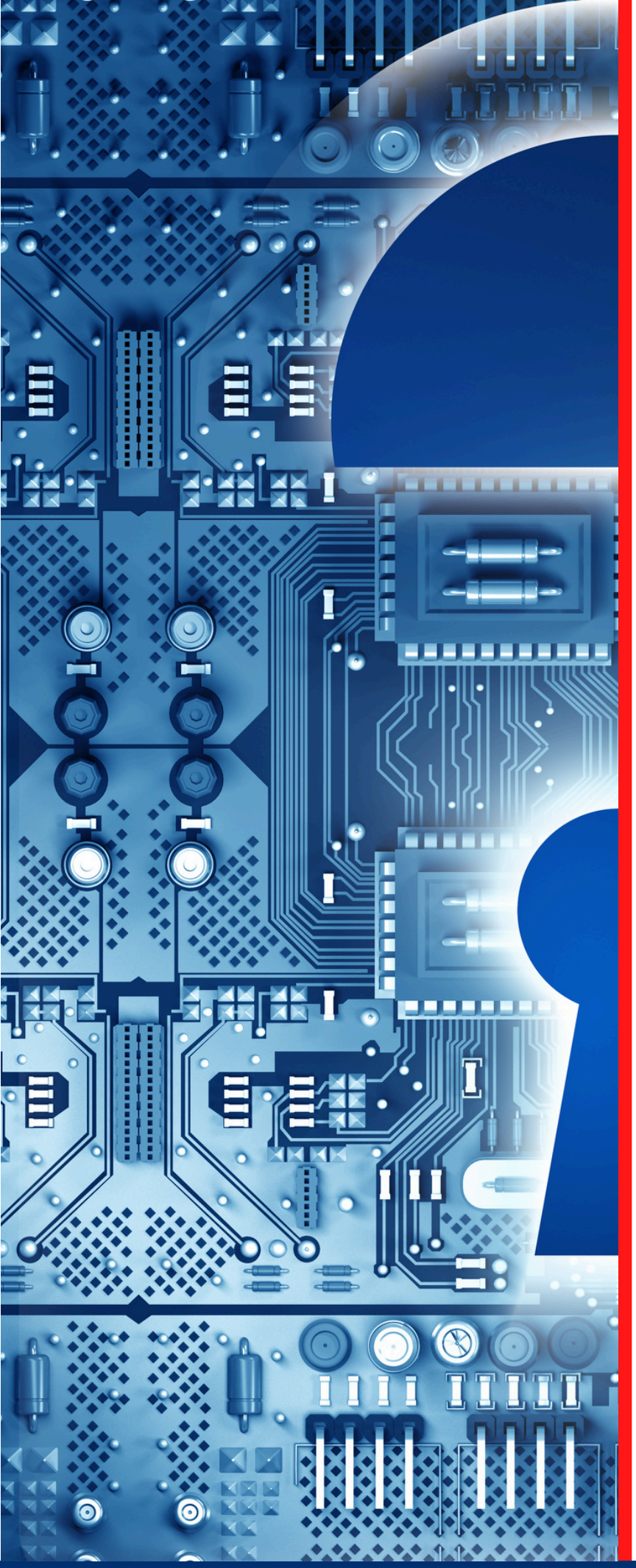


OSIC

ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

15/2024

Normatização e regulação de tecnologias emergentes no contexto da cibersegurança

Espaço cibernético inclusivo, seguro, estável, acessível e pacífico.

TLP:CLEAR

Introdução

Esta Orientação de Segurança da Informação e Cibernética (OSIC) traz um panorama da regulação e da normatização de tecnologias emergentes, no contexto da cibersegurança, para servir de referência aos servidores públicos que lidam com os temas de segurança da informação e de cibersegurança, seja nas atividades de governança, regulação, desenvolvimento, suporte, administração de serviços digitais ou qualquer outra que empregue essas tecnologias, tanto para entregar produtos e serviços diretamente à sociedade como para fornecê-los em suporte às missões de outros órgãos e entidades da Administração Pública.

O conteúdo foi estruturado sob os seguintes títulos:

1. **Inteligência artificial (IA): o que é e suas implicações para a segurança da informação**
2. **Computação em nuvem: definição e seus desafios regulatórios**
4. **Computação quântica e criptografia pós-quântica: impactos esperados e necessidades de regulação**
5. **Internet das coisas (IoT): riscos e desafios específicos de segurança**
6. **Blockchain e tecnologias correlatas**

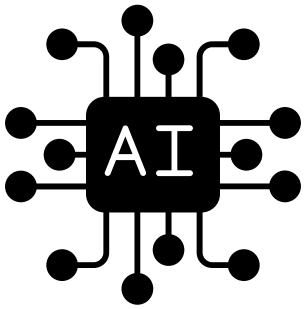
Cada um desses títulos está dividido nos seguintes subtítulos:

- definição conceitual da tecnologia emergente à luz da legislação brasileira e de outros países e blocos de países e das normas nacionais e internacionais, conforme o caso e se existente;
- desafios apresentados pela tecnologia emergente para a segurança da informação e a cibersegurança e respectivas soluções;
- normas e iniciativas nacionais e internacionais de regulação sobre a tecnologia emergente, conforme o caso e se existente; e
- conclusões.

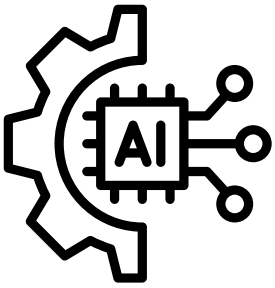
1. INTELIGÊNCIA ARTIFICIAL (IA): O QUE É E SUAS IMPLICAÇÕES PARA A SEGURANÇA DA INFORMAÇÃO

1.1 Definições de IA à Luz da ISO/IEC 22989 e da Legislação dos EUA e da UE

Inteligência Artificial (IA) é uma disciplina de pesquisa e desenvolvimento de mecanismos e aplicações de sistemas de IA, sendo que a pesquisa e o desenvolvimento podem ocorrer em vários campos, como ciência de dados, ciências humanas, matemática e ciências naturais. Por sua vez, **sistema de IA** é um sistema projetado que gera resultados como conteúdo, previsões, recomendações ou decisões para um determinado conjunto de objetivos definidos por humanos, que pode usar várias técnicas e abordagens relacionadas à IA para desenvolver um modelo para representar dados, conhecimento, processos, etc. usado para realizar tarefas e que pode operar com vários níveis de automação.



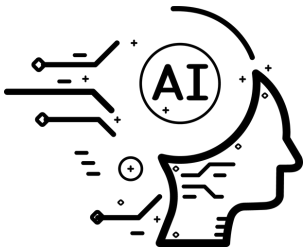
[tradução livre da definição da ISO/IEC 22989:2022(en)]



"(...) entende-se por: 1) **'Sistema de IA'**, um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais; (...)"

[art. 3º do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho (pt)]

O termo **'Inteligência Artificial'** (IA) se refere a um sistema baseado em máquina que pode, para um determinado conjunto de objetivos definidos por humanos, fazer previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais. Os sistemas de IA utilizam informações oriundas de máquinas e humanos para: a) perceber ambientes reais e virtuais; b) abstrair tais percepções em modelos por meio de análise de forma automatizada; e c) usar inferência de modelo para formular opções de informação ou ação.



[tradução livre da 'SEC. 3. DEFINITIONS' do National Artificial Intelligence Initiative Act of 2020, dos EUA]

1.2 Desafios da IA para a Segurança da Informação e a Cibersegurança

A Inteligência Artificial (IA) oferece muitos benefícios, mas também traz desafios significativos para a segurança da informação e a cibersegurança. A seguir listamos alguns dos principais desafios e possíveis soluções para mitigá-los.

