CAPÍTULO 25

SGBD (SISTEMA DE GERENCIAMENTO DE BANCO DE DADOS) NA PERPECTIVA DA LGPD (LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS)

Data de aceite: 01/09/2023

Josias Fellipe Arnold
Centro Universitário de Brusque - UNIFEBE

Hannelore Nehring
Centro Universitário de Brusque - UNIFEBE

Cláudio Ratke
Centro Universitário de Brusque - UNIFEBE

RESUMO: A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018 dispõe sobre o tratamento de dados pessoais, seja por meios digitais, por pessoa natural ou jurídica. Foi promulgada para proteger os direitos fundamentais de liberdade, privacidade e livre formação de personalidade de cada indivíduo, fazendo com que as empresas se preocupem com a coleta, processamento e armazenamento de dados, garantindo sua adequação ao que requer a lei. Na sua essência, a LGPD é um novo conjunto de regras destinadas a dar aos cidadãos brasileiros mais controle sobre esses dados pessoais que são usados pelas organizações. Nesse contexto, o objetivo central desse trabalho foi realizar um estudo sob a ótica dos requisitos de configuração para um SGBD (Sistema gerenciador de Banco de dados), avaliando a consonância dos mecanismos de segurança utilizados em sua proteção, perante os requisitos da LGPD para proteção dos dados pessoais armazenados. Com base na análise realizada, foi sugerido melhorias para os mecanismos de segurança avaliados que necessitam de revisão, para que fiquem de acordo com o que a LGPD requer.

PALAVRAS-CHAVE: LGPD. Base de Dados. Mecanismos de Segurança.

DMS (DATABASE MANAGEMENT SYSTEM) IN THE OVERVIEW OF THE LGPD (GENERAL DATA PROTECTION LAW)

ABSTRACT: The General Law for the Protection of Personal Data (LGPD), Law No. 13,709, of August 14, 2018, provides for the processing of personal data, whether by digital means, by natural or legal person. It was enacted to protect the fundamental rights of freedom, privacy and free personality training of each individual, causing companies to worry about the collection, processing and storage of data, ensuring its suitability to what the law requires. In essence, the LGPD is a new set

of rules designed to give Brazilian citizens more control over this personal data that is used by organizations. In this context, the central objective of this work was to conduct a study from the perspective of the configuration requirements for a DBMS (Database Manager System), evaluating the consonance of the security mechanisms used in its protection, in view of the requirements of the LGPD for the protection of stored personal data. Based on the analysis performed, improvements to the evaluated safety mechanisms that need review have been suggested, so that they are in line with what the LGPD requires
KEYWORDS: LGPD. Database. Security Mechanisms.

1 | INTRODUÇÃO

Com o desenvolvimento de novas tecnologias, a interação contínua entre dispositivos e pessoas agilizam o processo de troca de informações, gerando uma grande quantidade de dados que estão sendo armazenados e processados de modo que questões sobre segurança da informação sejam levantadas (RAPOSÔ, 2019).

A LGPD é um novo paradigma, pois envolve a maneira como as empresas lidam com os dados pessoais nos meios online e offline, tendo a função de proteger os direitos de liberdade e privacidade em qualquer relacionamento que envolva dados pessoais (SÁ, 2019).

Entre as novidades trazidas pela legislação está o princípio da segurança, que determina a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais. Contudo, a implementação de sistemas seguros envolve desafios, que não são apenas questão de implementação do sistema, mas também o fator humano (SÁ, 2019).

É importante que as empresas ajustem suas tecnologias para se enquadrar a Lei Geral de Proteção dos dados Pessoais e consequentemente garantir ao usuário plena consciência sobre a forma que os seus dados estão sendo armazenados e utilizados (RAPOSÔ, 2019).

Elas devem estar preparadas para classificar, proteger e rastrear as informações pessoalmente identificáveis sobre os usuários, à medida que essas passam por seus ambientes de armazenamento, fazendo com que as empresas tenham que avaliar suas práticas de gerenciamento de dados, minimizando sua exposição no tratamento de dados pessoais e mantendo apenas aqueles necessários para atender às necessidades comerciais e legais (BHS, 2020).

Como prática recomendada, devem usar políticas de armazenamento que identifiquem instâncias de dados pessoais, excluam, criptografem e/ou movam os dados para locais mais seguros, que sejam totalmente rastreáveis (BHS, 2020).

Com a entrada em vigor da LGPD, as empresas devem garantir que os dados pessoais sejam coletados, armazenados e gerenciados de forma correta, protegendo-os do uso indevido. A não proteção desses dados, pode fazer com que fiquem expostos e sofram vazamentos, levando a empresa detentora sofrer penalizações junto a ANPD, assim

como perder sua credibilidade perante o mercado, clientes, fornecedores e colaboradores.

Dessa forma, faz-se necessário que a base de dados dos sistemas de informação estejam em consonância perante os requisitos da LGPD, pois armazena dados pessoais de clientes, fornecedores, transportadores, representantes e o acesso ao sistema dos colaboradores que o utilizam.

Ao fim do estudo, será descrito o levantamento realizado na empresa, assim como as sugestões de melhorias para os processos avaliados. Pretende-se que os pontos de avaliação aqui citados e suas melhorias possam ser considerados pelas empresas, e que sirvam de base para os estudos e empresas que buscam se adequar a LGPD dentro do mesmo contexto.

2 | REFERENCIAL TEÓRICO

Este capítulo será destinado a toda literatura envolvida no processo da análise deste estudo de caso, com uma abordagem sobre os principais conceitos da LGPD, armazenamento de dados e alguns dos principais mecanismos de proteção a base de dados, tais como criptografia, controle de acesso, auditoria de log e a segurança física da base de dados.

