Segurança em Banco de Dados para Adequação a LGPD

Kamilla Dória da Silveira

Universidade Tiradentes (UNIT)
Aracaju-SE

kamilla.silveira@souunit.com.br

Abstract. *The General Data Protection Law (GDPL) establishes de responsibility of companies regarding the personal data of Brazilian citizens. In this context considering the scope of database (DB) security, it was found that the related works present a strategic view of necessary actions to ensure the adequacy of databases for the law, neglecting practical aspects for implementation. As a contribution to the problem, this work proposes a set of instructions related to security in DB to adapt companies to GDPL. As a proof of concept, this instructions are used to develop the LGPD DBSec system, which was used in a use case.*

Resumo. *A Lei Geral de Proteção a Dados (LGPD) estabelece a responsabilidade das empresas perante os dados pessoais dos cidadãos brasileiros. Nesse contexto, considerando o escopo da segurança em Banco de Dados (BD), constatou-se que os trabalhos relacionados apresentam uma visão estratégica das ações necessárias para garantir a adequação dos BDs para a lei, negligenciando os aspectos práticos para a implementação. Como contribuição para o problema, este trabalho propõe um conjunto de instruções relacionados a segurança em BD para adequar empresas a LGPD. Como prova de conceito, essas instruções são utilizadas para desenvolver o sistema LGPD DBSec, que foi utilizado em um caso de uso.*

1. Introdução

A Lei Geral de Proteção a Dados (LGPD) se aplica a pessoas físicas ou jurídicas que lidam com dados pessoais e visa proteger a liberdade e privacidade dos brasileiros [Brasil 2018]. Além disso, suas seções estabelecem quais são os dados pessoais e dados pessoais sensíveis, assim como as operações consideradas como tratamento de dados.

O art. 42 estabelece a responsabilidade do controlador sobre o tratamento dos dados pessoais; o operador executa o tratamento de acordo com o que foi definido pelo controlador [SERPRO 2022]. Assim, o controlador responde por eventuais danos causados ao cidadão em decorrência da violação da lei. Por esse motivo, o art. 46 define as medidas necessárias para evitar tal violação.

Dessa forma, a LGPD levanta algumas questões [Padovan Neto, A. 2020], [Donda, D. 2020], [Santos 2019], dentre elas: (i) a necessidade de mapeamento e classificação dos dados pessoais; (ii) a responsabilização do controlador e operador sobre esses dados; (iii) o impacto associado a violação da lei; (iv) o grau de dificuldade das empresas em se manter adequadas. Isso significa que a empresa tem que garantir a segurança da informação, de forma que os dados somente sejam acessados por quem possui autorização para tal, além de assegurar que haja meios de detectar e prevenir

falhas de segurança. Nesse sentido, é necessária a criação e revisão constante de políticas de segurança, revisão e monitoramento de acessos indevidos, além de criptografia de dados sensíveis.

Tendo em vista essas constatações, porém, delimitando ao escopo de segurança em Banco de Dados (BD), já que (i) a informação é o ativo de maior valor da empresa e (ii) e a segurança da informação é uma exigência da LGPD, a motivação para realizar este trabalho vem da verificação de que os trabalhos relacionados apresentam uma visão mais estratégica das ações necessárias para estar em conformidade com a lei. Ou seja, estes não apresentam guias práticos para implementar parâmetros de segurança em BD que garantam essa conformidade.

