Universidade Fernando Pessoa

Doutoramento em Ciências da Informação

Linha de Pesquisa: Sistemas, Tecnologia e Gestão da Informação

Mecanismos de segurança Blockchain integrados aos ecossistemas de IoT

Doutorando: Ronaldo Borges do Val

Orientador: Professor Doutor Luís Borges Gouveia

Porto-PT – 26 de Janeiro 2024

APRESENTAÇÃO

Blockchain

Tecnologia originária da teoria dos Sistemas Distribuídos, acrescida de algoritmos criptográficos, validam a transação de dados através de mecanismos de consenso a fim de garantir segurança em diferentes dispositivos conectados em rede sem um elemento central para gerenciar os dados. Dentre os dispositivos: ***IoT***.

Garantir a segurança na troca de dados imutável entre esses dispositivos é um desafio, pela complexidade de modelos, funções e funcionamento na Internet.

MOTIVAÇÃO

Apresentar proposta na integração de objetos físicos com o mundo cibernético, visando facilitar as relações de negócios e a melhor convivência humana através da coleta, transmissão e armazenamento de dados, muitas vezes pela Internet.

As transações realizadas nesse ambiente estão cada vez mais suscetíveis de serem interceptadas causando diferentes danos durante a sua operação pelos usuários de variados tipos de aplicações.

PROBLEMA

À medida que as tecnologias emergem, crescem as preocupações com a segurança, suscetíveis a incidentes de variadas proporções e danos: como acesso não autorizado, copia de dados durante o seu tráfego, ataques a dispositivos entre outros.

Analisar impactos e fatores de segurança entre aplicativos Blockchain aos ecossistemas de IoT caracteriza o problema a ser pesquisado, bem como *propor melhorias* a partir da identificação de situações de vulnerabilidade de um *modelo que visa contribuir para melhor aproveitamento das tecnologias quanto à segurança e privacidade*.

JUSTIFICATIVA DA PESQUISA

Investigar vulnerabilidades dentro do conjunto de tecnologias que compõem a Blockchain numa abordagem baseada na complexidade na integração com dispositivos de IoT, a partir de estudos de caso e pesquisa metodológica visando apresentar evidências que podem gerar elementos de inconsistência, vulnerabilidade ou falhas de segurança.

HIPÓTESE

Considerando as abordagens tratadas sobre a segurança da tecnologia Blockchain no ecossistema de IoT, apresentaremos no trabalho uma contribuição ao tema, com *recomendações às boas práticas de uso das tecnologias* discutidas, baseada na revisão da literatura, em estudos de caso apresentados, e nos dados levantados a partir da pesquisa por questionário exploratório, no qual formamos um conjunto de conhecimentos a fim de apresentarmos uma visão a respeito da preocupação sobre a segurança referida no problema da pesquisa.

RESULTADO ESPERADO

Propor mecanismos de proteção e segurança quando da utilização da Blockchain utilizando IoT integrados;

Apresentar requisitos de segurança e privacidade que garantem resiliências a ataques, autenticação de dados, controle de acesso e privacidade do usuário aos diversos aplicativos a serem desenvolvidos a favor de melhor utilização ao usuário.

OBJETIVOS

Identificar vulnerabilidades nos mecanismos de segurança no sistema Blockchain na integração a dispositivos IoT.

OBJETIVOS GERAIS

- Identificar anormalidades de segurança e propor padrões que atendam à tecnologia na adequação a diferentes soluções na economia digital, nas relações com a sociedade e governos;

- Levantar estudo sobre os problemas encontrados no que se refere à falta de critérios de segurança que possam impactar na falha de sistemas.

OBJETIVOS ESPECÍFICOS

Identificar vulnerabilidades nos mecanismos de segurança no sistema Blockchain integrados a dispositivos IoT.

- Verificar impactos na mensurações ofertadas de segurança;
- Avaliar pensamentos dos autores e a sua contribuição para a pesquisa;
- Verificar diferentes padrões e normas de segurança no uso das tecnologias pesquisadas;
- Estimar o nível de melhoria na qualidade após a inclusão de elementos de mensuração;
- Investigar processos de implantação da tecnologia com o propósito de catalogar evidências na identificação de possíveis falhas e dificuldades de uso na tecnologia.

OBJETIVOS ESPECÍFICOS

- Apresentar proposta metodológica quali-quantitativa para análise dos estudos relacionados com o uso e exploração da Blockchain em um ecossistema de IoT;

- Avaliar a dinâmica de surgimento de novas tecnologias e dispositivos, as suas práticas de normalização ou padronização na fabricação, comercialização, implementação e manutenção de diferentes dispositivos de IoT e desenvolvimento de aplicações Blockchain.

ORGANIZAÇÃO DA TESE

O documento está organizado e estruturado em ***09 (nove) capítulos***.

Capítulo I

Escopo do trabalho, o que se propõe na tese e as etapas para se chegar através de um roteiro apresentado, a partir da Introdução, a Motivação, sua preparação a partir da Definição do Problema, Justificativa, Hipótese e seus Objetivos Gerais e Específicos.

Capítulos II, III e IV

Descrevemos a ***Revisão de Literatura ou Estado da Arte***, que estão contextualizadas no conhecimento referente ao estudo do problema.

ORGANIZAÇÃO DA TESE

Capítulo II

- Fundamentos de Sistemas Distribuídos, base da Tecnologia de Blockchain e a sua arquitetura com os desafios em sua implementação;

- Estudos de caso através de modelos de ecossistemas criados, a sua aplicação nos negócios a partir do modelo DAO e uma breve explanação sobre as Criptomoedas;

ORGANIZAÇÃO DA TESE

Capítulo II

- Tecnologia de Internet das Coisas a partir dos conceitos da Computação Ubíqua, de Ambientes Inteligentes, das Redes de Sensores sem Fio e da aplicação da Internet das Coisas na Indústria, IIoT.

ORGANIZAÇÃO DA TESE

Capítulo III

- Aspectos de segurança em Sistemas Blockchain e IoT, suas principais propriedades;
- Histórico dos principais tipos de ataques realizados, sua estrutura, a integração com o ecossistema de IoT;
- Padrões, Normas e Recomendações de uso para as tecnologias Blockchain e IoT;

ORGANIZAÇÃO DA TESE

Capítulo IV

- Parte final da revisão da literatura, tem um papel importante na formação do documento que trata dos mecanismos de segurança a partir de métodos de prevenções e recomendações.

ORGANIZAÇÃO DA TESE

Capítulo V

- Apresenta a Metodologia de Investigação;

- Pesquisa exploratória e um modelo de dados qualitativo e quantitativo.

ORGANIZAÇÃO DA TESE

Capítulos VI e VII

Apresentam os resultados e a análise do questionário exploratório que comparado com as teorias apresentadas nos Capítulos II e III e os dados estatísticos darão suporte ao desenvolvimento do Capítulo VIII.

ORGANIZAÇÃO DA TESE

Capítulo VIII

- Apresenta um modelo de referência a respeito da integração de Blockchain com IoT nos seus aspectos de segurança.

ORGANIZAÇÃO DA TESE

Capítulo IX

- Concluímos o trabalho, apresentando as considerações finais, as nossas contribuições, as restrições na pesquisa, as publicações resultantes da investigação bem como trabalhos futuros e recomendações.

Referências e Apêndices

FUNDAMENTAÇÃO TEÓRICA

Fonte: Elaborado pelo Autor.

FUNDAMENTAÇÃO TEÓRICA

Partimos do conceito de Sistemas Distribuídos, apresentando uma visão alternativa e complementar para se entender os fundamentos da Blockchain, em outra perspectiva relacionada com as aplicações de moedas digitais.

Apresentamos sua arquitetura, funcionamento e utilização nas mais diversas áreas, seus desafios em uma implantação.

FUNDAMENTAÇÃO TEÓRICA

Adicionamos na revisão da literatura, um breve relato sobre moedas digitais como subsistema da Blockchain e seu comparativo entre as duas principais, Bitcoin e Ethereum.