1.2.1 Desafios da IA para a Segurança da Informação e a Cibersegurança

Desafio: a IA pode ser usada por agentes maliciosos para automatizar ataques cibernéticos, tornando-os mais sofisticados e difíceis de detectar. Exemplos incluem ataques *ransomware*, *phishing* e DDoS automatizados, criação de *malware* avançado e exploração de vulnerabilidades em grande escala.

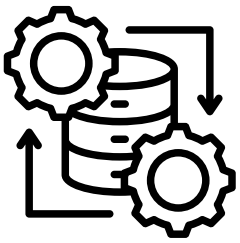
Soluções:

IA defensiva: utilizar IA para detectar padrões anômalos em tempo real, prever comportamentos maliciosos e automatizar a resposta a incidentes.

Sistemas de detecção de intrusões baseados em IA: implementar sistemas que usam aprendizado de máquina para identificar atividades suspeitas e bloquear ameaças Ide forma proativa.

Análise comportamental: analisar o comportamento de usuários e sistemas para detectar desvios que possam indicar um ataque automatizado.

1.2.2 Desafios da IA para a Segurança da Informação e a Cibersegurança



Desafio: os algoritmos de IA dependem de grandes quantidades de dados para treinamento. Um ataque de modelagem adversária pode alterar esses dados (ataques de "*data poisoning*"), comprometendo os modelos de IA e levando-os a tomar decisões incorretas ou inseguras.

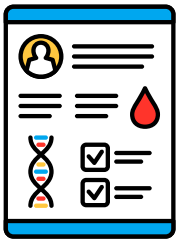
Soluções:

Treinamento robusto: desenvolver modelos de IA que sejam robustos contra perturbações nos dados de treinamento, incluindo a utilização de técnicas de aprendizado resistente a ataques adversários.

Validação de dados: implementar controles rigorosos de integridade e verificação dos dados usados para treinar os modelos de IA.

Defesa adversária: treinar os modelos para reconhecer entradas maliciosas associadas a ataques de *data poisoning*, em suma, testá-los contra modelos adversários durante o treinamento para que aprendam identificar e corrigir vulnerabilidades.

1.2.3 Desafios da IA para a Segurança da Informação e a Cibersegurança



Desafio: a IA processa enormes quantidades de dados, incluindo informações pessoais e sensíveis. Isso levanta preocupações sobre a privacidade e o controle dos dados. O uso indevido ou vazamento dessas informações pode resultar em violações de privacidade.

Soluções:

Anonimização e pseudonimização de dados: garantir que os dados utilizados para treinamento e inferências sejam adequadamente anonimizados ou pseudonimizados, reduzindo o risco de identificação.

Técnicas de IA com preservação de privacidade: implementar IA federada e aprendizado criptográfico, que permitem o treinamento de modelos sem compartilhar dados pessoais diretamente.

Conformidade com regulamentações: seguir as leis e regulamentos de privacidade, tais como a Lei Geral de Proteção de Dados (LGPD) e as normas da Autoridade Nacional de Proteção de Dados – ANPD e o *General Data Protection Regulation* (GDPR) europeu, para garantir que a coleta e o uso de dados estejam dentro dos padrões de privacidade.

1.2.4 Exploração de vulnerabilidades de IA

Desafio: Sistemas baseados em IA podem conter falhas e vulnerabilidades que os tornam alvos para exploração. Ataques de IA podem explorar fraquezas nos modelos para obter acesso não autorizado a informações confidenciais ou realizar manipulações indesejadas.

Soluções:

Auditoria de modelos: realizar auditorias e testes de penetração em sistemas de IA para identificar e corrigir vulnerabilidades.

Transparência e interpretabilidade: desenvolver IA que seja transparente e cujos processos de tomada de decisão possam ser compreendidos e verificados.

Monitoramento contínuo: implementar processos e sistemas de monitoramento e resposta rápida para detectar e corrigir vulnerabilidades à medida que surgem.

1.2.5 Exploração de vulnerabilidades de IA

Desafio: a IA pode ser usada para criar conteúdos falsos realistas (*deepfakes*) ou manipular informações em larga escala, o que pode ser usado para fraudes, manipulação de opiniões públicas ou ataques de engenharia social. Algoritmos de IA podem ser usados para manipular algoritmos de recomendação, mesmo que com conteúdo verídico, e influenciar tendenciosamente opiniões e comportamentos de usuários e da sociedade.

Soluções para *deepfakes* e desinformação:

Tecnologias de verificação de autenticidade: desenvolver e utilizar ferramentas baseadas em IA para identificar *deepfakes* e outros conteúdos falsos. Adotar ferramentas ou fomentar comunidades para executar a verificação de veracidade de conteúdos (*fact check*).

Educação e conscientização: promover a educação sobre desinformação e treinar usuários a reconhecer sinais de manipulação.

Canais para denúncias: criar processos e canais nas plataformas de conteúdo para receber e tratar denúncias de usuários e da comunidade.

Autenticação baseada em *blockchain*: utilizar *blockchain* ou outras tecnologias que possibilitem autenticar e verificar a origem de conteúdos digitais.

Soluções para manipulação:

Diretrizes éticas: empresas que usam algoritmos de recomendação podem aderir a diretrizes éticas, como as promovidas por organizações de IA ética, para garantir que seus sistemas de recomendação respeitem os direitos dos usuários e não explorem vieses comportamentais de maneira prejudicial.

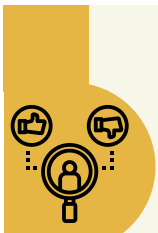
Desenvolvimento de IA centrada no ser humano: adotar princípios de *design* que priorizem o bem-estar dos usuários, garantindo que os algoritmos de recomendação não sejam apenas lucrativos, mas também benéficos à sociedade.

Transparência no funcionamento de algoritmos: mediante a explicação pelas plataformas aos usuários sobre como as recomendações são feitas, para melhorar a confiança e permitir que eles avaliem melhor a relevância.

Exposição do critério de recomendação: inclusão de informações sobre os critérios utilizados (baseados em histórico de compras, perfis semelhantes, preferências explícitas, etc.), dando ao usuário mais controle sobre as recomendações que recebe.

Regulação de algoritmos: governos e órgãos reguladores podem estabelecer normas que exijam maior transparência e controle sobre os algoritmos de recomendação, como ocorre em discussões sobre o uso de IA em decisões comerciais e sociais.

Controle sobre a exploração de dados pessoais: limitar o uso de dados pessoais sensíveis para recomendações e respeitar as preferências dos usuários em relação à privacidade e ao controle dos dados.



Ajuste de parâmetros de personalização e de preferências: para oferecer aos usuários a opção de ajustar o nível de personalização das recomendações como, por exemplo, controles para escolher entre sugestões personalizadas, mais amplas ou com base em tendências globais; capacidade de excluir certos tipos de informações ou preferências que influenciam os algoritmos; e opção de desativar completamente as recomendações baseadas no histórico do usuário ou em dados pessoais, optando por listas de conteúdos não personalizadas ou curadas por critérios objetivos.

Diversidade algorítmica e **diversidade forçada:** incentivar algoritmos de recomendação a promoverem variedade, expondo os usuários a conteúdos, opiniões e opções que diferem de suas preferências tradicionais. Isso pode ser implementado através da adição de elementos aleatórios ou diversificados nas sugestões, evitando que as recomendações reforcem comportamentos predefinidos (‘bolhas algorítmicas’), em que os usuários são expostos apenas a um conjunto limitado de opções com base em comportamentos anteriores.