Nesse contexto, levando em conta que: a norma 27001 define o Sistema de Gestão de Segurança da Informação (SGSI) e é a norma que apresenta as melhores práticas para a gestão da segurança da informação [ABNT 2013a], e que a norma 27002 define como implementar os controles para o SGSI [ABNT 2013b], e o ORACLE [Huey, P. 2017] é um dos Sistemas de Gerenciamento de Banco de Dados Relacional (SGBDRs) mais utilizados no mercado, este trabalho tem como objetivo responder as seguintes perguntas: (i) "Quais são os controles das normas ISO 27001 e 27002 e parâmetros do Oracle que podem ser implementados nos banco de dados para a garantir a adequação com a LGPD?"; e (ii) "Como esses controles e parâmetros podem ser combinados a fim de melhorar a segurança em banco de dados para a adequação com a LGPD?". Portanto, este trabalho avança os estados da arte e da técnica a partir da proposição de duas contribuições: i) um conjunto de instruções sobre controles e parâmetros que permitam implementar, segundo as especificações da LGPD, a segurança dos dados do BD e ii) uma ferramenta que, com base neste conjunto de instruções, permita implementar e monitorar de forma prática os parâmetros do BD. Dessa forma, as demais seções deste trabalho apresentam: a fundamentação teórica, os trabalhos relacionados, o conjunto de instruções e a ferramenta propostos, a avaliação de um caso real de uso da ferramenta e as considerações finais.

2. Referencial Teórico

A Lei n. 13.709/2018, também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), regulamenta o tratamento de dados pessoais, incluindo meios digitais, por pessoas naturais ou pessoas jurídicas, públicas ou privadas. Tem como princípio proteger os direitos fundamentais de liberdade e privacidade dos brasileiros [Brasil 2018]. Nesse contexto, a LGPD é composta por dez capítulos e 11 seções, os quais se referem ao tratamento de dados pessoais por meios digitais ou manuais, aplicáveis a todas as empresas brasileiras ou que operacionalizam dados em território brasileiro. Esse tratamento pode ser considerado conforme as operações: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, modificação, comunicação, transferência, difusão e extração.

Segundo Donda [Donda, D. 2020], dado pessoal é qualquer informação relacionada a um indivíduo, pessoa natural identificada ou identificável: nome, data de nascimento, CPF, RH, CNH, carteira de trabalho, passaporte, título de eleitor, sexo, endereço, e-mail, telefone, origem racial ou étnica, convicção religiosa, opinião política,

filiação a sindicato ou organização, informações sobre saúde ou orientação sexual e dados genéticos ou biométricos.

A lei especifica ainda que deve haver o consentimento do cidadão para que haja o tratamento dos seus dados. O controlador, pessoa física ou jurídica, de natureza pública ou privada, é quem decide sobre o tratamento dos dados; e o operador é aquele que realiza o tratamento dos dados de acordo com o que o controlador definiu. De acordo com o art. 42, caso haja violação da lei, o controlador ou operador responsável irá responder pelos danos causados (patrimonial, moral, individual ou coletivo) [SERPRO 2022]. Por esse motivo, o controlador e operador devem adotar as medidas de segurança, conforme previsto no art. 46.

A própria lei recomenda algumas técnicas de prevenção, como [Brasil 2018]: anonimização (embaralhamento ou ofuscamento de dados), pseudonimização (redução da vinculação de um conjunto de dados), controle de acesso de usuário privilegiado, controle de acesso refinado (garantia de que dados sejam acessados seletivamente) e minimização de dados (reduzir ao máximo possível a coleta e armazenamento de dados). Além disso, deve haver mecanismos para monitoramento de violações, os quais podem ser implementados por meio de dados de auditoria e alertas.

A ISO 27001 é uma norma que especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI), os quais são utilizados para elaborar controles de segurança personalizados para as necessidades individuais de organizações ou suas partes [ABNT 2013a]. A sua atual edição (2013) contém 14 seções e 114 controles recomendados (excluindo as seções informativas, de 0 a 4). Para este trabalho foram consideradas 4 seções, pois estas são aplicáveis à segurança em banco de dados: (i) 8 – Gestão de Ativos; (ii) 9 – Controle de Acesso; (iii) 10 – Criptografia; (iv) Segurança nas Operações.

Já a ISO 27002 fornece requisitos operacionais e técnicos para segurança da informação, sendo utilizada como um guia para elaboração de uma política de segurança. Nesse sentido, são 14 seções 114 controles que a compõe (excluindo as seções informativas, de 0 a 4) [ABNT 2013a]. Dado que a própria norma recomenda que a mesma seja implementada em conjunto com a ISO 27001, as mesmas seções correspondentes foram consideradas: (i) 8 – Gestão de Ativos; (ii) 9 – Controle de Acesso; (iii) 10 – Criptografia; (iv) Segurança nas Operações.