FUNDAMENTAÇÃO TEÓRICA

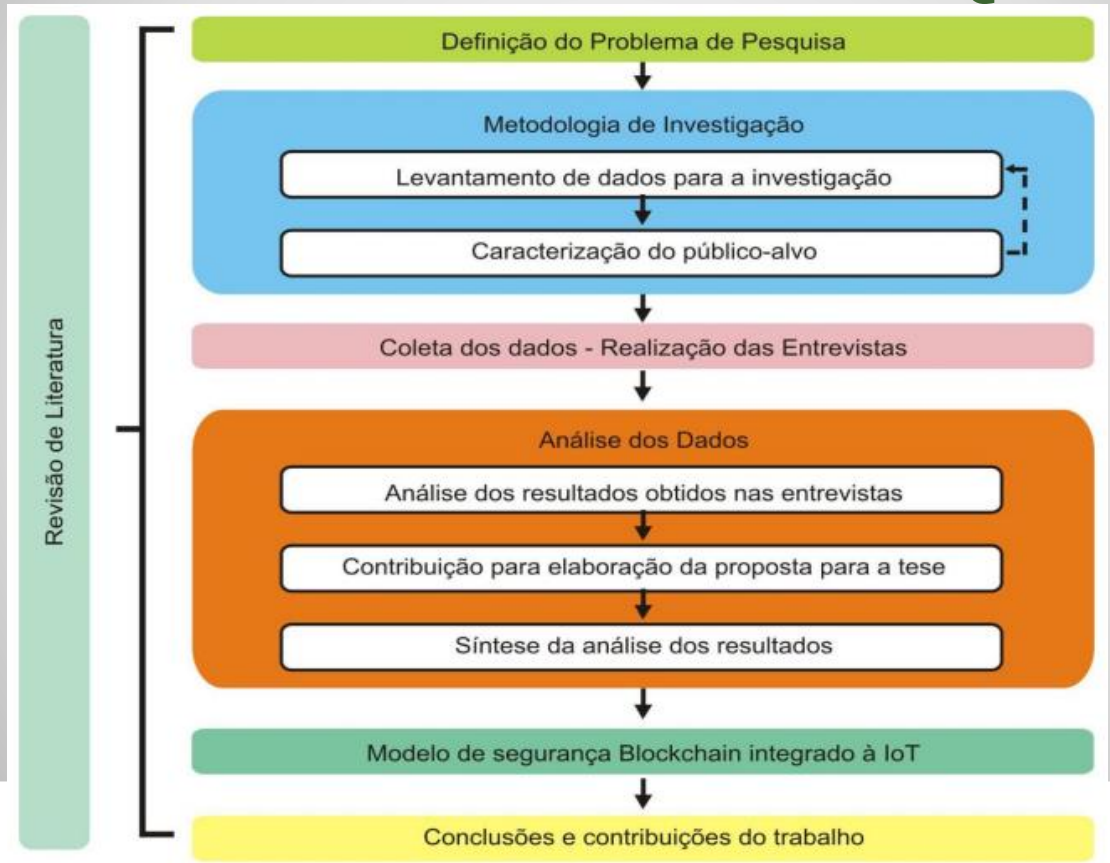
Para integração da Blockchain com dispositivos de IoT, o princípio da ***computação móvel e pervasiva***, sua arquitetura, componentes, ecossistemas IoT, conceitos de ***IIoT***, Internet das Coisas na Indústria, conceitos de ***Hiperconectividades*** e os desafios na implantação dessas tecnologias, acrescentando o conceito de cidades inteligentes a uma visão macro das tecnologias integradas.

FUNDAMENTAÇÃO TEÓRICA

SEGURANÇA DA INFORMAÇÃO

Princípios
Requisitos
Políticas e Gestão

METODOLOGIA DA PESQUISA



Fonte: Elaborado pelo Autor.

METODOLOGIA DA PESQUISA

- Questionário exploratório, devidamente autorizada pela autoridade brasileira, no caso o Comitê de Ética em Pesquisa do Ministério da Saúde do Brasil;

- Conjunto de questões relacionadas ao objeto de estudo da tese, elencando pontos de opiniões de diferentes perfis dos entrevistados;

-

- Público-alvo definido;

- Sigilo dos dados pessoais dos entrevistados, conforme legislação brasileira;

- Coleta de dados por uma entrevista em plataforma virtual.

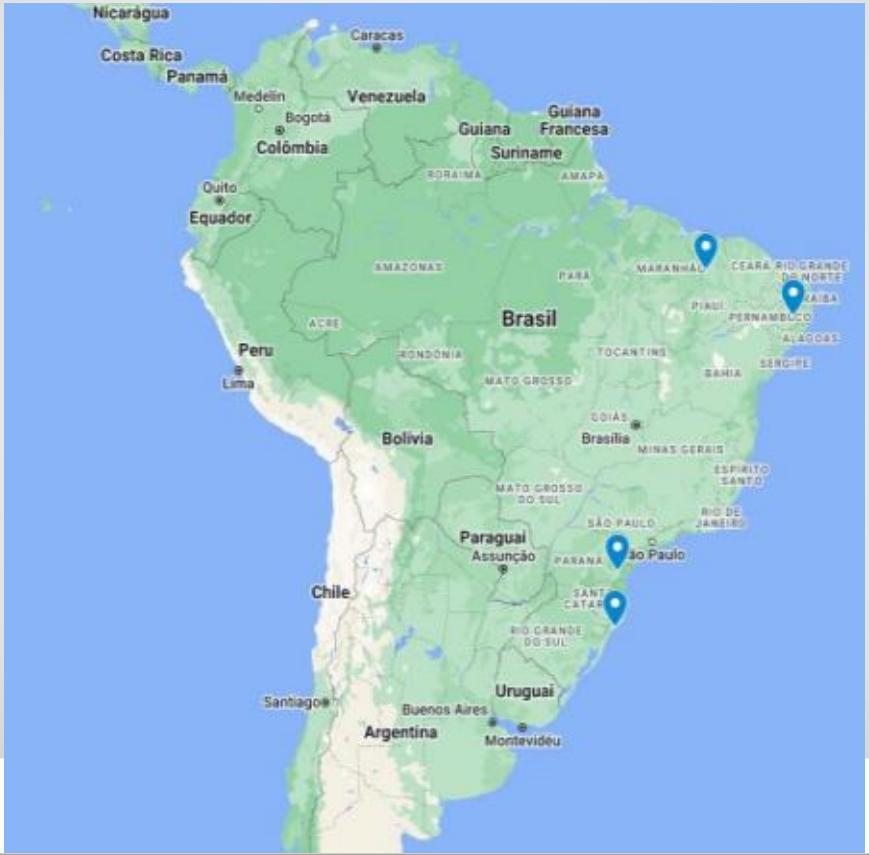
PESQUISA EXPLORATÓRIA
Público-alvo

Quantidade de Entrevistados: 15 (quinze) entrevistados, 02 (duas) mulheres e 13 (treze) homens.

Pesquisa: No período de 11/122 a 19/12/2022.
Realizado pela ferramenta Google Forms, 25 (vinte e cinco) perguntas e 375 (trezentos e setenta e cinco) respostas de diferentes formatos nas questões.

