RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

ACESSO À INFORMAÇÃO NA SEGURANÇA PÚBLICA: O USO DA CRIPTOGRAFIA NOS BANCOS DE DADOS

ACCESS TO INFORMATION IN PUBLIC SAFETY: THE USE OF ENCRYPTION IN DATABASES

ACCESO A LA INFORMACIÓN EN LA SEGURIDAD PÚBLICA: EL USO DE LA CRIPTOGRAFÍA EN LAS BASES DE DATOS

Alexandre Lima Richter[1]

e626242
https://doi.org/10.47820/recima21.v6i2.6242

PUBLICADO: 2/2025

RESUMO

O objetivo deste estudo foi examinar a relação da informação com a Segurança Pública e a proteção de seus bancos de dados por meio da criptografia, destacando a importância dessa ferramenta. Metodologicamente, o artigo foi desenvolvido a partir de uma revisão de literatura de cunho exploratório e qualitativo, baseada em pesquisas realizadas em mecanismos de busca como Google Acadêmico, SciELO e bancos de teses. Os resultados mostraram que os bancos de dados demandam criptografia para garantir a segurança das informações. Observou-se que existem diversas configurações para a implementação da criptografia em bancos de dados, sendo que a melhor flexibilidade é alcançada quando a criptografia é realizada dentro do Sistema de Gestão de Banco de Dados, influenciando significativamente a segurança e o desempenho dos dados. A criptografia de bancos de dados deve considerar modelos de formatação e os principais desafios relacionados à segurança da informação, incluindo sobrecarga de criptografia e gerenciamento de chaves. Para isso, é necessário adotar critérios como design da criptografia, configuração da criptografia, granularidade da criptografia e armazenamento de chaves. Concluiu-se que a gestão da informação no âmbito da Segurança Pública precisa estar alinhada com os processos de estruturação e modernização, considerando aspectos estratégicos, técnicos e operacionais. Dessa forma, é fundamental desenvolver e manter atualizada a integração das bases de dados e o compartilhamento de informações entre os órgãos que compõem esse sistema, garantindo respostas imediatas às demandas da área.

PALAVRAS-CHAVE: Banco de dados. Criptografia. Segurança pública.

ABSTRACT

This study aimed to investigate the relationship between information and Public Security and the protection of its databases through cryptography, exploring the use of this important tool. Methodologically, the article was developed from an exploratory and qualitative literature review based on research conducted in search engines such as Google Scholar, Scielo, and Thesis Bank. The results showed that databases require cryptography to ensure the security of this information, therefore it can be seen that there are various configurations for implementing database encryption, with the best flexibility being achieved when encryption is done within the Database Management System, having a significant influence on data security and performance. Database encryption should consider formatting models, and the main challenges related to data security, encryption overhead, and key management, using the following encryption design criteria, encryption configuration, encryption granularity, and key storage. It was concluded that information management in the context of Public Security needs to be linked to the structuring and modernization processes related to strategic, technical, and operational aspects to develop and keep up to date the integration of databases and the sharing of information among the bodies that are part of this system that work with situations that demands immediate responses.

KEYWORDS: *Database. Cryptography. Public security.*

[1] Bacharel em Segurança Pública pela Academia Policial Militar do Guatupê, em Direito pela Universidade Cruzeiro do Sul, Técnico em Gestão de Tecnologia da Informação pela Universidade Dom Bosco.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

RESUMEN
El objetivo de este estudio fue examinar la relación de la información con la Seguridad Pública y la protección de sus bases de datos a través de la criptografía para la utilización de esta importante herramienta. Metodológicamente, el artículo se desarrolló a partir de una revisión de literatura de carácter exploratorio y cualitativo desarrollada a partir de investigación realizada en mecanismos de búsqueda como Google Académico, Scielo y Banco de Teses. Los resultados mostraron que las bases de datos demandan criptografía para asegurar la seguridad de estas informaciones, por lo que se puede percibir que existen varias configuraciones de implantación de criptografía de base de datos, siendo que la mejor flexibilidad se alcanza cuando la criptografía se realiza dentro del Sistema de Gestión de Base de Datos teniendo influencia significativa en la seguridad y en el desempeño de los datos. La criptografía de la base de datos debe considerar modelos de formatación y los principales desafíos relacionados con la seguridad de datos, sobrecarga de criptografía y gestión de claves, usando los siguientes criterios de diseño de criptografía, configuración de la criptografía, granularidad de criptografía y almacenamiento de claves. Se concluyó que la gestión de la información en el ámbito de la Seguridad Pública necesita estar concatenada con los procesos de estructuración y modernización relacionados con los aspectos estratégicos, técnicos y operacionales para desarrollar y mantener actualizados la integración de las bases de datos y el compartimiento de informaciones entre los órganos que forman parte de ese sistema que trabajan con situaciones que demandan respuestas inmediatas.