Segundo Silveira e Fidalgo [Silveira e Fidalgo 2018], o SGBD Oracle possui um esquema de segurança dividido em três grupos: 1) Políticas de segurança contra acesso não autorizado; 2) Políticas de auditoria; e 3) Gestão de usuários e privilégios. Esses grupos apresentam 34 parâmetros de segurança. Para este trabalho são considerados 30 parâmetros (exibidos na Tabela 1), os quais foram selecionados a partir de uma associação com a os controles selecionados das ISO 27001 e 27002.

3. Trabalhos Relacionados

Para ter uma perspectiva da segurança em banco de dados em função da adequação para a LGPD, foram selecionados alguns trabalhos relacionados a partir da estratégia a seguir: (i) definição de uma expressão de busca (ii) uso dos motores de busca Google Scholar e Science Direct, devido as suas amplas coberturas via acesso gratuito. Dessa maneira, foram testadas algumas expressões de busca com foco na existência de

conteúdo relevante nos resultados da primeira página retornada pelos motores de busca. A expressão usada foi: ("database" OR "banco de dados") AND ("Lei Geral de Proteção a Dados" OR "LGPD"); (iii) verificação da aderência ao tema. Foram retornados 690 trabalhos, sendo 32 do Science Direct e 658 do Google Scholar. Após uma pesquisa nos títulos desses trabalhos, com o objetivo constatar a aderência ao tema e excluir trabalhos duplicados, restaram 27 trabalhos; (iv) levantamento final dos trabalhos relacionados. Para a seleção dos principais trabalhos relacionados foi utilizado o seguinte critério de exclusão: apresenta informações, que, de acordo com a LGPD, permite implementar parâmetros de segurança do BD? Após analisar os 27 trabalhos usando este critério de exclusão, constatou-se que estes apresentam uma visão geral da área de segurança da informação para cumprir com os requisitos da lei, não apresentando assim um detalhamento que permita a implementação de parâmetros de segurança em bancos de dados, a partir de uma análise específica dos comandos de segurança dos BDs, alinhado com um padrão reconhecido amplamente. Além disso, não apresentam uma ferramenta de apoio para aplicar e monitorar os parâmetros implementados. Os dois trabalhos apresentados a seguir, substanciam esta constatação, a qual motivou o desenvolvimento deste trabalho.

Padovan Neto [Padovan Neto, A. 2020], apresenta orientações básicas para obter aderência da LGPD para banco de dados utilizando algumas seções da ISO 27001 como apoio, mas não demonstra quais parâmetros específicos do banco de dados devem ser controlados e como devem ser utilizados. Além disso, não fornece um meio de monitorar tais parâmetros para garantir a continuidade da aderência.

Almeida Et al. [Almeida Et al. 2019], apresenta indicações sobre algumas ferramentas de mercado para banco de dados que auxiliam na implementação de mecanismos de segurança, no entanto, não oferece uma correlação com algum modelo reconhecido amplamente. Além disso, não apresenta uma ferramenta que permita unificar o monitoramento dos controles de todos os bancos de dados da empresa.

O que distingue é que esse trabalho propõe um conjunto de instruções que possa auxiliar empresas a implementar controles e parâmetros de segurança em BD para estar adequado para a LGPD, assim como prover uma ferramenta que centraliza e automatiza o monitoramento desses parâmetros, de forma que o controlador possa ter todas as informações referentes à segurança dos dados pessoais em um repositório único.