PESQUISA EXPLORATÓRIA

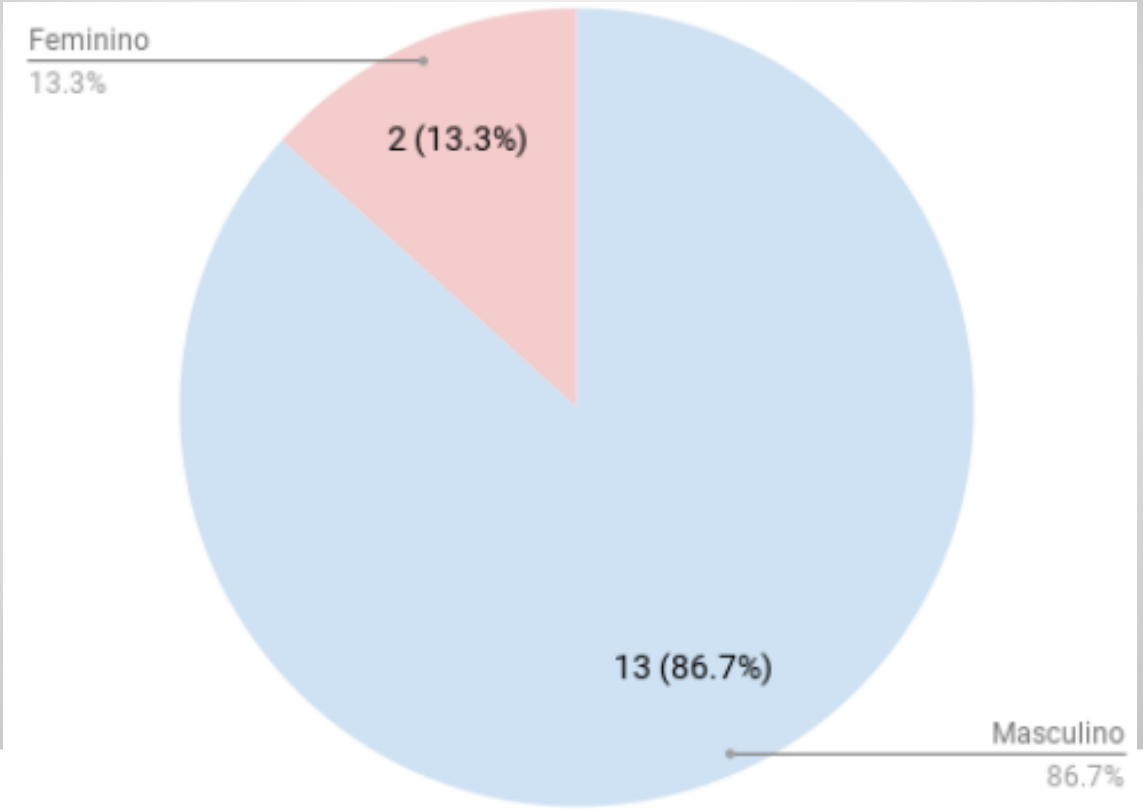
Público –alvo:
Localização geográfica



Fonte: Elaborado pelo Autor.

PESQUISA EXPLORATÓRIA

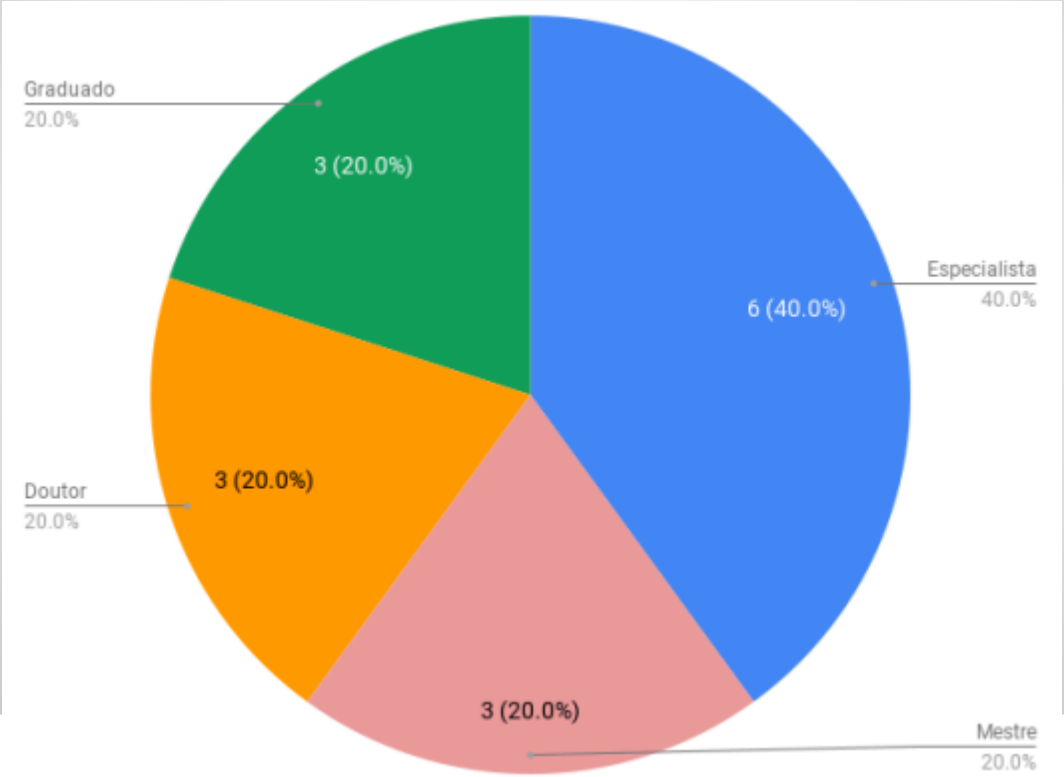
Público-alvo:
Sexo



Fonte: Elaborado pelo Autor.

PESQUISA EXPLORATÓRIA

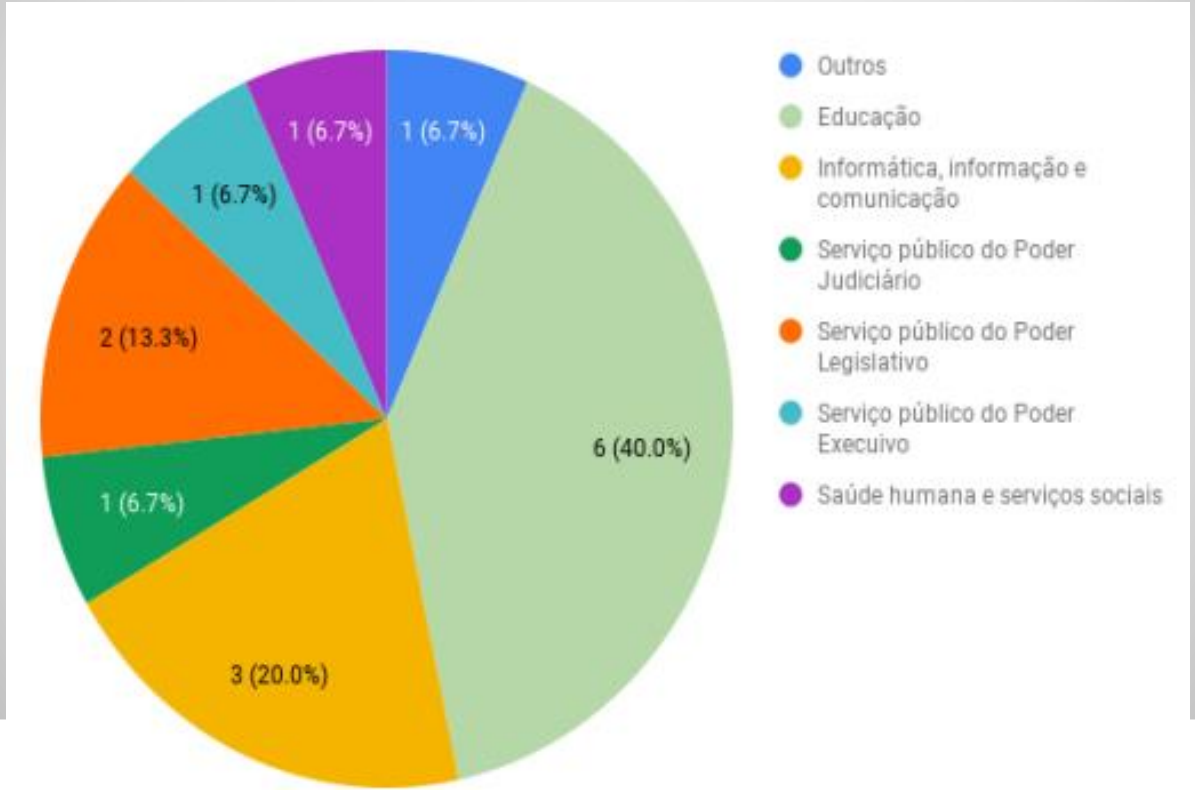
Público-alvo:
Formação



Fonte: Elaborado pelo Autor.