2.1 LGPD

A Lei n° 13.709/2018 A Lei Geral de Proteção de Dados Pessoais é uma lei federal, sancionada no governo do ex presidente Michel Temer em 2018. Foi criada com base no Regulamento Geral sobre a Proteção de Dado, regulamento do direito sobre a privacidade e proteção dos dados pessoais, aplicável a todos os indivíduos na União Europeia (MACIEL, 2019).

O texto institui um marco regulatório da proteção de dados pessoais e privacidade no Brasil. No entanto, após uma série de debates no Congresso Federal, ficou determinado que as sanções administrativas e multas previstas na LGPD entraram em vigor a partir de 1º de agosto de 2021.

O Brasil possui diversas leis e diretrizes que tratam a proteção e privacidade dos dados, como o Marco Civil da Internet, Código do Consumidor, criando um cenário com diversas legislações e uma estrutura legal complexa. A LGPD substitui esse cenário complexo com muitas diretrizes, leis, e traz uma regulamentação específica para o uso, proteção e transferência de dados pessoais no Brasil. (SÁ, 2019).

Antes da implementação da LGPD no Brasil, o uso indevido dos dados não tinha uma legislação específica, sendo monitorados pelos fundamentos normativos do direito à vida e intimidade. O regulamento visa dar às pessoas maiores poderes sobre seus dados e tornar as empresas mais transparentes na forma como lidam com os dados pessoais (BHS, 2020).

De acordo com art. 1º da LGPD:

> A lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Segundo Pinheiro (2021), o espírito da lei é proteger os direitos básicos de liberdade e privacidade e o livre desenvolvimento da personalidade das pessoas físicas. Ela fornece um pré-requisito de honestidade e credibilidade para todos os tipos de processamento de dados pessoais. Agora, o processamento de informações pessoais deve estar em conformidade com uma série de aspectos, na vida do uso da informação: Usar informação dentro do ciclo que identifique ou possa identificar uma pessoa e é relevante para ela, incluindo categorias de dados sensíveis.

O art.5 da LGPD estabelece que tipos de dados são informações que identificam a identidade direta do titular ou tornam a identidade de uma pessoa natural identificável, como dados pessoais e qualquer procedimento realizado com esses dados, tais como coleta, uso, acesso, transmissão, processamento, arquivamento, armazenamento e transferência (BRASIL, 2018).

O Quadro 1 traz a definição de dado pessoal, dado pessoal sensível e dado anonimizado.

Conceito	Definição
Dado Pessoal	Qualquer dado relacionado a pessoa natural diretamente identificada ou identificável, tais como: nome, sobrenome, data de nascimento, CPF, RG, CNH, carteira de trabalho, passaporte, título de eleitor, sexo, endereço, e-mail, telefone.
Dado Pessoal Sensível	Se refere a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico. Esses dados merecem proteção mais rigorosa, com consentimento específico dos titulares de dados.
Dado Anonimizado	Qualquer dado relativo a um indivíduo que não permita ser identificado, considerando os meios técnicos disponíveis no momento do tratamento. O dado perde a possibilidade de associação direta ou indireta a um indivíduo, tal como as estatísticas sobre a idade de pessoas que compraram determinado produto.

Quadro 1 – Conceito de tipos de dados e suas definições.

Fonte: Adaptado de Donda (2020).

No art.5 da Lei nº 13.709, tem-se a definição de quem é o titular, encarregado e os agentes responsáveis pelo tratamento de dados (controlador e operador).

- Titular: Indivíduo possuidor dos dados, que são os objetos de tratamento. Em um formulário de cadastro, quando preencho meus dados pessoais para serem armazenados, mesmo em posse da empresa, eu continuo sendo o titular dos dados.

- Encarregado: Pessoa indicada pelo controlador e operador, que atua como canal de comunicação entre as partes (controlador, os titulares e a ANPD).
- Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O controlador possui relação direta com o titular, devendo adotar medidas de boas práticas de segurança e governança para que o tratamento de dados estejam em conformidade com as diretrizes da LGPD.
- Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

A Figura 1 relaciona cada um dos sujeitos envolvidos no tratamento de dados e o vínculo existente entre eles.

Figura 1 – Sujeitos envolvidos no tratamento de dados.

Fonte: SEBRAE (2020).

A LGPD relaciona o cumprimento de obrigações e responsabilidades ao papel exercido nas atividades de tratamento de dados. O Quadro 2 descreve algumas dessas responsabilidades, assim como o responsável por elas.

Responsável (eis)	Responsabilidade	Dispositivo (LGPD)
Controlador	Provar que houve o consentimento do titular dos dados e informar o mesmo a respeito de alterações do consentimento para tratamento de dados, com destaque de forma específica do teor das alterações, quando se tratar de mudança de finalidade, prazo, controlador e do compartilhamento dos dados.	§ 2º e § 6º do Art. 8º
	Adotar medidas para garantir a transparência do tratamento de dados e dar acesso ao relatório de impacto à proteção de dados pessoais à ANPD, quando requerido.	§ 2º e § 3º do Art. 10
	Fornece ao titular dos dados pessoais, mediante requisição a confirmação da existência de tratamento de dados, bem como, acesso, correção e ainda a anonimização, bloqueio ou eliminação desses dados, observadas as disposições da LGPD.	Art. 18
	Elaborar relatório de impacto à proteção de dados pessoais.	Art. 38
	Elaborar instruções para o tratamento de dados feitos por operador, observando as próprias regras e as normas sobre a matéria.	Art. 39
	Nomear o encarregado, salvo nas hipóteses de dispensa, a critério da ANPD.	Art. 41
	Comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.	Art. 48
Controlador e Operador	Adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e inclusive, da eficácia dessas medidas.	Art. 6º, inciso X
	Manter registro das operações de tratamento de dados pessoais que realizarem.	Art. 37
	Reparar o titular dos dados quando, em razão do tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, observadas as demais disposições legais.	Art. 42
	Adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.	Art. 46
	Formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.	Art. 50
Operador	Realizar o tratamento segundo as instruções fornecidas pelo controlador.	Art. 39
Encarregado	Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.	Art. 41
	Receber comunicações da autoridade nacional e adotar providências.	
	Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.	