4. Apresentação da Proposta

Nesta seção é apresentado o método utilizado para a definição dos parâmetros de segurança em banco de dados para conformidade com a LGPD. Primeiramente é realizada a escolha dos requisitos necessários para criar ou melhorar a política de segurança da informação, por meio da implementação da ISO 27001, e os controles necessários garantir o cumprimento da lei, por meio implementação da ISO 27002. Dessa forma, uma lista de controles é gerada, a qual é comparada com os parâmetros de segurança do Oracle, gerando assim o conjunto de instruções nesse trabalho. Finalmente, é apresentado o sistema LGPD DBSec, o qual permitirá que empresas implementem e monitorem os parâmetros gerados a partir do conjunto de instruções proposto, servindo como apoio para adequação a lei.

4.1. Definição dos Controles de Segurança

As ISO 27001 e 27002 abrangem temas que vão além da segurança em banco de dados. Dessa forma, é necessário selecionar quais controles fazem parte do escopo. Segundo a própria norma [ABNT 2013b], a ISO 27002 foi projetada para ser utilizada em conjunto com a ISO 27001 (uma com uma visão holística e a outra com uma visão operacional). Ao analisa-las, utilizando como critério os princípios da LGPD e a segurança em BD, é possível selecionar 4 seções que são coerentes com o objetivo desse trabalho: 8, 9, 10 e 12. Em seguida, da mesma forma são destacadas as subseções que pertencem as seções selecionadas anteriormente. Assim, da seção 8, duas subseções são selecionadas (8.1 e 8.2), da seção 9 tem-se duas subseções selecionadas (9.1 e 9.4), da seção 10 apenas uma subseção destacada, e por fim, da seção 12 são selecionadas 3 subseções (12.4, 12.6 e 12.7). Finalmente, das subseções destacadas, apenas 16 controles do framework estão de acordo com o critério de seleção.

A seguir, a lista de controles selecionados das normas ISO 27001 e 27002, e a justificativa para cada seleção:

1) 8.1.1 - Inventário dos ativos: registro de bancos de dados que possuem dados pessoais sensíveis;
2) 8.1.2 - Proprietário dos ativos: registro do proprietário dos bancos de dados que possuem dados sensíveis;
3) 8.2.1 - Classificação da informação: classificação das informações armazenadas pelos bancos de dados em dados pessoais e dados pessoais sensíveis;
4) 8.2.2 - Rótulos e tratamento da informação: identificação do tratamento realizados com os dados pessoais nos bancos de dados;
5) 9.2.3 - Gerenciamento de direitos de acesso privilegiado: gestão dos acessos aos bancos de dados;
6) 9.2.4 - Gerenciamento da informação de autenticação secreta de usuários: gestão do padrão de senhas dos bancos de dados;
7) 9.2.6 - Retirada ou ajuste de direitos de acesso: gestão dos acessos aos bancos de dados;
8) 9.4.1 - Restrição de acesso à informação: gestão dos acessos aos bancos de dados;
9) 9.4.2 - Procedimentos seguros de entrada no sistema (log on): método seguro de autenticação no banco de dados;
10) 9.4.3 - Sistema de gerenciamento de senha: gestão de parâmetros para gestão de senhas do banco de dados;
11) 10.1.1 - Política para o uso de controles criptográficos: implementação de criptografia no banco de dados;
12) 12.4.1 - Registros de evento: registos de eventos das principais de segurança no banco de dados;
13) 12.4.2 - Proteção das informações dos registros de eventos (logs): registos de logs das principais de segurança no banco de dados;
14) 12.4.3 - Registros de eventos (log) de Administrador e Operador: registos de eventos das atividades de administração do banco de dados;
15) 12.6.1 - Gestão de vulnerabilidades técnicas: implementação de parâmetros para garantir a segurança do banco de dados assim como a apresentação de informações relacionadas em tempo hábil;

16) 12.7.1 - Controles de auditoria de sistemas de informação: parâmetros para controle de informações de auditoria no banco de dados.

Os demais controles da ISO não fazem parte do escopo deste trabalho, dado que tratam da criação de políticas e organização da segurança da informação, segurança relacionado a recursos humanos, segurança física do ambiente, segurança de redes, processo de desenvolvimento de sistemas, aquisições, gestão de incidentes de segurança e conformidade legal, as quais não se aplicam diretamente à segurança em banco de dados.