PESQUISA EXPLORATÓRIA

Público-alvo:
Área de atuação



Fonte: Elaborado pelo Autor.

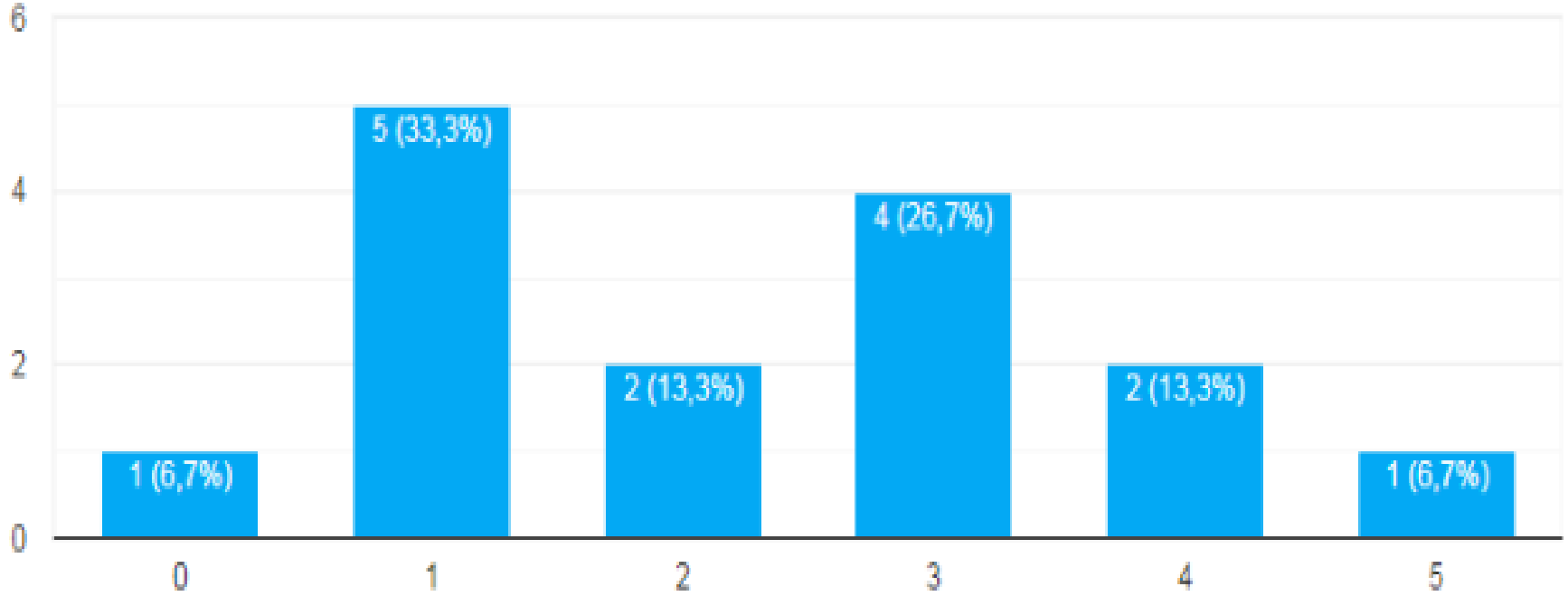
ANÁLISE DOS RESULTADOS

Grau de confiança em aplicativos e a SI:

ANONIMATO
CONFIDENCIALIDADE
PRIVACIDADE
DISPONIBILIDADE
INTEGRIDADE
TRANPARÊNCIA
AUDITABILIDADE
ATAQUES E INVASÕES

ANÁLISE DOS RESULTADOS

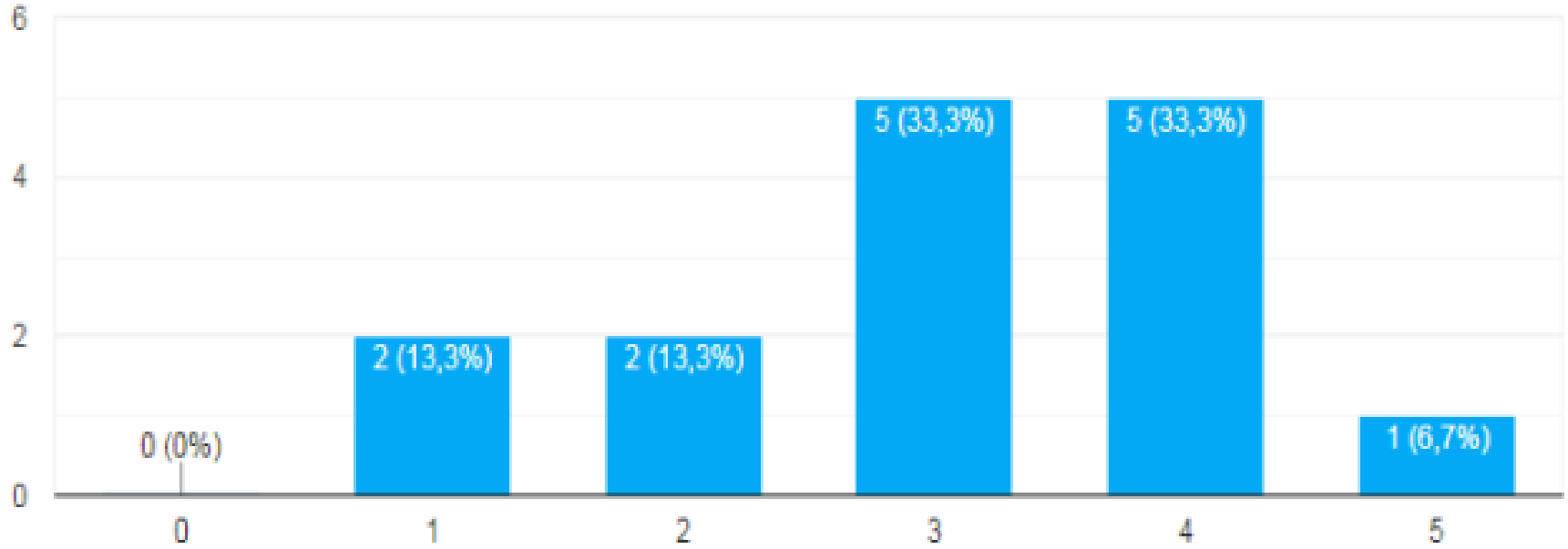
Grau de confiança ao ANONIMATO em aplicativos e a SI.



Fonte: Elaborado pelo Autor.

