APLICAÇÃO DA LGPD EM UMA EMPRESA DA REGIÃO DE CRICIÚMA: ESTUDO DE CASO EM BANCO DE DADOS

Vinicius Spada Melo[1], Matheus Leandro Ferreira [2]

[1]Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC)

Resumo

Com o avanço da tecnologia, tem-se cada vez mais disponível o processamento de grandes volumes de dados variados, fazendo com que formem bancos de dados mais amplos e com maior exatidão. E para tentar controlar o acesso e a proteção dos dados pessoais no Brasil, foi sancionada a Lei Geral de Proteção dos Dados Pessoais (LGPD), a qual exige que as organizações cumpram uma ampla variedade de questões relacionadas à coleta, processamento e proteção de informações pessoais**.** Neste contexto, utilizando da bibliografia disponível, o presente artigo contempla os pontos mais importantes da lei, além de destacar as medidas que devem ser tomadas por uma empresa da região para a adequação do banco de dados à LGPD. Após um breve período, foi possível observar que a empresa não contemplava nenhuma norma da LGPD em seu banco de dados, porém a ferramenta que a empresa utiliza, o SQL Server Management Studio, dispõe de uma série de mecanismos presentes que auxiliaram na implementação das normas no banco de dados da empresa. Além disso, se fez necessário vários treinamentos com os colaboradores, para reeducação com relação às novas práticas de segurança.
Palavras-chave: LGPD; Proteção de Dados pessoais; Banco de dados.

Abstract

Mainly because of the advancement of technology, the processing of large volumes of varied data is increasingly available, making them form larger and more accurate databases. In order to try controlling the access and protection of personal data in Brazil, the General Law for the Protection of Personal Data (LGPD) was enacted, which requires organizations to comply with a wide variety of issues related to the collection, processing and protection personal information. In this context, using the available bibliography, this article covers the most important points of the law as well as highlighting the measures that must be taken by a company in the region to adapt the database to the LGPD. After a brief period, it was possible to observe that

[1] Vinicius Spada Melo. viniciusspmelo@gmail.com

[2] Matheus Leandro Ferreira. mlf@unesc.net

the company did not contemplate any LGPD standard in its database. However the tool that the company uses, SQL Server Management Studio, has a series of mechanisms present that helped in the implementation of the standards in the company's database. In addition, several training sessions with employees were necessary for re-education regarding the new safety practices.
Keywords: LGPD; Protection; Personal Data; Databases.

1 INTRODUÇÃO

A utilização sempre mais ampla de dados pessoais para as mais variadas atividades – identificação, classificação, autorização e tantas outras – torna tais dados elementos essenciais para que a pessoa possa se mover com autonomia e liberdade nos corredores do que hoje costuma-se denominar de Sociedade da Informação. Os dados pessoais chegam a fazer às vezes da própria pessoa em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável (DONEDA D, 2011).

Por meio da inteligência artificial e algoritmos cada vez melhores, as grandes empresas do setor de tecnologia conseguem a cada dia que passa reunir mais informações sobre nós, tentando preliminarmente influenciar nos nossos hábitos de consumo (SANSANA A, 2018). E isso torna-se um grande problema quando não se tem controle sobre os dados pessoais que circulam na Internet.

De acordo com o jornal americano The Washington Post, a rede social Facebook, uma das mais utilizadas no mundo, possui inúmeras informações de caráter íntimo e pessoal como por exemplo dos usuários que: desejam comprar um carro novo, que escutam rádio, ou até mesmo suas tendências políticas. Ou seja, se não há proteção de dados, as empresas que os detém, podem usá-los ao seu favor, influenciando desde uma simples compra, como até mesmo uma votação.

Após observar a proporção da influência e valor dos dados pessoais na sociedade, consequentemente as suas implicações éticas (MOOR, 2005), criou-se a Lei Geral de Proteção de Dados, Lei nº 13.709, em 14 de agosto de 2018, na qual entrou em vigor no dia 18 de setembro de 2020.

Baseada na *General Data Protection Regulation* (GDPR), elaborado pela União Europeia, obriga organizações a seguirem uma série de itens quanto à coleta, ao tratamento e à proteção dos dados pessoais (DE ALMEIDA, 2019). A LGPD trata da proteção de dados como regra, sendo um dos objetivos principais da legislação, em

seu Art. 1º (BRASIL, 2018ª). Seu impacto inclui todas as informações pessoais coletadas, armazenadas e processadas por organizações, sejam públicas ou privadas, tendo como objetivo garantir todos os direitos dos potenciais titulares dando a maior autonomia possível sobre seus dados.

O GDPR estabelece oito princípios de tratamento: Licitude, lealdade e transparência; limitação das finalidades; minimização dos dados; exatidão; limitação da conservação; integridade e confidencialidade; e responsabilidade. No entanto, a LGPD especifica dez princípios: Finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização. Portanto, as organizações que estão sujeitas à LGPD devem garantir com que o tratamento seja feito de acordo com os princípios recentemente estabelecidos, caso não sejam abrangidos pelos princípios do GDPR.

Conforme a lei, o conceito de dado pessoal é qualquer informação que por meio dela, consiga identificar de forma direta ou indireta, um indivíduo que esteja vivo. Algumas informações que se enquadram nesse conceito são desde nome, RG, CPF, data de nascimento, endereço, fotos, renda, até cookies que ficam gravados em computadores pessoais e informações compartilhadas em redes sociais. Informações sobre a vida sexual, dados genéticos, dados sobre origem racial ou étnica também se enquadram nesse conceito.

A LGPD determina que o titular do dado possua poder sobre seus dados no que se referem a coleta, tratamento e armazenamento. Com isso, o titular possui direito de saber de que forma suas informações estão sendo tratados, para que finalidade estão sendo usadas, e caso desejar, corrija ou solicite sua exclusão. O Art. 18, estabelece o direito do titular dos dados de obter do controlador, a qualquer momento e mediante requisição, a adoção das seguintes providências:

i. Confirmação da existência de tratamento;
ii. Acesso aos dados;
iii. Correção de informações incompletas, inexatas ou desatualizadas;
iv. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei;
v. Portabilidade das informações pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a

regulamentação da autoridade nacional, observados os segredos comercial e industrial;

vi. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas na lei;

vii. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

viii. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

ix. Revogação do consentimento.