Exposição a opiniões opostas: em contextos como recomendações de notícias ou opiniões, os algoritmos podem incluir recomendações de fontes diferentes, ajudando a ampliar o espectro de pontos de vista acessíveis ao usuário.

Detecção de manipulação artificial mediante **monitoramento contínuo:** implementar sistemas de IA que monitorem atividades suspeitas e manipulações em larga escala. Por exemplo, comportamentos como cliques repetidos de *bots* ou criação de avaliações falsas podem ser identificados e neutralizados.

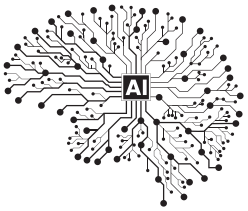
Detecção de manipulação artificial mediante **verificação de conteúdo e fontes** mediante a criação de camadas de verificação para identificar quando algoritmos externos estão manipulando recomendações e, também, a inclusão da análise de padrões anômalos de uso e de avaliações falsas ou exageradas.

Dissuasão do uso de manipulação artificial mediante **penalização de manipulações**, por exemplo, pelo uso de mecanismos como a redução da visibilidade de recomendações provenientes de contas suspeitas ou a avaliação mais rigorosa de certos tipos de conteúdo.

Auditorias independentes: realizar auditorias de algoritmos por partes externas pode identificar falhas ou manipulações, garantindo a integridade do sistema de recomendação.

Intervenção humana em casos críticos: integrar um processo de revisão humana nas recomendações em casos críticos (como avaliações e recomendações de profissionais ou serviços de saúde) pode evitar influências indevidas.

1.2.6 IA como uma caixa-preta (falta de transparência)



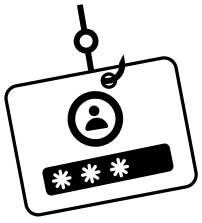
Desafio: muitos modelos de IA, especialmente os mais complexos, funcionam como 'caixas-pretas', ou seja, seus processos de decisão são pouco ou nada compreensíveis pelos usuários e até mesmo por técnicos externos. Isso dificulta a identificação de falhas de segurança ou decisões tendenciosas.

Soluções:

***Explainable* AI (XAI):** desenvolver algoritmos de IA que possam explicar seus processos de decisão, oferecendo maior transparência e auditabilidade.

Revisões de conformidade: criar políticas de revisão para garantir que os sistemas de IA usados em operações críticas de segurança estejam em conformidade com requisitos de transparência e segurança.

1.2.7 Uso malicioso de IA em ciberespionagem



Desafio: a IA pode ser usada para automatizar a coleta de informações sensíveis ou realizar ataques persistentes e sofisticados (como *phishing* altamente personalizado) de forma contínua e escalável.

Soluções:

Inteligência artificial de contrainteligência: utilizar IA para detectar comportamentos anômalos que possam indicar espionagem ou atividades de coleta de dados.

Treinamento e conscientização de funcionários: treinar os colaboradores para reconhecer e se proteger contra ataques de phishing, incluindo os sofisticados, e outros tipos de engenharia social.

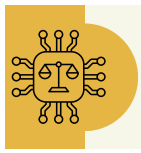
Sistemas de monitoramento avançados: implementar sistemas de detecção de intrusões com IA para monitorar tráfego de rede e identificar atividades suspeitas em tempo real.

1.2.8 Viés e discriminação

Desafio: sistemas de IA podem perpetuar preconceitos e vieses se forem treinados em conjuntos de dados enviesados. Isso pode resultar em decisões discriminatórias, afetando a segurança e a privacidade de certos grupos.

Soluções:

Auditoria de dados: analisar os dados utilizados no treinamento para garantir que sejam representativos e livres de viés.



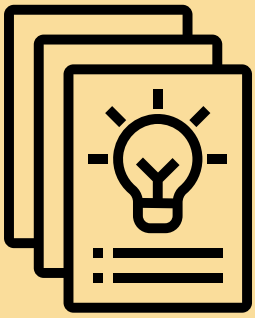
IA ética: desenvolver políticas de IA ética e responsabilidade para garantir que os sistemas respeitem princípios de justiça e não-discriminação.

Diversificação de equipes: garantir que as equipes responsáveis pelo desenvolvimento de IA incluam uma diversidade de perspectivas para identificar possíveis fontes de viés.

Esses desafios ilustram a necessidade de abordagens equilibradas e colaborativas entre governos, indústrias e especialistas em cibersegurança para garantir que a IA seja utilizada de maneira segura e ética.

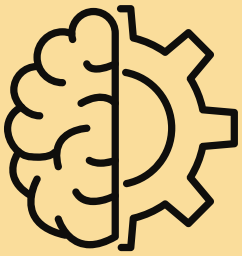
1.3 Normas e Iniciativas de Regulação

- Estratégia Brasileira de Inteligência Artificial – EBIA (2021) **[em revisão]**: visa potencializar o desenvolvimento e o uso da tecnologia com vistas a promover o avanço científico e solucionar problemas concretos do País, identificando áreas prioritárias nas quais há maior potencial de obtenção de benefícios, com a expectativa de que a IA possa trazer ganhos na promoção da competitividade e no aumento da produtividade brasileira, na prestação de serviços públicos, na melhoria da qualidade de vida das pessoas e na redução das desigualdades sociais.

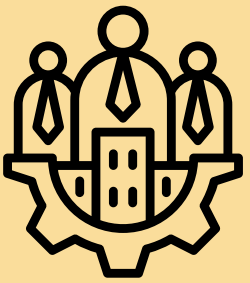


- **Plano Brasileiro de Inteligência Artificial 2024-2028 – IA para o Bem de Todos**: visa transformar a vida dos brasileiros por meio de inovações sustentáveis e inclusivas baseadas em IA; equipar o Brasil de infraestrutura tecnológica avançada com alta capacidade de processamento, incluindo um dos cinco supercomputadores mais potentes do mundo, alimentada por energias renováveis; desenvolver modelos avançados de linguagem em português, com dados nacionais que abarcam nossa diversidade cultural, social e linguística, para fortalecer a soberania em IA; formar, capacitar e requalificar pessoas em IA em grande escala para valorizar o trabalhador e suprir a alta demanda por profissionais qualificados; e promover o protagonismo global do Brasil em IA por meio do desenvolvimento tecnológico nacional e ações estratégicas de colaboração internacional.

- **Resolução CNJ Nº 332, de 21 de agosto de 2020**, que dispõe sobre a ética, a transparência e a governança na produção e no uso de IA no Poder Judiciário, e a **Portaria CNJ Nº 271, de 4 dezembro de 2020**, que regulamenta o uso de AI no âmbito do Poder Judiciário.
- **ABNT NBR ISO/IEC 22989:2023**: estabelece terminologia para IA e descreve conceitos no campo da IA.

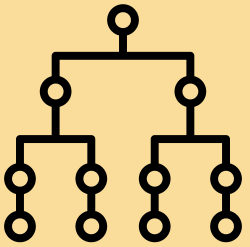


- **ISO/IEC 23053:2022 (en)**: estabelece uma estrutura de IA e Aprendizado de Máquina (ML) para descrever um sistema de IA genérico usando tecnologia de ML. A estrutura descreve os componentes do sistema e suas funções no ecossistema de IA. É aplicável a todos os tipos e tamanhos de organizações, incluindo empresas públicas e privadas, entidades governamentais e organizações sem fins lucrativos, que estão implementando ou usando sistemas de IA.