ANÁLISE DOS RESULTADOS

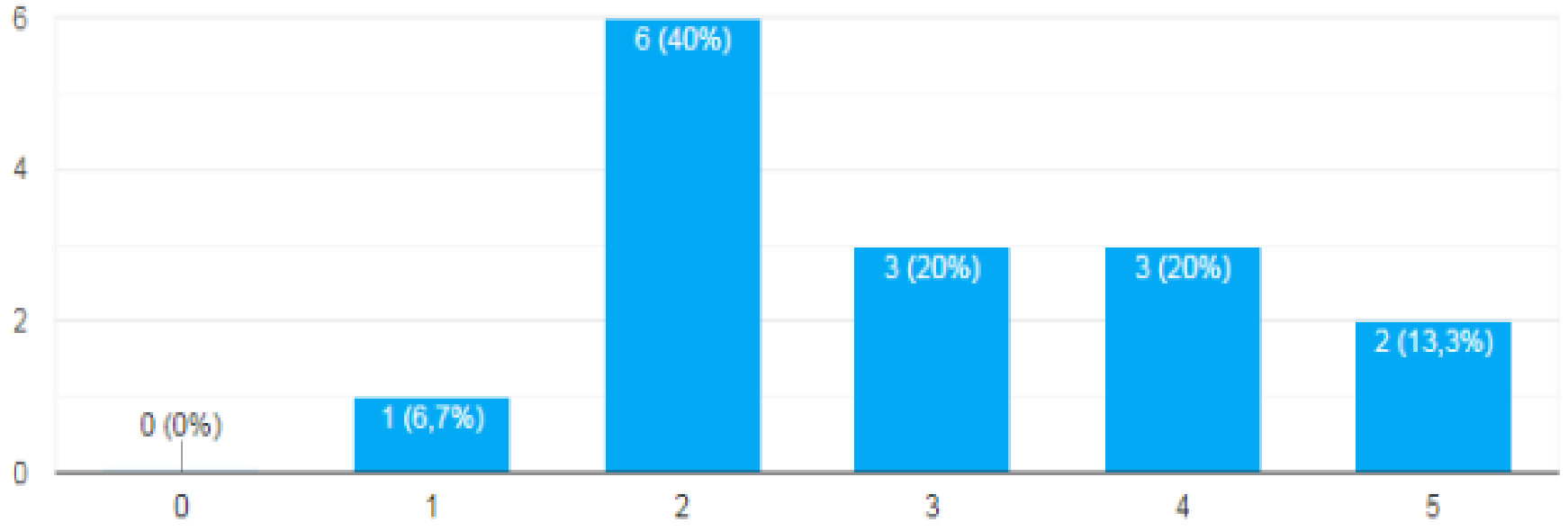
Grau de confiança na CONFIDENCIALIDADE em aplicativos e a SI.



Fonte: Elaborado pelo Autor.

ANÁLISE DOS RESULTADOS

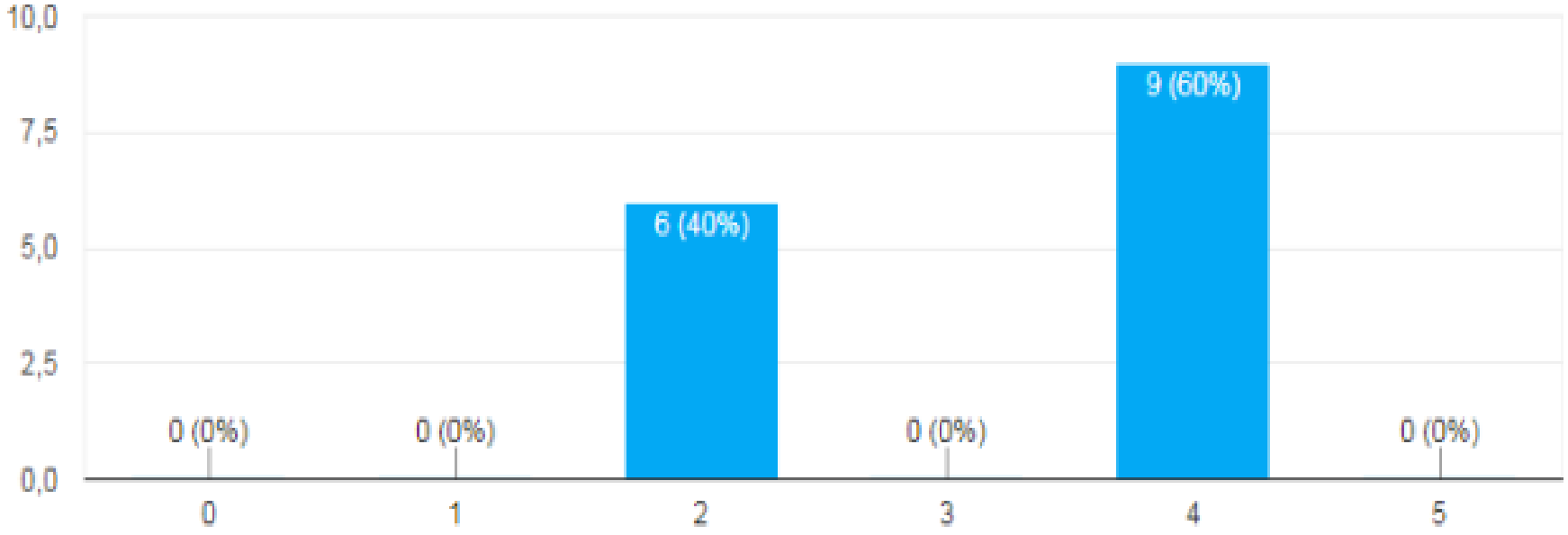
Grau de confiança na PRIVACIDADE em aplicativos e a SI.



Fonte: Elaborado pelo Autor.

ANÁLISE DOS RESULTADOS

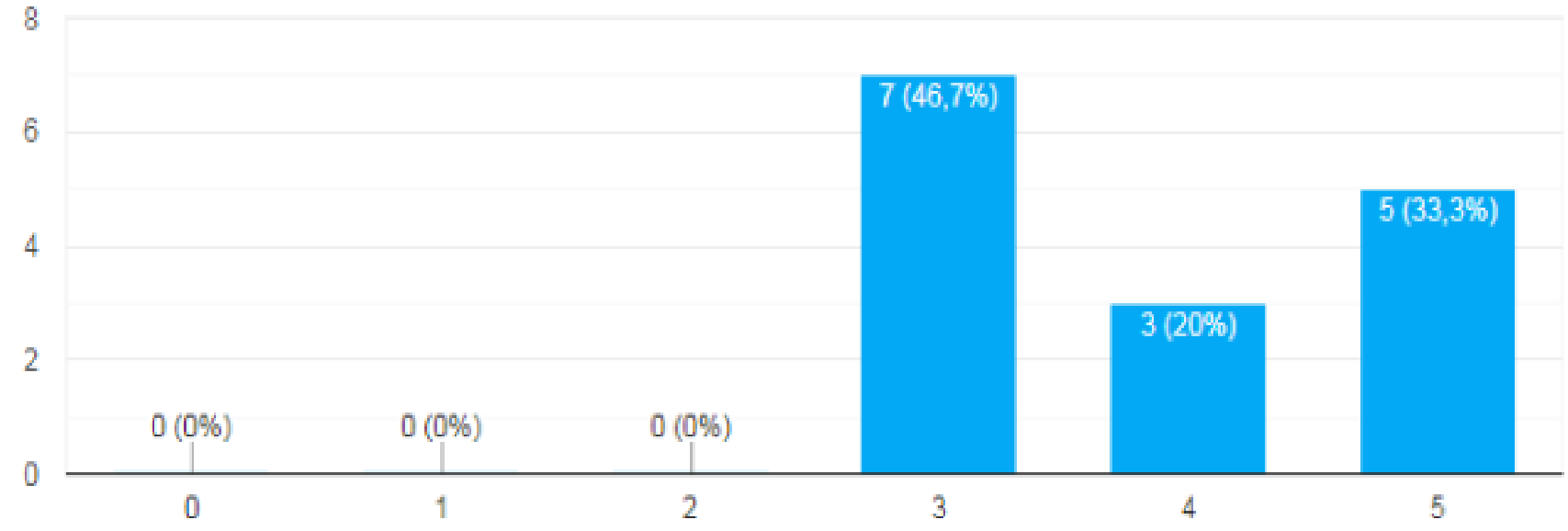
Grau de confiança na DISPONIBILIDADE em aplicativos e a SI.



Fonte: Elaborado pelo Autor.