O não cumprimento à lei, conforme Art. 52, da LGPD, os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

i. Advertência, com indicação de prazo para adoção de medidas corretivas;

ii. Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

iii. Multa diária, observado o limite total a que se refere o inciso II;

iv. Publicização da infração após devidamente apurada e confirmada a sua ocorrência;

v. Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

vi. Eliminação dos dados pessoais a que se refere a infração;

Tendo em vista o cenário em questão, o presente trabalho visa a adequação de uma base de dados de uma empresa de tecnologia da região de Criciúma/SC às normas da LGPD, utilizando os mecanismos presentes no SGBD SQL Server.

2 TRABALHOS CORRELATOS

Para o desenvolvimento da pesquisa em questão, foram realizadas buscas por meio da base do Google Acadêmico, sobre trabalhos relacionados ao tema LGPD e banco de dados, para garantir maior conhecimento sobre o tema apresentado.

Almeida (2019) analisou três ambientes de banco de dados, e elencou as melhores soluções disponíveis para ajudar na adequação da LGPD. O objetivo principal é possibilitar uma visão geral da LGPD tanto com a perspectiva de usuário quanto com a perspectiva de um administrador de banco de dados, exemplificando recursos de alguns dos principais SGBDs do mercado. O artigo também faz uma pesquisa bastante completa nos SGBD's que propuseram, elencando os principais mecanismos de segurança presente nos ambientes de banco de dados SQL Server, Oracle, Amazon Web Services (AWS) e PostgreSQL, sendo que um deles, o SQL Server, serviu de objeto de estudo para este projeto em questão.

Miragem (2019) examinou a repercussão da Lei Geral de Proteção de Dados sobre as relações de consumo e os direitos do consumidor no Brasil, em especial, considerando sua harmonia com o Código de Defesa do Consumidor (MIRAGEM B, 2019). Tal artigo apresenta informações bem descritas sobre a LGPD, desde sua origem, trazendo os motivos da criação da lei, até sua aplicabilidade e interpretação, além de trazer os principais conceitos e princípios de uma forma bastante detalhada e precisa. O artigo é divido em 4 capítulos, sendo que no primeiro capítulo é feito uma breve introdução sobre o tema LGPD e sua origem. Já o segundo capítulo, é composto pelos princípios descritos na lei, apresentando-os e fazendo uma interpretação bastante detalhada do que cada princípio significa. O capítulo três ficou reservado para explicar os direitos do consumidor e a relação com o tratamento de dados pessoais. E o quarto e último capítulo foi apresentado as considerações finais do autor.

O trabalho elaborado por Alexandre Gomes Sansana (2018) tem como objetivo analisar a evolução da tutela da privacidade na Internet, o consentimento do detentor dos dados pessoais inseridos dentro da Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados (SANSANA, 2018). O artigo fora dividido em quatro seções, sendo que na primeira seção é demonstrado a evolução da tutela da privacidade, os motivos que levaram à criação da lei. A segunda seção, analisa o consentimento por parte do usuário, apresentando que o usuário deve possuir total consentimento dos seus dados, sem quaisquer vícios. Já a terceira seção, analisa o interesse no tratamento dos dados pessoais por parte do controlador dos dados. E a quarta e última seção, é composta pela conclusão final do autor, mostrando o que fora obtido por meio das pesquisas realizadas.

3 MATERIAIS E MÉTODOS

A presente pesquisa caracteriza-se por ser aplicada e de base tecnológica, contempla a adequação da base de dados da empresa à lei. Para isso, foi necessário o auxílio do Tech Lead e do CEO da empresa, bem como a cooperação dos colaboradores da empresa.

3.1 PASSOS PARA IMPLEMENTAÇÃO

Com o estudo realizado sobre a lei, foi possível obter compreensão sobre a LGPD, seus princípios e conceitos. Conforme estudo realizado sobre a RGPD (RAJASEKHARAN, 2017), pode-se classificar em três categorias os principais requisitos de segurança de dados da LGPD: avaliação, detecção e prevenção. As três categorias amplas de diretrizes de segurança (Avaliação, Prevenção e Detecção) permitem que as organizações abordem as ameaças de diferentes ângulos e protejam os dados do acesso não autorizado (RAJASEKHARAN, 2017).

Diante desse cenário, a empresa que está envolvida neste presente estudo, usa como ferramenta de banco de dados o SGBD Microsoft SQL Server, portanto o presente artigo, irá contemplar os principais mecanismos disponíveis neste SGBD em conformidade com as recomendações provenientes da LGPD. Ressalta-se que, para ser possível a implementação das features propostas, utilizou-se um banco de dados de teste da empresa, bem semelhante ao de produção. Além disso, todas as imagens utilizadas são provenientes desse banco de teste com dados fictícios.

Conforme a documentação da Microsoft (MICROSOFT 2020a), seu SGBD possui diversos mecanismos de segurança para auxiliar os clientes na adequação da LGPD, seja controlando acesso, até na detecção de intrusos.

Com base nas três principais categorias dos principais requisitos de segurança de dados que a LGPD recomenda, e na documentação da Microsoft os mecanismos presentes no SGBD da Microsoft são (ALMEIDA et al., 2018):

> a) Avaliação: *data discovery and classification* e *sql vulnerability assessment*.
>
> b) Prevenção: *dynamic data masking* (DDM), *sql server authentication*, *object-level permissions*, *transport layer security* (TLS) e *transparent data encryption* (TDE).

c) Detecção: *sql server audit*, *sql server temporal tables* e *sql vulnerability assessment*.

3.1.1 CATEGORIA DE AVALIAÇÃO

Organizações que fazem o uso de dados pessoais, possuem um grande volume de dados. Por conta disso, é necessário que o controlador possua alguma ferramenta que consiga avaliar os dados pessoais, para que o controlador fique apenas preocupado na melhor forma de guardar esses dados.

Por conta disso, está seção contempla a aplicação das *features data discovery and classification* e *sql vulnerability assessment*.