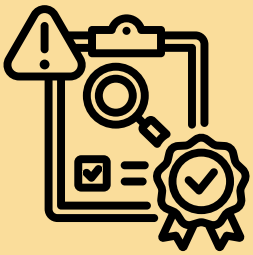
- **ABNT NBR ISO/IEC 38507:2023**: trata das implicações de governança do uso de IA pelas organizações, oferecendo princípios e estruturas que asseguram uma integração de IA responsável e alinhada com os objetivos estratégicos das organizações. Essa versão da ABNT é comentada em relação à original.
- **ABNT NBR ISO/IEC 42001:2024**: especifica os requisitos e fornece orientações para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de IA no contexto de uma organização.

- **ISO/IEC JTC 1/SC 42 Artificial Intelligence**: é um subcomitê de padronização do Comitê Técnico Conjunto ISO/IEC JTC 1 da International Organization for Standardization (ISO) e da International Eletroctechnical Commission (IEC) que desenvolve e facilita o desenvolvimento de padrões internacionais, relatórios técnicos e especificações técnicas nas áreas de IA e big data. As normas ISO/IEC 22989 e 42001 e várias outras aplicáveis a esses temas se originaram dos trabalhos do subcomitê (ver: https://jtc1info.org/sd-2-history/jtc1-subcommittees/sc-42/)



- **ENISA Multilayer Framework for Good Cybersecurity Practices for AI**: estrutura escalável para orientar autoridades nacionais de cibersegurança e partes interessadas em IA sobre os passos que devem seguir para proteger seus sistemas, operações e processos de IA, utilizando os conhecimento e as melhores práticas existentes e identificando elementos faltantes. O *framework* ENISA consiste de três camadas – fundamentos de cibersegurança, cibersegurança específica para IA e cibersegurança para IA específica do setor-alvo.

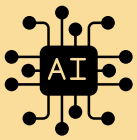
- **AI Act da União Europeia** [Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho (pt)]: regula o uso de IA com base em níveis de risco, sendo a primeira legislação abrangente sobre IA no mundo.



- **ENISA Cybersecurity of AI and Standardisation**: publicação que prove uma visão geral sobre normas relacionadas à cibersegurança de IA existentes, em elaboração, sob consideração e planejadas.

- **H.R.6216 – National Artificial Intelligence Initiative Act of 2020 (EUA)**: lei que visa assegurar a liderança contínua dos EUA na pesquisa e desenvolvimento de IA; liderar o mundo no desenvolvimento e utilização de sistemas de IA confiáveis nos setores público e privado; maximizar os benefícios dos sistemas de IA para todo o povo americano; e preparar a força de trabalho atual e futura dos EUA para a integração de sistemas de IA em todos os setores da economia e da sociedade.
- **Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence**: ordem executiva do presidente dos EUA com vistas a garantir que o país lidere o caminho para a realização das promessas e a gestão dos riscos da IA. Estabelece, entre outras coisas, padrões para segurança e proteção no desenvolvimento e no uso de IA, proteção da privacidade dos norte-americanos, promoção da equidade e dos direitos civis, defesa dos consumidores e dos trabalhadores, promoção da inovação e da concorrência e promoção da liderança mundial norte-americana. Dá um prazo de 365 dias, que encerra em 30/10/2024, para que órgãos e agências concluam os trabalhos designados em suas áreas de atuação.

- **NIST AI 600-1 Risk Management Framework (EUA)**: estrutura desenvolvida em colaboração com os setores público e privado para gestão de riscos associados à IA para proteger pessoas, organizações e a sociedade. O *framework* NIST é de uso voluntário e destina-se a melhorar a capacidade de incorporar recomendações e boas práticas de confiabilidade no projeto, no desenvolvimento, no uso e na avaliação de produtos, serviços e sistemas de IA.
- **Projeto de Lei nº 2338, de 2023**: dispõe sobre o uso da IA.
- **GSI/PR**: tem acompanhado desde 2019 as discussões do tema nos organismos e grupos de trabalho e da legislação, nacionais e internacionais, com vistas à eventual elaboração de norma com diretrizes de segurança da informação e cibersegurança para uso de soluções de IA pela APF.



1.4 Conclusões

A IA trouxe grandes oportunidades, porém, também trouxe desafios de mesma proporção (será?), desde questões de ordem ética e social (p.ex.: desemprego, discriminação, *fakenews* e desinformação, manipulação), até questões relacionadas à segurança da sociedade (p.ex.: biológica, química, nuclear e outras, passando pela SI e cibersegurança).

Para fazer frente a esses desafios, é necessário, entre outras coisas:

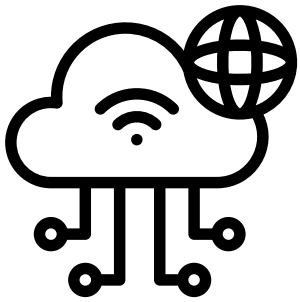
- superar as dificuldades para criar normas uniformes entre os países;
- mecanismos e instâncias para acompanhar e, quando necessário, regular a evolução do desenvolvimento e dos usos da IA; e
- equilibrar as necessidades de regulação com as de inovação.

2. COMPUTAÇÃO EM NUVEM: DEFINIÇÃO E SEUS DESAFIOS REGULATÓRIOS

2.1 Definições de Computação em Nuvem à Luz da Legislação GSI/PR e da ISO/IEC 17788

Computação em nuvem - modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN).

[Portaria GSI/PR nº 93, de 18 de outubro de 2021. Glossário de Segurança da Informação]



O Glossário de Segurança da Informação do GSI/PR também traz as definições de IaaS, PaaS e SaaS, entre outras.

As definições de nuvem privada (ou interna), nuvem comunitária, nuvem pública (ou externa) e nuvem híbrida são apresentadas na Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos de segurança da informação para uso de soluções de computação em nuvem pelos órgãos e pelas entidades da APF.

Computação em nuvem: paradigma para permitir o acesso em rede a um conjunto escalável e flexível de recursos físicos ou virtuais compartilháveis com provisionamento em autoatendimento e administração sob demanda. Exemplos de recursos incluem servidores, sistemas operacionais, redes, *software*, aplicativos e equipamentos de armazenamento.

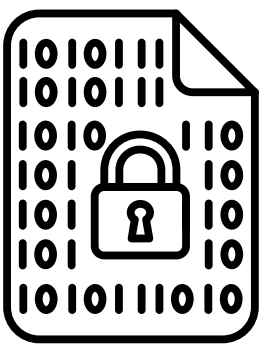
[tradução livre da definição da ISO/IEC 17788:2014(en)]

A ISO/IEC 17788 também traz as definições de nuvem privada, nuvem comunitária, nuvem pública, nuvem híbrida, IaaS, PaaS e SaaS, entre outras.

2.2 Desafios da Computação em Nuvem para a Segurança da Informação e a Cibersegurança

2.2.1 Perda de controle sobre dados

Desafio: Ao migrar dados para a nuvem, as organizações podem perder o controle direto sobre como esses dados são armazenados e gerenciados, aumentando o risco de acessos não autorizados.



Solução: Implementar criptografia de ponta a ponta para proteger os dados em repouso e em trânsito. Além disso, garantir que o provedor de nuvem cumpra com certificações de segurança e práticas de conformidade relevantes, como a ISO/IEC 27001, os gestores públicos federais observem na contratação desses serviços as normas federais, como a IN GSI/PR nº 5/2021 e a Portaria SGD/MGI nº 5.950/2023, e os órgãos e entidades da APF adotem normas internas e boas práticas de controle de acesso, tais como o Modelo de Política e Gestão de Controle de Acesso, da SGD/MGI.

2.2.2 Violação de dados (*data breaches*)

Desafio: Acesso não autorizado aos dados armazenados na nuvem pode resultar em violações de dados, prejudicando a privacidade e segurança da informação.

