Metodologia e Tópicos de Pesquisa em Computação

Prof. Dr. Vagner Luiz Gava (IPT)

Exercício II

Wesley Rodrigues da Silva <wesley.it@gmail.com>

São Paulo – Julho, 2023

Conteúdo

Informações Gerais e Título

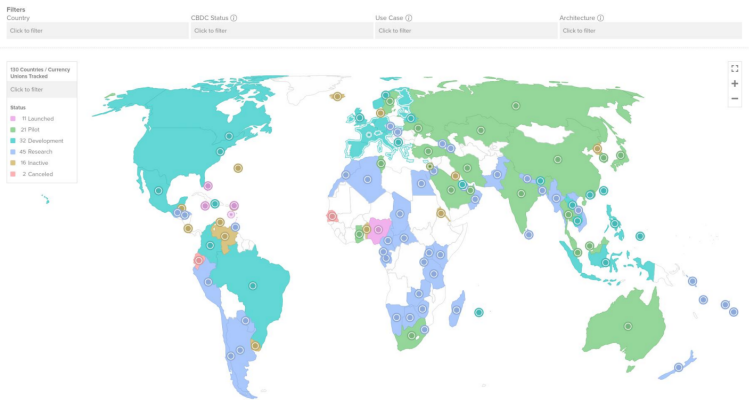
Autor: Wesley Rodrigues da Silva

Título: Um Framework de Segurança de Dados na Nuvem para Indústria Financeira.

Conteúdo

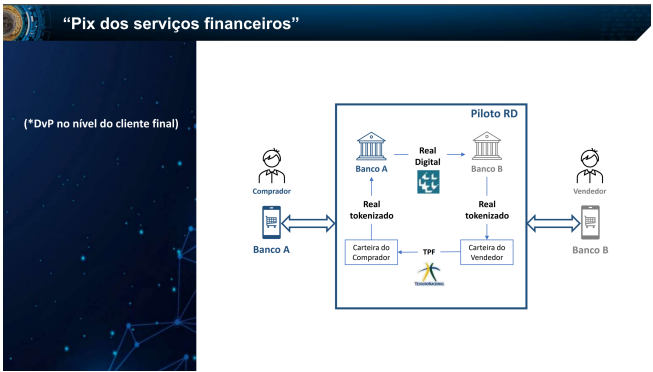
Problema - Contexto

Figura 1 – Captura de tela mostrando novos países com CBDCs.



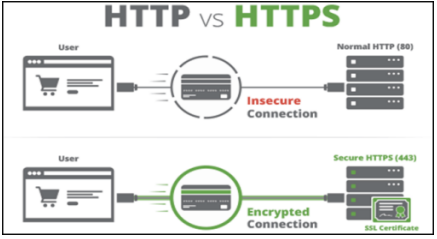
Fonte: Adaptado de Atlantic Council (2022).

Figura 2 – BACEN mostrando a arquitetura do Real Digital.



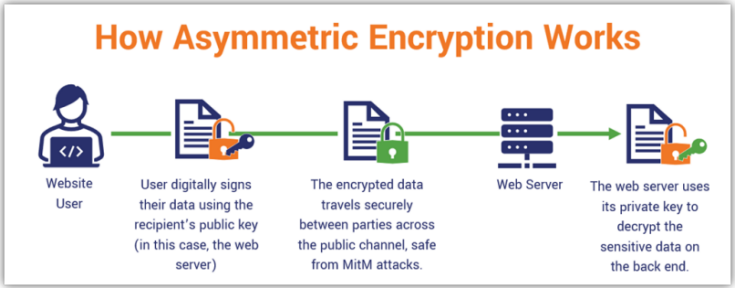
Fonte: BACEN (2023).

Figura 3 – HTTP vs HTTPS.