ANÁLISE DOS RESULTADOS

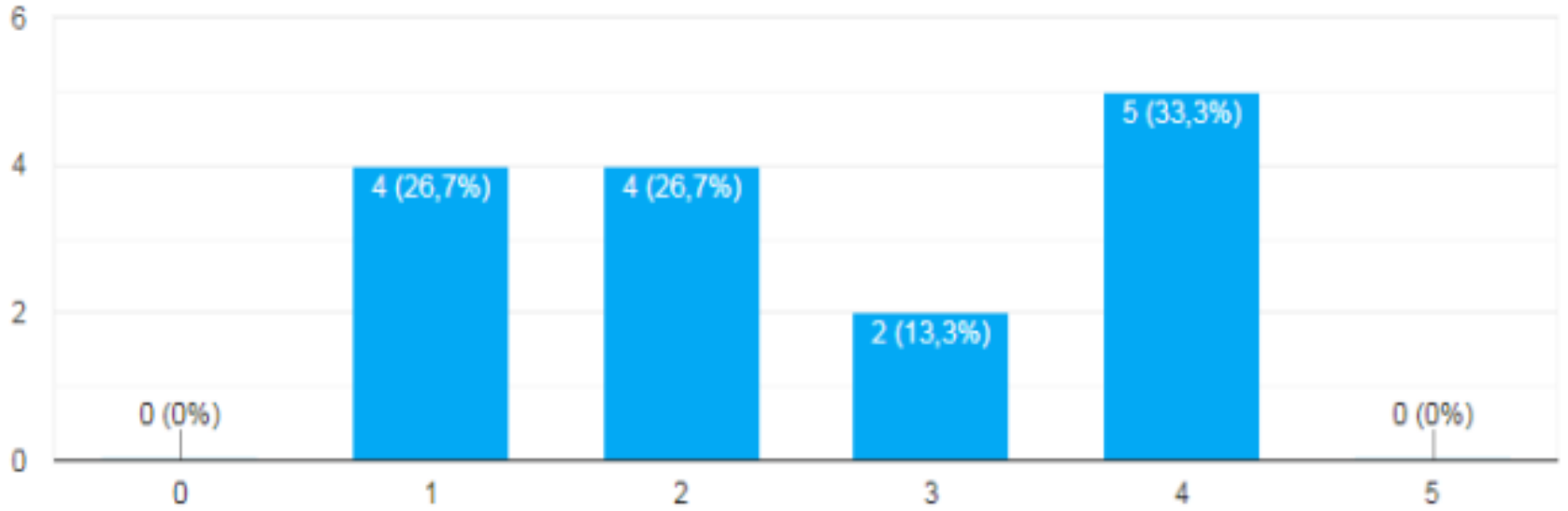
Grau de confiança na INTEGRIDADE em aplicativos e a SI.



Fonte: Elaborado pelo Autor.

ANÁLISE DOS RESULTADOS

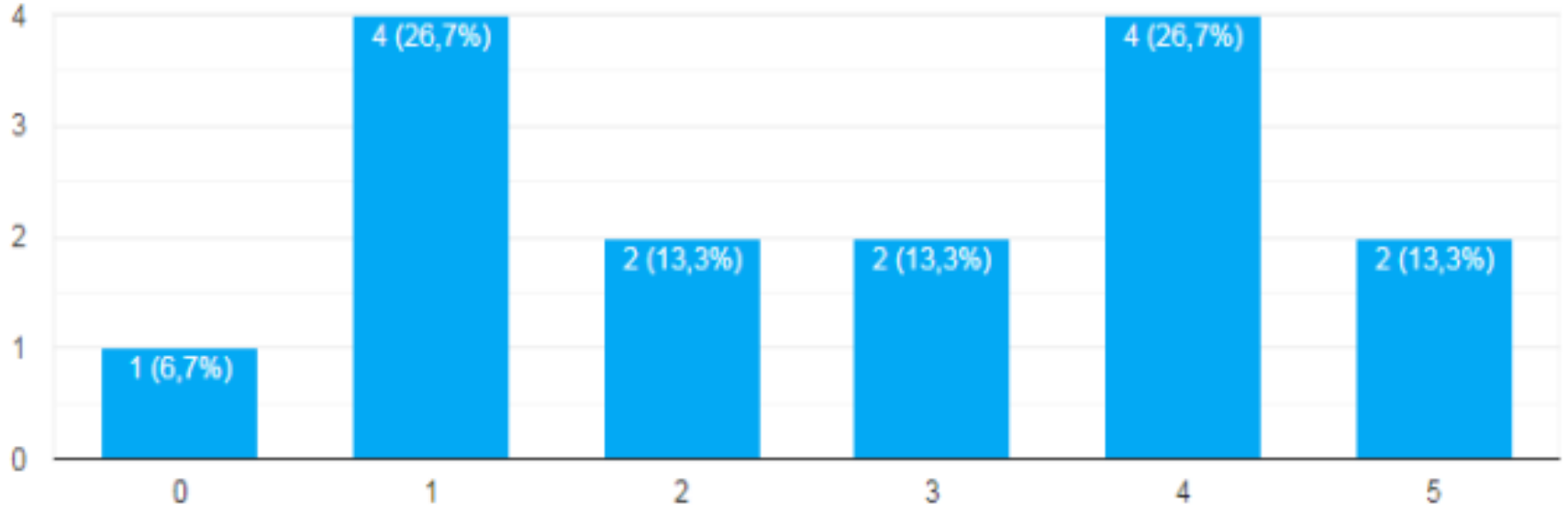
Grau de confiança na TRANSPARÊNCIA em aplicativos e a SI.



Fonte: Elaborado pelo Autor.

ANÁLISE DOS RESULTADOS

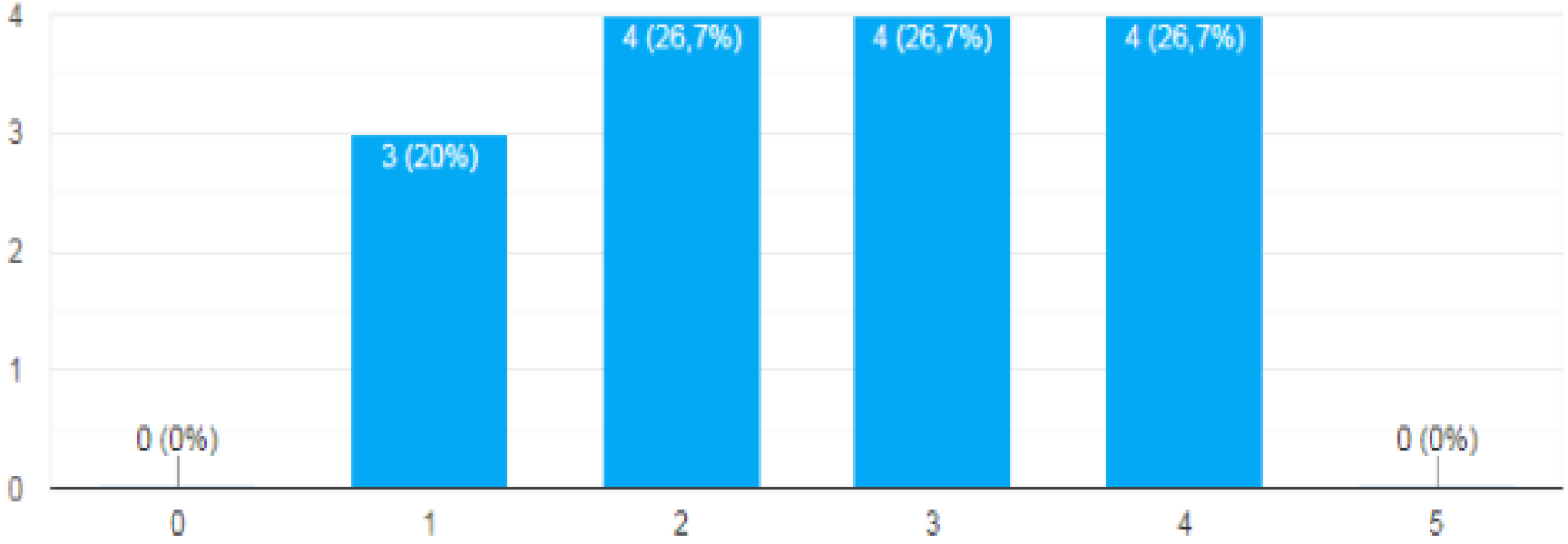
Grau de confiança na AUDITABILIDADE em aplicativos e a SI.



Fonte: Elaborado pelo Autor.

