PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

A PERCEPÇÃO DE PROFISSIONAIS DE SOFTWARE SOBRE SEGURANÇA EM BANCO DE DADOS

MARIANA SANTA CLARA CAMPELO ZANATTA

GOIÂNIA
2023

MARIANA SANTA CLARA CAMPELO ZANATTA

A PERCEPÇÃO DE PROFISSIONAIS DE SOFTWARE SOBRE SEGURANÇA EM BANCO DE DADOS

Projeto de Trabalho de Conclusão de Curso II apresentado Escola Politécnica e Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para aprovação da disciplina de Trabalho de Conclusão de Curso II – CMP1072 – A25.

Orientadora:Profª Msc. Adriana Silveira de Souza

GOIÂNIA

2023

MARIANA SANTA CLARA CAMPELO ZANATTA

A PERCEPÇÃO DE PROFISSIONAIS DE SOFTWARE SOBRE SEGURANÇA EM BANCO DE DADOS

Trabalho de Conclusão de Curso aprovado em sua formação final pela Escola Politécnica, da Pontifíca Universidade Católica de Goiás, para obtenção do título de Bacharel em Engenharia da Computação, em __/__/____.

_____ _____

Orientadora: Prof.a Me. Adriana Silveira de Souza

_____

Prof. Dra. Solange Silva

_____

Prof. Me. Joriver Rodrigues Canêdo

_____

Prof. Dr. Juliano Lopes de Oliveira

RESUMO

Apresenta-se um estudo dos principais problemas em relação ao Sistema de Banco de Dados e os resultados de um questionário, em que o público-alvo são os Desenvolvedores de Software e a percepção deles em relação à Segurança do Sistema de Banco de Dados. As respostas foram dadas por diferentes profissionais, apesar de ter tido uma amostra pequena.

Os resultados foram analisados e foi percebido que a maioria desses profissionais não tiveram problemas em relação à segurança, visto que tem as próprias credenciais para cada, ou seja, cada um tem seu próprio login e sua própria senha, porém existem ainda alguns especialistas que compartilham sua credencial. O profissional de Banco de Dados foi o único que não assinou o termo de confidencialidade.

Palavras Chaves: Segurança, Banco de Dados, Desenvolvedor de *Software*, Ataques,Controles.

Abstract

A study of the main problems in relation to the Database System is presented and also the results of a questionnaire where the target audience is Software Developers and their perception in relation to the Security of the Database system. The answers were given by different professionals, despite having a small sample.

The results were analyzed and it was noticed that the majority of these professionals had no problems regarding safety; each person has their own credentials, that is, each person has their own login and password; however, there are still some experts who share their credentials. The Database professional was the only one who did not sign the confidentiality agreement.

Keywords: Security, Database, Software Developer, Attacks, Controls.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

- CID = Confiabilidade, Integridade e Disponibilidade
- DBA = Dependência de Administradores de Banco de Dados
- DM = Gerenciamento de Acesso a Dados
- DDoS = *Distributed Denial of Service* ou Negação de Serviço Distribuído em português
- SBD = Sistema de Banco de Dados
- TM = Gerenciador de Transações
- VPN = *Virtual Private Network* ou Rede Privada Virtual em português

SUMÁRIO

1. Introdução

A tecnologia está cada vez mais presente nas vidas das pessoas e nas organizações. Ela tem sido utilizada para tornar mais eficientes processos de trabalho nas diversas áreas. Por exemplo, na área agrícola, o banco de dados é usado para monitorar e guardar informações sobre o solo e o clima, monitorar as pragas e tomada de decisões. Também favorece na área de E-Commerce, Sistemas de Educação, Jogos e Entretenimento, Redes Sociais. Na área de E-commerce, os Bancos de Dados foram usados para Gestão de Inventário e de pedidos; Segurança de Pagamentos e Dados do cliente. Na área da Educação, para Gestão de Funcionários e Professores; avaliações e notas; matérias que já foram administradas; salas destinadas às matérias; na questão de matrículas.

Em Jogos e Entretenimento, na área de estatísticas e análises de jogabilidade; sistemas de pontuação e classificação e, por último, mas não menos importante, em Redes Sociais, em que os Bancos de Dados são usados em relação à Gestão de Relacionamentos; Suporte ao Cliente e Resolução de Problemas.

Portanto, percebe-se necessidade cada vez maior da criação de sistemas de banco de dados.

Um sistema de banco de dados é um conjunto de programas que permitem aos usuários criarem e manter um sistema computacional que gera informações relevantes para tomada de decisões.

Entre as vantagens de se utilizar um Sistema de Banco de Dados, estão o acesso rápido e centralizado aos dados, redução de informações duplicadas, facilidade de compartilhamento de dados, maior visibilidade e controle sobre as informações, maior agilidade nos processos durante a execução de transações, menos tempo gasto com manutenção (Backups), mais segurança dos dados (vantagens de ter um único banco de dados para todos os sistemas, 2023). Na área de E-commerce, as vantagens de usar um Banco de Dados são: facilidade na administração de dados, mas especificamente na otimização de tarefas; Alinhamento das Estratégias. (Mateus, 2023).

Já na área de Redes Sociais, os dados são recuperados mais rápido, já que o sistema faz gestão multimídia e de amigos e conexões. Já como desvantagens, este trabalho identificou a possibilidade de ataques de hackers, o desconforto de usuários em relação ao direcionamento aos anúncios.

Um aspecto muito pertinente em Banco de Dados é em relação à segurança.

Segurança de Banco de Dados refere-se às medidas de proteção empregadas para proteger os dados contra acesso não aprovado e para preservar a confidencialidade, integridade e disponibilidade dos dados. As boas práticas de segurança de dados incluem técnicas de proteção de dados, como criptografia de dados, a qual é uma prática de proteger informações por meio do uso de algoritmos codificados; gerenciamento de chaves, que consiste em armazenar, proteger, organizar e garantir o uso adequado delas, gerir seu ciclo de vida e manter cópias de segurança de forma

segura e consistente; edição de dados, subconjunto de dados, o qual é o conjunto de dados que será feito Backups e mascaramento de dados, é um método de proteção de dados sensíveis que substitui o valor original por um valor equivalente fictício, mas realista (“principais técnicas de mascaramento de dados”, [s.d.]); bem como controles de acesso de usuário privilegiado, é um mecanismo de proteção a informações (infosec) que protege as identidades com recursos ou acesso especial além dos usuários normais (“o que é gerenciamento de acesso privilegiado (PAM)?”, [s.d.]); auditoria, que é um exame cuidadoso e sistemático das atividades desenvolvidas em determinada organização, cujo objetivo é averiguar se elas estão conforme as planejadas e/ou estabelecidas previamente, se foram implementadas com eficácia e adequadas à consecução dos objetivos e monitoramento que consiste na coleta e análise de informações que podem ajudar as empresas a tomarem melhores decisões (“como fazer o monitoramento de dados da sua empresa?”, 2022).

Caso exista a possibilidade de a Segurança do Sistema de Banco de Dados ser violada, dados podem ser vazados, informações podem ser perdidas, acesso pode ser eliminado, impedindo utilização dos dados. Assim, tornando o sistema ineficaz ou inoperante. Um exemplo de violação de segurança em Banco de Dados foi o caso da Equifax. Um dos três maiores serviços de proteção ao crédito nos EUA, que foi invadida por hackers. Os atacantes levaram dados de 143 milhões de pessoas, incluindo nome completo, endereço, data de nascimento, o número de seguridade social e mais 209 mil números de cartões de crédito.

Para a resolver esse ataque, a empresa decidiu que não iria atualizar o *framework* que eles usavam, além de ser invadido, expor os dados e avisar seus clientes quarenta dias depois (Ventura, 2017).

Problemas relacionados à falta de segurança de banco de dados em termos de integridade, que é um conjunto de processos que visam no armazenamento o uso adequado e consistente dos dados (kondado.com.br, 2023). Confidencialidade trata-se de uma propriedade da informação que pretende garantir o acesso unicamente às pessoas autorizadas (“conceito de confidencialidade”, [s.d.]). E disponibilidade diz respeito ao acesso dos dados sempre que esse for necessário (Batistella, 2020), mas podem trazer falhas. Algumas dessas falhas podem trazer as seguintes consequências:

- Perda de Dados: dados que não podem ser mais acessados ou estão danificados.
- Inconsistência de Dados: ocorre quando há imprecisão, contradições nos dados, ou seja, os dados tornam-se errados.
- Acesso não autorizado: ocorre quando a estrutura dos dados é mudada, fazendo com que o banco de dados não represente mais fidedignamente à realidade.
- Problemas de Desempenho: é o resultado de alguma transação de Banco de Dados que não obtém os recursos necessários para concluir em tempo hábil, levando mais tempo que o necessário para sua conclusão.

- Extorsão e chantagem por conta de dados sequestrados: é um crime cibernético, em que os criminosos invadem os sistemas de uma empresa ou indivíduo e sequestram seus dados. Eles, então, exigem um resgate em troca da devolução dos dados ou ameaçam publicá-los na internet.
- Mancha na reputação da empresa tanto para os clientes quanto para as organizações, pois com os dados vazados, é difícil acreditar na credibilidade da empresa e na questão do usuário, e, dependendo da situação, afeta como ele é visto pelas outras pessoas.

A justificativa de estudar esse tema é porque cada vez mais os dados armazenados nas empresas precisam ser seguros e protegidos. Caso a empresa sofra um ataque em seus sistemas de banco de dados, a sua confiabilidade pode ser abalada. Consequentemente, prejuízos advindos das falhas de segurança podem propiciar perda de clientes, depreciação da marca, perdas financeiras, perda de dados, sistema de banco de dados inoperante, entre outros. Os profissionais de desenvolvimento de software devem incorporar boas práticas de segurança na construção de software. Eles são os responsáveis por pensar em como um sistema deve manter a segurança, visando zelar pela qualidade dos dados armazenados, bem como pela eficiência e eficácia dos processamentos de dados gerados para tomada de decisão mais efetiva.

Porém, às vezes, consequências como essas não são resolvidas adequadamente devido aos profissionais de software que são mal preparados, sendo assim temos a seguinte dúvida:

Como os profissionais de software percebem e tratam a segurança de seus sistemas de banco de dados?

O **Objetivo Geral** deste trabalho é produzir uma pesquisa que investiga a percepção dos profissionais de desenvolvimento de Software sobre a segurança de Sistemas de Banco de Dados.

Como **Objetivos Específicos**:

- Efetuar um levantamento dos principais problemas que afetam a Segurança do Sistema de Banco de Dados.
- Fazer um *survey* para colher a percepção de profissionais de desenvolvimento de software em como tratam a Segurança no Sistema de Banco de Dados.
- Consolidar e analisar as respostas, correlacionando com o estudado.
- Gerar uma síntese dos resultados e conclusões sobre os dados obtidos.

Como **Resultado Esperado**, deseja-se que este trabalho possa contribuir para o entendimento de como os profissionais de Engenharia de Software compreendem o que é um Banco de Dados seguro.