PALABRAS CLAVE*: Base de datos. Criptografia. Seguridad pública.*

INTRODUÇÃO

A criminalidade e a violência têm crescido causando grande inquietude social e preocupação das autoridades da área de segurança pública na busca por soluções no enfrentamento do cenário (Brito, 2018). O fator Segurança Pública é considerado fundamental para sociedade, por isso a gestão das informações neste contexto é muito importante e depende da infraestrutura de seu banco de dados, assim, estudar a utilização da criptografia nestes ambientes se justifica, diante das inúmeras possibilidades de invasão cibernética às quais pode estar exposto.

Entende Brito (2018) que, neste contexto, fazer uso positivo dos recursos tecnológicos para combater a criminalidade possibilita a integração dos sistemas empregados nas atuações preventivas e repressivas, norteando o policiamento investigativo e tornando mais fácil mapear áreas de cometimento de ilícitos e identificar criminosos.

A Segurança Pública é responsável pela coleta, investigação e aplicação de diversos tipos de informações que podem afetar a segurança do país e estão passíveis de sofrer ataques cibernéticos que continuam a aumentar, por isso seus bancos de dados devem receber procedimentos estratégicos de tecnologia visando garantir suas ações, assim, a adoção da criptografia de dados se faz necessária.

Conforme descreve Nhacuongue (2011), cada vez fica mais evidente a importância dos bancos de dados que possibilitam o acesso e recuperação das informações neles contidas garantidas pelas ferramentas tecnológicas utilizáveis na Internet, por isso, os conteúdos informacionais devem ser protegidos.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Kamel (2009) informa que a utilização dos Bancos de Dados (BD) passou a ser evento recorrente com inúmeras aplicações que aportam o armazenamento de dados sensíveis a exemplo de salários, senhas e números de cartões de crédito entre outros que assumem caráter potencialmente sigiloso, onde acessos e modificações não autorizados podem acarretar muitos problemas para o seu responsável e usuários. Por isso, na esteira do desenvolvimento desta ferramenta surgem recursos que vislumbram maneiras de prevenir e minimizar os riscos relacionados com o armazenamento desses dados, incluindo-se os Sistemas de Gerenciamento de Banco de Dados (SGBDs) com o ativamento da função de segurança.

Diversas ações são tomadas em termos de segurança do banco de dados, contudo, não são suficientes para garantir a segurança quando o conteúdo do banco de dados é expresso na forma texto claro e legível, por isso, uma das medidas avançadas que estão sendo incorporadas para enfrentar esse desafio de exposição de dados privados em setores críticos como bancário, financeiro, saúde e governos, especialmente no contexto da segurança pública é a criptografia de banco de dados (Shmueli *et al.,* 2009).

Conforme entende Lima (2016), neste âmbito, pode-se observar que as organizações públicas e privadas têm investido em Tecnologia da Informação e Comunicação, que no caso específico da Segurança Pública necessitam para o cumprimento de seu dever constitucional dessa inserção e da concomitante proteção dos dados veiculados.

Diante do exposto, o objetivo deste trabalho foi estudar a relação dos dados e das informações com a Segurança Pública e a proteção dos seus bancos de dados por meio da criptografia para a utilização dessa ferramenta importante.

1. GESTÃO DA INFORMAÇÃO: CONCEITUAÇÃO E TECNOLOGIAS

Segundo descreve Freitas e Felipe (2012), a Gestão da Informação é entendida conceitualmente como um mecanismo que utiliza a tecnologia da informação, comunicação e recursos para desenvolver estratégias e estruturar as atividades organizacionais. Para Davenport (1998, p. 173), a aplicação da Gestão da Informação necessita passar pelo gerenciamento dos conteúdos produzidos pela organização que é definido pelo autor como “conjunto estruturado de atividades que incluem o modo como as empresas obtêm, distribuem e usam a informação e conhecimento”.

Entendem Dias e Belluzzo (2010, p. 23) que a disponibilidade de processamento eletrônico de dados/informações possibilita que se acesse mais rapidamente e com maior precisão as informações, beneficiando “a eliminação de custos excessivos, incentivando a busca da melhoria da qualidade e produtividade nas diversas atividades e serviços, principalmente naqueles que têm como matéria prima, a informação”.