4.2 Implementação dos Controles de Segurança

Após a criação da lista de controles, o próximo passo é a implementação nos SGBDs. Os controles selecionados das normas ISO podem ser organizados em dois grupos para atender a LGPD: os que dizem respeito ao mapeamento e classificação dos dados, e aqueles que refletem parâmetros de segurança no BD.

O primeiro grupo corresponde aos controles de mapeamento de ativos e classificação de informações, os quais são necessários para que o controlador mantenha um inventário de todos os bancos de dados e também um registro da classificação dos dados armazenados pelos BDs. A seguir a lista de controles selecionados que pertencem a esse grupo e as ações propostas para implementa-los:

1) 8.1.1 – Inventário dos ativos: mapear e listar todos os bancos de dados da empresa que armazenam dados pessoais;
2) 8.1.2 – Proprietário dos ativos: a partir do inventário dos ativos, registrar a informação sobre o proprietário do sistema associado ao BD listado;
3) 8.2.1 – Classificação da informação: classificar os dados armazenados nas tabelas do BD em dados pessoais e dados pessoais sensíveis;
4) 8.2.2 – Rótulos e tratamento da informação: registrar o tratamento que é dado para os dados classificados dos BDs (leitura, alteração, exclusão);

O registro de tais informações é necessário para que o controlador possa gerenciar o tratamento de dados pessoais na empresa, dado que ele é o responsável perante a lei e precisa garantir que estejam seguros.

O segundo grupo compreende os controles que devem ser implementados no banco de dados. Assim, é feita a validação de quais parâmetros de segurança do Oracle possuem relação com os controles selecionados das normas ISO. Para tal, é necessário avaliar cada parâmetro de segurança do SGBD, com o objetivo de encontrar um controle correspondente. O critério de escolha é a relação de um ou mais parâmetros do banco de dados que satisfaçam a condição de cada controle selecionado das normas.

O resultado pode ser visualizado na Tabela 1, que apresenta a relação dos parâmetros do Oracle correspondente aos controles das normas ISO selecionados anteriormente. Os demais parâmetros de segurança do banco de dados não são aplicados pois não possuem um controle correspondente nas normas.

4.3 Conjunto de Instruções Proposto

A Tabela 1 corresponde uma lista de parâmetros de segurança do Oracle, selecionada a partir de uma lista de controles das ISO 27001 e 27002, os quais atendem aos princípios da LGPD.

Tabela 1. Relação dos Parâmetros do Oracle para Adequação a LGPD

ISO 27001 / 27002	Parâmetro Oracle
9.2.3	%ANY%
	O7_DICTIONARY_ACCESSIBILITY
	ACCOUNT_STATUS - Administrative users
9.2.4	PASSWORD_VERIFY_FUNCTION
9.2.6	PASSWORD_GRACE_TIME
	PASSWORD_LIFE_TIME
9.4.1	DBMS_RANDOM, UTL_FILE, UTL_HTTP, UTL_SMTP, UTL_TCP
	ACCOUNT_STATUS - Non-administrative users
9.4.2	OS_ROLES
	REMOTE_OS_ROLES
	REMOTE_OS_AUTHENT
9.4.3	PASSWORD_LOCK_TIME
	sec_case_sensitive_logon
	PASSWORD_REUSE_MAX
	PASSWORD_REUSE_TIME
10.1.1	ENCRYPTED
12.4.1	DROP USER, CREATE USER, ALTER USER
	SYSTEM GRANT, GRANT ANY ROLE, GRANT ANY OBJECT PRIVILEGE, GRANT ANY PRIVILEGE
	CREATE SESSION - FAILURE
	CREATE SESSION - SUCCESS
12.4.2	ALTER TABLESPACE, PROFILE, DROP PROFILE, ALTER PROFILE, ROLE, CREATE ANY JOB, CREATE EXTERNAL JOB, ALTER ANY PROCEDURE, DROP ANY PROCEDURE, CREATE ANY PROCEDURE, DROP ANY TABLE, CREATE ANY TABLE, ALTER ANY TABLE
12.4.3	ALTER SYSTEM
12.6.1	sec_max_failed_login_attempts
	FAILED_LOGIN_ATTEMPTS
	sec_return_server_release_banner
12.7.1	AUDIT_TRAIL
	DELETE_CATALOG_ROLE
	AUDIT_SYS_OPERATIONS
	DBA_AUDIT_MGMT_CLEANUP_JOBS
	SELECT_CATALOG_ROLE, EXECUTE_CATALOG_ROLE