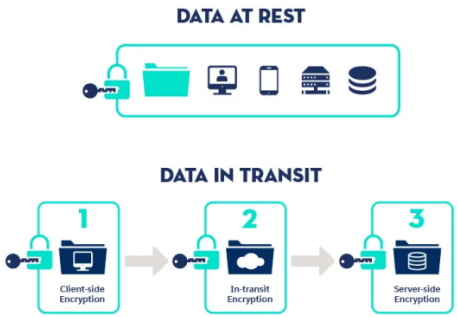
Fonte: Cloudways (2023).

Figura 4 – Chaves públicas e privadas.



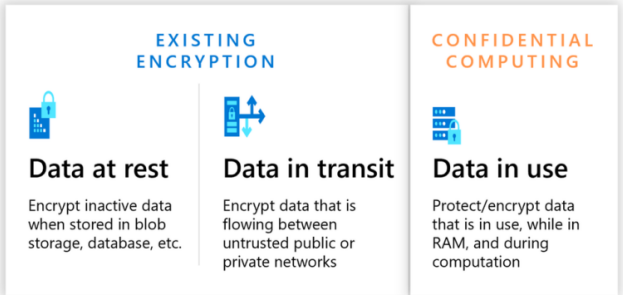
Fonte: DigiCert (2023).

Figura 5 – Dados criptografados em repouso e em trânsito.



Fonte: Salesforce (2023).

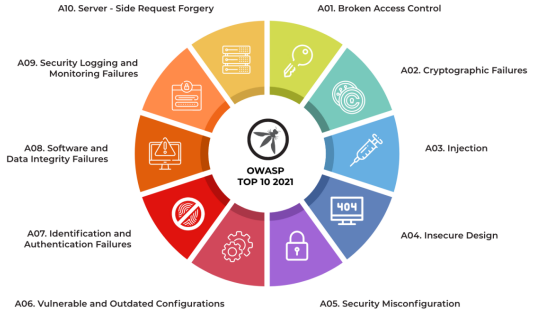
Figura 6 – Dados criptografados em repouso, em trânsito e em uso.



Fonte: Microsoft (2023).

Problema - Geral

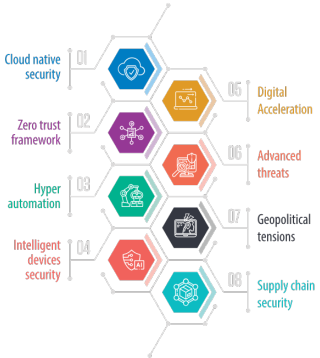
Figura 7 – Principais vulnerabilidades em aplicações web.



Fonte: OWASP (2021).

Problema - Geral

Figura 8 – Perspectivas em Cybersecurity.



Fonte: Infosys (2023).

Figura 9 – Ameaças emergentes em cybersecurity.

Fonte: ENISA (2023).

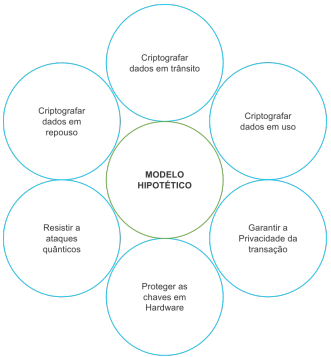
Problema - Geral

Os paradigmas de segurança evoluíram na última década, estamos perto de dois pontos de virada: na **economia** e na **tecnologia criptográfica**.
Soluções com defesa em múltiplas camadas são necessárias.

Bibliografia utilizada no contexto e levantamento dos problemas de pesquisa: Barros e Silva (2023), Boido e Aliano (2023), Wenhua et al. (2023), IBM (2023), Runge (2022), NIST (2022) e Xu et al. (2023)

Problema - Específico

Figura 10 – O processo de privacidade de dados tem múltiplos pontos de atenção.



Fonte: Autor (2023).

Problema - Falta Resolver

Falta um modelo que demonstre o papel das seis camadas aplicadas a uma mesma carga de trabalho, e que ajude no planejamento e na avaliação das práticas de criptografia de dados.