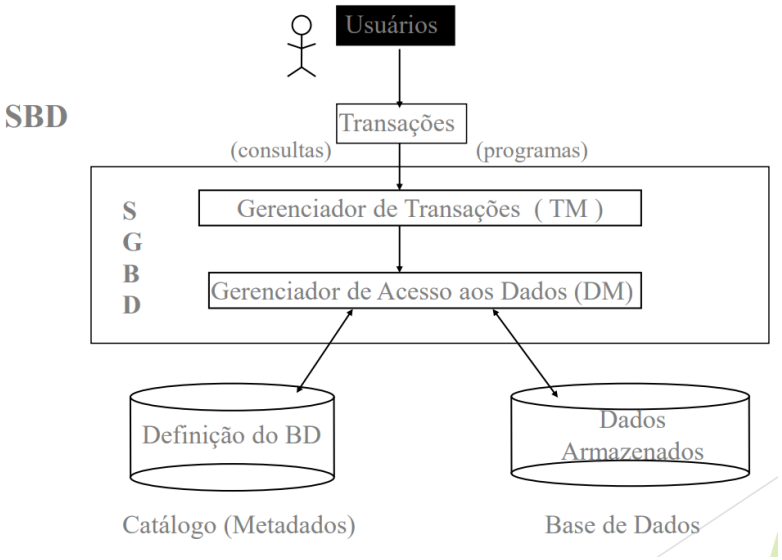
- Identificar os principais problemas de segurança relacionados ao Sistema de Banco de Dados.

Este trabalho está estruturado em mais cinco capítulos a partir desta introdução. O Capítulo 2 discute o Referencial Teórico, em que estão presentes os principais conceitos sobre: Banco de Dados, Sistema de Banco de Dados, Sistema de Gerenciamento de Banco de Dados e vantagens e desvantagens de sua utilização. Além disso, são discutidos os principais problemas de Segurança relacionados à Banco de Dados. O Capítulo 3 esclarece a Metodologia Científica utilizada neste trabalho. O *Survey* que mostra a percepção dos desenvolvedores de software em segurança de Banco de Dados é explicitado no Capítulo 4. No Capítulo 5, é discutida a Análise de Resultados. Por fim, no capítulo 6, as principais Conclusões e Trabalhos Futuros são sintetizadas.

2. Referencial Teórico

A Figura 01 retrata um Sistema de Banco de Dados que pode ser acessado por transações feitas pelo usuário, alguns exemplos dessas transações são consultas ou programas. Dentro desse sistema, temos o Gerenciador de Transações (TM) e o Gerenciamento de Acesso aos Dados (DM), em que dentro dele contém os Metadados, que são informações adicionais que descrevem os dados que estão sendo armazenados ou transmitidos (“o que são metadados? | Metadados”, [s.d.]) e a Base de Dados, que é qualquer coleção de informações interrelacionadas (“o que são as bases de dados? – o que é uma base de dados? | MICROSOFT AZURE”, [s.d.]).

Figura 01 – Sistema de Banco de Dados



Fonte: MATERIAL DE AULA – Prof. Juliano Lopes

Banco de Dados é uma grande quantidade de informações armazenadas em um sistema de computador, de tal forma que possam ser facilmente visualizadas ou alteradas. E um sistema de Banco de Dados é um conjunto de programas que permitem aos usuários criarem e manterem um Banco de Dados. (Silberschatz; Korth; s sudarshan, 2012)

O Banco de Dados é estruturado conforme a definição de um esquema, que define como as tabelas e suas respectivas linhas e colunas serão armazenadas (Sierro, 2020).

Quando não há existência do Sistema do Banco de Dados, o sistema se torna ineficiente, ocorre a chance de ter os dados perdidos.

Em contrapartida, tendo presente esses sistemas, aparece juntamente as vantagens em relação até os sistemas de arquivos: ele dá suporte em consultas complexas; automatiza as tarefas e personaliza os relatórios. E também aparece as desvantagens:

complexidade na questão de ser mal implementado; custo, na questão de caro de implementar; e flexibilidade, dificuldade em readaptação e mudanças.

2.1 Problemas de Segurança em SBD

Esta seção mostra os problemas relacionados à segurança de um Sistema de Banco de Dados. Na segurança de um Sistema de Banco de Dados, quando ineficaz, os dados tornam-se vulneráveis. Com isso, ocorrem riscos de serem vazados, tornarem-se inacessíveis, corrompidos, gerando dados não confiáveis.
Segurança de um Sistema de Banco de Dados são os processos, ferramentas e controles que protegem os bancos de dados contra ameaças acidentais e intencionais ("melhores práticas e soluções de segurança de banco de dados | MICROSOFT AZURE", [s.d.]). O objetivo da segurança do banco de dados é proteger dados confidenciais e manter a confidencialidade, disponibilidade e integridade do banco de dados. Além de proteger os dados dentro do banco de dados, a segurança do banco de dados auxilia o sistema de gerenciamento de banco de dados e aplicativos, sistemas, servidores físicos e virtuais associados e a infraestrutura de rede associada contra acesso não autorizado, alteração e destruição. A seguir, são apresentados os principais problemas relacionados à segurança de um SBD:

1. Roubo de Dados, que é acesso não autorizado aos dados sensíveis, caso ocorra tem um alto risco de comprometer o CID, pois sendo acessados podem ser alterados.
2. Backups Desprotegidos, que são cópias que não são devidamente protegidas. Também tem o alto risco em relação ao CID, pois os dados podem ser alterados, duplicados, tornando, assim, não confiáveis.
3. Problema de Interferência é uma ocorrência de situações em que interrupções externas ou internas causam falhas no funcionamento do sistema. Isso significa que fatores externos, como sinais elétricos indesejados ou atividades internas inesperadas, podem perturbar o funcionamento normal do banco de dados. Uma vez ocorrido isso, o risco na Disponibilidade se torna alto, e há médio risco em Confiabilidade e Integridade.
4. Quebras durante o processo de transação, que são falhas ao processar transações, levando às inconsistências. Com os dados sendo inconsistentes, a confiabilidade passa a ter um alto risco.
5. Corrupção de Dados, os dados tornam-se ilegíveis e, como consequência, os níveis de risco do CID são altos, pois podem causar danos significativos.

6. Ataques de Negação de Serviço, em que ocorre a sobrecarga do sistema, tornando-o inacessível, fazendo com que haja um alto risco na Disponibilidade, baixo risco em Confiabilidade e médio risco em Integridade.
7. Fácil Acesso Físico ocorre quando o sistema está localizado localmente, traz um alto risco tanto para a Confiabilidade, Integridade e Disponibilidade, pois, com acesso mal-intencionado, os dados podem ser alterados, duplicados.
8. Problemas com Autenticação Fraca podem trazer risco alto, pois pode ocorrer perda de dados críticos e acesso mal-intencionado em sistemas que podem ser considerados críticos.
9. Ataques de SQL *Injection*, que são injeções de códigos maliciosos em consultas SQL, traz um alto risco para a Confiabilidade e Integridade, pois ele acarreta os seguintes problemas: a perda de dados e uma violação na segurança, na qual compromete o sistema inteiro.
10. Classificação de informações torna-se um problema quando há uma falha em classificar dados de acordo com sua sensibilidade, sendo assim, ocorre um alto risco em Confiabilidade e Integridade, pois pode acarretar uma manipulação indevida e traz um baixo risco em Disponibilidade, pois, independente disso, o dado ainda estará disponível.
11. Rotulagem de Informações, quando há uma falha, a Confiabilidade e Integridade têm alto risco, pois, como consequência, pode ocorrer uma manipulação indevida.
12. Transferência de Informações, quando falha, traz um risco médio em relação à Confiabilidade, pois pode haver a possibilidade de perda de dados durante a transferência. Já para a Integridade, o risco é baixo, pois a única preocupação é a perda de dados, e em relação à Disponibilidade, o risco é médio, pois, nesse caso, pode ocorrer por diversos fatores, como, por exemplo, a falha na rede.
13. Controle de Acesso, quando ocorre sua falha, a Confiabilidade em consequência, tem um alto risco, pois pessoas mal-intencionadas podem acessar dados sensíveis. Em relação à Integridade, o risco é alto também, pois pode comprometer o sistema se o usuário não souber ou fizer de maneira errada uma modificação ou exclusão. Para a Disponibilidade, o risco é baixo,

pois somente em alguns casos o sistema pode ficar indisponível, quando a sobrecarga ou a autenticação foi feita de forma inválida.

14. Gestão de Identidade, ao ocorrer uma falha relacionada, o risco de Confiabilidade é alto, pois pode haver contas duplicadas ou o usuário legítimo pode ser mal identificado. O risco de Integridade é alto também, porque pode haver manipulação indevida das informações do perfil do usuário. E, no caso da Disponibilidade, pode ser média, por somente ocorrer se a conta for bloqueada devido aos erros na gestão.
15. Segurança da Informação para uso de serviço em nuvem que, quando falha, a Confiabilidade sofre um grande risco, por ter chance de vazamento de dados e acesso indevido. A Integridade também é de risco alto, porque o armazenamento pode ser feito de maneira inadequada, comprometendo a qualidade dos dados. A Disponibilidade, assim como os outros, são de risco alto, por conta das falhas de segurança.
16. Proteção de Registros, quando ocorre uma falha, a Confiabilidade tem risco baixo, pois pode haver somente a perda de dados. No caso da Integridade, também é baixa, pois está ligada diretamente com a falta de proteção. E Disponibilidade é de alto risco, pois a falta de proteção pode acarretar a perda de registros essenciais para as operações.
17. Conscientização, Educação e Treinamento em Segurança da Informação, quando há falha em relação a esse assunto, o risco da Confiabilidade é médio, resultado da ocorrência em que o usuário não é informado adequadamente sobre as práticas de segurança. Já o risco de Integridade também é médio, pois é resultado de quando os usuários não compreendem completamente as implicações de suas ações. E, por último, mas não menos importante, o risco da Disponibilidade é alto, resultado da situação dos usuários não estão cientes das práticas adequadas de segurança.
18. Falha em relação aos Acordos de Confidencialidade e não Divulgação, o risco em relação à Confiabilidade é alta, pois pode ocorrer a divulgação não autorizada de informações sensíveis. Em relação à Integridade, o risco é alto também, pois havendo a divulgação de não autorizada, em consequência, há manipulação inadequada e tomada de decisões erradas, prejudicando a

integridade dos processos. E, por fim, o risco da Disponibilidade é baixo, resultado somente dos possíveis ataques que pode ter.

19. Proteção contra Malware, quando falha, o risco da Confiabilidade é alto, pois pode resultar em comprometimento do sistema, abalando a confiança das operações, especialmente se os dados sensíveis são comprometidos. O risco da Integridade é alto, pois Malware pode alterar, excluir, modificar os dados e fazer com que as decisões sejam tomadas de forma inadequada. O risco da Disponibilidade também é alto, pois podem causar interrupções no sistema.
20. Quando não há uso de Criptografia, a Confiabilidade se torna de risco baixo, pois é consequência de uma criptografia implementada incorretamente, fazendo com que as chaves fiquem comprometidas e os dados não são bem protegidos. O risco da Integridade também é baixo, pois, com chaves comprometidas, podem comprometer na manipulação de dados criptografados, comprometendo a integridade das informações. E o risco da Disponibilidade desses dados é médio, por conta da complexidade da criptografia em relação ao sistema.