Solução: Adotar autenticação multifator (MFA), usar criptografia robusta e políticas de controle de acesso com base em identidade (IAM), além de monitorar continuamente a atividade na nuvem com ferramentas de detecção de intrusão.

2.2.3 Segurança de API e interfaces

Desafio: as interfaces e APIs públicas usadas para acessar os serviços de nuvem são alvos para ataques, como interceptação de comunicações e uso indevido.

Solução: implementar práticas seguras de desenvolvimento de API, como autenticação robusta, criptografia TLS (*Transport Layer Security*) e limitação de taxa de requisições. Realizar testes de penetração regulares nas APIs. Usar boas práticas e recomendações do GSI/PR e da SGD/MGI para desenvolvimento e uso de API, tais como as que constam na OSIC 10/23, da SSIC/GSI/PR, e no Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para APIs, da SGD/MGI.

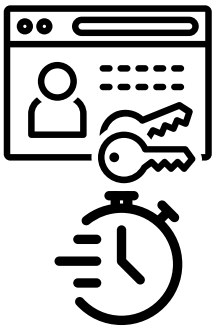
2.2.4 Conformidade e regulamentações

Desafio: organizações que usam serviços de nuvem precisam garantir que estão em conformidade com regulamentos de privacidade e segurança, como a Lei Geral de Proteção de Dados (LGPD) ou o General Data Protection Regulation (GDPR) europeu.

Solução: avaliar se o provedor de nuvem cumpre as regulamentações de proteção de dados e oferece ferramentas de conformidade. Prever auditorias regulares para garantir que as práticas de gestão de dados estejam alinhadas com os requisitos legais, tais como as normas da Autoridade Nacional de Proteção de Dados – ANPD e as já citadas IN GSI/PR nº 5/2021 e a Portaria SGD/MGI nº 5.950/2023. A ANPD, além de suas normas, também disponibiliza em sua página guias orientativos, documentos técnicos e outras publicações sobre o tema.

2.2.5 Gerenciamento de identidades e acessos

Desafio: Desafio: a gestão inadequada de permissões de usuários pode permitir acessos indevidos, elevando o risco de invasão e comprometimento dos dados.



Solução: adotar o princípio do menor privilégio (*Principle of Least Privilegie* – PoLP), onde os usuários têm apenas as permissões necessárias e pelo tempo necessário para realizar suas atividades funcionais e, quando envolver informações classificadas, conjugar isso com o princípio need to know. Integrar sistemas robustos de IAM (*Identity and Access Management*) com políticas de auditoria e revisão contínua de acessos.

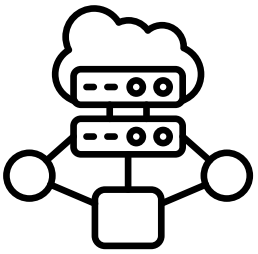
2.2.6 Ambientes multinuvem e híbridos

Desafio: muitas organizações adotam múltiplos provedores de nuvem, o que pode aumentar a complexidade na gestão de segurança, já que diferentes ambientes exigem diferentes práticas e ferramentas.

Solução: usar soluções de gerenciamento de segurança unificadas (como SIEMs—*Security Information and Event Management*) para centralizar o monitoramento e resposta a incidentes em ambientes multinuvem. Definir políticas consistentes para toda a infraestrutura de nuvem.

2.2.7 Falhas no isolamento de dados (*multitenancy*)

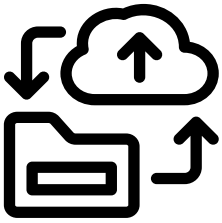
Desafio: em serviços de nuvem pública, os dados de diferentes organizações podem coexistir no mesmo ambiente físico, o que, em caso de falha, pode comprometer o isolamento dos dados.



Solução: escolher provedores de nuvem que ofereçam fortes mecanismos de isolamento, como virtualização segura e segmentação de rede. Avaliar a configuração de ambientes dedicados ou soluções de nuvem privada virtual (VPC) para aumentar a separação dos dados e, quando os requisitos e riscos do negócio assim exigirem, considerar até mesmo a separação física.

2.2.8 Disponibilidade e continuidade de negócios

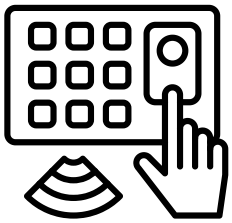
Desafio: ataques cibernéticos, falhas técnicas ou interrupções nos serviços de nuvem podem afetar a disponibilidade dos dados e serviços essenciais.



Solução: implementar planos robustos de recuperação de desastres e continuidade de negócios, além de usar *backups* automatizados e distribuídos geograficamente. Garantir que o Acordo de Nível de Serviço (SLA, na sigla em inglês) do provedor de nuvem atenda às necessidades de disponibilidade da organização.

2.2.9 Ataques internos (*insider threats*)

Desafio: funcionários ou administradores de nuvem mal-intencionados podem explorar seus privilégios para comprometer dados ou sistemas.



Solução: estabelecer políticas rigorosas de controle de acesso baseadas em função (*Role-Based Access Control* – RBAC) e monitorar as atividades dos usuários internos com ferramentas de auditoria contínua. Implementar políticas de segurança *zero trust*, onde cada acesso é constantemente verificado.

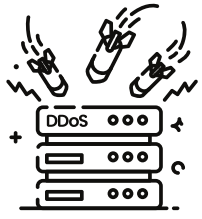
2.2.10 Falta de transparência no provedor de nuvem

Desafio: algumas organizações podem ter dificuldades em obter visibilidade completa sobre como os provedores de nuvem gerenciam a segurança, especialmente em áreas como governança e localização dos dados.

Solução: negociar contratos claros que incluam SLAs de segurança e visibilidade operacional. Buscar provedores que ofereçam dashboards de segurança transparentes e auditorias regulares para acompanhar a segurança e conformidade dos serviços.

2.2.11 Ataques distribuídos de negação de serviço (DDoS)

Desafio: serviços de computação em nuvem também podem estar suscetíveis a ataques distribuídos de negação de serviço (DDoS).

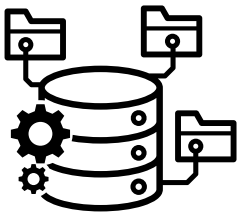


Solução: para mitigar esse risco é fundamental implementar soluções robustas de defesa DDoS, como o uso de firewalls de aplicação web (WAF) e sistemas de detecção de intrusões (IDS/IPS) que monitoram e filtram tráfego malicioso. Configurar a distribuição de tráfego em diferentes regiões geográficas por meio de redes de entrega de conteúdo (CDNs) e balanceadores de carga ajuda a absorver o impacto de ataques. Provedores de nuvem costumam oferecer serviços nativos anti-DDoS, que podem ser configurados para escalonar recursos automaticamente durante ataques, portanto, isso deve ser previstos no planejamento da contratação. Ademais, políticas de limitação de taxa e monitoramento constante garantem uma resposta rápida e eficaz a essa ameaça.

2.2.12 Contratação de serviços de computação em nuvem fornecidos a partir de país estrangeiro

Desafio: a regulação da computação em nuvem é complexa, pois envolve aspectos como jurisdição dos dados, especialmente quando os datacenters estão localizados em diferentes países, o que traz riscos à soberania nacional e dificulta a aplicação das normas nacionais e de muitas das soluções apresentadas nos itens anteriores.

Solução: observar o disposto no art. 18 da IN GSI/PR nº 5/2021 quanto à hospedagem de dados, metadados, informações e conhecimento produzidos e custodiados pelos órgãos e entidades da internet em provedor de serviço de nuvem. O GSI/PR e a ABIN estão avaliando alternativas para tratar em ambiente de computação em nuvem de Governo a informação classificada em grau de sigilo e o documento preparatório que possa originar informação classificada, cuja possibilidade ainda permanece vedada pela IN GSI/PR nº 5/2021 (art. 17, II).