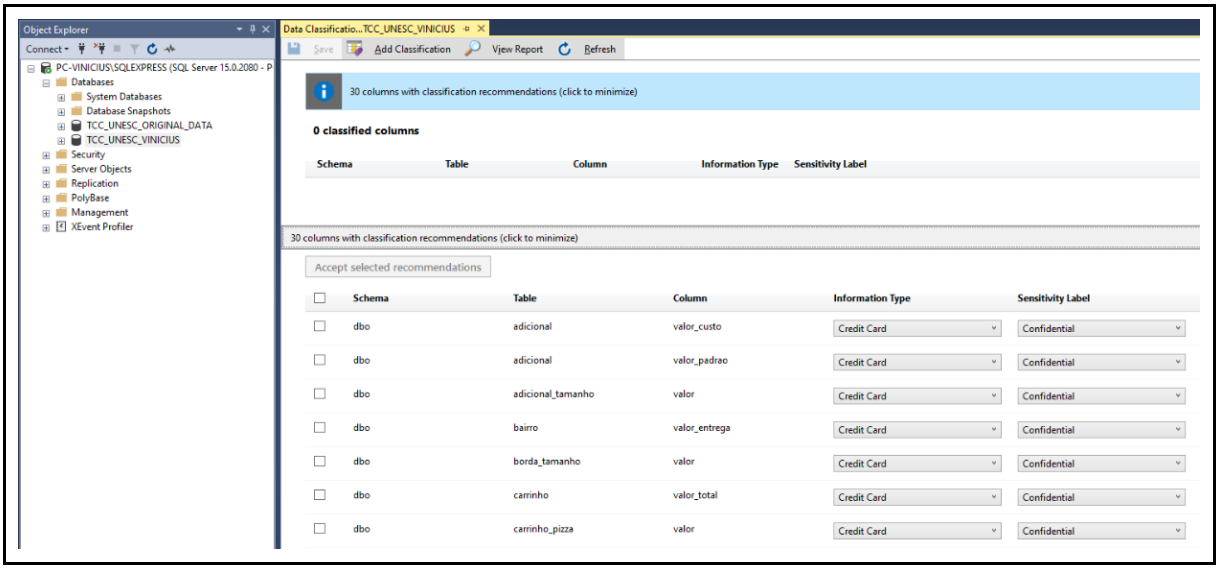
3.1.1.1 DESCOBERTA E CLASSIFICAÇÃO DE DADOS

Segundo a documentação da Microsoft (MICROSOFT 2021a), a *feature data discovery and classification* possui a finalidade de ajudar o controlador a entender os padrões de privacidade de dados e requisitos de conformidade regulatória, monitoramento (auditoria) de acesso anômalo a dados confidenciais, e auxilia no controle de acesso, fortalecendo a segurança de dados que contém dados confidenciais.

Essa *feature* é disponibilizada na ferramenta SQL Server Management Studio, e para utilizá-la, basta conectar-se ao SQL Server e selecionar o banco de dados.

Após selecionar o banco de dados desejado, o mecanismo de classificação verifica o banco de dados em busca de colunas que contenham dados confidenciais, apresentados abaixo na Figura 1.

Figura 1 - Exemplo de lista de classificação dos dados



Fonte: Do autor.

Conforme demonstrado acima, a ferramenta fornece uma lista de classificações de coluna recomendadas (MICROSOFT 2021a) para o administrador, tendo a opção de selecionar as recomendações as quais concorda. No caso da empresa em questão, as recomendações que a *feature* propôs foram todas aceitas.

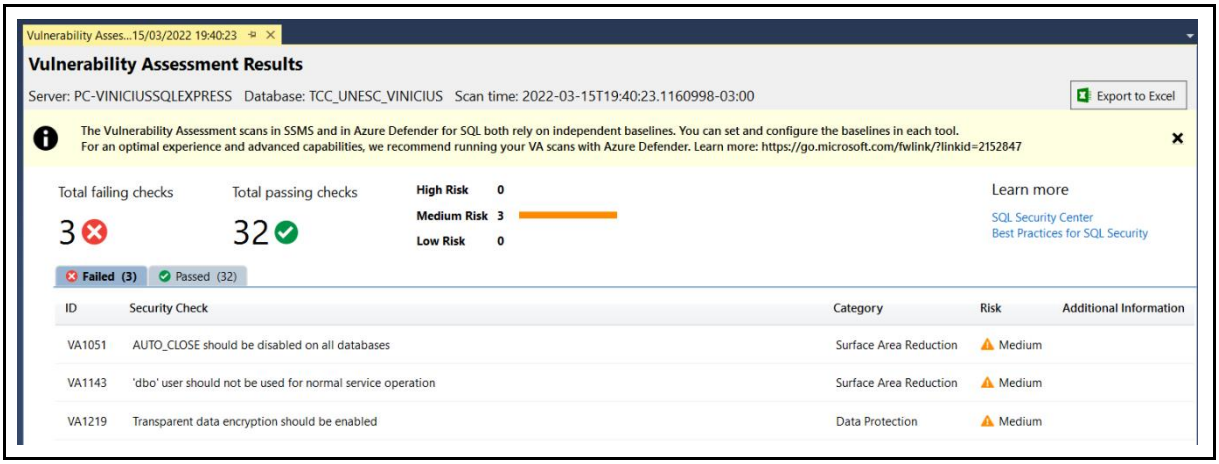
3.1.1.2 AVALIAÇÃO DE VULNERABILIDADE SQL

A *feature sql vulnerability assessment*, é um serviço que fornece visibilidade ao seu estado de segurança, além de incluir etapas acionáveis para resolver problemas de segurança e aprimorar a segurança do banco de dados. Além disso, a *feature* em questão pode ajudar a monitorar um ambiente dinâmico de banco de dados, onde as alterações são difíceis de serem rastreadas, melhorando sua postura de segurança do SQL (MICROSOFT 2021b).

Para utilizar a feature, no *SQL Server Management Studio*, basta selecionar o banco de dados no menu da ferramenta.

Observa-se na figura 3 que a própria *feature* dá sugestão de como resolver o problema.

Figura 3 - Exemplo de lista de classificação dos dados



Fonte: Do autor.

Para finalizar, basta o administrador seguir os passos apresentados.

3.1.2 CATEGORIA DE PREVENÇÃO

A Microsoft disponibiliza *features*, de acordo com as recomendações da LGPD na categoria de prevenção, para a anonimização e pseudonimização por meio do mascaramento dinâmico, o controle de acesso de usuário privilegiado e a criptografia de dados, que apesar de não constar explicitamente na LGPD, é um meio de segurança para os dados, em caso de vazamento (ALMEIDA et al., 2018).