Conteúdo

Critério PICO e Pergunta

(P): Arquitetos de soluções que utilizam plataformas de nuvem.
(I): Desenvolvimento e uso de um framework baseado em uma métrica de maturidade e definição de práticas de criptografia de dados na avaliação das arquiteturas de nuvem.
(C): levantamento exploratório de evidências na literatura científica e/ou cinzenta.
(O): um framework que auxilia os arquitetos na avaliação da maturidade e nas boas práticas modernas de criptografia de dados.

A seguinte questão de pesquisa da revisão foi elaborada por meio dos critérios PICO:

Como desenvolver um framework de melhores práticas modernas de criptografia de dados e avaliação com score de soluções em nuvem que apoie os arquitetos de soluções que utilizam essas plataformas?

Conteúdo

Palavras Chave (pt e en)

Quadro 1 – Palavras em português e inglês

português	**inglês**
criptografia de dados	data encryption
computação na nuvem	cloud computing
avaliação de segurança	security assessment
criptografia pós-quântica	post-quantum cryptography
módulo de segurança em hardware	hardware security module
computação confidencial	confidential computing
protocolos de conhecimento zero	zero knowledge protocols

Fonte: Elaborado pelo autor.

String de Pesquisa

As buscas em português no Web of Science não foram promissoras. A string de pesquisa foi montada em inglês usando o seguinte racional:

What?

- privacy
- data encryption
- security assessment

String de Pesquisa

As buscas em português no Web of Science não foram promissoras. A string de pesquisa foi montada em inglês usando o seguinte racional:

Where?

- cloud computing
- AWS
- AZURE
- GCP

String de Pesquisa

As buscas em português no Web of Science não foram promissoras. A string de pesquisa foi montada em inglês usando o seguinte racional:

How?

- post-quantum cryptography
- hardware security module
- confidential computing
- zero knowledge protocols

- HSM
- SGX
- SEV-SNP

String de Pesquisa

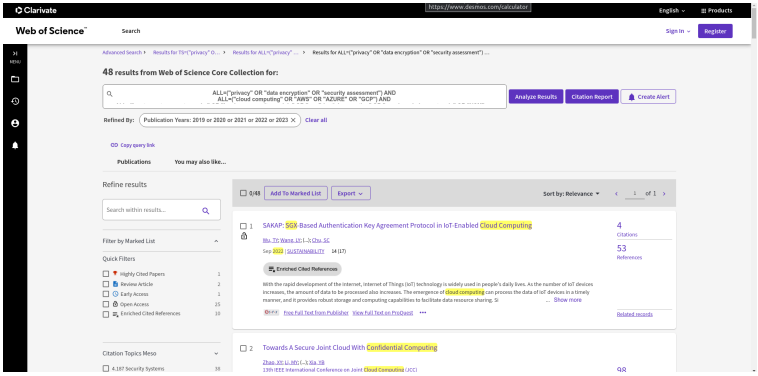
A string final ficou definida da seguinte forma:

```
TS=("privacy"OR "data encryption"OR "security assessment") AND
TS=("cloud computing"OR "AWS"OR "AZURE"OR "GCP") AND
TS=("post-quantum cryptography"OR "hardware security module"OR
"confidential computing"OR "zero knowledge protocols"OR
"HSM"OR "SGX"OR "SEV-SNP")
```

Foi aplicado um critério de restrição temporal permitindo artigos dos últimos 5 anos.

Web of Science – Busca Avançada

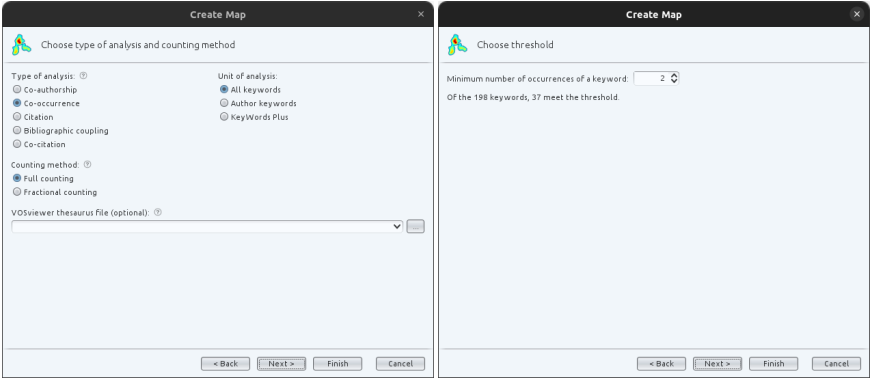
Figura 11 – Tela de busca do Web of Science.