2.3 Normas e iniciativas de regulação

- **Instrução Normativa GSI/PR Nº 5, de 30 de agosto de 2021**: dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

- **Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023**: estabelece modelo de contratação de *software* e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

- **Resolução CMN Nº 4.893, de 26 de fevereiro de 2021** (Banco Central do Brasil): dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

- **ABNT NBR ISO/IEC 17788**: fornece uma visão geral de computação em nuvem, juntamente com um conjunto de termos e definições. É uma fundação de terminologia para norma de computação em nuvem.
- **ABNT NBR ISO/IEC 27017**: Código de prática para controles de segurança da informação com base NBR ISO/IEC 27002 para serviços em nuvem; fornece diretrizes para os controles de segurança da informação aplicáveis à prestação e utilização de serviços em nuvem, fornecendo o seguinte: diretrizes adicionais para implementação de controles relevantes especificados na NBR ISO/IEC 27002; controles adicionais com diretrizes de implementação que são relacionadas especificamente a serviços em nuvem. Esta recomendação/norma fornece controles e diretrizes de implementação para provedores de serviços em nuvem e clientes de serviços em nuvem.

- **ABNT NBR ISO/IEC 27018:2021**: estabelece objetivos de controle, controles e diretrizes comumente aceitos para implementação de medidas para proteção de dados pessoais (DP), de acordo com os princípios de privacidade descritos na NBR ISO/IEC 29100 (**Estrutura de Privacidade** para o tratamento de DP), para o ambiente de computação em nuvem pública.

- **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho** (*General Data Protection Regulation* – GDPR/EU): Regulamento da UE que "estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" (art. 1º, § 1), sendo abrangente quanto às operações e à forma pela qual esse tratamento possa ocorrer (art. 4º, § 2).

- **H.R.4943 - Cloud Act (EUA)**: lei norte-americana de 2018 que altera o código penal federal para especificar que um provedor de serviço de comunicação eletrônica (ECS) ou serviço de computação remota (RCS) deve cumprir os requisitos existentes para preservar, fazer backup ou divulgar o conteúdo de uma comunicação eletrônica ou registros ou informações não relacionadas a conteúdo (tais como metadados), pertencentes a um cliente ou assinante, independentemente de a comunicação ou registro estar localizado dentro ou fora dos EUA.

2.4 Conclusões

A computação em nuvem transformou o cenário tecnológico, permitindo às organizações operar com maior agilidade e eficiência.

No entanto, o crescimento do uso de nuvem traz preocupações crescentes sobre a segurança e a privacidade dos dados e, mais recentemente, sobre a soberania de dados.

Tais preocupações demandam não apenas processos de segurança e privacidade melhores (governança) e soluções técnicas robustas (tecnologia), como também um arcabouço regulatório internacional (direito internacional e diplomacia) coerente e abrangente sobre o uso de dados e o direito inalienável dos Estados e de seus cidadãos sobre seus próprios dados.

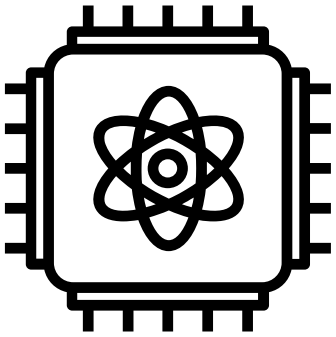
Para garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados na nuvem em nível nacional e nas organizações, é essencial, respectivamente, uma regulação clara e a adoção de boas práticas de segurança por parte de provedores e usuários.

3. COMPUTAÇÃO QUÂNTICA E CRIPTOGRAFIA PÓS-QUÂNTICA: IMPACTOS ESPERADOS E NECESSIDADES DE REGULAÇÃO

3.1 Definições de Computação Quântica, Criptografia Quântica e Criptografia Pós-Quântica

Processamento de informação quântica [ou] processamento quântico: processo, algoritmo ou computação que armazena e processa informação quântica usando, essencialmente, propriedades como superposição quântica e emaranhamento quântico. Exemplos de processos quânticos comuns onde fidelidades são relatadas incluem portas quânticas e medições quânticas.

Comunicação quântica: comunicação que utiliza essencialmente processamento de informação quântica para troca de informações. Protocolos que usam processamento e transmissão de informação clássicos em todos os estágios da comunicação, como a criptografia pós-quântica, se encaixam na categoria mais ampla de comunicação 'a prova de computação quântica', em vez de comunicação quântica.



Criptografia quântica: criptografia que utiliza essencialmente comunicação quântica.

[tradução livre da definição da ISO/IEC 4879:2024(en)]

A ISO/IEC 4879 também traz várias outras definições relacionadas à computação quântica, tais como informação quântica, superposição quântica, emaranhamento quântico, porta quântica, medição quântica e fidelidade que são usadas na definição acima.

3.2 Desafios da Computação Quântica para a Segurança da Informação e a Cibersegurança

A computação quântica apresenta desafios significativos para a segurança da informação e cibersegurança, especialmente em relação à criptografia, que é a base para a proteção de dados digitais. Abaixo estão os principais desafios e as soluções emergentes:

3.2.1 Quebra da criptografia assimétrica

Desafio: algoritmos quânticos, como o Shor's algorithm, poderiam quebrar a maioria dos sistemas de criptografia assimétrica (como RSA e ECC) usados atualmente. Esses sistemas dependem da dificuldade de fatoração de grandes números ou do problema do logaritmo discreto, que podem ser resolvidos eficientemente com computadores quânticos.

Soluções:

Criptografia pós-quântica: desenvolvimento de novos algoritmos resistentes a ataques quânticos, como a criptografia baseada em reticulados (*lattice-based cryptography*) e assinaturas *hash-based*. O NIST divulgou em agosto diferentes padrões de algoritmos pós-quânticos, baseados em reticulados, *stateless hash-based* e *stateful hash-based*.

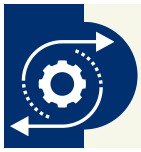
Adoção gradual: governos e empresas devem começar a implementar criptografia pós-quântica em fases para garantir que os sistemas estejam prontos antes que os computadores quânticos em grande escala estejam disponíveis.

3.2.2 Ataques a sistemas de criptografia simétrica

Desafio: algoritmos de pesquisa quântica, como o algoritmo de Grover, podem reduzir a segurança de criptografia simétrica (como AES) ao diminuir o tempo necessário para realizar uma busca por chave.

Soluções:

Aumento do tamanho das chaves: para compensar a redução da segurança, dobrar o tamanho das chaves usadas na criptografia simétrica pode fornecer a mesma proteção que os sistemas atuais fornecem contra ataques clássicos. Por exemplo, chaves AES de 256 bits são consideradas seguras contra ataques quânticos baseados no algoritmo de Grover.



Criptografia híbrida: utilizar algoritmos pós-quânticos juntamente com algoritmos clássicos em soluções híbridas, aumentando a resiliência dos sistemas.

3.2.3 Quebra da assinatura digital

Desafio: a maioria dos sistemas de assinatura digital, como os usados em redes *blockchain* e autenticação de identidades, dependem de criptografia assimétrica. O surgimento de computadores quânticos capazes de quebrar RSA e ECC comprometeria a integridade das assinaturas digitais.

Soluções:

Novos esquemas de assinatura: usar novos esquemas de assinatura digital pós-quânticos, como aqueles *hash-based* disponibilizados pelo NIST (ver item 4.2.1), esquemas de assinaturas Merkle (*hash-based* baseado em árvores Merkle) e outros resistentes a ataques quânticos.