Fonte: a autora

A implementação prática dos controles de segurança selecionados junto com tais parâmetros, conforme disposto, compreende o conjunto de instruções proposto nos objetivos deste trabalho, apresentando assim um meio para garantir a segurança em banco de dados para adequação a LGPD. A aplicação do mesmo deve ser realizada por meio dos passos apresentados abaixo:

1. Avaliar a adequação da empresa aos controles da ISO 27001 selecionados;

2. Avaliar a adequação da empresa aos controles da ISO 27002 selecionados;
3. Aplicar a ferramenta LGPD DBSec nos SGBDs da empresa.

4.4 Sistema LGPD DBSec

O LGPD DBSec é uma ferramenta de apoio ao controle de parâmetros de segurança em banco de dados para adequação de empresas à LGPD. Dessa forma, é baseado nos dados apresentados na Tabela 1, apresentando-se como uma ferramenta para automatizar a aplicação prática do conjunto de instruções proposto.

C#.NET foi a linguagem utilizada no desenvolvimento desse sistema. Dessa forma, possui como pré-requisito um servidor de aplicação IIS. A aplicação pode se conectar com vários bancos de dados que apresentem informações relevantes para a LGPD, ou seja, que armazenam dados pessoais.

O sistema possui uma interface que permite se conectar a um banco de dados da empresa e apresenta uma consulta de status da adequação do banco de dados em relação aos parâmetros de segurança relacionados, informando se o parâmetro está ou não de acordo com a proposta. Adicionalmente a ferramenta oferece um mecanismo para adequar os parâmetros que não estiverem de acordo. Essa interface também serve para monitorar periodicamente a manutenção desses parâmetros.

5. Aplicação Prática

Para a aplicação do conjunto de instruções proposto, assim como da ferramenta desenvolvida, foi selecionada uma base de dados Oracle produtiva. Devido a questões de segurança, o nome da empresa e da base não foi divulgada, sendo tratada neste trabalho como empresa A e base de dados X.

O processo de adequação da base de dados para a LGPD se dá por meio da sequência de instruções propostas. Nesse caso, seguindo a proposta, o primeiro passo foi realizar uma avaliação da adequação dos controles selecionados das normas ISO em relação a empresa A. Para tal, cada controle das normas foi detalhado junto a equipe de sistemas da empresa em questão, que, em seguida, deveria indicar se há aderência ou não ao controle proposto.

