2017. Disponível em: <https://adm.senado.gov.br/normas/ui/pub/normaConsultada?idNorma=13901154>. Acesso em: 21/08/2019. Citado na página 41.

SENADO FEDERAL. *Manual de Transparência e Classificação de Informações do Senado Federal*. [S.l.], 2017. Disponível em: <https://adm.senado.leg.br/normas/ui/pub/normaConsultada?idNorma=13875200>. Acesso em: 08/10/2019. Citado 2 vezes nas páginas 23 e 24.

SENADO FEDERAL. *Regulamento Administrativo do Senado Federal*. [S.l.], 2018. Disponível em: <https://intranet.senado.leg.br/informacao-e-documentacao/normas-do-senado-federal/regulamento-administrativo>. Acesso em: 08/10/2019. Citado na página 24.

SILBERSCHATZ ABRAHAM.; KORTH, H. F. S. S. *Sistema de Banco de Dados*. 3. ed. [S.l.]: Pearson, 2001. Acesso em: 10 outubro 2019. Citado na página 29.

THE NEW YORK TIMES. *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*. [S.l.], 2018. Disponível em: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>. Acesso em: 21/08/2019. Citado na página 21.

Anexos

ANEXO A – Arquivo de Controle do SQL Loader

```
1  LOAD DATA
2  INFILE 'C:\Users\edmilsonfr\Senado\TCC\fonte.dat'
3  BADFILE 'C:\Users\edmilsonfr\Senado\TCC\fonte.bad'
4  DISCARDFILE 'C:\Users\edmilsonfr\Senado\TCC\fonte.dsc'
5
6  INTO TABLE "SABD"."importacao"
7  INSERT
8  REENABLE DISABLED_CONSTRAINTS
9  EXCEPTIONS "SABD"."erros_importacao"
10 FIELDS TERMINATED BY ','
11 ENCLOSED BY '"' AND '"'
12 ("db_user" VARCHAR2,
13 "tabela" VARCHAR2)
```

ANEXO B – Identificação hierárquica dos privilégios de acesso dos usuários

```
1  DECLARE
2     v_table      DBA_TABLES.TABLE_NAME%TYPE;
3     v_owner      DBA_TABLES.OWNER%TYPE;
4
5     CURSOR c_tabelas
6     IS
7        SELECT table_name tabela, owner
8          FROM dba_tables
9         WHERE      owner NOT IN ('SYS',
10                                 'SYSTEM',
11                                 'WMSYS',
12                                 'SYSMAN',
13                                 'MDSYS',
14                                 'ORDSYS',
15                                 'XDB',
16                                 'WKSYS',
17                                 'EXFSYS',
18                                 'OLAPSYS',
19                                 'DBSNMP',
20                                 'DMSYS',
21                                 'CTXSYS',
22                                 'WK_TEST',
23                                 'ORDPLUGINS',
24                                 'OUTLN');
25
26    CURSOR c_privs
27    IS
28           SELECT p1,
29                  p2,
30                  obj,
31                  own,
32                  typ,
33                  CONNECT_BY_ISLEAF FOLHA
```

```
34              FROM ( /* Objetos */
35                     SELECT NULL p1,
36                            NULL p2,
37                            object_name obj,
38                            owner own,
39                            object_type typ
40                       FROM dba_objects
41                      WHERE     object_type = 'TABLE'
42                            AND object_name = v_table
43                            AND owner = v_owner
44           /*Relacoes entre objetos e roles*/
45                     UNION
46                     SELECT table_name p1,
47                            owner p2,
48                            grantee,
49                            grantee,
50                            privilege
51                       FROM dba_tab_privs
52                      WHERE privilege = 'SELECT'
53           /* Relacoes entre roles */
54                     UNION
55                     SELECT granted_role p1,
56                            granted_role p2,
57                            grantee,
58                            grantee,
59                            NULL
60                       FROM dba_role_privs
61                                          )
62
63          START WITH p1 IS NULL AND p2 IS NULL
64          CONNECT BY p1 = PRIOR obj AND p2 = PRIOR own;
65  BEGIN
66     FOR r_tabela IN c_tabelas
67     LOOP
68        v_table := r_tabela.tabela;
69        v_owner := r_tabela.owner;
70
71        FOR r_privs IN c_privs
72        LOOP
```

```
73          IF r_privs.FOLHA = 1
74          THEN
75             INSERT INTO SABD.tab_user_privs (own,
76                                              tab,
77                                              priv,
78                                              grantee)
79                  VALUES (v_owner,
80                          v_table,
81                          'SELECT',
82                          r_privs.own);
83
84             END IF;
85       END LOOP;
86    END LOOP;
87 END;
```