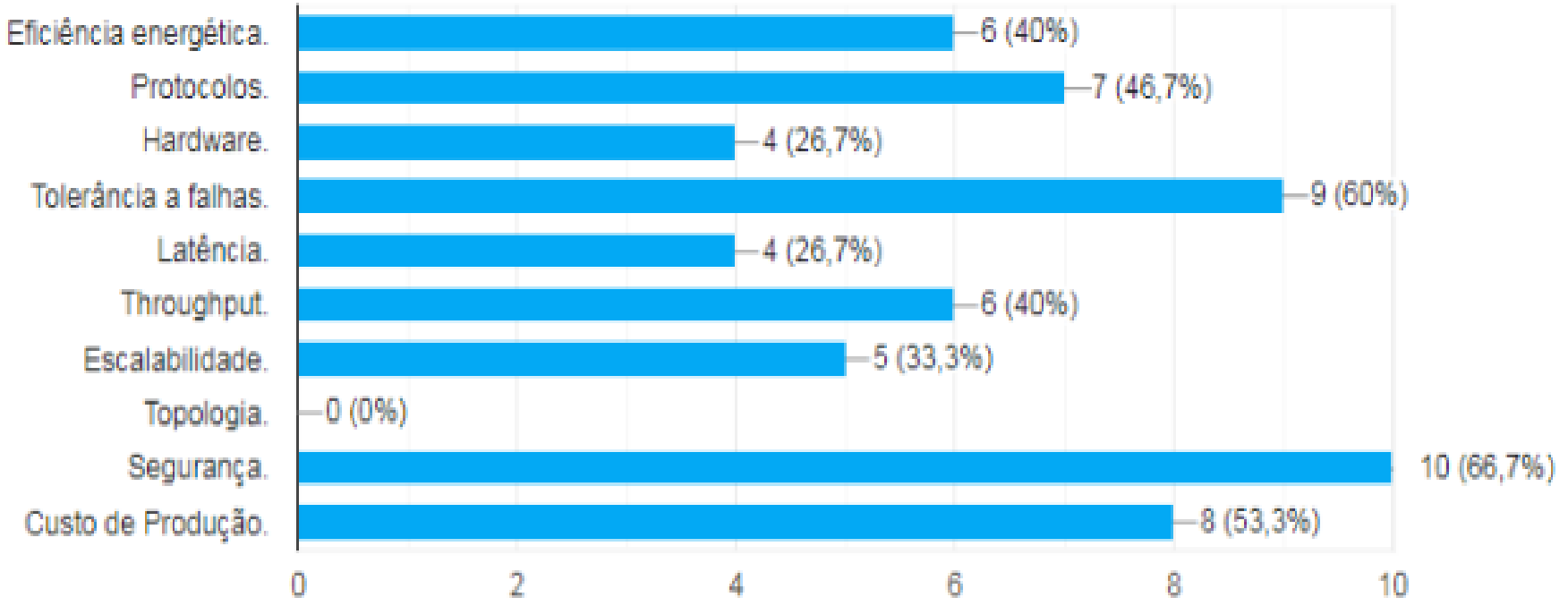
ANÁLISE DOS RESULTADOS

Grau de confiança na GRAU DE ATAQUE E INVASÕES em aplicativos e a SI.



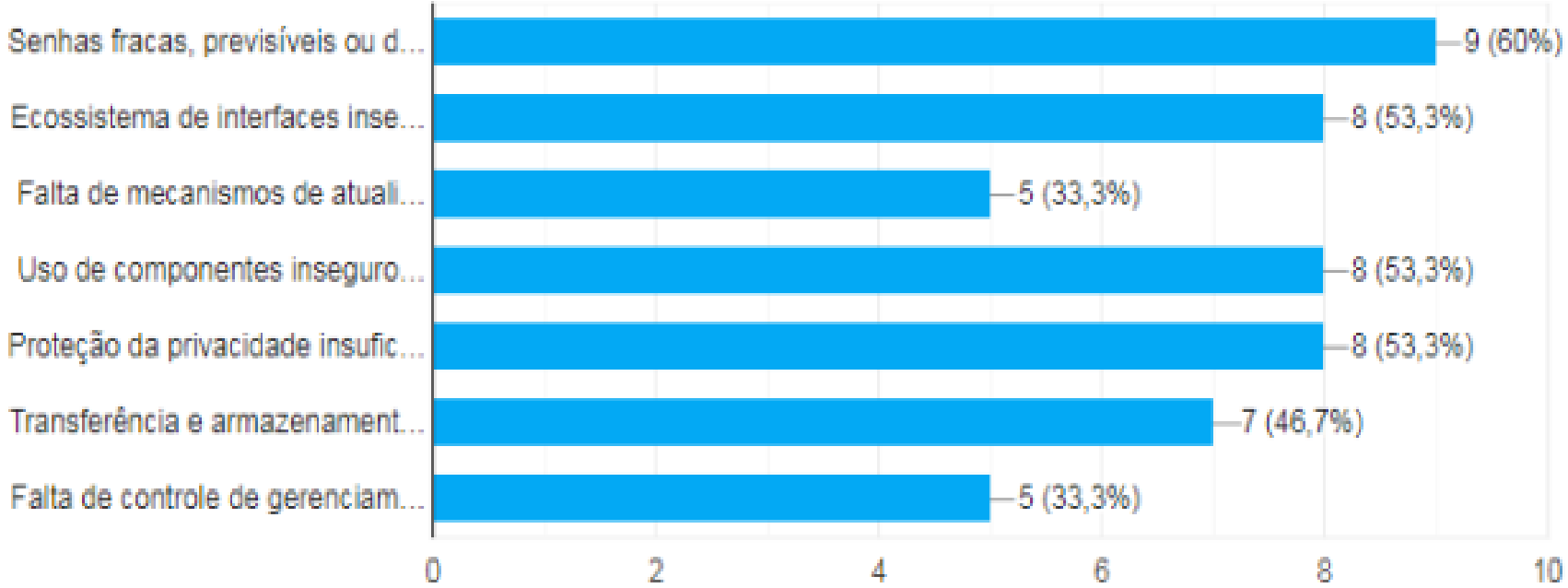
Fonte: Elaborado pelo Autor.

BARREIRAS OU DIFICULDADES DE IMPLANTAÇÃO DE IoT



Fonte: Elaborado pelo Autor.

DESAFIOS
INTEGRAÇÃO DE BLOCKCHAIN E IoT



Fonte: Elaborado pelo Autor.

MECANISMOS DE SEGURANÇA BLOCKCHAIN INTEGRADO À IoT (Modelo)

MECANISMOS DE SEGURANÇA BLOCKCHAIN INTEGRADO À IoT

A velocidade que diferentes dispositivos e softwares surgem a cada dia, aumentam os riscos na segurança, por não estarem de acordo com normas ou padrões de segurança, na fabricação, comercialização, implementação ou manutenção.

Efeito:

Potencialidade nas condições de violação à segurança.

MECANISMOS DE SEGURANÇA BLOCKCHAIN INTEGRADO À IoT

Processos de elaboração

Construção do Modelo

Modelo Conceitual

Modelo Final

Construção do Modelo

Estudo de riscos no gerenciamento de sistemas integrados Blockchain - IoT

Modelo Conceitual

- Gestão da Segurança da Informação;
- Avaliação de riscos para a organização;
- Referências Normativas.

Modelo Final

Estratégia de negócios

Infraestrutura

(recomendações de segurança)

Segurança da Informação

ETAPAS DE CONSTRUÇÃO DA PROPOSTA DE MECANISMO

Construção do Modelo

Estudo de riscos no gerenciamento de sistemas integrados Blockchain – IoT

Características inerentes à Blockchain tornam-na segura por sua arquitetura de projeto.

Fatores externos podem estar relacionados com a perda de confiança no sistema, entre elas soluções off-chain (fora da Blockchain);

Utilização sem critérios de governança e planejamento voltado à segurança pode gerar situações de inviabilidade na implantação ou na manutenção.

Modelo Conceitual

De onde vem a maioria dos casos de incidentes na Blockchain?

Sua segurança, definida pela própria arquitetura, pode não ser suficiente?

Modelo Conceitual

RESPOSTAS:

- Criptografia forte não protege senhas fracas.