Neste contexto, é utilizada a Tecnologia da Informação (TI) que, de acordo com Nhacuongue (2011), tem se constituído enquanto elemento que norteia a própria evolução da sociedade dos seus primórdios até a atualidade, incentivando o processo de comunicação. Discorrendo sobre o tema se

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

colocam Rossetti e Morales (2007) considerando a tecnologia da informação como elemento que se associa diretamente à geração e agregamento do conhecimento dos indivíduos também com o objetivo de aumento da produção de bens e serviços, garantia da comunicação e gestão organizacionais em conformidade com as conjunturas e características do momento. Os autores apontam como motivação da evolução das tecnologias da informação a disseminação dos sistemas de informação computadorizados para prover o suporte da informação e a transformação de dados, informação e conhecimento.

Partindo dessa ideia, Pacievitch (2021) define a tecnologia da informação como sendo o conjunto de recursos tecnológicos que são empregados de maneira integrada com um objetivo comum e próprio que possibilita, por meio do trabalho colaborativo, que profissionais que estejam separados geograficamente possam trabalhar em equipe e trocar informações. Cabe aqui um entendimento geral sobre a questão da segurança dessas informações.

1.1. Segurança da informação

No âmbito da segurança pública existe a necessidade de proteção máxima das informações relacionadas com a aplicação da lei, por isso, as metodologias de segurança da informação armazenada em Banco de Dados visam prevenir danos ou ameaças sobre as informações de investigações em curso, operações, planos, dados de indivíduos, processos e outros de caráter policial. Partindo desta ideia, concordam Silberschatz; Korth e Sudarshan (2020) com Silva *et al.,* (2017) que a segurança da informação parte de alguns princípios essenciais:

- confidencialidade: que assegura que a acessibilidade da informação é feita apenas por indivíduos autorizados;
- integridade: a alteração da informação é realizada somente por indivíduos autorizados;
- disponibilidade: que garante que os indivíduos autorizados possam acessar a informação e os ativos correspondentes sempre que necessitar;
- autenticação do remetente: o destinatário precisar estar capacitado para promover a verificação do remetente ser efetivamente quem afirma ser;
- não repúdio ou irretratabilidade do remetente: não deve haver a possiblidade do remetente negar a autoria de mensagem enviada por ele.

Neste caso, Silberschatz; Korth e Sudarshan (2020) entendem que a garantia da segurança da informação deve assegurar a confiabilidade, integridade e disponibilidade das informações para o indivíduo correto na hora certa.

Definem Stallings e Brown (2014) que a segurança da informação se constitui no conjunto de medidas que devem ser implementadas para garantir a integridade, confidencialidade e disponibilidade das informações armazenados em *softwares*, aplicativos, banco de dados de forma a diminuir a possibilidade de qualquer dano ao sistema. A segurança do sistema é tão importante porque fragilidades no acesso indevido de informações podem acarretar muitos problemas para as

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

organizações, inclusive nos órgãos da Segurança Pública por isso é relevante compreender o que é banco de dados e como se pode garantir sua segurança.

2. DESCREVENDO O BANCO DE DADOS E SUA SEGURANÇA

O Banco de Dados é definido por Oliveira (2018, p. 57) como sendo “uma coleção organizada de dados e informações que pode atender às necessidades de muitos sistemas, com um mínimo de duplicação, e que estabelece relações naturais entre dados e informações”. No entendimento de Machado (2020, p. 20), trata-se de “um conjunto de dados devidamente relacionados”. Pode-se observar que os conceitos englobam a ideia de armazenamento de dados onde as informações inseridas podem ser usadas na sua forma inicial ou podem ser processadas por meio dos sistemas de informação e transformadas em outras informações visando atender diversas necessidades. Contudo, a segurança destas informações em Banco de Dados deve ser garantida por algum meio, entre eles, a criptografia.

Segundo Silva (2020), entendendo-se um banco de dados como um sistema de armazenamento de dados, tem-se como seu objetivo precípuo o registro e a manutenção das informações consideradas significativas para a organização que é servida pelo sistema. Assim, o Sistema de Gerenciamento de Banco de Dados (SGBD) se conforma como um conjunto de condições e aplicabilidades que disponham segurança, integridade, controle de concorrência e recuperação a falhas. Neste cenário, os SGBDs mais empregados são PostgreSQL, MySQL, MariaDB, Oracle e SQLServer.

Normalmente, a maioria dos SGBDs já contam com sistema de segurança próprio que asseguram níveis de acesso de leitura e escrita, contudo, existe a permissão de acesso e permissão de leitura, para resguardar o conteúdo da informação armazenada, que pode ser senhas privadas de usuários (Becker; Perin, 2013). Aqui entra a necessidade da criptografia em bancos de dados.