3.1.2.1 MASCARAÇÃO DE DADOS DINÂMICOS

A *feature dynamic data masking* (DDM), é o processo de ocultação de dados com diferentes regras, e seu principal objetivo é proteger as informações pessoais e dados confidenciais de acessos não autorizados. Apesar de permitir o acesso aos dados de fato, essa *feature* não permite ver valores reais, mas exibe valores abstratos conforme configuração realizada.

Para utilização da *feature*, foi necessário fazer o levantamento dos dados sensíveis de todas as tabelas da base de dados junto ao Tech Lead da empresa, para realizar o mascaramento apenas do que é considerado sensível. Após o levantamento, foram realizados vários comandos como a Figura 4, variando de acordo com cada tipo de dado, tendo em vista que o mascaramento padrão (default), é aplicado conforme o tipo de dados da coluna. Em uma coluna do tipo texto, o valor padrão será “XXXX”, já em uma coluna do tipo numérico, o valor padrão será 0 e uma coluna do tipo data, possui como valor padrão a data “01/01/1900 00:00:00”.

Figura 4 - Exemplo de comando para criação do mascaramento

```
-- Tabela de adicional
begin
ALTER TABLE TCC_UNESC_VINICIUS.DBO.ADICIONAL
    ALTER COLUMN descricao ADD MASKED WITH (FUNCTION = 'default()');
ALTER TABLE TCC_UNESC_VINICIUS.DBO.ADICIONAL
    ALTER COLUMN valor_padrao ADD MASKED WITH (FUNCTION='random(1,9)');
ALTER TABLE TCC_UNESC_VINICIUS.DBO.ADICIONAL
    ALTER COLUMN valor_custo ADD MASKED WITH (FUNCTION='random(1,3)');
end;
```

Fonte: Do autor.

Após adicionar o mascaramento as tabelas, foi necessário entender quantos e quais usuários tem acesso ao banco de dados, para ser possível criar os usuários que teriam ou não permissão de ver os dados sensíveis.

Ao todo foram levantados cinco (5) perfis com permissões totais no banco, dos quais: dois (2) desenvolvedores, dois (2) analistas de suporte e um (1) Tech Lead. Com isso, foi acordado que apenas o Tech Lead possuiria o perfil de usuário de administrador do banco (*role sysadmin*), cujo qual tem permissão para fazer todas as modificações e leituras existentes no banco de dados. Os demais, desenvolvedores e analistas de suporte, tem apenas permissão de visualizar no banco de dados e com mascaramento dos dados (*role public*).

Para realizar as medidas levantadas acima, foram criados cinco (5) usuários, um (1) para o tech lead, dois (2) para os desenvolvedores e (2) para os analistas de suporte e dados suas devidas permissões (Figura 5).

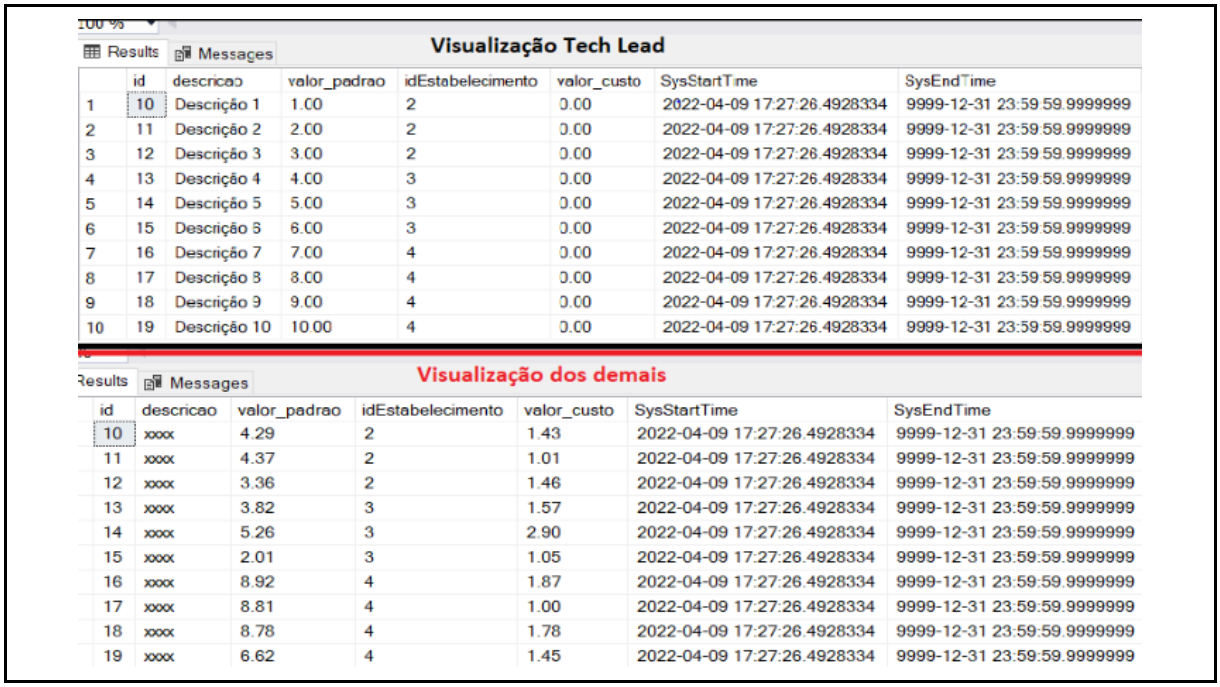
Figura 5 - Criação dos usuários e permissões de acesso

```
CREATE LOGIN dev1 WITH PASSWORD = 'dev1';
CREATE USER dev1 FOR LOGIN dev1;

CREATE LOGIN dev2 WITH PASSWORD = 'dev2';
CREATE USER dev2 FOR LOGIN dev2;

CREATE LOGIN sup1 WITH PASSWORD = 'sup1';
CREATE USER sup1 FOR LOGIN sup1;

CREATE LOGIN sup2 WITH PASSWORD = 'sup2';
CREATE USER sup2 FOR LOGIN sup2;
```

```
-- dev1
begin
    GRANT SELECT ON "dbo"."carrinho_produto" TO "dev1"
end;
```

Fonte: Do autor.