- Arquitetura de segurança sem ***um sistema de gestão da segurança da informação*** que regule processos e procedimentos de gerenciamento de riscos torna-se incapaz de oferecer controle sobre os ativos existentes em todo sistemas (On e Off Chain).

- Boas práticas de gestão garantem: gestão de identidades, controle de acesso, autenticação de usuário e proteção dos negócios, baseados nos mecanismos de consenso.

Modelo Conceitual

Gestão da Segurança da Informação

Requisitos de:

Avaliação de riscos para a Organização;

Regulamentos;

Princípios, objetivos e requisitos.

Modelo Conceitual

Análise de Riscos

- Identificação
- Avaliação
- Tratamento
- Ação Preventiva
- Ação Corretiva
- Melhoria Contínua

Modelo Conceitual

Referências Normativas

ABNT - Associação Brasileira de Normas Técnicas
ANSI X9 - Comitê de Padrões Acreditado
BSI - Escritório Federal Alemão de Segurança da Informação
CENELEC - Comitê Europeu de Normalização Eletrotécnica
DIN - Instituto Alemão de Normalização
ENISA - Agência da União Europeia para a Cibersegurança
ETSI – European Telecommunications Standards Institute
IEEE-SA - Instituto de Engenheiros Eletricistas e Eletrônicos
ISO - International Organization for Standardization
ITU-T - União Internacional de Telecomunicações
NIST - Instituto Nacional de Padrões e Tecnologia

Modelo Conceitual

Referências Normativas

DIN. 16597:2018-02. (2018): DIN fornece a terminologia para Blockchains, abrange a terminologia da TI tradicional e da criptografia.

DIN. 4997:2020-04. (2020): Especifica um modelo para processamento de dados pessoais usando Blockchain se preocupa com o Regulamento Geral de Proteção de Dados da UE (GDPR).

Modelo Conceitual

Referências Normativas

ISO/TC 307: Norma geral para Blockchain.
ISO 22739:2020: Blockchain e tecnologias de contabilidade distribuída – Vocabulário.
ISO 23257:2022: Blockchain e tecnologias de contabilidade distribuída – Arquitetura de referência.
ISO/TS 23258:2021: Blockchain e tecnologias de contabilidade distribuída – Taxonomia e Ontologia.

Modelo Conceitual

Referências Normativas

ISO/TR 23244:2020: Descreve uma visão geral da proteção de privacidade e informações de identificação pessoal (PII) aplicada a sistemas Blockchain e tecnologias de contabilidade distribuída (DLT).

ISO/TR 23455:2019: Descreve uma visão geral dos contratos inteligentes em sistemas BC/DLT, o que são contratos inteligentes e como eles funcionam.

ISO/AWI TS 23516: Tecnologia Blockchain e Distributed Ledger – Estrutura de Interoperabilidade.

Modelo Conceitual

Referências Normativas

ISO/WD TR 23642: Blockchain e tecnologias de contabilidade distribuída – Visão geral das boas práticas e problemas de segurança de contrato inteligente.

ISO/TR 23576:2020: Blockchain e tecnologias de contabilidade distribuída – Gerenciamento de segurança de custodiantes de ativos digitais.

ISO/TS 23635:2022: Blockchain e tecnologias de contabilidade distribuída – Diretrizes para governança.

Modelo Conceitual

Referências Normativas

ISO/IEC – 27000, 27001 e 27002: Técnicas de segurança e gerenciamento da informação.
ISO/IEC – 28000: Relacionada às questões de segurança em cadeias de suprimentos.
ISO/PRF TR 3242: Blockchain e tecnologias de contabilidade distribuída – Casos de uso.

Modelo Final

Prevenção à segurança no uso de Blockchain e IoT

Modelo Final

Proposta de Mecanismos de Segurança na Integração das tecnologias de Blockchain e IoT

- Recomendações baseadas nas boas práticas de gestão (prevenção, recomendações e estratégias de negócios).

- Suporte na elaboração de projetos de implantação, operação, monitorização, auditoria e revisão.

- Garantir boa utilização das tecnologias em ecossistemas seguros e confiáveis, consolidando os pontos fortes de segurança inerentes à arquitetura Blockchain.

Modelo Final

Prevenção à segurança no uso de Blockchain e IoT

Estratégia de Negócios

Infraestrutura (recomendações de segurança)

Segurança da informação (classificação e tratamento)

Prevenção à segurança no uso de Blockchain e IoT

Estratégia de Negócios

-Utilização dos ativos
-Recursos Humanos
-Regulamentações, legislação e contratos
-Segurança na cadeia de suprimentos
-Mecanismos de consenso

Prevenção à segurança no uso de Blockchain e IoT

Infraestrutura – recomendações de segurança

- Infraestrutura de Blockchain
- Infraestrutura de IoT
- Redes locais e Internet
- Redes Blockchain: Públicas ou Privadas
- Virtualização
- Fatores externos (Off Chain)
- Segurança física e do ambiente
- Gerenciamento de vulnerabilidades (técnicas)

Prevenção à segurança no uso de Blockchain e IoT

Segurança da Informação

- **Classificação e tratamento da informação**
- **Chaves e controles de acesso**
- **Acesso remoto e segurança nas comunicações**
- **Procedimentos de Backup**
- **Hiperconectividades e a segurança da Informação**

CONCLUSÃO

Apresentamos uma proposta para se explorar novos projetos baseados nas duas tecnologias, Blockchain com IoT, através de recomendações apresentadas nos mecanismos de segurança, na ***utilização técnicas de segurança da informação e governança como ferramentas*** de apoio à garantia de segurança e confiança na solução de novos desafios.

CONTRIBUIÇÕES DO TRABALHO

• Elaboração e avaliação de modelos de serviços baseados na plataforma de Blockchain e IoT.

• Avaliação de desempenho e elaboração de um modelo de segurança para as tecnologias citadas.

• Identificar problemas relacionados à integração da Blockchain com IoT.

• Direções futuras de pesquisa sobre a segurança na Blockchain integrados a ecossistemas de IoT.

CONTRIBUIÇÕES DO TRABALHO

• Elaboração e avaliação de modelos de segurança baseados na plataforma de Blockchain e IoT.

• A importância na normalização e regulamentação dos processos para a inclusão da Blockchain e IoT como parte das infraestruturas de sistemas descentralizados.

• Apresentar conceitos de ambas tecnologias e sua integração, na intenção ***de apresentar ao leitor leigo um novo olhar para ambas tecnologias*** além do estereótipo de uma tecnologia dirigida apenas às criptomoedas, provando, sua capacidade além dessa aplicação.

PUBLICAÇÕES

Val, R., & Gouveia, L. B. (2023). ***Escalabilidade no armazenamento na Blockchain.*** Brazilian Applied Science Review, 7(2), 587–599. https://doi.org/10.34115/basrv7n2-012.

do Val, R. B. e Gouveia, L. B. (2023). ***Origens da Blockchain: relato das tecnologias subjacentes às criptomoedas.*** Brazilian Applied Science Review, 7(2), 469–494. https://doi.org/10.34115/basrv7n2-004

PUBLICAÇÕES

Viana, T.; Val, R. e Gouveia, L. (2022). ***O uso de Blockchain na identificação de fake news: ferramentas de apoio tecnológico para o combate à desinformação.*** XII Congresso SOPCOM, Comunicação e Disrupção. Disrupção Informacional III: Jornalismo e Tecnologias Digitais. Nova FCSH. 11 abril. Lisboa.

Val, R. e Gouveia, L. (2020). ***Estudo prévio sobre mecanismos de segurança nas aplicações de sistemas distribuídos Blockchain.*** Relatório Interno 04/2020. *TRS, Tecnologia, Redes e Sociedade. Maio. Universidade Fernando Pessoa.

TRABALHO RESULTANTE DA PESQUISA

Elaboração de Projeto de Política de Segurança da Informação no âmbito do Legislativo Estadual no Brasil:

- Protocolo de Proteção e de Segurança de Dados Pessoais.
- Protocolo de Proteção a Incidentes Cibernéticos.

TRABALHOS FUTUROS
CIDADES INTELIGENTES