A Tabela 01 segue uma esquematização com resumo desses problemas e dos níveis correspondentes de cada um, respectivamente:

Tabela 01 – Relação de Problemas

Problema	Explicação	Confiabilidade	Integridade	Disponibilidade
Roubo de Dados	Acesso não autorizado às informações sensíveis.	Alta	Alta	Alta

Backups Desprotegidos	Cópias de dados não estão devidamente protegidas. Além de explorar as vulnerabilidades deles, tais como: a falta de criptografia, senha fraca, Backups desatualizados e conseguir atacar sem ser rastreado.	Alta	Alta	Alta
Problema de Interferência	Interferências causam falhas no sistema.	Média	Média	Alta
Quebras durante o processamento de transação	Falhas ao processar transações, levando às inconsistências.	Alta	Média	Alta
Corrupção de Dados	Dados se tornam corrompidos ou ilegíveis.	Alta	Alta	Alta
Ataques de Negação de Serviço Distribuídos – DDoS	Sobrecarga do sistema, tornando-o inacessível.	Baixa	Média	Alta

Fácil Acesso Físico	Se os dados estiverem protegidos localmente, tem um possível risco de pessoas não autorizadas acessarem aos servidores ou aos sistemas que hospedam os dados, e, assim, alterem os dados.	Alta	Alta	Alta
Problema de Autenticação Fraca	Permite que os invasores obtenham a identidade do Banco de Dados autorizado. Uso de contas e senhas-padrão ou senhas facilmente adivinhadas, em que os invasores têm como alvo os usuários finais em vez dos computadores.	Alta	Alta	Média
Ataques de SQL *Injection*	Injeção de código malicioso em consultas SQL.	Alta	Alta	Baixa
Classificação de Informações	Falha em classificar dados de acordo com sua sensibilidade.	Alta	Alta	Baixa
Rotulagem de Informações	Falha na rotulagem correta de informações sensíveis.	Alta	Alta	Baixa

Transferência de Informações	Falha na segurança durante a transferência de dados.	Média	Baixa	Média
Controle de Acesso	Convém que não há regras para controlar o acesso físico e lógico às informações e outros ativos associados sejam estabelecidos e implementados com base nos requisitos de segurança da informação e de negócios.	Alta	Alta	Baixa
Gestão de Identidade	Não permitir a identificação única de indivíduos e sistemas que acessam as informações da organização e outros ativos associados e para permitir a cessão adequada de direitos de acesso.	Alta	Alta	Média

Segurança da Informação para uso de serviço em nuvem	Não há especificação e gerenciamento da segurança da informação para o uso de serviços em nuvem.	Alta	Alta	Alta
Proteção de Registros	Ocorre quando os registros não são protegidos contra perdas, destruição, falsificação, acesso não autorizado e liberação não autorizada.	Baixa	Baixa	Alta
Conscientização, Educação e Treinamento em Segurança da Informação	Falta de treinamento e conscientização sobre segurança.	Média	Média	Alta
Acordos de Confidencialidade e não Divulgação	Falta de acordos para proteger informações sensíveis.	Alta	Alta	Baixa
Proteção contra Malware	Falha em prevenir a infecção por software malicioso.	Alta	Alta	Alta
Uso de Criptografia	Falha em usar criptografia para proteger dados em trânsito e em repouso.	Baixa	Baixa	Média

2.2 Vantagens e Desvantagens do Sistema de Banco de Dados

As vantagens de se utilizar um Sistema de Banco de Dados são:

- Centralização de Dados: os sistemas de banco de dados centralizam o armazenamento de dados, fornecendo um repositório único e unificado para armazenar e gerenciar dados.
- Escalabilidade: os sistemas de banco de dados podem ser dimensionados para acomodar quantidades crescentes de dados e usuários. Essa escalabilidade é essencial para aplicativos que experimentam crescimento no volume de dados e na atividade do usuário.
- Consistência de dados: as alterações feitas nos dados são consistentes em todo o banco de dados, evitando anomalias nos dados e garantindo que todos os dados relacionados permaneçam sincronizados.

E as desvantagens a utilizar o Sistema são:

- A Complexidade: implementar e manter um sistema de banco de dados pode ser complexo. As organizações podem precisar investir em hardware, software e pessoal qualificado para design, desenvolvimento e administração de banco de dados.
- Curva de Aprendizagem: os sistemas de banco de dados geralmente apresentam uma curva de aprendizado, e os usuários, especialmente aqueles não familiarizados com os conceitos de banco de dados, podem achar difícil navegar e usar o sistema de maneira eficaz.
- Problema de Compatibilidade: podem surgir problemas de compatibilidade ao integrar diferentes sistemas de banco de dados ou ao migrar dados entre sistemas. Isso pode ser uma preocupação quando as organizações utilizam diversas aplicações que podem não suportar totalmente uma determinada tecnologia de banco de dados.
- Dependência de Administradores de Banco de Dados (DBAs): os sistemas de banco de dados dependem geralmente de administradores de banco de dados qualificados para gerenciar e otimizar seu desempenho. A dependência de DBAs pode ser uma restrição, especialmente em organizações com acesso limitado a esse tipo de conhecimento.

2.3 Boas práticas e a Norma Técnica ISO/IEC 27002

A norma ISO/IEC 27002 - Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação é uma norma técnica que

estabelece tipos de controles que podem ser implementados em uma organização para definir ambientes seguros em relação a um sistema de gestão de segurança da informação. Controles são o conjunto de atividades administrativas, planos, rotinas, métodos e procedimentos interligados, estabelecidos para assegurar que os objetivos da organização sejam alcançados, de forma confiável, concreta, eficiente e eficaz, evidenciando eventuais desvios ao longo da gestão até a consecução dos objetivos fixados. Esses controles estão divididos em Controles Organizacionais, Controle de Pessoas, Controles Físicos e Controles Tecnológicos.

A seguir, será apresentado os principais controles usados neste trabalho.

No caso do controle Organizacional, foram usados os seguintes requisitos: Classificação de Informações (as informações devem ser classificadas de acordo com as necessidades de segurança da informação da organização, com base na Confiabilidade, Integridade, Disponibilidade e requisitos das partes interessadas relevantes); Informações de Autenticação (a alocação e a gestão de informações de autenticação devem ser controladas por uma gestão de processo, incluindo aconselhar o pessoal sobre o manuseio adequado de informações de autenticação).

Controle de Pessoas, alguns requisitos são: Conscientização, Educação e Treinamento em Segurança da Informação (o pessoal da organização e partes interessadas relevantes devem receber treinamento, educação e conscientização em segurança da informação apropriados e atualizações regulares da política de segurança da informação da organização, políticas e procedimentos específicas por tema, pertinentes para as suas funções); Acordos de Confiabilidade ou não divulgação (Acordos de Confiabilidade ou não divulgação que reflitam as necessidades da organização para a proteção das informações devem ser identificados, documentados, analisados criticamente em intervalos regulares e assinados pelo pessoal e por outras partes interessadas pertinentes).

Em relação aos Controles físicos, os requisitos são: Entrada Física (na qual as áreas seguras devem ser protegidas por controles de entrada e pontos de acessos apropriados) e, por fim, mas não menos importante, os Controles Tecnológicos que são: Backup das informações (cópias de Backup de informações, software e sistemas devem ser mantidas e testadas regularmente de acordo com a política específica por tema acordada sobre Backup).

Além da ISO27002, existem também as boas práticas, tais como: testes de segurança, como testes de penetração e análises de vulnerabilidade, para identificar e corrigir potenciais pontos fracos; Gestão de Configuração, a qual esteja alinhada com as melhores práticas de segurança.

3 PROCEDIMENTO METODOLÓGICO

Segundo os procedimentos metodológicos, este trabalho, quanto à natureza, caracteriza-se como um resumo de assunto. Isso porque busca explicar a área do conhecimento do projeto, indicando sua evolução histórica, como resultado da investigação das informações obtidas, levando ao entendimento de suas causas e explicações (Wazlawick, 2014).

Quanto aos objetivos, é uma pesquisa exploratória e descritiva. A pesquisa descritiva busca dados mais consistentes sobre determinado assunto, porém não ocorre a interferência do pesquisador, apenas expõe os fatos como realmente são (Wazlawick, 2014). As pesquisas descritivas descrevem as características de certo fenômeno ou população. Também pode ser elaborada com o intuito de identificar as relações entre as variáveis (Gil, 2017).

A pesquisa exploratória muitas vezes é considerada como a primeira parte do processo de pesquisa, porque não necessariamente o autor tem um objetivo ou hipótese definida (Wazlawick, 2014). Essa pesquisa tem como objetivo a maior familiaridade do autor com o problema, tornando mais explícito, ou facilitar a construção de hipóteses. Geralmente é uma pesquisa flexível, porque considera os variados aspectos referentes aos fatos ou fenômeno estudado (Gil, 2017).

Quanto aos procedimentos técnicos, será uma pesquisa bibliográfica e qualitativa. A pesquisa bibliográfica requer o estudo de teses, artigos, entre outros. A pesquisa qualitativa tem como foco os processos do objeto de estudo (Gil, 2017)

A pesquisa bibliográfica será elaborada a partir de materiais já publicados, podendo incluir livros, teses, materiais disponibilizados na internet, revistas, entre outros. A principal vantagem é permitir uma sucessão de fenômenos maior do que seria capaz de pesquisar diretamente (Gil, 2017).

De acordo com Gil (2017), a pesquisa bibliográfica se desenvolve a partir das seguintes etapas:

a) A escolha de um tema: é necessário estar relacionada com o interesse do aluno. Além disso, possuir conhecimento prévio sobre a área de estudo para que as seguintes etapas sejam bem desenvolvidas.

b) Levantamento bibliográfico preliminar: realizar um levantamento bibliográfico para o pesquisador se habituar com à área de estudo escolhida, facilitando a definição do problema.

c) Formulação do problema: ao final da etapa b, o aluno estará em condições de definir o problema de forma clara, precisa e objetiva. O problema de pesquisa pode ser avaliado, verificando se possui relevância teórica e prática, se existe material bibliográfico suficiente para sua solução, se o aluno possui interesse no tema, entre outras questões.

d) Elaboração do plano provisório de assunto: elaboração de um plano provisório para definir a estrutura do trabalho, contendo uma apresentação organizada de suas partes.

e) Busca das fontes: identificar as fontes bibliográficas capazes de fornecer informações para ser possível responder o problema proposto, consultando dissertações, periódicos científicos, obras de referência, entre outros.
f) Leitura do material: identificar as informações e dados constando no material adquirido, estabelecendo relações com o problema proposto, e analisar a coerência das informações e dados apresentados pelos autores.
g) Fichamento: possui o objetivo de identificar as obras consultadas, anotar as ideias que surgiram, identificar as informações relevantes, registrar os comentários das obras e organizar as informações adquiridas.
h) Organização lógica do assunto: organizar as ideias com o propósito de atender os objetivos da pesquisa. A etapa g seria um dos elementos essenciais para elaboração dessa parte.
i) Redação do texto: constitui pela elaboração do relatório.

A pesquisa qualitativa é aquela que não se pode mensurar apenas com números e dados obtidos por meio de um questionário, por exemplo. É uma pesquisa focada em entender aspectos mais subjetivos, como comportamentos, ideias, pontos de vista, entre outros (Mathias, 2016).