Fonte: Autor (2023).

Conteúdo

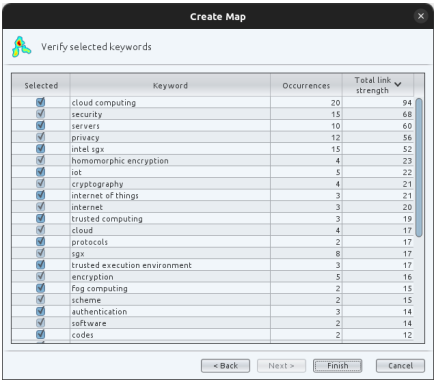
Figura 12 – Parâmetros para obter as redes de palavras chaves no VosViewer.

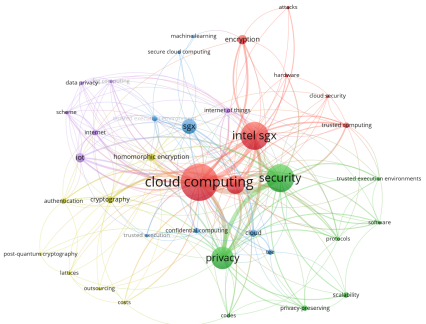


Fonte: Autor (2023).

Correlação de Palavras Chave – VosViewer

Figura 13 – Principais palavras chaves e suas redes de conexões.





Fonte: Autor (2023).

Correlação de Palavras Chave – VosViewer

O gráfico de rede de palavras do VosViewer mostra que há grupos que não estão diretamente nos termos originais, mas que podem ser adicionados na literatura principal ou complementar.

Por exemplo, as **lattices**, que são famílias de algoritmos resistentes aos ataques quânticos, a **criptografia homomórfica**, que é uma técnica usada em computação confidencial, e os termos **fog computing** e **IoT**, que tem relação direta com a conexão entre o mundo físico e a nuvem.

Conteúdo

Hipóteses e Proposições

A hipótese levantada neste trabalho é que com um estudo da Revisão Sistemática da Literatura somado ao estudo de caso de como os três maiores provedores de nuvem atualmente (Amazon, Google e Microsoft) recomendam o uso dos serviços de proteção de dados, é possível criar um framework que apoie os arquitetos de sistemas que utilizam a nuvem na avaliação (incluindo um score de maturidade) e planejamento de seus sistemas para utilizar as práticas recentes de criptografia de dados.

Premissas

O estudo tem como objeto de verificação soluções de Sistemas de Informação que utilizam provedores de nuvem pública, focando em Amazon Web Services, Microsoft Azure e Google Cloud Platform, que juntos têm mais de 65% do mercado.

Objetivos

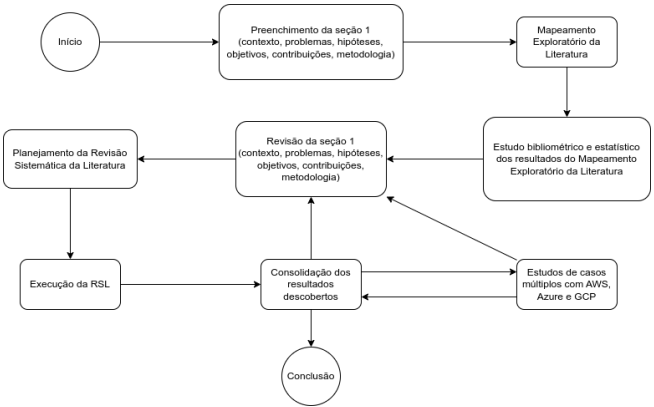
- Realizar uma RSL sobre as práticas de criptografia de dados.
- Realizar estudos de casos múltiplos sobre as práticas de criptografia de dados.
- Criar um modelo de avaliação de maturidade nos aspectos de práticas de criptografia de dados.
- Criar um framework que apoie os arquitetos no planejamento de práticas modernas de criptografia das camadas de segurança de dados.