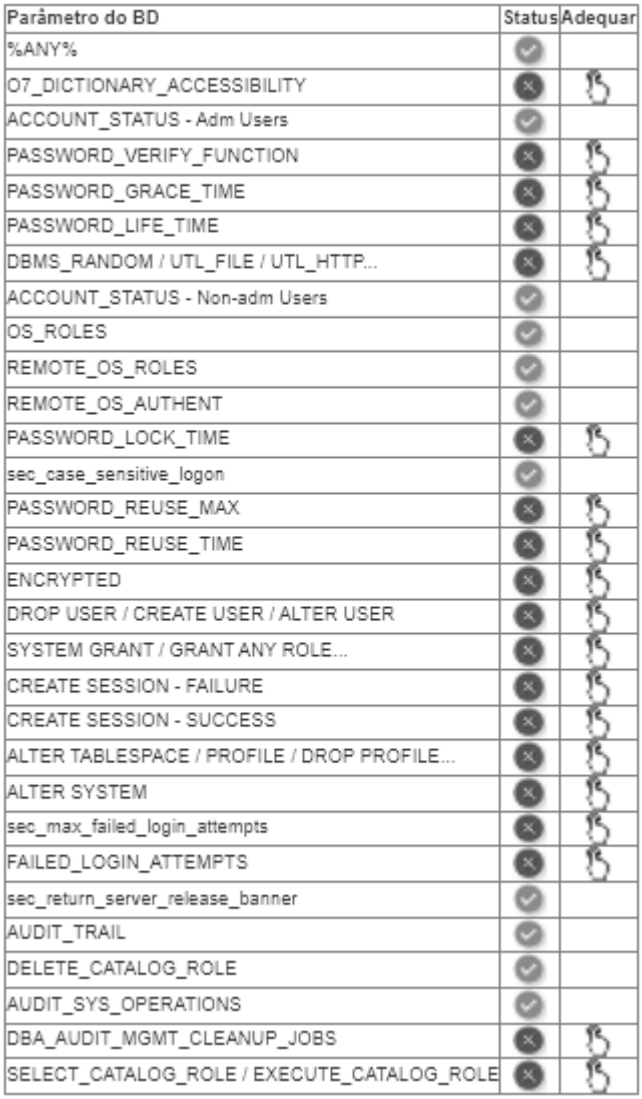
Na sequência foi realizada a instalação da ferramenta LGPD DBSec, e foi selecionada a base de dados X, a qual contém dados pessoais armazenados. Após isso, um DBA (Database Administrator) com acesso privilegiado utilizou a ferramenta para conectar a base de dados X, que apresentou 19 parâmetros de segurança não adequados e 11 parâmetros adequados de acordo com a proposta (a Figura 1 apresenta o resultado da verificação da ferramenta). Ao final, o DBA analisou o impacto de adequar cada parâmetro não conforme no banco de dados.

5.1 Discussão sobre a aplicação prática

Uma vez obtidos os resultados da aplicação da ferramenta, foram realizadas análises para constatar o impacto da adequação desses parâmetros no banco de dados e no sistema relacionado ao banco de dados. Essa análise foi realizada pelo DBA da empresa A, que constatou não haver impacto negativo nas adequações. Após isso, a adequação foi realizada por meio da ferramenta LGPD DBSec em uma cópia do ambiente produtivo, dado que algumas mudanças afetariam os usuários diretamente e necessitava

de alinhamento e comunicação prévios. Após realizar testes, não foram constatadas anomalias.

Analisando a Figura 1, é possível verificar que os parâmetros de segurança que não estavam adequados eram referentes a gestão do *logon* e características de senhas dos usuários; e ativação de registro de logs, eventos e auditoria. Dessa forma, é possível concluir que a ferramenta facilita a adequação da segurança do banco de dados para a LGPD, no entanto, algumas adequações (como a gestão de *logon* e características de senhas dos usuários), necessitam de alinhamento com a gestão da empresa e comunicação para os usuários, pois afeta-os diretamente em sua forma de trabalho. Além disso, também é necessária uma análise da infraestrutura da empresa antes de ativar os registros de logs, eventos e auditoria, já que impactará em maior armazenamento de dados.