Figura 6 - Exemplo de visualização do Tech Lead X demais usuários



Visualização Tech Lead

Results | Messages

	id	descricao	valor_padrao	idEstabelecimento	valor_custo	SysStartTime	SysEndTime
1	10	Descrição 1	1.00	2	0.00	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
2	11	Descrição 2	2.00	2	0.00	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
3	12	Descrição 3	3.00	2	0.00	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
4	13	Descrição 4	4.00	3	0.00	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
5	14	Descrição 5	5.00	3	0.00	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
6	15	Descrição 6	6.00	3	0.00	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
7	16	Descrição 7	7.00	4	0.00	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
8	17	Descrição 8	8.00	4	0.00	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
9	18	Descrição 9	9.00	4	0.00	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
10	19	Descrição 10	10.00	4	0.00	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999

Visualização dos demais

Results | Messages

id	descricao	valor_padrao	idEstabelecimento	valor_custo	SysStartTime	SysEndTime
10	xxxx	4.29	2	1.43	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
11	xxxx	4.37	2	1.01	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
12	xxxx	3.36	2	1.46	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
13	xxxx	3.82	3	1.57	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
14	xxxx	5.26	3	2.90	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
15	xxxx	2.01	3	1.05	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
16	xxxx	8.92	4	1.87	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
17	xxxx	8.81	4	1.00	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
18	xxxx	8.78	4	1.78	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999
19	xxxx	6.62	4	1.45	2022-04-09 17:27:26.4928334	9999-12-31 23:59:59.9999999

Fonte: Do autor.

Após a criação dos perfis de acesso, apenas o Tech Lead obtém a visualização completa dos dados, os demais conseguem apenas visualizar os dados mascarados conforme o mascaramento definido (Figura 6). Com isso, foi possível prevenir o acesso não autorizado a dados sensíveis na empresa.

3.1.2.2 AUTENTICAÇÃO DE SERVIDOR SQL

A *feature sql server authentication* está ligada ao controle de acesso ao banco de dados por parte do usuário. O SQL Server oferece suporte a dois modos de autenticação, modo de autenticação do Windows e modo misto. Sendo que a autenticação do Windows é o padrão e geralmente é chamada de segurança integrada porque esse modelo de segurança do SQL Server é totalmente integrado ao Windows. Já o modo misto oferece suporte à autenticação pelo Windows e pelo SQL Server, onde os pares de nome de usuário e senha são mantidos (MICROSOFT 2018a).

Como a empresa em questão já utilizava a autenticação do Windows que é a recomendada pela Microsoft, não foi necessário realizar nenhum procedimento.

3.1.2.3 SEGURANÇA DA CAMADA DE TRANSPORTE

A *feature transport layer security* (TLS) disponível no SQL Server, está ligada com a questão de criptografia, sendo que O TLS é um protocolo de comunicação, e

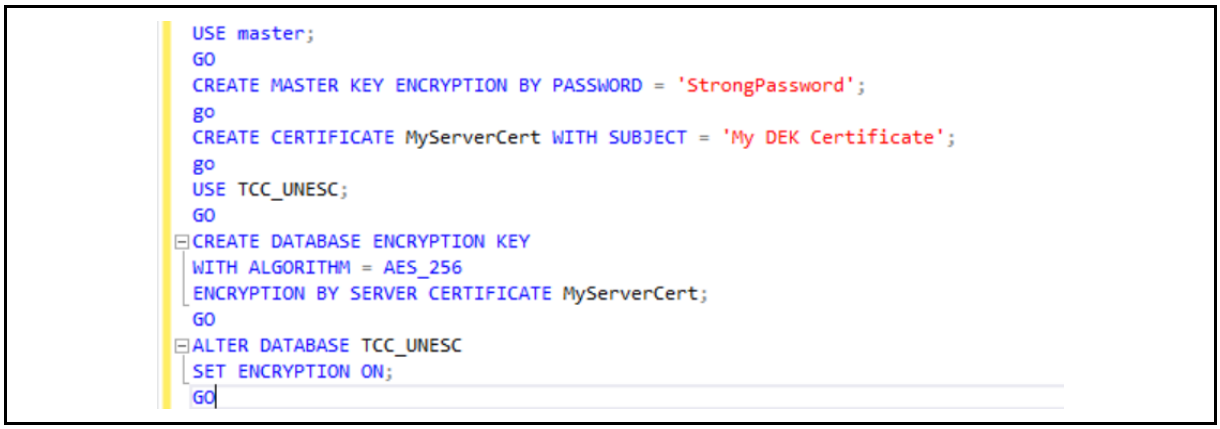
pode ser usado para validação de servidor quando uma conexão de cliente solicita criptografia. Se a instância do SQL Server estiver sendo executada em um computador ao qual foi atribuído um certificado de uma autoridade de certificação pública, a identidade do computador e a instância do SQL Server serão emitidas pela cadeia de certificados que leva à autoridade raiz confiável. Essa validação de servidor exige que o computador no qual o aplicativo cliente está sendo executado seja configurado para confiar na autoridade raiz do certificado que é usado pelo servidor (MICROSOFT 2021d). Habilitando o protocolo TLS foi aumentada a segurança dos dados transmitidos pelas redes.

3.1.2.4 CRIPTOGRAFIA DE DADOS TRANSPARENTE

A *feature transparent data encryption* (TDE) é responsável por criptografar os arquivos de dados SQL Server, sendo conhecida como criptografia de dados em repouso (MICROSOFT 2021e), servindo para proteger os dados mesmo que mídias físicas sejam perdidas ou que os dados por algum motivo sejam descartados incorretamente.

Conforme demonstrado na figura 7, a TDE realiza a criptografia e a descriptografia de entrada e saída em tempo real dos arquivos de log e de dados, usando uma DEK (chave de criptografia de banco de dados).

Figura 7 - Exemplo de visualização do Tech Lead X demais usuários



Fonte: Do autor.

O registro de inicialização do banco de dados armazena a chave para disponibilidade durante a recuperação, sendo que O DEK é uma chave simétrica, e é protegido por um certificado que o banco de dados mestre do servidor armazena ou por uma chave assimétrica que o módulo EKM (gerenciamento extensível de chaves) protege.

A figura 7 demonstra ainda um exemplo de uma série de comandos que possibilita a utilização da TDE, conforme criado na base de dados da empresa, sendo necessário executar os seguintes procedimentos:

1. Criar uma chave mestra (CREATE MASTER KEY) e atribuir uma senha a chave.
2. Criar um certificado que será protegido pela chave mestra (CREATE CERTIFICATE).
3. Criar uma chave de criptografia de banco de dados (CREATE DATABASE ENCRYPTION KEY), e protegê-la com o certificado criado anteriormente.
4. Definir o banco de dados que será utilizada a criptografia (ALTER DATABASE .... SET ECRYPTION ON).