O objetivo desse tipo de mensuração é entender, de forma mais profunda, o tema pesquisado e o que as pessoas pensam a esse respeito (Mathias, 2016).

A pesquisa qualitativa é composta das seguintes etapas:

a) Definir a problemática: ***Como os profissionais de software percebem e tratam a segurança de seus Sistemas de Banco de Dados?;***
b) Redigir as perguntas: fazer as escolhas de quais perguntas seriam pertinentes para conseguir coletar informações sobre a percepção do público-alvo em relação à segurança de Banco de Dados da empresa que eles trabalham;
c) Coletar dados;
d) Analisar os dados;
e) Compartilhar os dados.

4 Definição do Instrumento – Questionário (*Survey*) sobre a percepção dos Desenvolvedores em relação à Segurança de Banco de Dados

Um *Survey* é um instrumento de pesquisa, que visa construir um questionário, com a finalidade de colher amostras de opinião pertencentes ao público-alvo da pesquisa (Forza, 2002).
Este foi construído com base em problemas de Segurança na área de Banco de Dados discutidos na seção 2. O objetivo das perguntas foi coletar o nível de conhecimento que os Desenvolvedores de Software conhecem sobre Segurança de Banco de Dados e que medidas e cuidados tomam na hora de construção de seus sistemas.
Ao todo, foram entrevistados: 1 profissional da área de Gerência de Projetos, 1 de Design de Software, 2 de Desenvolvimento de Software, 6 de Implementação e 1 de Banco de Dados. Identificamos esses profissionais como público-alvo, pois queríamos saber sobre o nível de conhecimento de segurança em relação ao Banco de Dados.
No total, foram elaboradas 31 perguntas, divididas nas seguintes categorias:
de ataques à segurança (quando foi perguntado sobre malware, DDoS, SQL *Injection*) parte física (pergunta sobre o Sistema de Gerenciamento de Banco de Dados), de gerenciamento de acesso (questão de senha, treinamento do sistema), tecnológica (em relação à proteção em locais diferentes dos Backups, fazer teste nos Backups, intercepção de dados, procedimentos de classificação de dados, transferência de informações, direitos de propriedade intelectual e tratamento de dados sensíveis).

A seguir, segue a explicação de cada pergunta do questionário:

1ª Em qual área você trabalha?

Motivo de Escolha da Pergunta: por mais que o público-alvo escolhido foi os Desenvolvedores de *Software*, precisava-se saber qual a área em específico de trabalho para fazer a análise das respostas individualmente.

2ª Você já passou por algum problema relacionado à segurança que envolveu Banco de Dados?

Motivo da Escolha da Pergunta: como o trabalho é direcionado aos problemas e à área de Segurança, então resolvi começar com uma pergunta de âmbito mais geral.

3ª Que tipo de problemas em relação ao Banco de Dados? Descreva.

Motivo da Escolha da Pergunta: pois se o respondente respondesse que já teve problema relacionado à segurança, o intuito era que ele especificasse o tipo de problema.

4ª Você costuma proteger seus Backups?

Motivo da Escolha da Pergunta: um dos mecanismos importantíssimos dessa área é o Backup, por isso questionei onde os Backups que eles usam ficam protegidos.

5ª Caso você tenha marcado "outra" na questão anterior, quais medidas de segurança você usa?

Motivo da Escolha da Pergunta: pois existe a possibilidade de mecanismo que eles usem que eu não coloquei como opção de resposta.

6ª Periodicamente, você testa os Backups para ver se estão funcionando adequadamente?

Motivo da Escolha da Pergunta: pela existência da possibilidade de o Backup conter dados duplicados, incorretos, ou o Backup estar corrompido.

7ª Você já passou por alguma situação em que tenha ocorrido alguma interceptação de dados entre a Aplicação e o Servidor?

Motivo da Escolha da Pergunta: um dos problemas encontrado na minha pesquisa foi a intercepção de dados, sendo assim, queria saber se onde eles trabalham já passaram por isso.

8ª Se a resposta anterior foi "sim", qual o problema que teve?

Motivo da Escolha da Pergunta: somente para especificar qual o problema, se o entrevistado tivesse passado.

9ª Já passaste por algum problema relacionado à interrupção inesperada do fluxo de uma transação por motivos de falta de segurança?

Motivo da Escolha da Pergunta: quando se trata de Banco de Dados, o fluxo de transação acontece constantemente e quis saber se eles já passaram por algum problema em relação a isso.

10ª Se você respondeu sim na resposta anterior, descreva aqui o que aconteceu?

Motivo da Escolha da Pergunta: foi criada com um intuito de obter mais informações sobre a pergunta anterior.

11ª Você já passou por algum tipo de ataque de negação de serviço distribuído (*DDoS - Distributed Denial of Service*)?

Motivo da Escolha da Pergunta: enquanto estava fazendo a pesquisa sobre os problemas, eu vi falando bastante sobre esse ataque, que inclusive foi citado na Norma Técnica – ISO27002, que retrata sobre a Segurança da Informação, segurança cibernética e proteção à privacidade. Sendo assim, resolvi adicionar uma pergunta ao questionário, já que tem a ver com o assunto do trabalho.

12ª Onde seu o Sistema Gerenciador de Banco de Dados da empresa está alocado?

Motivo da Escolha da Pergunta: quando a empresa lida com diversos Bancos de Dados, há necessidade de se ter um sistema desse. Partindo desse princípio, resolvi perguntar onde o sistema que a organização que eles trabalham deixa alocado.

13ª Na sua opinião e vivência profissional, só pessoas autorizadas podem acessar o local onde estão os servidores de Banco de Dados?

Motivo da Escolha da Pergunta: pesquisando cada vez mais sobre Segurança em relação à Banco de Dados, percebe-se o quão é importante a questão do controle de acesso, que também foi citado na ISO27002. Por esse motivo, resolvi questionar aos entrevistados sobre a opinião deles em relação a esse assunto.

14ª Você usa senha-padrão no Sistema de Banco de Dados?

Motivo da Escolha da Pergunta: uso de senha-padrão, apesar de, às vezes, ser fácil de lembrar, mas é um meio para atrair problemas para essa área, como fazer uma modificação nos dados inadequadamente. Ou até uma exclusão indevida.

15ª Você troca a senha?

Motivo da Escolha da Pergunta: é bom ter esse hábito de fazer troca de senha, especialmente em relação aos sistemas, pois uma vez hackeado, pode acontecer outras vezes. Por isso, resolvi fazer o questionamento, para ver o quanto são cuidadosos em relação a isso.

16ª Você já teve algum problema relacionado com SQL *Injection*?

Motivo da Escolha da Pergunta: além de pesquisar sobre os problemas, também procurei sobre os ataques (que também são problemas) em relação ao Banco de Dados, e um dos mais comuns foi o SQL *Injection*. E, como consequência disso, decidi saber se, na vida profissional, já passaram por esse ataque.

17ª Onde você trabalha existe algum procedimento para classificação de dados sigilosos de acordo com a sensibilidade?

Motivo da Escolha da Pergunta: esse procedimento de dados é importante falar dele, pois caso a classificação seja feita de modo errado, o manuseio acaba sendo inadequado e, como consequência, acabam ocorrendo problemas bastante graves em relação a isso.

18ª Onde você trabalha existe algum procedimento para transferência de informações?

Motivo da Escolha da Pergunta: outro procedimento importante, na minha opinião, pois um manuseio errado pode trazer como consequência problemas mais graves.

19ª Onde você trabalha existe algum procedimento para direitos de propriedade intelectual?

Motivo da Escolha da Pergunta: achei justo questionar por se tratar de uma questão em que os códigos desenvolvidos de diferentes formas na empresa têm relação aos Bancos de Dados, e que, caso divulgados de forma inadequada, podem manchar a imagem da empresa.

20ª Na sua organização, existem serviços de infraestrutura?

Motivo da Escolha da Pergunta: achei importante questionar, pois, durante a construção desse trabalho, eu descobri que é a área de Infraestrutura que mantém o sistema da empresa seguro e que lida com o Banco de Dados diariamente. Ou seja, ela faz com que a segurança se torne cada vez mais forte, além de fazer a mitigação dos riscos associados às ameaças cibernéticas.

21ª Na organização, cada desenvolvedor tem seu próprio login e sua senha para acessar o Sistema de Banco de Dados?

Motivo da Escolha da Pergunta: sobre esse assunto, achei interessante perguntar, pois um acesso indevido pode acarretar, como consequência, problemas piores, como corromper os dados e modificar dados que são sensíveis.

22ª Dentro da sua organização, as pessoas compartilham seus login e senha?

Motivo da Escolha da Pergunta: para saber o quanto que esses profissionais se importam nessa questão, já que, para área de Banco de Dados, o credenciamento é um quesito muito importante.

23ª Você obteve treinamento sobre a Segurança do Sistema de Banco de Dados da sua empresa?

Motivo da Escolha da Pergunta: por mais que pareça algo insignificante, é uma coisa importante, pois, com treinamento, a pessoa consegue resolver os próprios problemas que aparecerem para ela e não tem risco de fazer algum manuseio errado dentro do sistema ou do Banco.

24ª Na organização, você assinou contrato ou Termo de Confidencialidade para preservar informações importantes?

Motivo da Escolha da Pergunta: É de extrema importância, pois, com esse contrato, tenta-se garantir que os dados não saiam da empresa, principalmente porque, no Banco de Dados, há presença de dados sensíveis que, em mãos erradas, podem ter manipulação inadequada.

25ª Sua organização já foi vítima de um ataque de malware (software malicioso, que se refere a qualquer tipo de software projetado com a intenção de causar danos ou realizar atividades maliciosas em um sistema ou dispositivo)?

Motivo da Escolha da Pergunta: esse é assunto tão sério que, na ISO27002, existe um controle que trata disso, e é comum de acontecer, além de que existem diversos tipos de malware.

26ª Existe algum tratamento para os dados sensíveis na sua organização?

Motivo da Escolha da Pergunta: esse tratamento é muito importante, pois feito de maneira errada, pode trazer diversos problemas, como: dados duplicados, corrompidos, ou causar a perda desses dados.

27ª Se a resposta à questão anterior for "sim", qual seria esse tratamento?

Motivo da Escolha da Pergunta: foi criada para obter mais informações sobre a questão, nesse caso, do tratamento para dados sensíveis.

28ª Quais as medidas de Segurança são tomadas para garantir a Confidencialidade do Sistema de Banco de Dados?

Motivo da Escolha da Pergunta: como, no trabalho, eu faço a relação dos problemas com a Confidencialidade, Integridade e Disponibilidade (CID), achei importante perguntar as medidas de Segurança em relação a cada um desses aspectos.

29ª Quais as medidas de Segurança são tomadas para garantir a Integridade do Sistema de Banco de Dados?

Motivo da Escolha da Pergunta: mesmo motivo da questão anterior, achei importante saber quais são as medidas usadas pelos entrevistados para deixar os dados íntegros no sistema.

30ª Quais as medidas de Segurança são tomadas para garantir a Disponibilidade do Sistema de Banco de Dados?