Segundo descreve Semidão (2014), a criptografia está relacionada ao diferenciamento entre dado e informação. Para o autor, os dados não apresentam significados de relevância e nenhuma compreensão sozinho, não tem sentido a princípio, e por isso não tem valor algum. Já a informação consiste na ordenação e organização dos dados de maneira a fazerem sentido, abrangendo um significado que dê respaldo ao conhecimento, sendo, portanto, sensíveis.

Conforme informam Moreno; Pereira e Chiaramonte (2005), a criptografia se constitui no conjunto de técnicas elaboradas para dar proteção para uma informação de maneira que somente seu emissor possa descriptografar. O processo de criptografia envolve a execução de um algoritmo que faça a codificação dos dados para que se tornem irreconhecíveis, sendo necessário um algoritmo para descriptografar estes dados utilizando-se uma chave específica. Contudo, Luciano e Prichett (1987) reforçam o uso dessas técnicas de criptografia na segurança do banco de dados, mas alertam que o mal uso da criptografia pode trazer comprometimento significativo para o desempenho do banco de dados.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Segundo descreve Anjos (2016), no processo de criptografia são aplicados algoritmos com o propósito de embaralhar os bits dos dados da mensagem original pelo uso de uma ou mais chaves conforme o sistema criptográfico adotado. Corroboram Silberschatz; Korth e Sudarshan (2020) com Dias e Sakude (2008) que a criptografia também apresenta quatro princípios essenciais, a confidencialidade da mensagem; integridade da mensagem; autenticação do remetente e não-repúdio ou irretratabilidade do emissor.

Dias e Sakude (2008); Anjos (2016) e Silberschatz; Korth e Sudarshan (2020) descrevem como os principais tipos de criptografia o MD2, MD4, SHA, Hash, MD5, MD6, que é inutilizável, descrevendo como os mais indicados o MD5, SHA e Hash. O Message-Digest algorithm 5 (MD5) se constitui em um algoritmo de *hash* de 128 *bits* unidirecional que foi desenvolvido pela RSA Data Security Inc., sendo muito empregado por *softwares* com protocolo ponto-a-ponto (P2P) para a verificação de integridade de arquivos e logins. Devido a se tratar de algoritmo unidirecional, o MD5 não pode ser transformada de novo no texto original, por isso o método de verificação é desenvolvido a partir da comparação de uma da mensagem original confiável e outra da mensagem recebida.

Ainda de acordo com Dias e Sakude (2008); Anjos (2016) e Silberschatz; Korth e Sudarshan (2020) o Secure Hash Algorithm (SHA) se refere às funções criptográficas, sendo que a função mais utilizada a SHA-1 que é empregada em grande variedade de aplicações e protocolos de segurança, que incluem Transport Layer Security (TLS), Secure Sockets Layer (SSL), Pretty Good Privacy (PGP), Secure Shell (SSH), Secure Email Communication (S/MIME) e Internet Protocol Secured (IPSec).

Os algoritmos e protocolos ainda se subdividem em quatro tipos principais áreas: encriptação simétrica; encriptação assimétrica; algoritmos de integridade de dados e protocolos de autenticação. Utiliza-se a encriptação assimétrica para cifrar dados pequenos, sendo que seu principal uso é na assinatura digital e na realização de troca de chaves de maneira segura, estando este tipo de criptografia relacionada com a criptografia de chaves, pública e privada, empregadas para cifrar e decifrar, concomitantemente, esses dados. Já a encriptação simétrica é usada na ocultação de conteúdo dos blocos ou fluxos contínuos de dados de qualquer tamanho, abrangendo mensagens, arquivos, chaves de encriptação e senhas (Stalling; Brown, 2014; Anjos, 2016; Dias; Sakude, 2008).

A criptografia era utilizada quase que de maneira exclusiva em eventos diplomáticos e militares antigamente, e atualmente se constitui em mais do que uma forma de trocar informação secreta (Luciano; Prichett, 1987) porque se conforma a urgência atual de prover proteção para uma enorme quantidade de dados presentes nos meios digitais, e segundo Becker e Perin (2013), existem inúmeros algoritmos criptográficos para cifrar e decifrar mensagens por meio de duas entradas, uma refere-se ao conteúdo da informação sigilosa e a outra é um valor secreto chamado chave que pode ser simétrica constituída por sistemas de chaves secretas compartilhadas ou assimétrica constituída duas chaves, uma pública e outra privada. De maneira usual, a chave pública é disseminada em repositórios públicos para livre acesso, já a chave privada é mantida secreta.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

2.1. Segurança em banco de dados no âmbito da segurança pública

No contexto da segurança pública, os bancos de dados possibilitam o armazenamento de todo tipo de informação dos cidadãos individualmente que precisam ser compartilhadas entre os diversos sistemas para possibilitar que os órgãos da segurança pública possam expressar maior eficiência e eficácia relacionadas com o combate da criminalidade (Brito, 2018).