Quadro 2 – Responsáveis e suas obrigações no tratamento de dados.

Fonte: Adaptado de Scherer (2020).

No art.6 da LGPD, se encontra dez princípios de boa-fé que se pode levar em consideração no tratamento de dados pessoais. O Quadro 3 relaciona esses princípios e suas definições (BRASIL, 2018).

Princípio	Definição
Finalidade	Propósito legítimo da coleta e do tratamento de dados informados ao titular. Para o tratamento e uso dos dados é preciso existir um motivo para aquele dado ser tratado.
Adequação	O tratamento deve ser compatível com a finalidade. Se os dados forem coletados não tiverem uma relação lógica com a finalidade, o dado não é para aquela finalidade.
Necessidade	Limitar o tratamento ao mínimo necessário. Esse princípio garante que os dados não sejam tratados de forma desnecessária.
Livre acesso	Garantir aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.
Qualidade de dados	Exatidão, clareza e relevância dos dados de acordo com a necessidade e para cumprir a finalidade de seu tratamento.
Transparência	Garantir aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.
Segurança	Adotar medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
Prevenção	Os detentores dos dados devem tomar medidas para que nenhum dado seja acessado, alterado ou ocasionar a ocorrência de dados em virtude do tratamento realizado.
Não Discriminação	Não permitir a realização do tratamento para fins discriminatórios ilícitos ou abusivos.
Responsabilização	Demonstrar a adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção de dados pessoais e da eficácia dessas medidas.

Quadro 3 – Princípios da LGPD e suas definições.

Fonte: Adaptado de Brasil (2018).

2.2 Armazenamento de dados

O conceito de armazenamento de dados é amplo, partindo do princípio que existem repositórios tanto físicos quanto digitais, que podem ser usados para garantir a confidencialidade, integridade e acessibilidade das informações.

Portanto, o armazenamento de dados abrange métodos e tecnologias de retenção de informações que permitem operações em todas as fases do ciclo de vida dos dados, desde o armazenamento até o descarte, tais como: bancos de dados, dispositivos de *backup* e armazenamento em nuvem (ROCKCONTENT, 2021).

Banco de dados é um sistema computadorizado de manutenção de registros, com a finalidade geral de armazenar informações e possibilitar as aplicações ter acesso, realizar inserções, alterações e exclusões de dados e arquivos. São compostos por um extenso volume de armazenamento e de processamento, e controlados por um Software

de Gerenciamento do Banco de Dados (SGBD) que permite criação, gerenciamento, visualização e operações por parte do usuário (DATE, 2004).

Controles de acesso são uma combinação de controles de acesso lógico, relacionados a sistemas de informação e controles de acesso físico, implementando uma política de segurança que determina quem pode ter acesso a cada recurso específico do sistema, e o tipo de acesso que é permitido em cada instância. Segundo Donda (2020), pode-se definir controle de acesso como "Prevenção do uso não autorizado de um recurso, incluindo a prevenção do uso de um recurso de maneira não autorizada".

2.3 Acesso

Em um banco de dados, pode-se pensar em adotar uma política de controle de acesso, ditando quais tipos de acessos são permitidos e sob que circunstâncias. O Quadro 4 abaixo, descreve as principais categorias de controle de acessos utilizadas.

Categoria	Definição
Controle de acesso discricionário	Controla acesso com base na identidade do requisitante e em regras de acesso (autorizações) que declaram o que os requisitantes têm (ou não têm) permissão de fazer. Essa política é denominada discricionária porque uma entidade pode ter direitos de acesso que lhe permitem, por sua própria vontade, habilitar outra entidade a acessar algum recurso.
Controle de acesso mandatório	Controla o acesso baseado na comparação de rótulos de segurança (que indicam quão sensíveis ou críticos são os recursos do sistema) com autorizações de segurança (que indicam quais entidades do sistema têm direito de acessar certos recursos). Essa política é denominada obrigatória porque uma entidade que está autorizada a acessar um recurso não pode, apenas por sua própria vontade, habilitar outra entidade a acessar aquele recurso.
Controle de acesso baseado em papéis	Controla o acesso com base nos papéis que os usuários desempenham dentro do sistema e em regras que definem quais acessos são permitidos a usuários em determinados papéis.

Quadro 4 – Categorias de controle de acessos.

Fonte: Adaptado de Stallings; Brown (2014).

Alguns SGBDs fornecem controle sobre os direitos de acesso, que vão desde banco de dados inteiros, tabelas individuais, ou somente determinadas colunas de uma tabela. Essas permissões são em nível de criação, inserção, exclusão, atualização, escrita e leitura (STALLINGS; BROWN, 2014).