Contribuições Esperadas

Para a academia: O presente trabalho entrega para a academia um compêndio com os mais recentes avanços na área da criptografia aplicada à proteção dos dados pessoais, convidando novos pesquisadores para avançar os estudos deste ramo.

Para a indústria: O framework pode ser utilizado de forma prática por arquitetos de software que planejam soluções que utilizam a nuvem.

Figura 14 – A metodologia seguida será uma RSL somada a um estudo de caso.

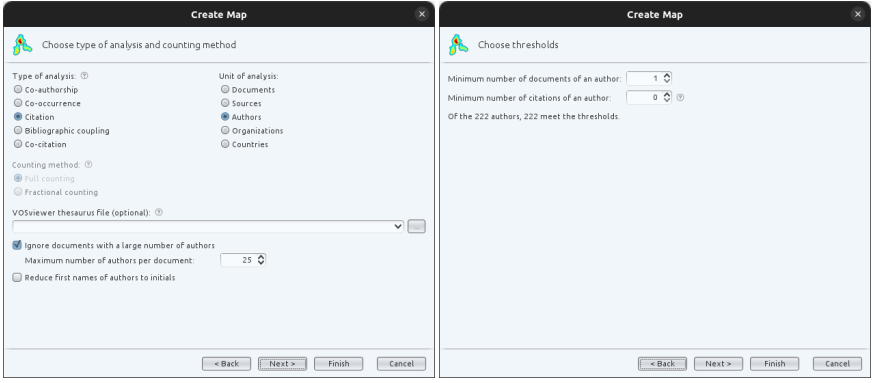


Fonte: Autor (2023).

Conteúdo

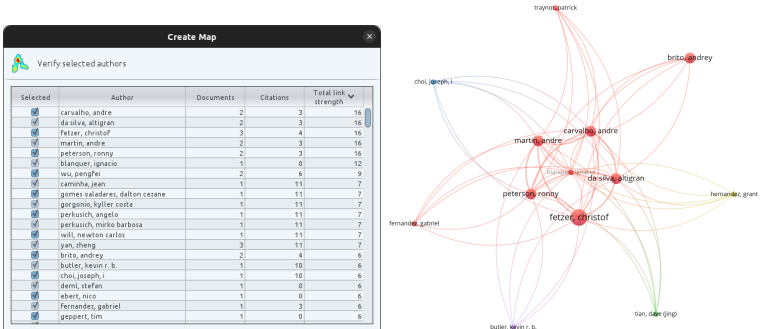
Citações por Autores – VosViewer

Figura 15 – Parâmetros para obter as redes de citações por autores no VosViewer.



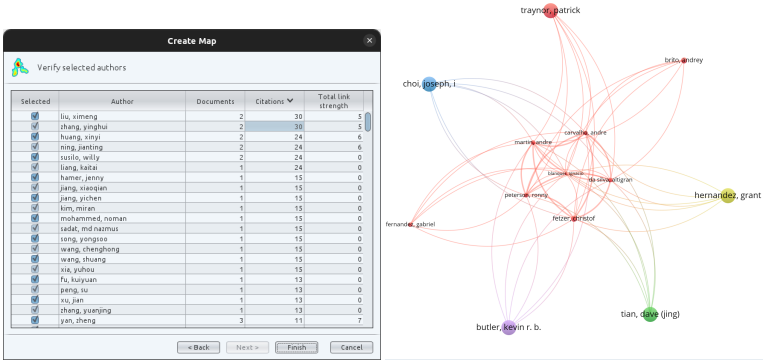
Fonte: Autor (2023).