Motivo de Escolha da Pergunta: mesmo motivo da questão anterior, achei importante saber quais são as medidas usadas pelos entrevistados para deixar os dados disponíveis no sistema.

31ª Existe alguma informação em relação à Segurança de Banco de Dados que você acha importante relatar que não foi perguntado nesse questionário?

Motivo de Escolha da Pergunta: fiz essa pergunta para saber sobre a opinião dos respondentes se estava faltando algum assunto relacionado à Segurança de Banco de Dados para fazer pergunta.

Em suma, neste capítulo, foi mostrado como foi criado o questionário sobre Segurança de Banco de Dados, em que foi abordado sobre os problemas, ataques, a relação das medidas de segurança e o CID.

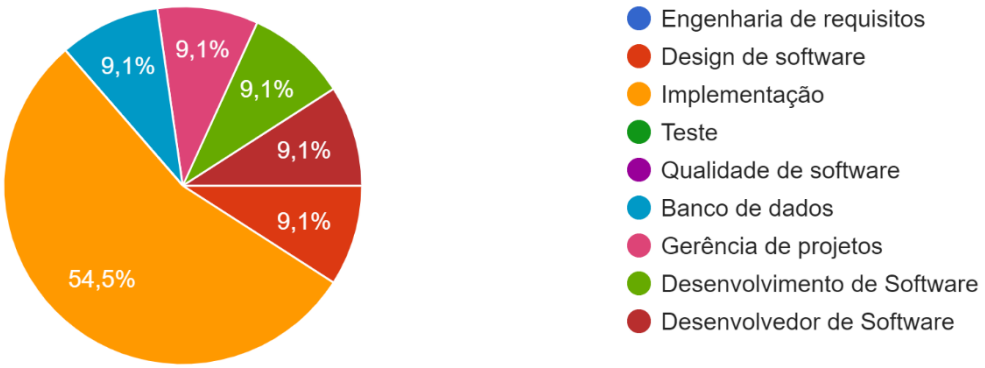
5 Resultados do Questionário

O questionário criado tem como objetivo avaliar o conhecimento dos desenvolvedores de software sobre a segurança dos Sistemas de Banco de Dados nas organizações onde trabalham. A construção do questionário teve como base os conceitos básicos citados na seção 2, que foram conceitos básicos sobre SBD, problemas relacionados à Segurança e as boas práticas, utilizando a norma ISO 27002 (“segurança da informação, segurança cibernética e proteção à privacidade -controles de segurança da informação *information security, cybersecurity and privacy protection -information security controls* norma brasileira exemplar para uso exclusivo -FORMAÇÃO DE LEAD IMPLEMENTER DE SGSI).

Assim que a elaboração do questionário foi finalizada, ele ficou disponível por uma semana, por conta dos prazos de TCC. Durante esse tempo, a amostra foi de 11 respondentes, entre eles: 1 Gerente de Projetos; 1 de Banco de Dados; 2 Desenvolvedores de Software; 1 Designer de Software; 6 Implementadores.

A seguir, os resultados de cada pergunta do questionário serão apresentados.

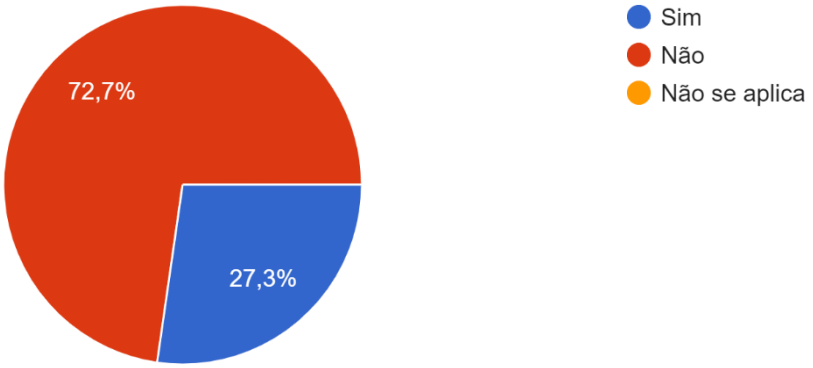
Figura 02 - Em qual área o entrevistado trabalha?



Resposta: percebe-se que a maior porcentagem foi da área de Implementação, em que tive 6 respondentes; em segundo lugar foi os Desenvolvedores de Software com 18,2%, correspondendo a 2 profissionais; o restante das porcentagens, ou seja, 9.1%, são das áreas de: Design de Software; Banco de Dados e Gerência de Projetos.

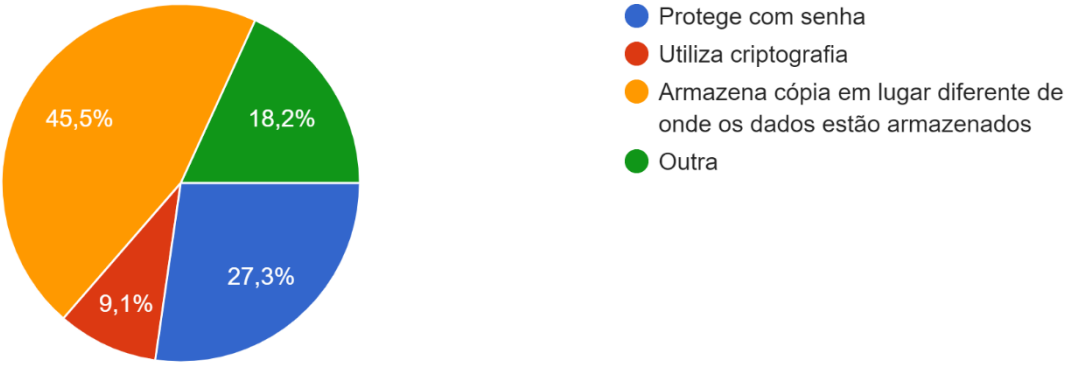
Análise: por mais que a amostra fosse pequena, a maioria dos respondentes são da área de Implementação.

Figura 03 - Se já passou por algum problema relacionado à segurança que envolveu o Banco de Dados?



Resposta: nesse gráfico, obtiveram-se 72,7% para não, ou seja, 8 votos de 5 profissionais da Implementação, Banco de Dados e um do Desenvolvimento de Software, e 3 votos, sendo 1 da Implementação, 1 de Desenvolvimento de Software e Design de Software, os quais falaram que os tipos de problemas sofridos foram: SQL *Injection*; Banco Corrompido e Fragilidade a salvar dados sensíveis que poderiam ser acessados se fizesse uma consulta pelo navegador. **Análise:** nesse ponto, percebe-se que os da área de Implementação, do Banco de Dados e um Desenvolvedor de Software têm mais segurança.

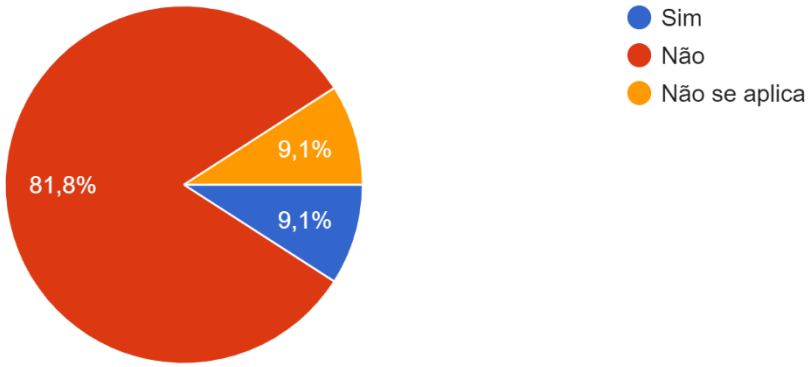
Figura 04 - Você tem costume de proteger os Backups?



Resposta: nessa questão, a maioria das pessoas protege o *Backup* em lugar diferente do que os dados realmente estão armazenados. Em segundo lugar, o maior mecanismo usado para a proteção de Backups é a proteção com senha. Em seguida, o mais usado é outro meio, tais como: cópia na nuvem e Backups que são feitos por hora e ficam armazenados na Azure. E, por último, mas não menos importante, é o uso de criptografia.

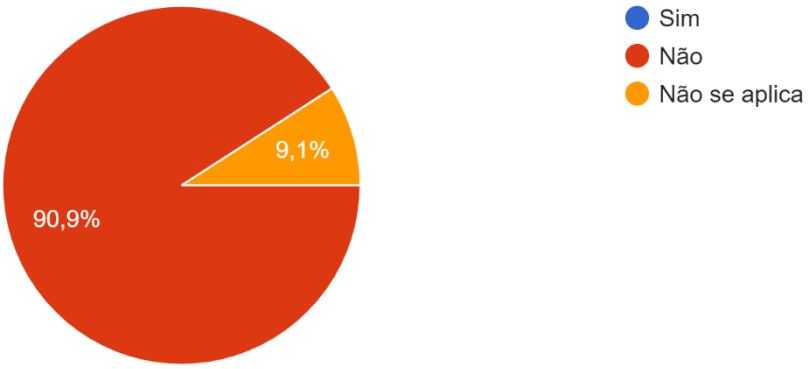
Possíveis Medidas: proteger o Backup com criptografia, chaves.
Análise: a maioria dos respondentes armazena o Backup da maneira mais segura, ou seja, o Backup em um lugar e a cópia em outro.

Figura 05 - Se testam os Backups periodicamente para ver se estão funcionando adequadamente?



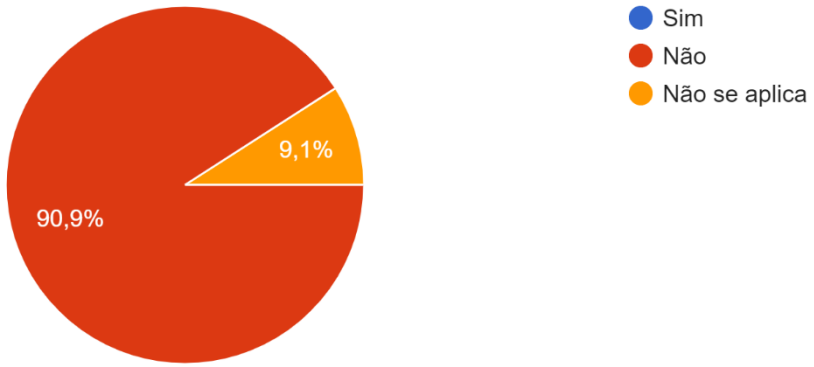
Resposta: como o gráfico apresenta, a maioria das pessoas entrevistadas, 9 de 11, disseram que não testam os Backups. Somente um profissional de Implementação faz esse teste, e um Desenvolvedor respondeu que não se aplica.
Análise: a maioria dos entrevistados não se preocupa em testar os Backups periodicamente.

Figura 06 - Você já passou por alguma situação que tenha ocorrido uma interceptação de dados entre Servidor e Aplicação?