2.4 Criptografia

Pode-se definir criptografia como a arte ou ciência de se escrever em cifra ou em códigos, de forma a inibir qualquer acesso não autorizado a dados sigilosos, servindo com um meio de manter a informação confidencial (HINTZBERGEN, 2018).

Segundo STALLINGS, (2010, p.18):

> As mensagens originais a serem criptografadas são conhecidas por texto claro (plaintext), enquanto a mensagem codificada é chamada de texto cifrado

ciphertext). O processo de converter texto claro em cifrado é conhecido como cifragem ou criptografia, enquanto o processo inverso, que restaura o texto claro a partir do texto cifrado é a decifragem ou decriptografia.

O Quadro 5 abaixo, traz a definição de cada uma dessas categorias, suas vantagens, desvantagens e os principais algoritmos de uso.

Categoria	Definição	Vantagens	Desvantagens	Principais Algoritmos
Criptografia simétrica	Este método realiza a cifragem e decifragem de uma informação através de algoritmos que utilizam à mesma chave. Para isso, tanto o emissor quanto o receptor da mensagem devem possuir a mesma chave, pois é a única maneira de obter a confidencialidade.	O processamento necessário para a encriptação e decriptação é menor quando comparado ao da criptografia assimétrica.	Distribuição da chave secreta, que para ser segura precisa ser transmitida através de um canal de comunicação seguro e independente do destinado a comunicação sigilosa.	DES, 3DES, AES.
Criptografia assimétrica	Está pautada no conceito de par de chaves (privada e pública). Uma das chaves é utilizada para cifrar uma informação e a outra para decifrá-la. As mensagens cifradas com uma das chaves do par só podem ser decifradas com a outra chave correspondente. A chave privada deve ser mantida em sigilo, enquanto a chave pública deve ser disponibilizada para os interessados em visualizar a informação em sua íntegra.	O não compartilhamento de chaves, visto que o emissor utiliza a chave pública e o receptor a chave privada.	A utilização de algoritmos reversos para desencriptação acaba por elevar o tempo computacional dos algoritmos, requerendo alto poder computacional e tornando inviável o seu uso em uma comunicação intensa.	RSA, Diffie-Helman, DAS.

Quadro 5 – Categorias de criptografia.

Fonte: Adaptado de HINTZBERGEN (2018).

Com os dois tipos de criptografia descritos tendo suas vantagens e desvantagens, se buscou um método capaz de unir as vantagens de cada um, minimizando assim suas desvantagens. Dessa forma, foi criado um método que realiza a junção dos dois tipos de criptografia, visando compensar o problema do segredo preestabelecido da chave simétrica e o alto poder computacional necessário na chave assimétrica, conforme mostra a Figura 2.

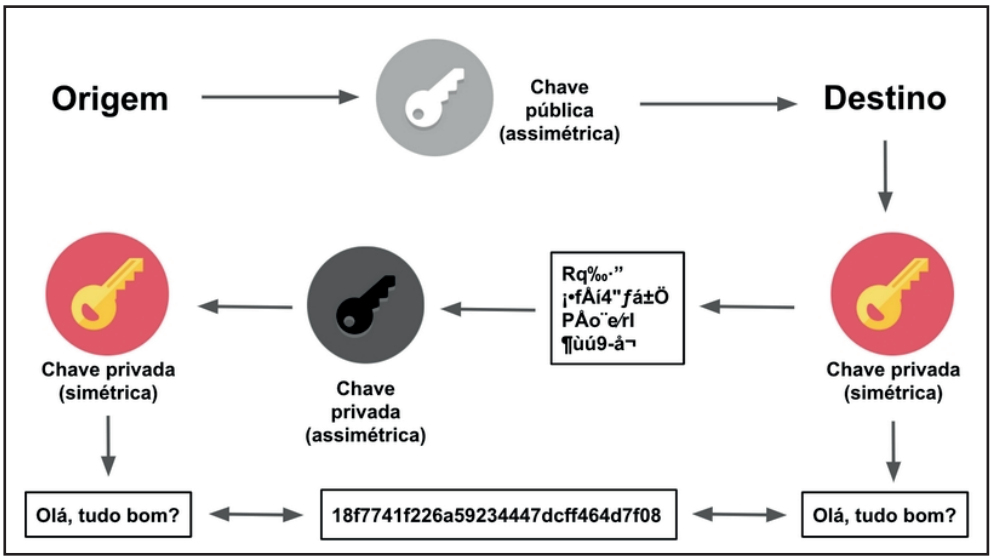

Figura 2 – Combinação de criptografia simétrica e assimétrica

Fonte: Adaptado de UNIVERSIDADE JAVA (2022).

Mesmo que a LGPD em seu texto não recomende ou mencione nada sobre a utilização e aplicação de criptografia, ela é reconhecida como um mecanismo de segurança confiável, e sua utilização é uma boa prática quando se fala em proteção de dados pessoais armazenados, tornando-se um diferencial competitivo, pois empresas que preservam a privacidade preferem negociar com organizações que se mostram atualizadas e preocupadas com a proteção de suas informações (ALMEIDA et al., 2021).

2.5 Auditoria

Pode-se definir log como registro de informações relevantes sobre diversas ocorrências e eventos realizados em um sistema, podendo ser gravado em arquivos de extensões e formatos variados (STALLINGS; BROWN, 2014).

Os bancos de dados costumam armazenar informações confidenciais ou de acesso restrito e que precisam ser mantidas consistentes e íntegras. Dessa forma, arquivos de logs, são ações fundamentais a serem consideradas na implementação de uma auditoria de segurança de banco de dados, registrando quem acessou, alterou, ou excluiu uma informação, e de que forma isso foi realizado. Com base nessa necessidade, diversos SGDBs permitem que sejam armazenadas informações das ações tomadas no sistema com base nos arquivos de log, como eventos de sistema, transações feitas no banco de dados e mudanças de privilégios de usuários (NASCIMENTO, 2011).