3.1.3 CATEGORIA DE DETECÇÃO

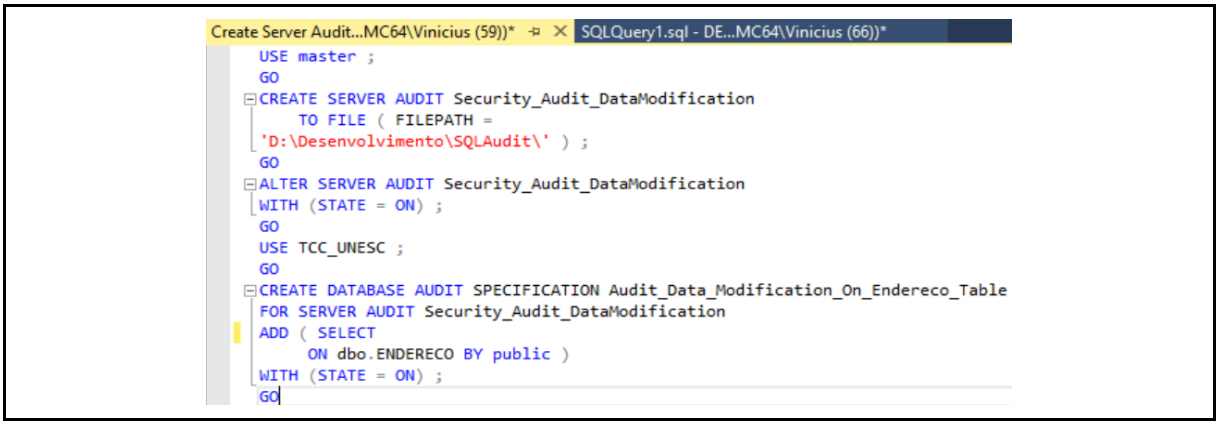
Notícias e relatórios sobre vazamentos de dados têm surgido com uma frequência cada vez maior. As estatísticas mostram um volume enorme de dados vazados nos últimos anos. Além do número e da frequência dos vazamentos, outro aspecto estarrecedor e o impacto dos dados vazados, como o reprojeto de dezenas (e até centenas) de sistemas, como ocorreu recentemente nos EUA devido ao caso de vazamento da Equifax (NG 2019).

Tendo em vista esse cenário, apesar da empresa adotar medidas preventivas de segurança, não é possível eliminar totalmente um possível vazamento de dados, portanto se faz necessário que a organização possua mecanismos que ajudem a detectar atividades fora do comum, e consiga monitorar comportamentos suspeitos.

3.1.3.1 AUDITORIA DE SERVIDOR SQL

A *feature sql server audit* envolve o controle e o registro em log dos eventos que ocorrem no Mecanismo de Banco de Dados, também permitindo criar auditorias de servidor, que podem conter especificações de auditoria de servidor para eventos no nível de servidor, além de especificações de auditoria de banco de dados para eventos no nível de banco de dados (MICROSOFT 2021f).

Figura 8 – Exemplo de comando para criação de auditoria a nível de servidor



Fonte: Do autor.

Na empresa em questão, foram criadas auditorias de servidor para os usuários de desenvolvimento e analista de suportes. A Figura 8 exemplifica os comandos necessários para criar uma auditoria de servidor (CREATE SERVER AUDIT), a habilitação da auditoria (ALTER SERVER...STATE=ON), e em seguida a criação de uma auditoria de banco de dados que audita as instruções SELECT por usuários da função *public* (função padrão quando cria-se novos usuários) e para todos os objetos que estão presentes no esquema (endereco) e no banco de dados em questão (TCC_UNESC).

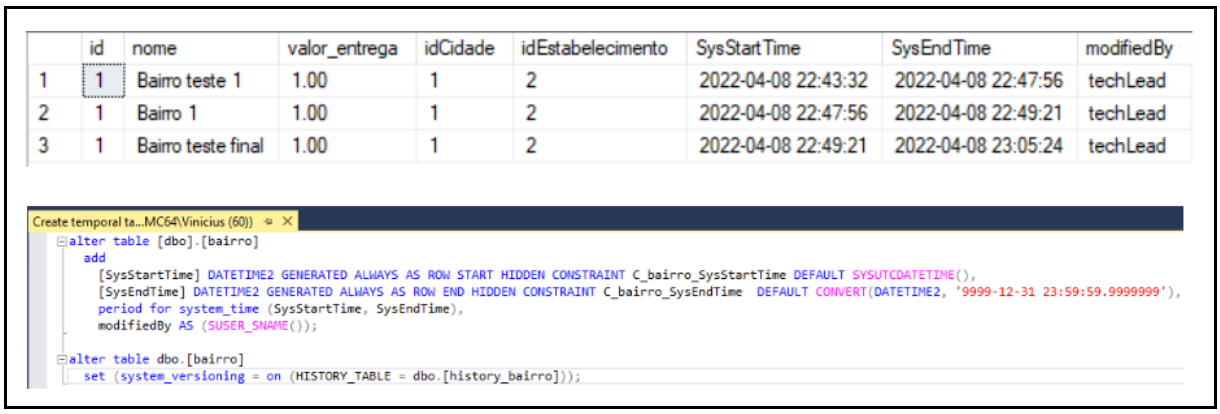
3.1.3.2 TABELAS TEMPORAIS DO SERVIDOR SQL

O SQL Server 2016 introduziu o suporte para a *feature sql server temporal tables* (também conhecidas como tabelas temporais com versão do sistema) como um recurso de banco de dados que oferece suporte interno para fornecer informações sobre os dados armazenados na tabela em qualquer ponto no tempo, em vez de apenas os dados que estão corretos atualmente (MICROSOFT 2021g).

Para que uma tabela temporal seja nomeada como tabela temporal com versão de sistema, ela deve ser um tipo de tabela de usuário e criada para manter um histórico completo de alterações de dados, permitindo uma análise simplificada, com período de validade para cada linha e que é gerenciado pelo sistema (SGBD). Cada tabela temporal possui duas colunas com o tipo de dados datetime2, que são chamadas de colunas de período, sendo usadas pelo sistema para gravar o período de validade de cada linha, sempre que uma linha sofre alteração.