Figura 16 – Ordenados por força do link.



Fonte: Autor (2023).

Figura 17 – Ordenados por quantidade de citações.



Fonte: Autor (2023).

Artigos Mais Citados – VosViewer

Os 3 artigos lidos (abstract e keywords) são relevantes para o trabalho:

- Tian et al. (2019): Este artigo contribui com o tópico de proteção dos dados, isolando o ambiente em nuvem de forma que o operador da nuvem não tenha acesso aos dados do cliente, mesmo controlando o virtualizador e o hardware.
- Brito et al. (2019): Apesar de usar a nuvem, os dados normalmente são gerados fora da nuvem. Este artigo trata do processo de proteção de ponta a ponta.
- Peterson et al. (2019): Tópicos como criptografia homomórfica e suportada por hardware são abordados neste artigo que foca em privacidade de dados.

Referências I

BACEN. **Banco Central do Brasil - CBDCs**. Website institucional do Banco Central do Brasil, sediado em Brasília, DF, BRA. 2023. Disponível em: <https://www.bcb.gov.br/content/estabilidadefinanceira/real_digital_docs/workshop/Workshop_Sessao_2_ModelosDeNegocio_Piloto_RD.pdf>. Acesso em: 29 jun. 2023. Citado na página 6.

BARROS, Alice De Souza Araujo; SILVA, Paulo Vitor Jordão Da Gama. Análise do crescimento e impacto das Startups Fintechs nas economias dos países emergentes do BRICS. **Revista de Gestão e Secretariado (Management and Administrative Professional Review)**, São Paulo, SP, BRA, v. 14, n. 5, p. 8343–8362, 2023. ISSN 2178-9010. DOI: 10.7769/gesec.v14i5.2215. Disponível em: <https://ojs.revistagesec.org.br/secretariado/article/view/2215>. Acesso em: 29 jun. 2023. Citado na página 14.

BOIDO, Claudio; ALIANO, Mauro. Digital art and non-fungible-token: Bubble or revolution? **Finance Research Letters**, [s.l.], v. 52, p. 103380, 2023. ISSN 1544-6123. DOI: https://doi.org/10.1016/j.frl.2022.103380. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1544612322005578>. Acesso em: 29 jun. 2023. Citado na página 14.

BRITO, Andrey et al. Secure end-to-end processing of smart metering data. English. In: 1. v. 8. DOI: 10.1186/s13677-019-0141-z. Citado na página 40.

CLOUDWAYS. **HTTP versus HTTPS**. Blog da empresa de comércio eletrônico Cloudways, sediada em Saint Julian's, Malta, MT. 2023. Disponível em: <https://www.cloudways.com/blog/ecommerce-ssl-certificates/>. Acesso em: 29 jun. 2023. Citado na página 7.

COUNCIL, Atlantic. **Central Bank Digital Currency Tracker**. Mantido pelo Conselho do Atlântico, sediado em Washington, DC, USA. 2022. Disponível em: <https://www.atlanticcouncil.org/cbdctracker/>. Acesso em: 29 jun. 2023. Citado na página 5.

DIGICERT. **DigiCert - How does SSL Works?** Website institucional da autoridade em certificados DigiCert, St. Petersburg, FL, USA. 2023. Disponível em: <https://www.thesslstore.com/blog/asymmetric-encryption-what-it-is-why-your-security-depends-on-it/>. Acesso em: 29 jun. 2023. Citado na página 8.

Referências II

ENISA. **Central Bank Digital Currency Tracker**. Mantido pelo The European Union Agency for Cybersecurity, sediada em Atenas, GRC. 2023. Disponível em: <https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030>. Acesso em: 29 jun. 2023. Citado na página 13.

IBM. **IBM Quantum Computing**. Site institucional do departamento de computação quântica da IBM, USA. 2023. Disponível em: <https://www.ibm.com/quantum>. Acesso em: 29 jun. 2023. Citado na página 14.