Pensando na LGPD, faz-se necessário que as organizações mantenham registro de suas atividades de armazenamento de dados, utilizando para isso métodos como

monitoramento e auditoria das informações pessoais. Em caso de uma ocorrência de segurança, será necessário comunicar a autoridade nacional, e a auditoria de log é um recurso que pode justamente cumprir esse papel, permitindo auditar onde a violação se originou e o que foi acessado ou alterado (DONDA, 2020).

2.6 Segurança física da base de dados

A segurança física corresponde ao uso de ferramentas e equipamentos que permitam uma forma de controle tangível (material) da informação, ou seja: câmeras de vigilância, controle de intrusão, controle de acesso ao meio físico, entre outros, sendo primordial para manter a integridade das informações (REGO, 2011).

As salas de servidores ou *datacenters* contêm equipamentos sensíveis que são vulneráveis à umidade e ao calor, e produzem seu próprio aquecimento. Para evitar isso, o ar tem que ser resfriado, através de equipamentos como ar-condicionado, e o calor produzido pelos equipamentos deve ser dissipado para fora. Também se faz necessário não dispor mais equipamentos na sala sem avaliar se a capacidade de refrigeração é o suficiente (HINTZBERGEN, 2018).

Além disso, um sistema de informação pode parar de funcionar devido a uma falha de energia. As empresas devem estar preparadas para lidar com todas essas situações, mantendo opções de contingência para atenuar essa situação e evitar que a disponibilidade dos servidores seja comprometida, tal como utilização de nobreaks e geradores de longa duração. Em uma situação mais grave, como fogo, deve-se utilizar extintores específicos para materiais elétricos e componentes, porém, as chamas, calor e fumaça podem danificar circuitos e componentes, levando a indisponibilidade do serviço e a perda de informações, caso a base de dados estiver armazenada somente em ambiente interno (HINTZBERGEN, 2018).

Pensando na LGPD, parte do art. 46 diz que se deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição (BRASIL, 2018). Devido aos riscos à segurança física descritos acima, medidas de segurança como disponibilizar backup da base de dados em locais externos, como em nuvem e *data warehouses*, podem ser fundamentais para manter as informações pessoais protegidas e resguardadas, mantendo a integridade e disponibilidade das informações.

3 I PROCEDIMENTOS METODOLÓGICOS

O presente trabalho se caracteriza como um estudo de caso, pois analisou o SGBD utilizado pelo ERP de uma empresa da região, apresentando sugestões de melhorias para os mecanismos que foram avaliados para proteção da base de dados perante a LGPD.

De acordo com GIL (2002, p. 54) o estudo de caso consiste no estudo profundo

e exaustivo de um ou pouco objetos, de maneira que permita seu amplo e detalhado conhecimento, tarefa praticamente impossível mediante outros delineamentos considerados.

Referente aos objetivos, a pesquisa é descritiva, pois descreve a realidade do estudo de caso focado dento do cenário da empresa avaliada, relacionando a necessidade de aplicação das sugestões realizadas.

O trabalho será desenvolvido observando as seguintes etapas:

a)levantamento bibliográfico: realizar o levantamento bibliográfico sobre a LGPD, armazenamento, base de dados e mecanismos de segurança que podem ser aplicados para proteção da base de dados;

b)coleta de dados: elaborar e aplicar uma avaliação da situação atual dos mecanismos de segurança;

c)apresentação: avaliar a situação atual dos mecanismos de segurança analisados, identificando e sugerindo melhorias para os pontos avaliados que não estão em consonância perante os requisitos da LGPD para proteção dos dados pessoais armazenados;

Nessa seção da pesquisa são descritos detalhadamente os passos que foram utilizados e o tratamento destinado aos dados. São detalhados os seguintes itens: abordagem e as ferramentas de coleta dos dados, o universo e a amostra da pesquisa e o tratamento dessas informações (BRASILEIRO, 2013).

3.1 Estudo de caso

Essa seção lista as questões formuladas para avaliar os mecanismos de segurança aplicados à proteção da base de dados do ERP.

Questão	Pergunta	Mecanismo de Segurança
1	Como você avalia a adequação do controle de acesso lógico empregado ao software de SGBD utilizado para acessar o banco de dados do ERP?	Controle de acesso lógico
2	Como você avalia o nível de segurança empregado para manipulação de dados do ERP via SGBD?	Controle de acesso lógico e auditoria de log
3	Como você avalia a adequação de criptografia e anonimização para proteção das colunas que armazenam dados pessoais na base de dados do ERP?	Criptografia e anonimização de colunas
4	Como você avalia a adequação de criptografia aplicada a proteção do backup da base de dados do ERP?	Criptografia de backup
5	Como você avalia a adequação de criptografia aplicada a proteção dos discos de dados do servidor de banco de dados do ERP?	Criptografia de dados em repouso
6	Como você avalia a adequação do controle de acesso ao meio físico, empregado na proteção da infraestrutura de TI, como o servidor da base de dados do ERP?	Controle de acesso ao meio físico

Quadro 6 – Questões e o mecanismo de segurança correspondente.

Fonte: Elaborado pelo Autor (2022).

Essa seção aborda a sugestão de melhoria para cada uma das análises realizadas na seção anterior (4.3.4), com objetivo de que possam atender os critérios utilizados para proteção de dados pessoais.