Além disso, cada tabela temporal possui uma referência à outra tabela, em um esquema espelhado (conhecida como tabela de histórico), pois quando uma linha sofre alteração, seja exclusão ou edição, o sistema automaticamente, usa essa tabela para armazenar a versão anterior da linha. A Figura 9 demonstra a visualização obtida através da tabela histórico de bairro após duas atualizações de determinado registro na tabela principal.

Figura 9 – Exemplo de visualização e criação de uma tabela temporal



	id	nome	valor_entrega	idCidade	idEstabelecimento	SysStartTime	SysEndTime	modifiedBy
1	1	Bairro teste 1	1.00	1	2	2022-04-08 22:43:32	2022-04-08 22:47:56	techLead
2	1	Bairro 1	1.00	1	2	2022-04-08 22:47:56	2022-04-08 22:49:21	techLead
3	1	Bairro teste final	1.00	1	2	2022-04-08 22:49:21	2022-04-08 23:05:24	techLead

Fonte: Do autor.

Ainda demonstra um exemplo de criação de tabela temporal para a tabela bairro, onde foi necessário alterar a tabela principal adicionando os campos *SysStartTime, SysEndTime, period e modifiedBy.* Após adicionar os campos necessários para utilizar a *feature*, é necessário ativar o versionamento da tabela (HISTORY_TABLE = dbo.HISTORY_BAIRRO), inserindo o nome da tabela que servirá de histórico. Com isso, foram adicionadas tabelas temporais para todo o banco de dados da empresa, que servirá para auditorias.

3.1.3.3 AVALIAÇÃO DE VULNERABILIDADE SQL

Conforme já mencionado no item de avaliação (3.1.1.2), a *feature sql vulnerability assessment* é um serviço que fornece visibilidade ao seu estado de segurança e que consegue emitir relatórios detalhados, que auxiliam na categoria de detecção da LGPD, e conforme acordado com a empresa, a princípio o relatório será emitido uma vez por mês.

4 RESULTADOS E DISCUSSÕES

Neste trabalho, foram analisados os impactos da LGPD em uma empresa do setor tecnológico da região de Criciúma/SC. A maior dificuldade encontrada ao realizar a implementação foi o levantamento de dados pessoais, o qual levou vários dias por conta da quantidade de tabelas presentes no banco de dados da empresa.

Outra deficiência identificada foi na hora de criptografar os dados, o mecanismo disponível pela Microsoft, o *dynamic data masking* (3.1.2.1), apenas fornece o mascaramento a nível dinâmico, ou seja, backups por exemplo, não estão cobertos pelo mascaramento. A Microsoft fornecia a *feature static data masking*, que consistia no mascaramento a nível de banco de dados, e não apenas na hora de consultar os dados das tabelas. Porém na versão atual do SGBD que a empresa utiliza (v18.11.1), a *feature* em questão foi removida. Com isso, se alguma pessoa má intencionada, tiver acesso aos backups realizados pela empresa, terão acesso às informações reais do banco de dados.

Além disso, a *feature dynamic data masking* não protege o banco de dados contra consultas AD-HOC, que consistem em permitir com que o próprio usuário consiga gerar consultas conforme sua necessidade, podendo adicionar cláusulas WHERE que cheguem no resultado esperado. Por conta disso, se fez necessário a criação da auditoria, que consiste no monitoramento do que cada usuário faz no banco de dados, fazendo com que caso haja algum vazamento de dados dentro da empresa, seja possível identificar se houve algum comando mal-intencionado executando dentro do SGBD e possibilitando qual usuário realizou o comando.

Após muitas reuniões e consultas nos referenciais teóricos, foram encontradas algumas soluções, como criar scripts que fazem o mascaramento do banco de dados antes do backup, porém por conta do tempo estipulado, a única solução viável encontrada, foi deixar os acessos de inteira responsabilidade do tech lead, fazendo com que apenas ele consiga realizar os backups utilizá-los.

Apesar disso, durante a realização da implementação, o sistema se comportou corretamente, não apresentando nenhum problema e garantindo a segurança dos dados armazenados.

Na tabela abaixo (Tabela 1) demonstra os valores do banco de dados anteriores a pseudoanonimização e os dados já pseudoanonimizado (Tabela 2).

Tabela 1 – Exemplo de visualização antes da pseudoanonimização

ID	NOME	DESCRIÇÃO	VALOR_TOTAL

1	Nome 1	Descrição 1	1.54
2	Nome 2	Descrição 2	10.54
3	Nome 3	Descrição 3	20.98
4	Nome 4	Descrição 4	65.87

Fonte: Do autor.

Tabela 2 – Exemplo de visualização após a pseudoanonimização

ID	NOME	DESCRIÇÃO	VALOR_TOTAL
1	XXXX	XXXX	0.00
2	XXXX	XXXX	0.00
3	XXXX	XXXX	0.00
4	XXXX	XXXX	0.00

Fonte: Do autor.

Com os mecanismos presentes no SGBD aplicados no banco de dados da empresa, foi possível aumentar o nível de segurança, porém apesar disso, vazamentos de dados podem acontecer, além do nível de segurança aumentado, foi adicionado uma auditoria sobre os usuários que possuem permissão no banco de dados, fazendo com que seja possível identificar o motivo de um possível vazamento de dados.

5 CONCLUSÃO

No presente artigo foi acompanhado a implementação parcial da LGPD em uma empresa de tecnologia da região de Criciúma/SC. O processo de implementação gerou muitas dúvidas por ser uma lei relativamente nova e com poucos detalhes, além de possuir pouco referencial teórico nacional relacionado à implementação da lei dentro de um banco de dados. Porém as dúvidas puderam ser sanadas com o auxílio dos artigos levantados.

Dada a complexidade da lei, se fez necessário várias reuniões com a equipe para que fosse possível sanar todas as dúvidas levantadas ao longo do processo e possibilitar a compreensão de todas as normas da lei. Após a compreensão da lei e suas dificuldades, foi possível elencar quais as informações que são consideradas pessoais com RG, CPF, cartões de crédito, endereço, e-mail, telefone etc.

Apesar do curto período para implementação da LGPD no banco de dados da empresa, foi possível implementar todos os requisitos levantados, e isso se deu

através dos mecanismos já existentes no SGBD e por conta da documentação bem elaborada pela própria Microsoft, que facilitou a implementação dos mecanismos no banco de dados da empresa. Além disso, a empresa se mostrou bem interessada no processo e foi bem ágil quanto às informações necessárias para a execução dos requisitos levantados.