Atualização de infraestruturas existentes: redes e sistemas que utilizam assinaturas digitais precisam ser atualizados para suportar assinaturas pós-quânticas, garantindo a integridade e autenticidade no ambiente quântico.

3.2.4 Riscos para a infraestrutura de chaves públicas (ICP ou PKI, na sigla em inglês)

Desafio: a computação quântica pode comprometer toda a infraestrutura de chaves públicas usada para proteger comunicações seguras na internet, como HTTPS, VPNs e e-mails criptografados, e para garantir autenticidade de assinaturas digitais.

Soluções:

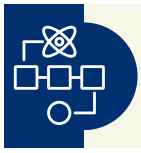
Redesenho da ICP: a introdução de algoritmos pós-quânticos requer o redesenho da infraestrutura de chaves públicas para suportar novos métodos de distribuição e gerenciamento de chaves.

Distribuição Quântica de Chaves (QKD, na sigla em inglês): tecnologias como a Distribuição Quântica de Chaves, que utiliza propriedades da mecânica quântica para garantir a segurança, podem ser utilizadas para aumentar a segurança da PKI em um 'futuro quântico'.

3.2.5 Ataques intermediários e persistência de dados

Desafio: adversários podem armazenar dados criptografados agora e, no futuro, quando computadores quânticos estiverem disponíveis, descriptografá-los retroativamente – estratégia conhecida na área inteligência como *store now*, *decrypt later* (SNDL) ou *harvest now*, *decrypt later* (HNDL) ou, ainda, *retrospective decryption*. Isso coloca em risco dados classificados de longo prazo e outros tipos de dados sensíveis de longo prazo.

Soluções:



Criptografia pós-quântica imediata: implementar algoritmos pós-quânticos o mais rápido possível, especialmente para dados classificados e outros dados sensíveis que precisam ser protegidos por décadas.

Segurança de dados transmitidos: organizações devem garantir que dados transmitidos hoje estejam protegidos contra futuros ataques quânticos, usando imediatamente criptografia híbrida ou algoritmos pós-quânticos.

3.2.6 Impacto em sistemas que usam tecnologia blockchain

Desafio: a tecnologia *blockchain* dependem da criptografia assimétrica para a verificação de transações. Computadores quânticos podem comprometer a segurança desses sistemas ao quebrar as chaves usadas para autenticação de transações.

Soluções:

Blockchain pós-quântico: algumas iniciativas já estão explorando a criação de *blockchains* resistentes a ataques quânticos, integrando criptografia pós-quântica em seus algoritmos de verificação.

Atualização das chaves existentes: para sistemas já estabelecidos que usam *blockchain*, uma migração para chaves públicas seguras contra computação quântica deve ser planejada e executada antes que o poder da computação quântica se torne uma ameaça prática.

3.2.7 Desafios operacionais e de implementação

Desafio: a transição para criptografia pós-quântica pode ser complexa e dispendiosa para organizações que precisam atualizar sua infraestrutura de segurança.

Soluções:

Planejamento estratégico: organizações devem começar a planejar a transição para a criptografia pós-quântica com antecedência, identificando quais sistemas críticos precisam ser atualizados primeiro.

Testes e validação: implementar novos algoritmos exige rigorosos testes e validações para garantir que eles ofereçam o nível de segurança necessário e funcionem sem comprometer a eficiência.

3.3 Normas e Iniciativas de Regulação:

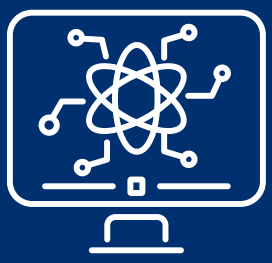
- **Instrução Normativa GSI nº 3, 6 de março de 2013**: dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia. Esta norma se encontra em processo de revisão e, entre outras coisas, tratará do uso de criptografia pós-quântica.

- **Comissão Europeia – Recomendação C(2024) 2393**: recomendação da Comissão Europeia, de 11/04/2024, sobre um roteiro para a execução da transição para criptografia pós-quântica (na página da CE há versões nas línguas da UE, incluindo português).

- **ISO/IEC 4879:2024 (en)**: define termos comumente usados no campo da computação quântica. É aplicável a todos os tipos de organizações (p.ex.: empresas comerciais, agências governamentais, organizações sem fins lucrativos) para o intercâmbio de conceitos de computação quântica.

- **ISO/IEC DIS 23837-1 (en)**: especifica requisitos de segurança, métodos de teste e avaliação para Distribuição Quântica de Chaves (QKD) tendo como referência a série de normas ISO/IEC 15408 (critérios de avaliação para SI).
- **ISO/IEC 18033 (en)**: trata sobre algoritmos de criptografia no âmbito da segurança da informação e estaria sendo atualizada para incluir algoritmos pós-quânticos (ver **ISO/IEC JTC 1/SC 27**, WG2, *Post-Quantum Cryptography*).

- **ISO/IEC JTC 1/WG 14** *Quantum Information Technology*: é um grupo de trabalho estabelecido pelo Comitê Técnico Conjunto ISO/IEC JTC 1 da ISO e da IEC com o seguinte escopo: 1) servir como foco e proponente do programa de padronização do JTC 1 em computação quântica. Identificar lacunas e oportunidades na padronização da computação quântica; 2) desenvolver e manter uma lista de normas existentes de computação quântica produzidas e de projetos de normas em andamento nos comitês técnicos da ISO, da IEC e do JTC 1; e 3) desenvolver entregáveis na área de computação quântica (entenda-se artigos técnicos, eventos, etc).



- **NIST *Post-Quantum Encryption Standards*:** em agosto de 2024 o NIST finalizou seus três primeiros padrões para criptografia pós-quântica, que protegem uma ampla gama de informações eletrônicas, desde mensagens de *e-mail* confidenciais até transações de comércio eletrônico, e incentivou os administradores de sistemas dos EUA a iniciarem o quanto antes a transição para os novos padrões.
- **ITU-T *Focus Group on Quantum Information Technology for Networks* (FG-QIT4N)**: grupo focal da UIT que visou, entre 2019 e 2021, fornecer uma plataforma colaborativa para aspectos de pré-padronização da *Quantum Information Technology* (QIT) para redes. Seus principais objetivos foram: estudar a evolução e aplicações da QIT para redes; focar na terminologia e nos casos de uso de QIT para redes; fornecer informações técnicas básicas necessárias e condições colaborativas para apoiar efetivamente o trabalho de padronização relacionado à *Quantum Information Network* (QIN) nos Grupos de Estudo da UIT-T; e fornecer uma plataforma de cooperação aberta com grupos de estudo da ITU-T e outras organizações de desenvolvimento de padrões (SDO, na sigla em inglês). Os entregáveis desse grupo estão disponíveis no *hyperlink* acima.

- **IEEE *Standards Association* (IEEE SA)**: vem facilitado o desenvolvimento de padrões para computação quântica tais como protocolo para comunicação quântica definida por *software*, segurança de rede pós-quântica, projeto e desenvolvimento de algoritmo quântico, arquitetura de computação quântica, práticas para migração para criptografia pós-quântica, etc.

3.4 Conclusões

A computação quântica promete avanços revolucionários em várias áreas, mas também traz ameaças significativas à segurança digital.

A criptografia pós-quântica e a criptografia quântica, em especial a primeira no curto prazo, surgem como soluções necessárias para proteger informações no futuro quântico.