3.1.1 Questão 1 (Controle de acesso lógico)

O gerente de TI deve ser o único detentor do superusuário, com privilégio total de acesso a todas as operações da administração do SGBD. Recomenda-se alterar a senha utilizada para uma nova, não realizando o compartilhamento com os demais usuários.

Como sugestão, recomenda-se que seja criado um usuário no SGBD para cada um dos integrantes que necessite realizar seu uso pela ferramenta PgAdmin, com os perfis de acesso de cada usuário baseado na política de papéis que cada um exerce perante a organização.

Assim, podem ser criados usuários com perfis somente de consulta e visualização, até usuários com perfis de manipulação de dados, porém, restringindo a funcionalidade em tabelas que armazenam os dados pessoais. O SGBD suporta esses perfis e recursos, sendo de grande valia para garantir a segurança das informações armazenadas.

Nesse cenário os usuários da equipe de TI interna que fazem uso da ferramenta de administração do SGBD, e na empresa responsável pela manutenção ERP, que tem acesso a uma conexão remota, se autenticando em um servidor com acesso à ferramenta, como sugestão, poderiam ser criados grupos de usuários com níveis de acesso baseados em papéis, conforme Quadro 7.

Grupo	Quantidade	Destinatário	Nível de Acesso
Super Usuário	1	Gerente de TI	Permissão total, acesso a todos os recursos do SGBD.
Suporte	2	Analista de Suporte Suporte Empresa de ERP	Permissão para realizar consultas e visualizações.
Analista	2	Analista de TI	Permissão para realizar consultas, visualizações, manipulações e exclusões de dados, com restrição a manutenções e exclusões em tabelas que armazenam dados pessoais.
Infraestrutura	1	Analista de Infraestrutura	Permissão para realizar consultas, geração e restauração de backups e monitoramento do banco de dados e seus serviços.

Quadro 7 – Grupos de usuários e níveis de acesso.

Fonte: Elaborado pelo Autor (2022).

Em uma situação em que algum serviço de manutenção ao banco de dados tenha que ser realizado, requerendo um acesso de superusuário, como sugestão se pode adotar o procedimento do gerente de TI realizar a autenticação ao SGBD com seu usuário, conceder acesso ao responsável pela manutenção via acesso remoto e monitorar o trabalho realizado.

Os usuários e grupos devem ser criados conforme a necessidade da empresa, mas o importante é não deixar espaço para uma violação de segurança, pensando sempre em proteger os dados armazenados.

3.1.2 Questão 2 (Controle de acesso lógico e auditoria de log)

Como sugestão de melhoria aplicada a esse tópico, visando sua consonância aos princípios da LGPD, se sugere ativar a auditoria de log do SGBD para as tabelas que armazenam dados pessoais ou para o banco de dados inteiro. Esse recurso é nativo em alguns SGBDs, requerendo apenas que o DBA responsável pela base de dados do ERP faça sua instalação e configuração.

Com o recurso ativo, se a manipulação de um campo pessoal for realizado em alguma tabela, será possível resgatar o gerenciamento de auditoria do banco de dados e auditar as informações manipuladas, assim como a data, hora e o usuário que realizou as alterações.

Na questão 1, sugerimos a criação de usuários para acesso ao SGBD com base nos papéis que eles exercem dentro da empresa. Essa ação é importante, pois se tivermos apenas um usuário para todos os integrantes do departamento, caso uma manipulação de dados pessoais acontecer, não saberemos qual o usuário que realizou o procedimento, pois o gerenciamento de auditoria teria apenas o registro do superusuário. Dessa forma, vemos a importância da implementação dos dois mecanismos de segurança, visando a atuação em conjunto, onde um determina o acesso dos grupos de usuários aos recursos do SGBD, e o outro, garante que quando uma informação for alterada, se tenha a confiabilidade de saber o que efetivamente foi alterado, quem realizou as alterações e em que momento.

Essa atividade também auxilia na obtenção de relatórios de acesso, que podem ser usados junto as auditorias realizadas.

3.1.3 Questão 3 (Criptografia e anonimização de colunas)

A maioria dos SGBDs possibilitam a utilização de recursos visando realizar a proteção dos dados pessoais armazenados, seja por meios próprios, disponíveis pela própria camada do banco de dados ou aquisição de camadas terceiras que podem ser instaladas e configuradas no SGBD. Um dos recursos nativos que podem ser utilizados é a extensão SGBD, utilizada para aplicação de criptografia em determinadas colunas das tabelas que contém dados pessoais.

Esse método é assimétrico, utilizando uma chave pública para criptografar as colunas e uma chave privada para descriptografar. Após ativação da extensão no banco de dados, todo o gerenciamento dos métodos deve ser realizados pela aplicação de desenvolvimento do ERP, que deve utilizar os métodos para armazenar as informações criptografadas nas colunas com dados pessoais do banco de dados, e utilizar o método

inverso, de descriptografia para apresentar as informações legíveis aos usuários que estejam utilizando o ERP.

Com a uma terceira camadas que pode ser instalada no SGBD, é a camada anonimização do próprio SGBD, que fornece recursos para realizar a anonimização das colunas das tabelas que contém os dados pessoais, através do mascaramento das informações, por meio de técnicas como substituição, codificação parcial, embaralhamento, adição de ruído, entre outras. Sua utilização consiste na aplicação da técnica de anonimização escolhida para as colunas que se deseja mascarar as informações, especificando qual tipo de método será aplicado e para quais usuários do SGBD.