Parâmetro do BD	Status	Adequar
%ANY%	✓	
O7_DICTIONARY_ACCESSIBILITY	✗	☜
ACCOUNT_STATUS - Adm Users	✓	
PASSWORD_VERIFY_FUNCTION	✗	☜
PASSWORD_GRACE_TIME	✗	☜
PASSWORD_LIFE_TIME	✗	☜
DBMS_RANDOM / UTL_FILE / UTL_HTTP...	✗	☜
ACCOUNT_STATUS - Non-adm Users	✓	
OS_ROLES	✓	
REMOTE_OS_ROLES	✓	
REMOTE_OS_AUTHENT	✓	
PASSWORD_LOCK_TIME	✗	☜
sec_case_sensitive_logon	✓	
PASSWORD_REUSE_MAX	✗	☜
PASSWORD_REUSE_TIME	✗	☜
ENCRYPTED	✗	☜
DROP USER / CREATE USER / ALTER USER	✗	☜
SYSTEM GRANT / GRANT ANY ROLE...	✗	☜
CREATE SESSION - FAILURE	✗	☜
CREATE SESSION - SUCCESS	✗	☜
ALTER TABLESPACE / PROFILE / DROP PROFILE...	✗	☜
ALTER SYSTEM	✗	☜
sec_max_failed_login_attempts	✗	☜
FAILED_LOGIN_ATTEMPTS	✗	☜
sec_return_server_release_banner	✓	
AUDIT_TRAIL	✓	
DELETE_CATALOG_ROLE	✓	
AUDIT_SYS_OPERATIONS	✓	
DBA_AUDIT_MGMT_CLEANUP_JOBS	✗	☜
SELECT_CATALOG_ROLE / EXECUTE_CATALOG_ROLE	✗	☜

Figura 1. Consulta de parâmetros de segurança da empresa A

Fonte: a autora

Por fim, foi verificado que a empresa, apesar de já estar em processo de adequação para a LGPD, havia negligenciado os parâmetros de segurança do banco de

dados, focando apenas na segurança sistêmica e armazenamento de dados. Tais parâmetros são importantes para garantir a segurança no acesso ao banco de dados e para que haja meios de detectar e rastrear ocorrências em caso de falhas.

6. Considerações Finais

Com base no que foi apresentado neste trabalho, pode-se concluir que a primeira questão declarada (i) "Quais são os controles das normas ISO 27001 e 27002 e parâmetros do Oracle que podem ser implementados nos banco de dados para a garantir a adequação com a LGPD?", e também a segunda questão (ii) "Como esses controles e parâmetros podem ser combinados a fim de melhorar a segurança em banco de dados para a adequação com a LGPD?" foram abordadas, dado que o trabalho apresenta um conjunto de instruções proposto para adequar um banco de dados a LGPD, assim como uma ferramenta para automatizar a aplicação prática do mesmo. Além disso, o trabalho também apresenta o resultado de uma aplicação prática em um ambiente real.

Espera-se ainda que o presente trabalho sirva como base para pesquisadores que desejem dar continuidade na análise das adequações dos demais ambientes que compõem os sistemas das empresas, como servidores, sistemas, redes, além da extensão para outros SGBDs.

Referências

Brasil (2018). Lei 13.709 de 14 de Agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 de novembro de 2021.

Donda, D. (2020). Guia Prático de Implementação da LGPD. São Paulo: Labrador.

SERPRO (2022). O que é a Lei Geral de Proteção de Dados Pessoais? Dê um "giro" pela lei e conheça desde já as principais transformações que ela traz para o país. Brasília. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-mudacom-a-lgpd>. Acesso em: 03 de Março de 2022.

ABNT (2013a). ABNT NBR ISO/IEC 27001.

ABNT (2013b). NBR ISO/IEC 27002.

Huey, P. (2017). Oracle Database Security Guide 11g Release 2.

Padovan Neto, A. (2020). "Proteção de dados aplicada em banco de dados", Monografia em Tecnologia em Segurança da Informação, Faculdade de Tecnologia de Americana.

Almeida, A. C. B.; Verona, L. D.; Campos, M. L. M.; Baião, F. A. (2019). "LGPD em Ambientes de Bancos de Dados nas Organizações", Minicurso da VI Escola Regional de Sistemas de Informação do Rio de Janeiro.

Santos, V. B. M. (2019). "Lei Geral de Proteção a Dados: Fundamentos e Compliance", Monografia em Direito, Universidade Federal do Ceará.

Silveira, K. D.; Fidalgo, R. N. Controles Internos de Segurança em Banco de Dados para Certificação da Lei SOX . In: SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO (SBSI), 14. , 2018, Caxias do Sul. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2018 . p. 350-357.