Estas novas capacidades tecnológicas podem auxiliar o trabalho investigativo e possibilitar novas estratégias de persecução criminal. Entre as possiblidades estão banco de identificação de perfil genético mediante extração de DNA, banco multibiométrico e de impressões digitais com foco no armazenamento de dados de registros biométricos, impressões digitais para subsidiar investigações criminais, utilização de videoconferência no processo penal já abordados em projetos de lei e a videovigilância da Segurança Pública (Antonialli; Fragoso; Massaro, 2019).

Um dos exemplos de banco de dados nacionais utilizados no âmbito da Segurança pública é o Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas (SINESP) que se constitui em uma plataforma de informações integradas que permite a realização de consultas operacionais, investigativas e estratégicas acerca da segurança pública que são inseridos por bases estaduais e órgãos federais. Trata-se de um sistema de ferramentas de tecnologia da informação que teve sua criação voltada para a produção de material apropriado à geração de conhecimento por meio da publicação de estatísticas e estudos ou pela oferta de informações com o intuito de conhecimento geral. A estrutura do Sinesp consiste em uma base nacional de dados relacionados à segurança pública (Brasil, 2018).

Contudo, se posiciona Brito (2018) que a própria integração entre sistemas informatizados de segurança pública permite a disseminação de informações críticas entre órgãos significativos por toda extensão territorial, que neste contexto, demanda a proteção desta permuta de informação entre os colaboradores ativos de diversas instituições que compõem a segurança pública.

De acordo com Santos (2018), é necessário que este compartilhamento e integração dos sistemas de segurança seja efetivado de maneira organizada e sistematizada, porque caso contrário, cada órgão gera suas informações e seu conhecimento de maneira isolada, sem que haja serventia para outros órgãos. Contudo este compartilhamento deve ser feito também de maneira segura.

No contexto do compartilhamento de informações surgem diversas atividades que tem o potencial de melhoria das chances das organizações de segurança pública, a exemplo da centralização do atendimento via telefone, emprego de um tipo de *software* comum a todos, facilitando o compartilhamento entre as agências da mesma informação, centralização dos estudos de relatórios, utilização das mesmas tecnologias que se constituem em fatores que podem colaborar para a melhoria da estratégia no combate à criminalidade.

O enfoque no conceito de compartilhamento de informações engloba a perspectiva tecnológica quanto à integração e a interoperabilidade de sistemas, também no que refere à troca de informações e intercâmbio de dados para efetivar a interoperação de sistemas (Santos, 2018).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Segundo descreve Brito (2018), a integração dos sistemas de informações é o que possibilita e viabiliza a unificação das informações entre polícia civil, polícia militar, corpo de bombeiros militar, perícia oficial, do sistema prisional, do departamento de trânsito, poder judiciário e a área criminal. O cruzamento das informações disponibilizadas pode auxiliar na geração de conhecimentos interinstitucionais que podem ser utilizadas pelas autoridades inseridas na segurança pública no processo de tomada de decisão.

Cardoso (2013) adentra o contexto da doutrina militar que entende o comando de controle como sendo um modelo de rede flexível que se constitui em um ambiente de compartilhamento que prove o conhecimento da situação para trazer contribuições no processo de obtenção da supremacia da informação e da iniciativa mesmo no caso de os elementos da força da segurança pública estarem distantes geograficamente. A integração e o desenvolvimento de canais de comunicação e protocolos de relacionamento pode assegurar um fluxo de informações que precisam ser compartilhadas com o objetivo de concretizar a integração das instituições de Segurança Pública.

Contudo, Santos (2018) explicita que a integração de sistema de informação não remete à abertura do banco de dados para cada instituição devido ao risco imposto para a preservação de informações sigilosas. Assim, toda consulta realizada em um banco de dados deve ser certificada e segura para que a transmissão de informações não sofra interferência ou alteração. Por isto, a importância da criptografia e sua eficácia na proteção dos bancos de dados, incluindo-se aqui as informações de banco de dados na Segurança Pública.