O levantamento realizado considerou as tabelas bases e seus respectivos campos, servindo para frisar a necessidade de proteção dessas informações, porém, cabe a empresa e junto com a empresa de desenvolvimento do ERP, realizar uma análise criteriosa, levantando todas as tabelas relacionadas e o recurso a ser considerado para proteção dessas informações pessoais, decidindo pela aplicação de criptografia ou anonimização, conforme nível de desempenho e segurança ao aplicar os recursos ao desenvolvimento do ERP.

3.1.4 Questão 4 (Criptografia aplicada ao backup)

O SGBD em sua forma nativa não podem não possuir uma ferramenta que permite gerar *backup* criptografado da base de dados, mas, devido a sua versatilidade permite a instalação e configuração de camadas terceiras. Após ser devidamente configurado no servidor de banco de dados, informando a senha a ser utilizada na cifração dos dados, o *backup* é gerado de forma abrangente, podendo ser completo, incremental ou diferencial, sendo criptografado pelo algoritmo simétrico AES-256 antes de ser salvo no diretório de saída configurado.

Caso o backup necessite ser restaurado, é necessário que se conheça a senha do algoritmo utilizado em sua cifragem, garantindo a integridade do *backup* perante um invasor que obtiver acesso não autorizado ao mesmo. Dessa forma, se garante a integridade e confidencialidade das informações armazenadas, visto que o segredo da chave será gerenciado pelo profissional responsável da empresa.

3.1.5 Questão 5 (Controle de acesso ao meio físico)

Como sugestão de melhoria para atender a situação da falta de chaveamento na porta de entrada da sala de data center, a ação mais simples a ser tomada é realizar o chaveamento manual, centralizando a chave somente a um membro do TI interno da TI, que poderia ser o analista de infraestrutura. Dessa forma já se evitaria que pessoas não autorizadas tenham acesso à sala.

Como uma sugestão mais elaborada, poderia ser implementado o controle de acesso

por uso de cartão ou biometria, sendo que somente as pessoas cadastradas poderão acessar o ambiente de infraestrutura da empresa. A vantagem dessa solução perante o controle manual é em relação a segurança e gerenciamento, visto que não se necessitaria centralizar a chave física do ambiente em um membro da equipe.

Aliada a sugestão anterior, se faz necessário manter a gravação do ambiente interno, pois possibilita que se tenha acesso as imagens e vídeos das atividades realizadas pelas pessoas autorizadas dentro do ambiente.

4 | RESULTADOS E DISCUSSÕES

O objetivo deste estudo de caso foi realizar a análise da situação atual da base de dados do ERP, avaliando a consonância dos mecanismos de segurança utilizados em sua proteção, perante os requisitos da LGPD para proteção dos dados pessoais armazenados.

Na primeira etapa do estudo, foi desenvolvida a fundamentação teórica sobre os principais conceitos da LGPD, armazenamento de dados e alguns dos principais mecanismos de segurança voltados a proteção da base de dados, além da apresentação da empresa e a estrutura da base de dados do seu ERP.

Essa etapa permitiu entender a LGPD perante sua legislação, aplicabilidade, princípios e sua importância no tratamento de dados pessoais, conforme sua abordagem no ambiente em que este estudo se encontra inserido.

Na segunda etapa do estudo, foi elaborado um questionário, que compreendeu seis questões construídas para avaliar a adequação do SGBD aos mecanismos de segurança utilizados para proteção da base de dados do ERP, que foram controle de acesso lógico ao software do SGBD, auditoria de log, criptografia e segurança física do servidor. O questionário contou com três opções de resposta, com somente uma opção de escolha, divididos em Adequado, Parcialmente Adequado e Inadequado, sendo direcionado para preenchimento do gerente de TI, que responde oficialmente por todo o setor de informática da empresa, assim como o ERP e sua base de dados. Com base nas questões contidas no questionário, foram realizados o levantamento e análise individual dos mecanismos de segurança abordados dentro do cenário do SGBD.

Essa etapa mostrou que as respostas e comentários realizados pelo gerente colaboram com a análise realizada pelo autor no estudo de caso, mostrando que existe necessidade e oportunidade de melhoria por parte da SGBD aos mecanismos de segurança avaliados, para que se tornem mais robustos e possam conferir maior capacidade de proteção as informações armazenadas na base de dados do ERP, cumprindo assim os requisitos da LGPD empregados a situação avaliada.

Na terceira etapa do estudo, foram sugeridas melhorias a serem consideradas pela empresa para atender os mecanismos de segurança avaliados na etapa anterior, que não estão em consonância com o que a LGPD requer para proteção dos dados pessoais

armazenados na base de dados do ERP.

Essa etapa mostrou que a aplicação das sugestões de melhorias abordadas são importantes para manter os dados pessoais de clientes, fornecedores, transportadores, representantes e o acesso ao sistema dos colaboradores que o utilizam o ERP adequados a LGPD. A adequação dos mecanismos de segurança abordados, se justifica pelos pontos abordados nesse projeto, da empresa transparecer para o mercado sua ética e idoneidade, sendo reconhecida como uma empresa que se preocupa em manter os dados que estão sob sua responsabilidade devidamente protegidos de qualquer vazamento, acesso, manipulação ou exposição indevida, evitando assim as sanções e multas previstas para as empresas que descumprem os princípios da lei.

Dessa forma, espera-se que esse trabalho possa mostrar para as empresas e organizações que a LGPD deve ser tratada como prioridade, pois protege seu bem mais precioso, que são os dados, o principal ativo que as empresas coletam, processam e armazenam.