Um dos pontos mais complicados para o sucesso da implementação da LGPD na empresa, foi a necessidade da mudança de hábitos e rotinas antigas dos colaboradores, como por exemplo a remoção dos privilégios dos usuários que não sejam o tech lead. Antes qualquer funcionário conseguia atualizar e ter acesso às informações sensíveis no banco de dados, agora com a centralização disso, o processo se tornou burocrático, pois é necessário que o responsável (tech lead) aprove e realize as alterações necessárias. Apesar da burocracia envolvida, a segurança do banco de dados foi aumentada.

Até a conclusão do presente trabalho, não foi perceptível algum tipo de evolução imediata por parte dos clientes ou colaboradores após a implementação da LGPD na empresa.

Para trabalhos futuros recomenda-se a implementação do mascaramento estático de dados (a nível de banco de dados) que fora uma das ferramentas removidas pelo SGBD da Microsoft, porém se faz importante por conta do mascaramento a nível de banco de dados incluir backups, fazendo com que tenham seus dados anonimizados, aumentando ainda mais a segurança do banco de dados. Além disso, também é recomendado o levantamento de referencial teórico sobre a GDPR, devido às diferenças encontradas o regulamento da União Europeia entre a LGPD, e por conta da escassez de conteúdos desse tipo implementados nos SGBD das empresas.

REFERÊNCIAS

Asanka, D (2021). "Dynamic Data Masking in SQL Server", disponível em: https://www.sqlshack.com/dynamic-data-masking-in-sql-server-2/, acessado em outubro de 2021.

BOFF, Salete Oro; FORTES, Vinícius Borges. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. Sequência (Florianópolis), p. 109-127, 2014.

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. Revista Direitos Sociais e Políticas Públicas–Unifafibe, v. 8, n. 2, 2020.

BRASIL. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados

DE ALMEIDA, Ana Carolina Brito et al. LGPD em Ambientes de Bancos de Dados nas Organizações. Sociedade Brasileira de Computação, 2019.

DE, LEI GERAL DE PROTEÇÃO. DADOS PESSOAIS (LGPD). 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 2011.

GK, Ravi Kumar; RABI, B. Justus; MANJUNATH, T. N. A study on dynamic data masking with its trends and implications. International Journal of Computer Applications, v. 38, n. 6, p. 19-24, 2012.

Gupta, R (2018). "Static Data Masking in SSMS 18", disponível em: https://www.sqlshack.com/dynamic-data-masking-in-sql-server-2/, acessado em outubro de 2021.

Gupta, R (2021). "Grant, With Grant, Revoke and Deny statements in SQL Server and Azure SQL Database", disponível em: https://www.sqlshack.com/grant-with-grant-revoke-and-deny-statements-in-sql-server-and-azure-sql-database/, acesso em outubro de 2021.

Larsen, G (2021). "SQL Server Security – Fixed server and database roles", disponível em: https://www.red-gate.com/simple-talk/databases/sql-server/database-administration-sql-server/sql-server-security-fixed-server-and-database-roles, acessado em outubro de 2021.

Microsoft (2021c). "Máscara de Dados Dinâmicos", disponível em: https://docs.microsoft.com/pt-br/sql/relational-databases/security/dynamic-data-masking?view=sql-server-ver15, acessado em outubro de 2021.

Microsoft (2021d). "Habilitar conexões criptografadas com o Mecanismo de Banco de Dados", disponível em: https://docs.microsoft.com/pt-br/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15, acessado em outubro de 2021.

Microsoft (2021e). "Criptografia de Dados Transparente (TDE)", disponível em: https://docs.microsoft.com/pt-br/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver15, acessado em outubro de 2021.

Microsoft (2021f). "Auditoria do SQL Server (Mecanismo de Banco de Dados)", disponível em: https://docs.microsoft.com/pt-br/sql/relational-

databases/security/auditing/sql-server-audit-database-engine?view=sql-server-ver15, acessado em outubro de 2021.

Microsoft (2021g). "Tabelas temporais", disponível em: https://docs.microsoft.com/pt-br/sql/relational-databases/tables/temporal-tables?view=sql-server-ver15, acessado em outubro de 2021.

Microsoft (2021a). "Descoberta e classificação de dados SQL", disponível em: https://docs.microsoft.com/pt-br/sql/relational-databases/security/sql-data-discovery-and-classification?view=sql-server-ver15&tabs=t-sql, acessado em outubro de 2021.

Microsoft (2021b). "A avaliação de vulnerabilidades do SQL ajuda a identificar vulnerabilidades de banco de dados", disponível em: https://docs.microsoft.com/pt-br/azure/azure-sql/database/sql-vulnerability-assessment?tabs=azure-powershell, acessado em outubro de 2021.

Microsoft. (2018a) “Autenticação no SQL Server”, disponível em: https://docs.microsoft.com/pt-br/previous-versions/dotnet/framework/data/adonet/sql/authentication-in-sql-server, acessado em outubro de 2021.

Microsoft. (2020a) “SQL Server and Azure SQL Database GDPR Guidance”, disponível em: https://www.intelogy.co.uk/wp-content/uploads/2020/10/SQL-Server-GDPR-Guidance-Paper.pdf, acessado em outubro de 2021.

MIRAGEM, Bruno. A lei geral de proteção de dados (lei 13.709/2018) e o direito do consumidor. Revista dos Tribunais, v. 1009, 2019.

Neves, T (2016). "SQL Server 2016 – Always Encrypted", disponível em: https://www.tiagoneves.net/blog/sql-server-2016-always-encrypted/, acessado em outubro de 2021.

Ng, A (2019). "Thanks to Equifax breach, 4 US agencies don't properly verify your data, GAO finds", disponível em: https://www.cnet.com/news/after-equifax-breach-some-us-agencies-arent-properly-protecting-americans-data/, acessado em outubro de 2021.

Pessoais (LGPD). Brasília, DF, ago 2018.

REGULATION, General Data Protection. General data protection regulation (GDPR). Intersoft Consulting, Accessed in October, v. 24, n. 1, 2018.

SANSANA, Alexandre Gomes. Privacidade, consentimento, legítimo interesse e a nova Lei Geral de Proteção de Dados Pessoais. 2018.