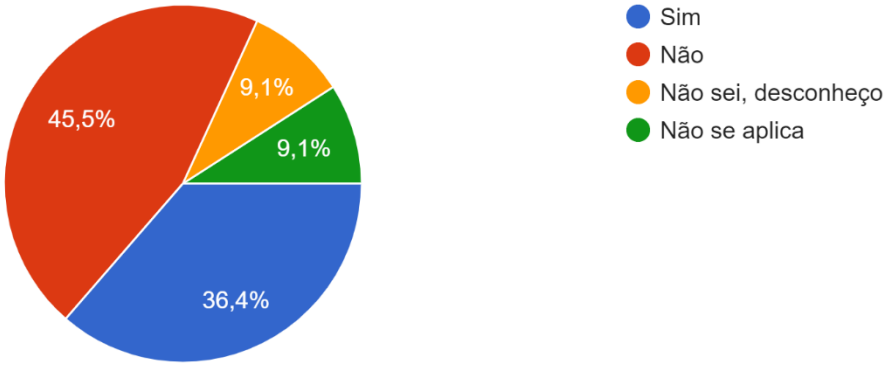
Resposta: nessa questão, tivemos 10 respostas não, e o único que respondeu não se aplica foi um profissional de Implementação.
Possível Medida: uso de protocolo HTTPS.
Análise: a maioria dos entrevistados é bem seguro em relação a esse quesito.

Figura 07 - Já passou por algum problema relacionado à interrupção inesperada do fluxo de uma transação por motivos de falta de segurança?



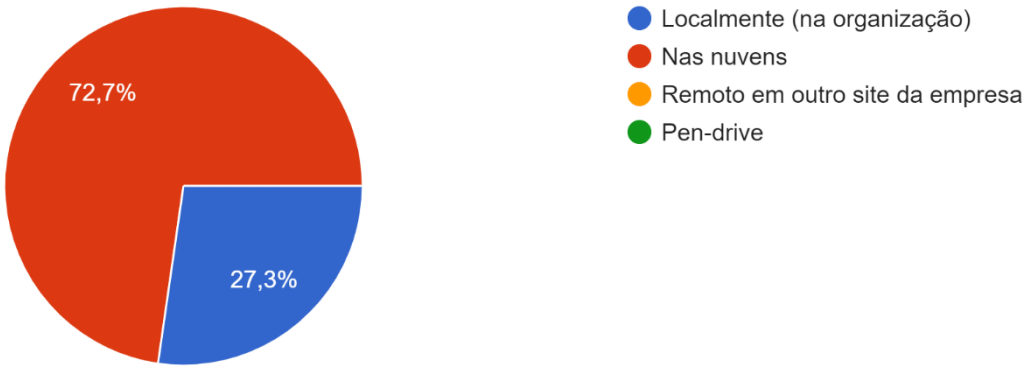
Resposta: para esse questionamento, tivemos 10 respostas não, e 1 resposta não se aplica, a qual foi respondida por um da área de Implementação.
Análise: a maioria das pessoas são bem seguras e o profissional da Implementação talvez não tenha entendido a pergunta.

Figura 08 - Você já passou por algum ataque de negação de serviço distribuído (DDoS – Distributed Denial of Service)?



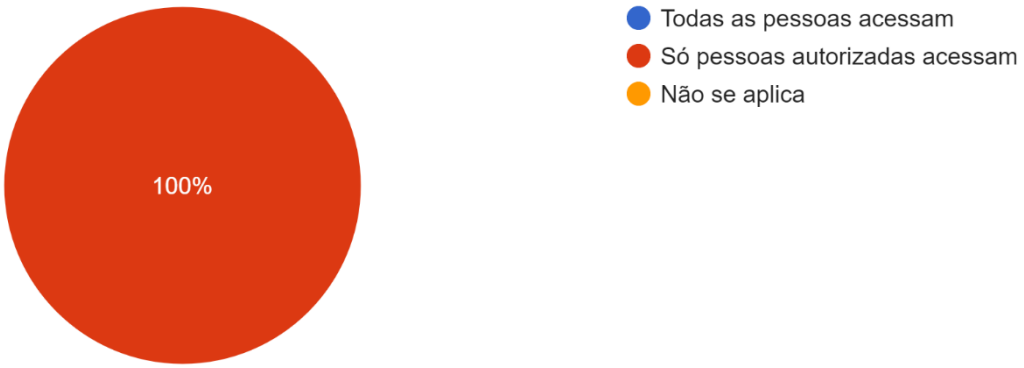
Resposta: nesse caso, tivemos 5 respostas não, sendo de 3 profissionais de Implementação; 1 Desenvolvedor de *Software* e 1 de Banco de Dados. Tivemos 4 respostas sim, uma do Gerente de Projetos; outra do Design de *Software*; 2 do pessoal de Implementação; 1 resposta não se aplica do outro Desenvolvedor de Software; e 1 profissional da Implementação que desconhecia.
Possível Medida: uso de Firewall e monitorar o tráfego.
Análise: a maioria das pessoas são seguros em relação a isso e o Desenvolvedor talvez não tenha entendido a pergunta.

Figura 09 - Onde o Sistema Gerenciador de Banco de Dados da empresa está alocado?



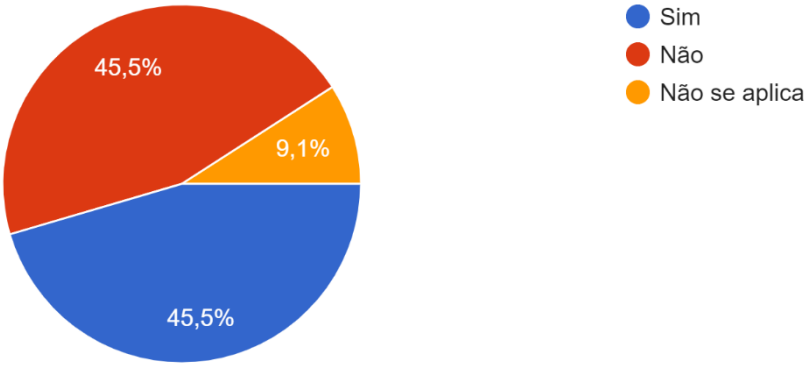
Resultado: nesse gráfico, a maioria das pessoas, mais especificamente, 8 pessoas responderam que o sistema está alocado nas nuvens, e outros 3 votaram que estão localmente, sendo eles: 1 de Desenvolvedor de Software e 2 da Implementação.
Análise: a maioria dos respondentes aloca-se o sistema no lugar mais seguro atualmente e os que responderam que alocam localmente correm um pouco de risco.

Figura 10 - Na sua opinião e vivência profissional, só pessoas autorizadas podem acessar o local onde estão os servidores de Banco de Dados?



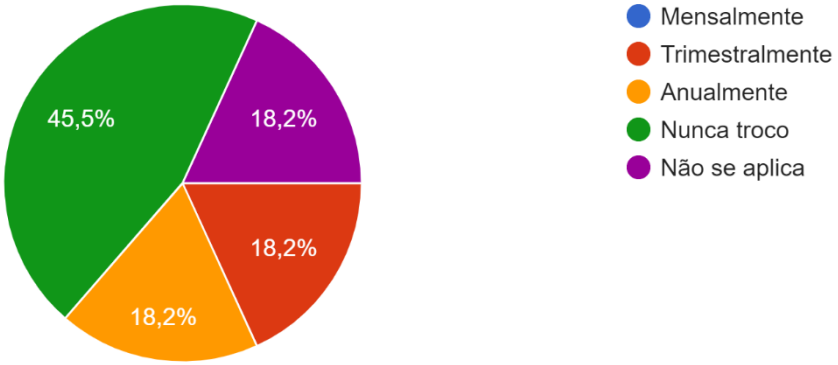
Resposta: como mostrado no gráfico, todos, ou seja, os 11 entrevistados, concordam que somente as pessoas autorizadas deveriam acessar o local onde os servidores estão.
Possível Medida: ter o próprio credenciamento.
Análise: todos concordam que somente as pessoas autorizadas podem acessar o local onde está o sistema.

Figura 11 - Você faz uso da senha-padrão no Sistema de Banco de Dados?



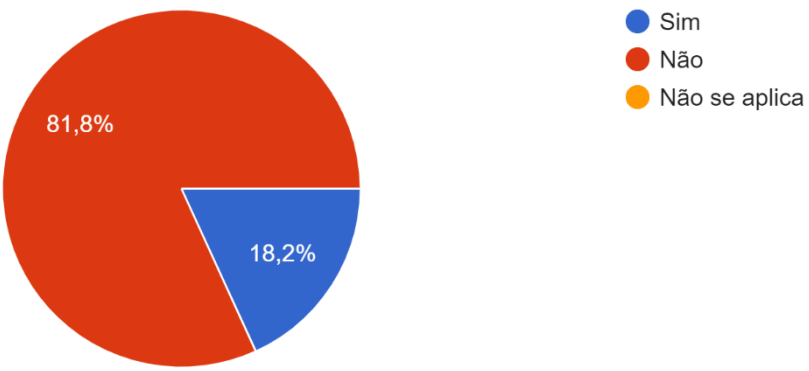
Resposta: há aqui um empate, em que 5 responderam sim e 5 responderam não, e teve uma única pessoa que respondeu não se aplica, que foi o profissional de Implementação.
Análise: os que responderam que não usa a senha-padrão mostram que são mais seguros dos que responderam que usam, e o que não se aplica deve não ter entendido a pergunta.

Figura 12 - Você troca a senha:



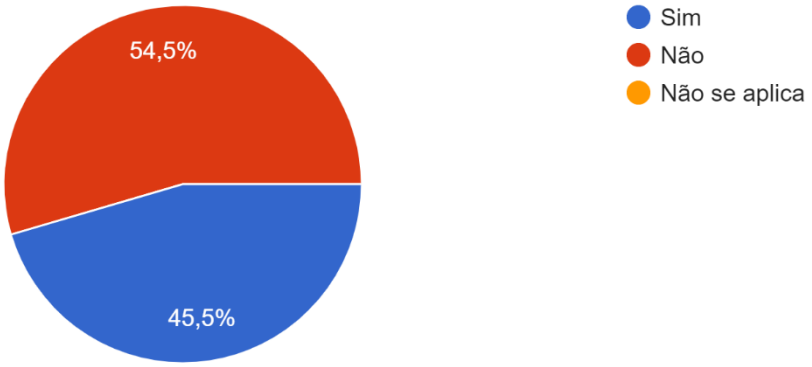
Resposta: a maioria das pessoas, mais especificamente 5 pessoas, responderam que nunca trocaram, entre elas: 1 Desenvolvedor de *Software*; 1 Designer de *Software*; 3 da área de Implementação. As outras 6 pessoas ficaram divididas entre: Não se aplica (respondido pelos 2 Implementadores); Trimestralmente (respondido por Gerente de Projetos e Desenvolvedor de *Software*); Anualmente (respondido por Banco de Dados e 1 da Implementação).
Análise: essas pessoas que responderam que nunca trocaram podem trazer um risco, pois quando a senha é descoberta, pode hackear o sistema e fazer alguma manipulação inadequada.

Figura 13 - Se já teve algum problema relacionado com SQL *Injection*?