INFOSYS. **Cybersecurity Perspectives**. Relatório sobre Cybersecurity da empresa Infosys, sediada em Bangalore, KA, IN. 2023. Disponível em: <https://www.infosys.com/iki/perspectives/2021-cybersecurity-trends-report.html>. Acesso em: 29 jun. 2023. Citado na página 12.

MICROSOFT. **Confidential Computing**. Site de documentos técnicos da Microsoft, sediada em Redmond, WA, USA. 2023. Disponível em: <https://techcommunity.microsoft.com/t5/azure-confidential-computing/navigating-confidential-computing-across-azure/ba-p/2520752>. Acesso em: 29 jun. 2023. Citado na página 10.

NIST. **The Beginning of the End: The First NIST PQC Standards**. Apresentação do NIST sobre criptografia pós-quântica e algoritmos selecionados. 2022. Disponível em: <https://csrc.nist.gov/csrc/media/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa/images-media/pqc2022-march2022-moody.pdf>. Acesso em: 29 jun. 2023. Citado na página 14.

OWASP. **TOP 10 OWASP - Principais Vulnerabilidades**. Site de documentos técnicos da OWASP, sediada em Wakefield, MA, USA. 2021. Disponível em: <https://owasp.org/www-project-top-ten/>. Acesso em: 29 jun. 2023. Citado na página 11.

PETERSON, Ronny et al. Vallum: Privacy, Confidentiality and Access Control for Sensitive Data in Cloud Environments. English. In: CHEN, J; YANG, LT (Ed.). (International Conference on Cloud Computing Technology and Science), p. 103–110. Backup Publisher: IEEE; IEEE Comp Soc. ISBN 978-1-72815-011-6. DOI: 10.1109/CloudCom.2019.00026. Citado na página 40.

Referências III

RUNGE, Tilman. **Dismantling the Quantum Threat**. 2022. 66 f. Diss. (Mestrado) – Universidade Técnica de Brandemburgo, Berlim, DE. Disponível em: <https://opus4.kobv.de/opus4-fhbrb/frontdoor/deliver/index/docId/2888/file/DismantlingTheQuantumThreat.pdf>. Acesso em: 29 jun. 2023. Citado na página 14.

SALESFORCE. **Criptografia de Dados em Trânsito e em Repouso**. Site de documentos técnicos da Salesforce, sediada em San Francisco, CA, USA. 2023. Disponível em: <https://trailhead.salesforce.com/pt-BR/content/learn/modules/public-key-infrastructure-and-encryption/encrypt-data-at-rest>. Acesso em: 29 jun. 2023. Citado na página 9.

TIAN, Dave (Jing) et al. A Practical Intel SGX Setting for Linux Containers in the Cloud. English. In: p. 255–266. Backup Publisher: Assoc Comp Machinery; ACM SIGSAC; Univ Texas Dallas. ISBN 978-1-4503-6099-9. DOI: 10.1145/3292006.3300030. Citado na página 40.

WENHUA, Zhang et al. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. **Electronics**, Basileia, CHE, v. 12, n. 3, 2023. ISSN 2079-9292. DOI: 10.3390/electronics12030546. Disponível em: <https://www.mdpi.com/2079-9292/12/3/546>. Acesso em: 29 jun. 2023. Citado na página 14.

XU, Guobin et al. An Overview of Quantum-Safe Approaches: Quantum Key Distribution and Post-Quantum Cryptography. In: 57. 2023 57th Annual Conference on Information Sciences and Systems (CISS). Baltimore, MD, USA: [s.n.], 2023. v. 1, p. 1–6. DOI: 10.1109/CISS56502.2023.10089619. Disponível em: <https://ieeexplore-ieee-org.ez67.periodicos.capes.gov.br/document/10089619>. Acesso em: 29 jun. 2023. Citado na página 14.

INSTITUTO DE PESQUISAS TECNOLÓGICAS

OBRIGADO!