ANEXO C – Rotina para limpeza e carga dos registros de acesso

```
1  CREATE OR REPLACE PROCEDURE SABD.CARGA_ACESSO
2  AS
3     v_tabela        DBA_TABLES.TABLE_NAME%TYPE;
4     v_user          DBA_TABLES.OWNER%TYPE;
5     v_registro      VARCHAR (200);
6     v_owner         DBA_TABLES.OWNER%TYPE;
7     v_id_tabela     SABD.TABELA.ID_TABELA%TYPE;
8     v_id_usuario    SABD.USUARIO.ID_USUARIO%TYPE;
9     contador        NUMBER (8);
10    sql_qry         VARCHAR2 (150);
11 -- Declara o cursor com os dados obtidos a partir da
12 -- tabela de staging
13    CURSOR c_importacao
14    IS
15       SELECT REPLACE (REPLACE (db_user, '"', ''), '␣', '') db_user,
16              SUBSTR (REPLACE (tabela, '"', ''),
17                       INSTR (REPLACE (tabela, '"', ''),
18                              '.',
19                              1,
20                              1)
21                       + 1)
22                 tabela,
23              SUBSTR (REPLACE (tabela, '"', ''),
24                       1,
25                       INSTR (REPLACE (tabela, '"', ''),
26                              '.',
27                              1,
28                              1)
29                       - 1)
30                 owner
31         FROM sabd.importacao
32        WHERE     REPLACE (REPLACE (db_user, '"', ''), '␣', '')
33        IS NOT NULL
```

```
34              AND LENGTH (db_user) > 3
35              AND db_user NOT LIKE '%␣%'
36              AND INSTR (TABELA, '.') > 0;
37 BEGIN
38    contador := 0;
39
40    FOR r_importacao IN c_importacao
41    LOOP
42       v_user := r_importacao.db_user;
43       v_owner := r_importacao.owner;
44       v_tabela := r_importacao.tabela;
45
46       BEGIN
47       --Pra cada registro na tabela de staging recupere o nome
48       -- do usuario do log de acesso e verifica
49       -- se ele ja esta no modelo
50          v_id_usuario := NULL;
51          sql_qry :=
52                '␣SELECT␣ID_USUARIO␣FROM␣SABD.USUARIO␣WHERE␣usuario='''
53             || v_user
54             || '''';
55
56          EXECUTE IMMEDIATE sql_qry INTO v_id_usuario;
57       EXCEPTION
58       -- Se nao esta, insere no modelo de log de acesso,
59       -- dentro da tabela usuario
60          WHEN NO_DATA_FOUND
61          THEN
62             SELECT sabd.seq_id_usuario.NEXTVAL INTO v_id_usuario
63                 FROM DUAL;
64
65             INSERT INTO SABD.USUARIO (ID_USUARIO, USUARIO)
66                  VALUES (v_id_usuario, v_user);
67
68             COMMIT;
69          WHEN OTHERS
70          THEN
71             DBMS_OUTPUT.PUT_LINE ('Codigo␣Oracle:␣' || SQLCODE);
72             DBMS_OUTPUT.PUT_LINE ('Mensagem␣Oracle:␣' || SQLERRM);
```

```
73      END;
74
75      BEGIN
76      --Pra cada registro na tabela de staging recupere o nome
77      -- da tabela acessada no log de acesso e verifica se ela
78      -- ja esta no modelo
79         SELECT SABD.TABELA.ID_TABELA
80           INTO v_id_tabela
81           FROM SABD.TABELA
82          WHERE tabela = v_tabela AND owner = v_owner;
83      EXCEPTION
84         WHEN NO_DATA_FOUND
85      -- Se nao esta, insere no modelo de log de acesso,
86      -- dentro da tabela tabela
87         THEN
88            SELECT sabd.seq_id_tabela.NEXTVAL INTO v_id_tabela
89                FROM DUAL;
90
91            INSERT INTO SABD.TABELA (ID_TABELA, OWNER, TABELA)
92                 VALUES (v_id_tabela, v_owner, v_tabela);
93         WHEN OTHERS
94         THEN
95            DBMS_OUTPUT.PUT_LINE ('Codigo␣Oracle:␣' || SQLCODE);
96            DBMS_OUTPUT.PUT_LINE ('Mensagem␣Oracle:␣' || SQLERRM);
97      END;
98
99      --Insere o relacionamento entre tabela e usuario, indicando
100     -- a ocorrencia de acesso do usuario a tabela
101     BEGIN
102        INSERT INTO SABD.ACESSO_TABELA (ID_TABELA, ID_USUARIO)
103             VALUES (v_id_tabela, v_id_usuario);
104     EXCEPTION
105        WHEN OTHERS
106        THEN
107           DBMS_OUTPUT.PUT_LINE ('Codigo␣Oracle:␣' || SQLCODE);
108           DBMS_OUTPUT.PUT_LINE ('Mensagem␣Oracle:␣' || SQLERRM);
109     END;
110
111     -- a cada 100 registros faz o commit para diminuir a
```

```
112         -- quantidade de recursos de undo necessarios a carga
113         -- bem como de outras estruturas de controle
114         IF MOD (CONTADOR, 100) = 0
115         THEN
116            COMMIT;
117         END IF;
118
119         contador := contador + 1;
120      END LOOP;
121  END;
122  /
```