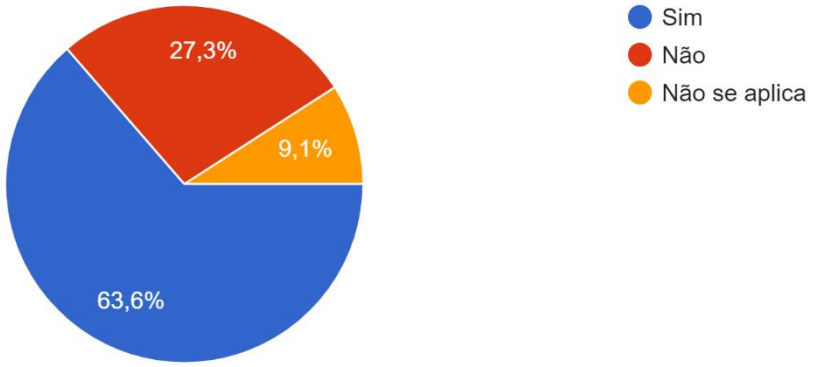
Resposta: como o gráfico mostra, o Gerente de Projetos; os 2 Desenvolvedores de *Software*; 5 profissionais da área de Implementação e da área de Banco de Dados votaram que não, e o Designer de Software e da área de Implementação votaram que sim.
Possível Medida: o Gerenciamento de Acesso, como, por exemplo: ter o próprio credenciamento.
Análise: os únicos que não têm segurança em relação a isso são o Designer e da Implementação.

Figura 14 – Se, onde eles trabalham, existe algum procedimento para a classificação de dados sigilosos de acordo com a sensibilidade?



Resposta: em relação a essa pergunta, 3 da área da Implementação; o Designer de *Software;* o de Banco de Dados; e um dos Desenvolvedores de *Software* votaram que não existe, e 3 da área da Implementação; o outro Desenvolvedor de *Software* e o Gerente de Projetos responderam sim. Em suma, foram 6 pessoas que responderam não e 5 responderam sim.
Análise: os 5 que responderam sim tem mais segurança, pois essa classificação é de suma importância do que os que responderam que não.

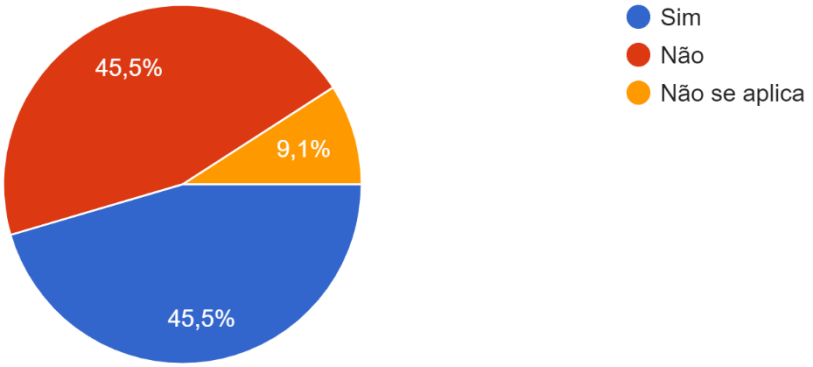
Figura 15 - Onde você trabalha existe algum procedimento para a transferência de informações?



Resposta: 7 pessoas votaram que sim, que existe esse procedimento, sendo eles: Gerente de Projeto; os Desenvolvedores de *Software*; 4 da área de Implementação. 3 votaram que não, sendo: 2 profissionais da Implementação e o de Banco de Dados. Além do Designer de *Software* que disse que não aplica.

Análise: as 7 pessoas que votaram sim são mais seguras e a pessoa que não aplica talvez não saiba da existência desse procedimento ou não tenha entendido a pergunta.

Figura 16 - Onde você trabalha existe algum procedimento para direitos de propriedade intelectual (que referem às proteções legais para criações originais da mente, como código)?



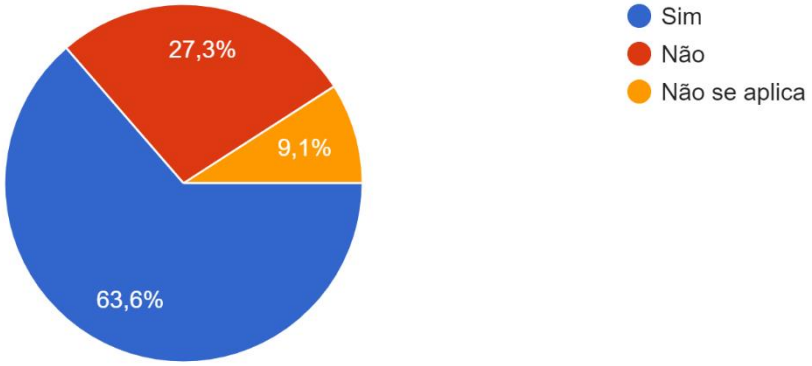
Resposta: tivemos um empate, ou seja, 5 votos para sim e 5 votos para não, e um único voto que não se aplica que foi dado por um Desenvolvedor de Software.

Análise: o que não se aplica talvez não saiba da existência desse procedimento e os que responderam que sim são os mais seguros do que os que responderam que não.

Figura 17 - Na sua organização, existem serviços de infraestrutura?

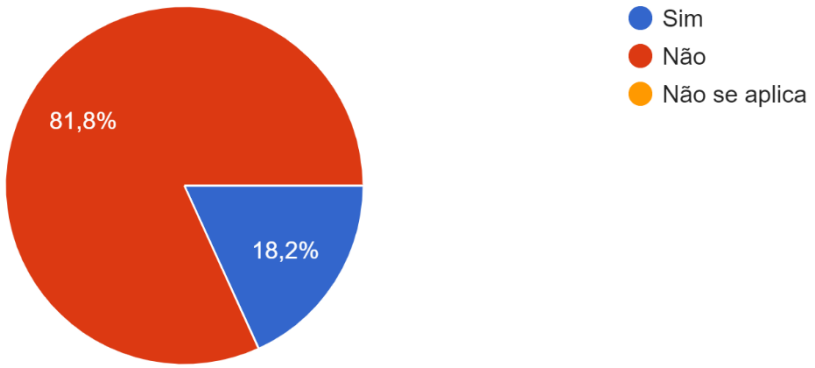
Resposta: como podemos ver, todos votaram que sim, que existem serviços de Infraestrutura onde eles trabalham.
Análise: todos os respondentes concordam que deveria existir o serviço de Infraestrutura

Figura 18 – Se, na organização, cada desenvolvedor tem seu próprio login e senha para acessar o sistema?



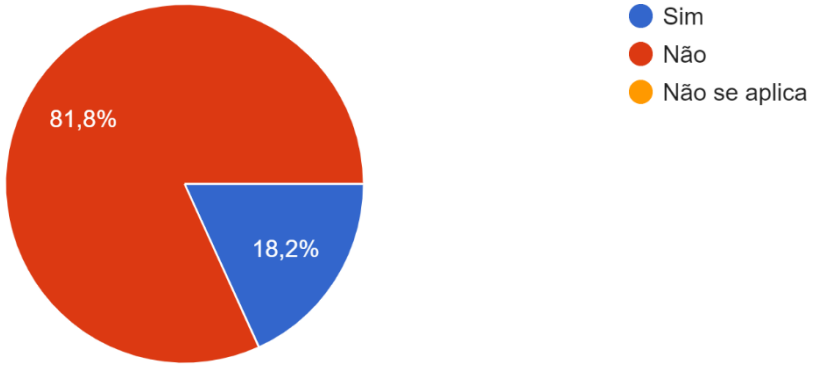
Resposta: a maioria votou que sim, sendo eles: Desenvolvedores de *Software*, 3 na área de Implementação; Designer de *Software* e Banco de Dados. Os 3 que votaram que não foram os 3 restantes da área da Implementação e o Gerente de Projetos votou que não aplica.
Análise: os que responderam que não tem o próprio login e senha têm mais risco de ter problemas do que responderam que sim.

Figura 19 - Dentro da sua organização, as pessoas compartilham seus login e senha?



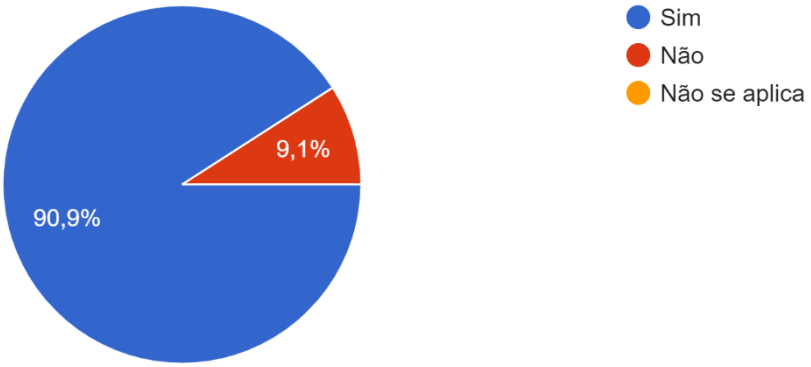
Resposta: Como mostrado nesse gráfico, a maioria dos respondentes respondeu que não compartilham, e apenas 2 pessoas votaram que sim, sendo os 2 profissionais da Implementação, e não se obteve resposta de não se aplica.
Análise: a maioria dos entrevistados são mais seguros do que os 2 da Implementação.

Figura 20 - Se obteve treinamento sobre a Segurança do Sistema de Banco de Dados da empresa?



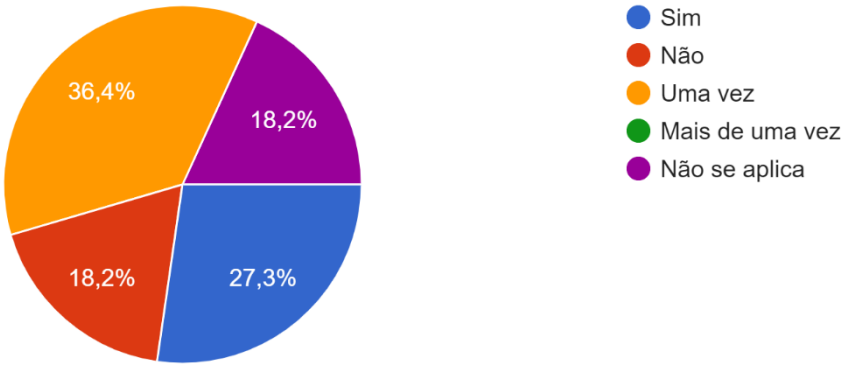
Resposta: observando o gráfico, percebe-se que 9 respondentes não receberam/tiveram o treinamento, e somente 2 respondentes tiveram, que são um dos Desenvolvedores de *Software* e o da área de Implementação.
Análise: os que tiveram treinamento garantem mais segurança, pois conseguem resolver os erros e entender do que se trata ao contrário do que os que não tiveram.

Figura 21 - Na organização, teve que assinar o contrato ou termo de Confidencialidade para preservar informações importantes?