5 I CONSIDERAÇÕES FINAIS

Diante das informações levantadas nesse estudo, pode-se observar a necessidade de regulamentar os dados pessoais que estão sob controle das empresas. É nesse sentido que a LGPD cumpre parte do seu papel, dispondo sobre a forma correta de realizar esse tratamento.

A lei é nova e abrangente, sofrendo adequações desde sua formulação e trazendo consigo desafios em sua implementação, porém, é importante ressaltar que suas intenções não são de atrasar ou complicar procedimentos e processos que já estão na rotina das empresas, mas sim, tornar o ambiente mais seguro e referência dentro da proteção de dados.

A proposta desse trabalho foi realizar um estudo de caso sobre a situação atual da base de dados do ERP da empresa, avaliando a consonância dos mecanismos de segurança utilizados em sua proteção, perante os requisitos da LGPD para proteção de dados pessoais armazenados. O estudo mostrou que os mecanismos de segurança empregados pela empresa para proteção da base de dados tem necessidade e oportunidade de melhoria, sendo que com a aplicação das sugestões realizadas, pode-se obter maior confidencialidade, integridade, disponibilidade e autenticidade dos dados armazenados.

Embora o estudo tenha focado em apenas uma parte da LGPD, referente aos dados pessoais armazenados pela empresa, a lei dispõe sobre qualquer operação realizada com dados pessoais, passando por coleta, produção, recepção, classificação, utilização, processamento até extração e eliminação. Dessa forma, cabe as empresas a percepção e entendimento da importância da LGPD e a necessidade de sua correta aplicação.

REFERÊNCIAS

Brasil. 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./. Acessado em: 01 mai. 2022.

BHS.[E-BOOK]. **LEI GERAL DA PROTEÇÃO DE DADOS: tudo o que você precisa saber.** Disponível em https://materiais.bhs.com.br/e-book-lgpd?utm_source=site&utm_medium=blog&utm_campaign=materiais/. Acessado em: 01 mai. 2022.

DATE, C.J. **Introdução a Sistemas de Banco de Dados.** 9. ed**.** Rio de Janeiro: Elsevier, 2004.

DONDA, Daniel. **Guia prático da implementação da LGPD: tudo o que sua empresa precisa saber para estar em conformidade.** São Paulo: Labrador, 2020. 144 p.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. São Paulo: Atlas S.A, 2002.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.** Rio de Janeiro: Brasport Livros e Multimídia Ltda., 2018.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/18). Goiânia: RM Digital Education, 2019.

NASCIMENTO, Guilherme de Mattos. **AUDIOLOG: Uma ferramenta para auditoria de banco de dados.** Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) - Universidade Federal de Santa Catarina, 2011. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/184594/audilog%20final.pdf?sequence=-1/. Acessado em: 01 mai. 2022.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18).** Goiânia: RM Digital Education, 2019.

PINHEIRO, Patrícia Peck. **Direito Digital.** 7. ed**.** Saraiva Jur, 2021.

RAPÔSO, Cláudio F L et al. **LGPD-LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO.** Disponível em: https://revistas.cesmac.edu.br/index.php/administracao/article/view/1035/802/. Acessado em: 01 mai. 2022.

REGO, Hugo Bauer. **A importância da Segurança da Informação para os Sistemas de Automação de Unidades de Informação.** Trabalho de Conclusão de Curso (Bacharel em Biblioteconomia) - Universidade Federal do Rio de Janeiro, 2011. Disponível em: https://pantheon.ufrj.br/bitstream/11422/1196/1/Hugo%20Bauer%20-%20TCC.pdf/. Acessado em: 01 mai. 2022.

ROCKCONTENT. **O que é armazenamento de dados e qual a sua importância nas empresas.** Disponível em: https://rockcontent.com/br/blog/o-que-e-armazenamento-de-dados//. Acessado em: 01 mai. 2022.

SÁ, MARCELO Dias de. **Análise do Impacto da Nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas: Aplicações mobile do governo.** Trabalho de Conclusão de Curso (Especialista em Informática) - Universidade Federal de Minas Gerais, Brasília, 2019. Disponível em: https://repositorio.ufmg.br/bitstream/1843/32040/1/MarceloDiasDeSa.pdf./. Acessado em: 01 mai. 2022.

SCHERER, João Luiz. **Tratamento de Dados em Sistemas de Informação Contábeis a partir da LEI 13.709/2018 (Lei de Proteção de Dados Pessoais): Um Estudo de Multicaso.** Trabalho de Conclusão de Curso (Bacharelado em Ciências Contábeis) - Universidade Federal de Caxias do Sul, 2020. Disponível em: < https://repositorio.ucs.br/xmlui/bitstream/handle/11338/6598/TCC%20Jo%c3%a3o%20Luiz%20Scherer%20Filho.pdf?sequence=1&isAllowed=y/>. Acessado em: 01 mai. 2022.

SEBRAE. **eBook LGPD: Lei Geral de Proteção de Dados.** Disponível em: https://www.sebrae.com.br/Sebrae/Portal%20Sebrae/UFs/PE/Anexos/LGPD-Connect-Sebrae.pdf/. Acessado em: 01 mai. 2022.

STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas.** 4. ed. São Paulo: PEARSON, 2010.

STALLINGS, William, BROWN, Lawrie. **Segurança de Computadores – Princípios e Práticas.** 2. ed. Elsevier, 2014.

UNIVERSIDADE JAVA. **Combinando criptografia simétrica e assimétrica.** Disponível em: http://www.universidadejava.com.br/outros/criptografia-assimetrica/. Acessado em: 28 mai. 2022.