Descrevendo as ferramentas de segurança dos bancos de dados, Shmueli *et al.,* (2009) citam que as soluções e mecanismos convencionais de segurança de banco de dados se dividem em três camadas; segurança física, segurança do sistema operacional e segurança do Sistema de gerenciamento de banco de dados. No que diz respeito à segurança dos dados armazenados, controle de acesso por meio da autenticação e autorização é de grande utilidade se os dados forem acessados usando as interfaces de sistema pretendidas. No entanto, o controle de acesso é inútil se o invasor simplesmente obtiver acesso aos dados brutos do banco de dados, contornando os mecanismos tradicionais. Esse tipo de acesso pode ser facilmente obtido por *insiders,* como por exemplo o administrador do sistema e o administrador do banco de dados.

Os ataques que podem comprometer a segurança dos bancos de dados conforme citam Shmueli *et al.*, (2009) e Gavioli e Seehagen (2015) podem prover de *intruders* que são indivíduos que obtém acesso ao computador e tentam acessar informações valiosas; *insiders* que são pessoas que fazem parte do grupo de usuários confiáveis e tenta acessar informações fora de seus próprios direitos; administradores que consistem em indivíduos que possuem privilégios para administrar um sistema de computador e utilizam estes direitos com o intuito de obter informações valiosas.

Acerca dos ataques passivos, de acordo com Shmueli *et al.*, (2009) e Gavioli e Seehagen (2015) um índice seguro em um banco de dados criptografado não deve revelar nenhuma informação sobre o teor de texto dele, contudo, podem acontecer algum tipo de vazamento dessas informações. Pode-se obter informações acerca de registros armazenados meramente pela observação de

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

padrões em momentos específicos. No âmbito dos ataques passivos estão categorizados os seguintes vazamentos de informações: a) vazamento estático pela obtenção de informações do banco de dados, observando um instantâneo do banco de dados em um determinado momento; b) vazamento de ligação com a obtenção de informações do banco de dados vinculando um valor de tabela à sua posição no índice; c) vazamento dinâmico pelo acesso a informações do banco de dados observando e analisando as alterações realizadas no banco de dados durante um período de tempo.

Ainda para Shmueli *et al.*, (2009) e Gavioli e Seehagen (2015), no que se refere aos ataques ativos, tem como objetivo promover a modificação de informações e dados, podendo ocasionar prejuízos irreparáveis. Os ataques ativos são mais problemáticos no sentido de que podem enganar o usuário por meio de modificações não autorizadas que podem ser feitas de algumas maneiras específicas, a saber: a) *spoofing* pela substituição de um dado por outro gerado; b) *splicing* a partir da mudança da informação cifrada por outra cifrada diferente; c) repetição pela substituição do dado cifrado por uma versão antiga previamente atualizada ou excluída.

Informam Gavioli e Seehagen (2015) que as medidas de segurança adicionais de maneira geral promovem uma sobrecarga no processamento computacional que pode afetar o banco de dados no tempo de execução de suas operações, o que torna imprescindível o planejamento de criptografia do mínimo possível. Complementam Shmueli *et al.,* (2009) descrevendo que devem ser criptografados apenas dados confidenciais, mantendo os dados insensíveis não criptografados; somente os dados de interesse devem ser criptografados/decriptografados ao longo da execução das consultas. Assim, é desejável que o banco de dados criptografado não demande muito armazenamento a mais do que o original.

Segundo Carvalho (2001), as chaves de criptografia e a forma como são empregadas influenciam de maneira expressiva o nível de segurança da base de dados. Para o autor, a criptografia de qualquer banco de dados com a mesma chave de acesso não é suficiente, mesmo que o seu controle apresente eficiência comprovada.

Conforme propõem Shmueli *et al.*, (2009), a maneira como as chaves de criptografia são usadas influenciam significativamente na segurança do banco de dados e na praticidade da solução, por isso, algumas questões precisam ser consideradas: a) controle de acesso criptográfico, porque não é suficiente criptografar toda a base de dados com a mesma chave, mesmo que sejam utilizados mecanismos de controle de acesso; b) armazenamento de chaves seguro, pois as chaves de criptografia devem ser mantidas com segurança, por exemplo, armazenar as chaves dentro do servidor de banco de dados permite que um invasor acesse as chaves e os dados criptografados e, portanto, a criptografia se torna inútil; c) recuperação de chave porque se as chaves de criptografia forem perdidas ou danificadas, os dados criptografados não terão valor. Portanto, deve ser possível recuperar as chaves de criptografia sempre que necessário.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

3. MÉTODO

O artigo foi desenvolvido a partir de uma revisão de literatura de cunho exploratório e qualitativo desenvolvida a partir de pesquisa realizada em mecanismos de busca como Google Acadêmico, Scielo e Banco de teses.