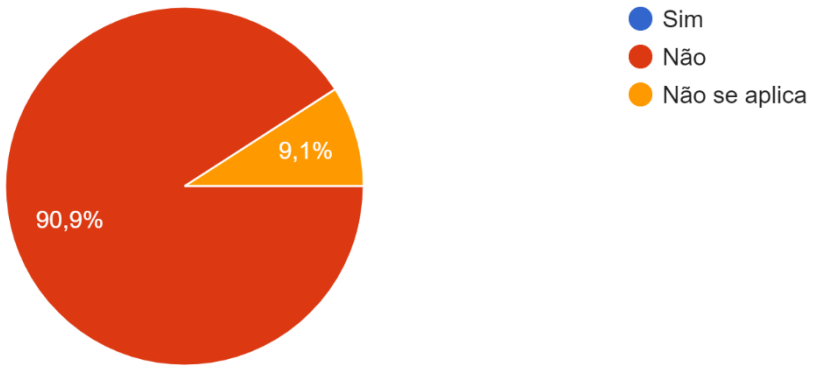
Resposta: observando-se o gráfico, vemos que a maioria dos respondentes falou que sim, e teve um único voto para que não, sendo do profissional de Banco de Dados.
Análise: o único que não assinou esse termo é o que mais deveria assinar, pois pode ser o que tenha mais contato com o Banco dentre todos os entrevistados.

Figura 22 - A organização onde trabalha já teve um ataque de malware (software malicioso, que se refere a qualquer tipo de software projetado com a intenção de causar danos ou realizar atividades maliciosas em um sistema ou dispositivo)?



Resposta: como mostrado no gráfico, 4 pessoas (Gerente de Projetos; 1 dos Desenvolvedores de *Software*; 1 da área de Implementação; e o de Banco de Dados) responderam falando que tiveram ataque pelo menos uma vez; em segundo lugar, responderam que sim: sendo 2 da área de Implementação e o Designer de Software, e por último obteve-se empate entre não se aplica e não, 2 votos para cada, respectivamente.
Possível Medida: uso de antivírus.
Análise: os que responderam que houve ataque pelo menos uma vez, talvez, na época, não tinha segurança necessária, mas agora tenha.

Figura 23 - Existe algum tratamento para os dados sensíveis (dados pessoais que, se expostos, podem causar danos a uma pessoa, por exemplo, dados de saúde) em sua organização?



Resposta: no gráfico, mostra que a maioria respondeu que não existe esse tratamento e um único respondente colocou que não se aplica, sendo ele um dos Desenvolvedores de *Software.*
Análise: o que respondeu não se aplica talvez não conhecesse o procedimento

24 - Quais as medidas de Segurança são tomadas para garantir a Confidencialidade do Sistema de Banco de Dados?

Para essa pergunta, obtive algumas respostas: senhas e restrições de acesso; controle de acesso, descaracterização dos dados (onde necessário); Termos de Confidencialidade e Logs que mantém registros de acessos aos Bancos de Dados; login e senha; VPN para trabalhos remotos; Criptografia dos Dados, Backups diários, além do isolamento da rede em que se encontra.

25 - Quais as medidas de Segurança são tomadas para garantir a Integridade do Sistema de Banco de Dados?

Para essa pergunta, obtive algumas respostas: checkups e Backups*;* utilização de sistema de gerenciamento de bancos de dados robusto, medidas protetivas em caso de falhas; o uso do *Liquibase*; réplicas; análise diária de dados por amostra nas tarefas que são testadas diariamente; login e senha; uso de *VPN*.

26 - Quais as medidas de Segurança são tomadas para garantir a Disponibilidade do Sistema de Banco de Dados?

Para essa pergunta, obtive algumas respostas: réplicas e *point in time recovery*; monitoramento automatizado dos servidores, ferramentas de recuperação automáticas; acesso restrito; divisão dos bancos de dados por servidores; subir o banco no Google drive; a gente se apoia muito na Microsoft para tomar conta da disponibilidade do sistema; login e senha; a empresa disponibiliza os dados no Jenkins, que somente é acessado por senha pessoal e via VPN (no caso de trabalho remoto); armazenamento em nuvem.

27 - Existe alguma informação em relação à Segurança de Banco de Dados que você acha importante relatar que não foi perguntado nesse questionário?

Resposta: nessa questão em específico, a maioria das respostas foram negativas, as únicas diferentes foram em questão à Criptografia e à adição de balanceamento de carga e *clustering*, que auxiliariam a aumentar a disponibilidade e a integridade de um banco de dados comercial.
Análise: a maioria dos respondentes acharam que perguntei tudo.

6 Conclusões e trabalhos futuros

Como os profissionais de software percebem e tratam a segurança de seus sistemas de banco de dados? Esse trabalho identificou que, apesar da amostra ter sido pequena, a prática de testar os Backups periodicamente não existe para a maioria dos Desenvolvedores; sobre a questão da proteção de Backups, a maioria respondeu que armazena a cópia em lugar diferente, onde os dados originais estão armazenados, mas teve resposta que existe proteção em nuvens e Backups feitos por hora e que ficam armazenados no Azure.
Além disso, mostrou que, na maioria das organizações, existe um login e senha específico para cada Desenvolvedor e a maioria deles não as compartilham.
Foi percebido também que, em relação ao Termo de Confidencialidade, o único que não assinou foi o profissional de Banco de Dados.
Em relação aos ataques mencionados neste trabalho, o que teve resultado positivo e o maior resultado foi o ataque de malware.
Foi-se questionado sobre algum problema relacionado à segurança de Banco de Dados, em que se obteve 72,7% de respostas negativas, ou seja, maioria dos respondentes falaram que não tiveram, porém, obtive respostas positivas, nas quais, mais especificamente, teve respondentes que especificaram os problemas que tiveram, como: Banco Corrompido; SQL *Injection*; Fragilidade ao salvar dados sensíveis que poderia se fizesse uma consulta pelo navegador.
Sobre Gerenciamento de Acesso, 100% dos respondentes disseram que somente pessoas autorizadas acessam o local onde estão os servidores de Banco de Dados; outro ponto questionado foi sobre o treinamento em relação à segurança do Sistema de Banco de Dados e a maioria dos respondentes disse que não.
No que se refere ao Gerenciamento Tecnológico, 6 das 11 respostas apontam que, na maioria das organizações, não existe procedimento para classificação de dados sigilosos de acordo com a sua sensibilidade e também não existe algum tratamento para os dados sensíveis, contudo, na maioria das empresas, existe procedimento para transferência de informações.

Em relação aos trabalhos futuros, uma sugestão é na questão de expansão do grupo de amostra, ou seja, aplicar esse mesmo questionário para outros profissionais da área ou até mesmo fazer pesquisa mais ampla em relação aos problemas de Segurança.
Outra sugestão é estudar mais a fundo quais problemas atingem essa área e também maneiras de melhores meios de preparar os Desenvolvedores de Software, caso passem por alguma situação parecida citada no Referencial Teórico deste trabalho.

REFERÊNCIAS

AL-SAYID, N.; ALDLAEEN, D. **Database Security Threats: A Survey Study.** [s.l: s.n.]. Acesso em: 22 out. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27002:2022**: segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação. Rio de Janeiro: [*s. n.*], 2022. 191 p.

A Equifax expôs 143 milhões de pessoas porque não atualizou software. Disponível em: <https://tecnoblog.net/noticias/2017/09/14/equifaxvazamentovulnerabilidade/>. Acesso em: 24 set. 2023

Como fazer uma pesquisa qualitativa? – Drag'n Survey Blog Português. Disponível em: <https://www.dragnsurvey.com/blog/pt/como-fazer-um-estudo-qualitativo/>. Acesso em: 16 dez. 2023.

Database.Dictionary.cambridge.org, dictionary.cambridge.org/dictionary/english/database. Acesso em: 11 Nov. 2023.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Fundamentals of Database Systems**. 2. ed. Vancouver, Canada: The Book Company, 1994. 871 p. ISBN 08053-1748-1.

GAIDARGI, J. **Erros que comprometem a segurança do seu banco de dados - Infonova**. Disponível em: <https://infonova.com.br/errosegurancabancodados/>. Acesso em: 15 out. 2023.

Gestão de banco de dados: 5 problemas causado pela falta dela. Disponível em: <https://www.advancedit.com.br/gestao-de-banco-de-dados-5problemascausados-pela-falta-dela/>. Acesso em: 20 out. 2023.

IBM Security. **Five common data security pitfalls to avoid**: Learn how to improve your data security and compliance posture. 29p.

KORTH, Henry F. et al**. Sistema de Banco de Dados**. 2. ed. rev. São Paulo: MAKRON Books, 1995. 754 p. ISBN 85-346-0372-3.

MATHIAS, L. **Pesquisa quantitativa e qualitativa: qual é a melhor opção?** Disponível em: <https://mindminers.com/blog/pesquisa-qualitativa-quantitativa/#:~:text=A%20pesquisa%20qualitativa%20%C3%A9%20aquela>. Acesso em: 10 nov. 2023.

O que é criptografia de dados? Definição e explicação. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/encryption>.

O Que é Redução de Dados | Pure Storage.*Www.purestorage.com*, www.purestorage.com/br/knowledge/what-is-data-reduction.html. Acesso em: 12 nov. 2023.

O que é Segurança de Dados? | Micro Focus. Disponível em: <https://www.microfocus.com/ptbr/whatis/datasecurity#:~:text=Seguran%C3%A7a%20de%20dados%20%C3 %A9%2 0o>. Acesso em: 7 out. 2023.

Práticas Recomendadas e Soluções de Segurança de Banco de Dados | Microsoft Azure, [s.d.]. Disponível em: <https://azure.microsoft.com/ptbr/resources/cloud-computingdictionary/whatis-database-security/#whyimportant>. Acesso em: 15 out. 23

Resiliência de dados. Disponível em: <https://www.ibm.com/docs/pt/i/7.3?topic=availability-data-resilience>. Acesso em: 7 out. 2023.

Savelli, Thiago. **Falhas de Segurança Digital: Conheça as 7 Mais Comuns Em PMEs.** *Dfndr Blog - PSafe*, 6 aug. 2021, www.psafe.com/blog/falhasdesegurancadigital/#:~:text=Entre%20as%20principais%20est%C3%A3o%3A %201%20Ext ors%C3%A3o%20e%20chantagem. Acesso em: 12 nov. 2023.

Schemes, Taynara. **Centralização de Informação: Qual a Importância E Como Fazer Na Empresa.** *Movidesk Blog*, 7 jan. 2021, conteudo.movidesk.com/centralizacao-de-informacao/. Acesso em: 12 nov. 2023.

Soluções de segurança e proteção de dados | IBM. Disponível em: <https://www.ibm.com/br-pt/data-security?utm_content=SRCWW&p1=Search&p4=43700075674345928&p5=p &gclid=CjwKCAjwseSoBhBXEiwA9iZtxggZ4zMhthKkexf63UkjtZvijsj6sc2CFTVMdcaPlaPihL6ozlnBoCN6UQAvD_BwE&gclsrc=aw.ds>. Acesso em: 15 out. 2023.

Soluções e benefícios de segurança de dados na nuvem. Disponível em: <https://cloud.google.com/learn/what-is-cloud-datasecurity?hl=ptbr#:~:text=A%20seguran%C3%A7a%20de%20dados%20do%2 0Cloud%20prot ege%20os%20dados%20armazenados>. Acesso em: 7 out. 2023.

YOUNG, R. **Five Common Data Security Pitfalls: Do You Know How to** Avoid **Them?** Disponível em: <https://securityintelligence.com/five-epicfailsindata-security-do-you-know-how-to-avoid-them/>. Acesso em: 15 out. 2023.