4. CONSIDERAÇÕES

Observou-se que, no âmbito da Segurança Pública, as ferramentas de tecnologia da informação têm se constituído como fator determinante no desempenho da atuação dos órgãos que a compõem, auxiliando em ações preventivas e concomitantemente na antecipação do cometimento de delitos. Assim, acredita-se que a criação de bancos de dados pode impulsionar a sistematização e desenvolvimento do conhecimento no contexto da segurança pública devido à preservação das informações dispostas em documentos digitais, pela viabilização da disponibilização de dados de outros órgãos que podem dar suporte as ações necessárias ao cumprimento das prerrogativas da segurança pública. O agrupamento propiciado pelos bancos de dados em termos de esquemas e estruturas que determinam as características comuns das informações que podem ser agrupadas logicamente e as relações que se estabelecem entre essas informações desempenham papel relevante na tomada de decisões mais precisas e efetivas

Contudo, estes bancos de dados demandam de criptografia, visando assegurar a segurança dessas informações, por isso, pode-se perceber que existem várias configurações de implantação de criptografia de banco de dados, sendo que a melhor flexibilidade é alcançada quando a criptografia é feita dentro do Sistema de Gestão de Banco de dados tendo influência significativa na segurança e no desempenho dos dados.

Pode-se observar os principais desafios e tipos de *design* relativos à criptografia do banco de dados que consideram modelos de formatação e os principais desafios relacionados com a segurança de dados, sobrecarga de criptografia e gerenciamento de chaves, podendo-se concluir que um banco de dados deve usar os seguintes critérios de *design* de criptografia, configuração da criptografia, granularidade de criptografia e armazenamento de chaves. Percebeu-se pela análise do material utilizado, que mesmo que a criptografia em nível de banco de dados não proteja os dados de todos os tipos de ataques, ela disponibiliza um bom nível de proteção de dados, garantindo que apenas usuários autorizados possam ver os dados e protegendo os *backups* em caso de perda, roubo ou outro comprometimento dos meios de comunicação.

Diante do exposto, a gestão da informação no âmbito da Segurança Pública precisa estar concatenada com os processos de estruturação e modernização relacionados aos aspectos estratégicos, técnicos e operacionais para desenvolver e manter atualizados a integração das bases de dados e o compartilhamento de informações entre os órgãos que fazem parte desse sistema que trabalham com informações que demandam respostas imediatos.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

REFERÊNCIAS

ANJOS, Leandro Terra Versiani dos. **Segurança da Informação na Programação com uso de Criptografia e Certificação Digital**. 2016. 97f. Trabalho de Conclusão de Curso (Tecnologia em Sistemas de Computação) - Universidade Federal Fluminense, Niterói, 2016.

ANTONIALLI, Dennys Marcelo; FRAGOSO, Nathalie; MASSARO, Heloisa Maria Machado. Da investigação ao encarceramento: as propostas de incremento do uso da tecnologia no Projeto de Lei Anticrime. **Boletim do Instituto Brasileiro de Ciências Criminais**, ano 27, n. 318, p. 21-23, maio 2019.

BECKER, Gabriel Garcia; PERIN, Lucas Pandolfo. **Segurança em banco de dados**. 2013. 78f. Trabalho de conclusão de curso (Ciências da Computação) - Universidade Federal de Santa Catarina, Florianópolis, 2013.

BRASIL. **Lei nº 13.675, de 11 de junho de 2018**. Brasilia: Casa Civil, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm. Acesso em: ago. 2021.

BRITO, Carlos Eduardo Carvalho de. **Interoperabilidade dos Sistemas Informatizados na Segurança Pública**. 2018. 40f. Monografia (Especialização em Altos Estudos de Política e Estratégia) - Escola Superior de Guerra (ESG), Rio de Janeiro, 2018.

CARDOSO, Bruno de Vasconcelos. Megaeventos esportivos e modernização tecnológica: planos e discursos sobre o legado em segurança pública. **Horizontes Antropológicos**, Porto Alegre, ano 19, n. 40, p. 119-148, jul./dez. 2013.

CARVALHO, Daniel Balparda de. **Segurança de Dados com Criptografia - Métodos e Algoritmos**. 2. ed. Rio de Janeiro: Book Express, 2001.

DAVENPORT, Thomas H. **Ecologia da informação**: porque só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

DIAS, Acrisio Domiciano; SAKUDE, Milton Teruaki Suetsugu. ITACRIPTO: uma proposta de aplicativo de criptografia para o ITA. **Anais** [...] do 14O Encontro de Iniciação Científica e Pós-Graduação do ITA – XIV ENCITA. São José dos Campos, p. 1-7, out. 2008.

DIAS, Maria Matilde Kronka; BELLUZZO, Regina Célia Baptista. **Gestão da informação em ciência e tecnologia sob a ótica do cliente**. Bauru: EDUSC, 2010.

FREITAS, Francisco Tércio de; FELIPE, André Anderson Cavalcante. Análise da gestão da informação desenvolvida no Centro Integrado de Operações de Segurança Pública – CIOSP- RN. **Biblionline**, João Pessoa, v. 8, n. 2, p. 97-109, 2012.

GAVIOLI, Everton Pereira; SEEHAGEN, Jonathan Rafael. A utilização da criptografia a nível de banco de dados. **Anais** […] do 11º ENCITEC, p. 1-9, 2015.

KAMEL, Ibrahim. A schema for protecting the integrity of databases. **Computers & Security**, v. 28, n. 7, p. 698-709, 2009.

LIMA, Vladmir Braga. **Ferramentas de tecnologia da informação e comunicação na segurança pública**: uma análise sobre o portal Sinesp e suas ferramentas. 2016. Trabalho de Conclusão de Curso (Especialização em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos) - Universidade Federal de Santa Catarina, Araranguá, 2016.

LUCIANO, Dennis; PRICHETT, Gordon. Cryptology: From Caesar Ciphers to Public-Key Cryptosystems. **The College Mathematics Journal**, v. 18, n. 1, p. 2-17, jan. 1987.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

MACHADO, Felipe Nery Rodrigues. **Banco de Dados**: projeto e implementação. 4 ed. São Paulo: Érica, 2020.

MORENO, Edward David; PEREIRA, Fabio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em Software e Hardware**. São Paulo: Novatec Editora, 2005.

NHACUONGUE, Januário Albino. **Informação e Segurança Pública**: modelo de banco de dados para a gestão de informações em Moçambique. 2011.154f. Dissertação de Mestrado em Ciência da Informação. Marília: Universidade Estadual Paulista "Júlio de Mesquita Filho" – UNESP, 2011.

OLIVEIRA, Djalma de Pinho Rebouças de. **Sistemas de Informações gerenciais**: estratégicas, táticas, operacionais. 17 ed. São Paulo: Atlas, 2018.

PACIEVITCH, Thais. Tecnologia da Informação e Comunicação. **Infoescola,** 2021. Disponível em: infoescola.com/informatica/tecnologia-da-informacao-e-comunicacao/. Acesso em jul. 2021.

ROSSETTI, Adroaldo Guimarães; MORALES, Aran Bey Tcholakian. O papel da tecnologia da informação na gestão do conhecimento. **Ci. Inf.**, Brasília, v. 36, n. 1, p. 124-135, jan./abr. 2007.

SANTOS, Ivens Giuliano Campos dos. **Análise dos facilitadores e das barreiras para integração e compartilhamento de informações de Segurança Pública**: Um Estudo de Caso no Centro de Comando e Controle do Rio Grande do Sul. 2018. 142f. Dissertação (Mestrado em Ciências Contábeis) - Universidade do Vale do Rio dos Sinos – UNISINOS, São Leopoldo, 2018.

SEMIDÃO, Rafael Aparecido Moron. **Dados, informação e conhecimento enquanto elementos de compreensão do universo conceitual da ciência da informação**: contribuições teóricas. 2014. 199f. Dissertação (Mestrado em Ciência da Informação) - Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP), Marília, 2014.

SHMUELI, Erez; VAISENBERG, Ronen; ELOVICI, Yuval; GLEZER, Chanan. Database Encryption – An Overview of Contemporary Challenges and Design Considerations. **SIGMOD Record**, v. 38, n. 3, p. 29-34, sep. 2009.

SILBERSCHATZ, Abraham; KORTH, Henry F.; SUDARSHAN, S. **Sistemas de Banco de Dados**. 7 ed. São Paulo: Makron Books, 2020.

SILVA, Antonio Tadeu Matias da; LOPEZ FILHO, Juarez; SOUZA, Matheus Ananias de; CANCELA, Lucas Borcard. Criptografia: mais do que uma necessidade, um imperativo. *In:* **XIV EVIDOSOL e XI CILTEC**, p. 1-5, jun. 2017.

SILVA, Lucas Henrique de Moura e. **Escolha da criptografia ideal e anonimação de dados sensíveis citados a lei geral de proteção de dados**. 2020. 42f. Trabalho de Conclusão de Curso (Engenharia de Computação) - Centro Universitário de Anápolis – UniEVANGÉLICA, Anápolis, 2020.

STALLINGS, William; BROWN, Lawrie. **Segurança de Computadores:** princípios e práticas. 2 ed. Rio de Janeiro: Gen/LTC, 2014.