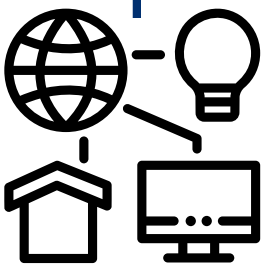
Em longo prazo, a tecnologia de distribuição quântica de chaves (QKD), uma tarefa da criptografia quântica, permitirá que duas partes gerem e compartilhem uma chave secreta aleatória para criptografar e descriptografar mensagens entre elas.

A coordenação regulatória global e nos níveis nacionais será essencial para garantir uma transição segura, tempestiva e eficaz para esses novos paradigmas tecnológicos, protegendo a integridade dos sistemas de informação diante de um 'futuro quântico' iminente.

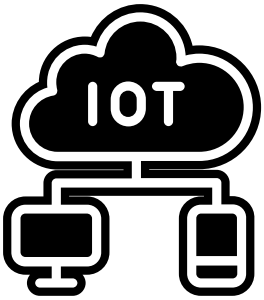
4. INTERNET DAS COISAS (IoT): RISCOS E DESAFIOS ESPECÍFICOS DE SEGURANÇA

4.1 Definição de Internet das Coisas (IoT)

Internet das Coisas (IoT) - infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas, com dispositivos baseados em tecnologias da informação existentes e nas suas evoluções, com interoperabilidade, conforme disposto no Decreto nº 9.854, de 25 de junho de 2019, que institui o Plano Nacional de Internet das Coisas



[Portaria GSI/PR nº 93, de 18 de outubro de 2021. Glossário de Segurança da Informação]



Dispositivo IoT: entidade de um sistema IoT que interage e se comunica com o mundo físico através de sensoriamento ou atuação.

Sistema IoT: sistema que fornece funcionalidades de Internet das Coisas. O sistema IoT inclui dispositivos IoT, *gateways* IoT, sensores e atuadores. No contexto desta norma, isso também inclui aplicativos e *backend* que dão suporte a soluções IoT.

[tradução livre da definição da ISO/IEC 27400:2022(en)]

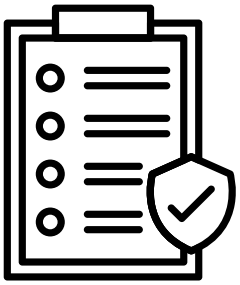
4.2 Desafios da Internet das Coisas para a Segurança da Informação e a Cibersegurança

A Internet das Coisas (IoT) apresenta muitos desafios para a segurança da informação e a cibersegurança devido à sua natureza distribuída, à diversidade de dispositivos conectados e à integração com redes críticas. Abaixo são apresentando os principais desafios e respectivas sugestões de soluções.

4.2.1 Diversidade de dispositivos e heterogeneidade

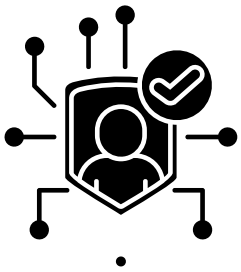
Desafio: a IoT envolve uma ampla gama de dispositivos (desde sensores simples até dispositivos complexos), que podem ter diferentes capacidades, sistemas operacionais e padrões de segurança. A falta de uniformidade dificulta a aplicação de medidas de segurança consistentes.

Solução: implementação de padrões de segurança universais e protocolos de comunicação que garantam a interoperabilidade de sistemas e dispositivos. Incentivar fabricantes a seguirem melhores práticas de segurança, como atualizações automáticas de *firmware* e certificações de segurança para dispositivos IoT.



4.2.2 Baixa capacidade computacional dos dispositivos

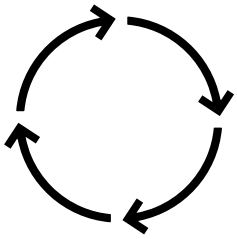
Desafio: muitos dispositivos IoT possuem recursos limitados de processamento e memória, o que restringe a implementação de medidas de segurança robustas, como criptografia avançada ou autenticação complexa.



Solução: utilização de criptografia leve e protocolos de autenticação simplificados, adequados para dispositivos com baixa capacidade computacional. Soluções baseadas em *Edge Computing* também podem ajudar a aliviar o processamento de rotinas de segurança para dispositivos mais potentes na borda da rede.

4.2.3 Atualizações de segurança inadequadas

Desafio: vários dispositivos IoT não possuem mecanismos para atualizações regulares de segurança ou os fabricantes descontinuam o suporte a dispositivos antigos, tornando-os vulneráveis a novas ameaças.



Solução: estabelecimento de políticas de ciclo de vida para dispositivos IoT, exigindo atualizações de *firmware* contínuas e negociando a extensão do suporte com os fabricantes. Deve-se avaliar, também, a edição de regulamentações governamentais que obriguem suporte de longo prazo para a segurança dos dispositivos.

4.2.4 Autenticação fraca

Desafio: muitos dispositivos IoT utilizam credenciais de acesso fracas ou compartilhadas, facilitando ataques de força bruta e invasões.

Solução: adoção de autenticação multifator (MFA) e protocolos de autenticação robustos, como OAuth 2.0 ou certificados digitais. Incentivar o uso de senhas fortes e a imediata mudança das senhas padrão.

4.2.5 Ataques distribuídos (DDoS)

Desafio: a IoT pode ser explorada para criar redes de bots (botnets), que lançam ataques de negação de serviço distribuído (DDoS), sobrecarregando serviços e infraestrutura.

Solução: implementação de *firewalls* específicos para IoT, uso de redes segmentadas para isolar dispositivos críticos e sistemas de detecção de anomalias que identifiquem atividades incomuns nos dispositivos conectados.

4.2.6 Privacidade de dados

Desafio: há dispositivos IoT que coletam grandes volumes de dados pessoais e sensíveis, o que pode resultar em violação de privacidade se essas informações não forem protegidas adequadamente.

Solução: aplicação de criptografia de ponta a ponta para dados em trânsito e em repouso, além de conformidade com regulamentações de privacidade, como a LGPD e o GDPR europeu. Também é importante garantir que os usuários possam gerenciar o consentimento sobre o que está sendo coletado nos dispositivos IoT, próprios ou não, que esteja usando.

4.2.7 Falta de visibilidade e monitoramento

Desafio: muitas organizações e usuários não possuem visibilidade completa de todos os dispositivos IoT conectados à rede, tornando difícil o monitoramento e a detecção de ameaças.

Solução: implementação de ferramentas de gestão de dispositivos IoT que permitam a descoberta automática e o monitoramento contínuo dos dispositivos conectados. Em organizações, soluções de *Security Information and Event Management* (SIEM) podem ajudar a centralizar os *logs* de eventos de segurança.

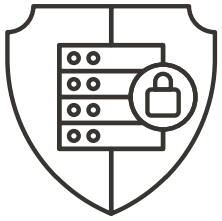
4.2.8 Comunicação insegura

Desafio: vários dispositivos IoT utilizam protocolos de comunicação inseguros, transmitindo dados sensíveis sem criptografia ou autenticação adequada.

Solução: utilização de protocolos de comunicação seguros, como TLS/SSL para a transmissão de dados, e *Virtual Private Networks* (VPN) para proteger a comunicação entre dispositivos e servidores centrais.

4.2.9 Ataques físicos

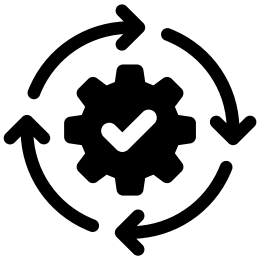
Desafio: dispositivos IoT muitas vezes são acessíveis fisicamente (p.ex.: sensores em áreas públicas), tornando-os vulneráveis a adulterações físicas.



Solução: utilização de técnicas de proteção física, como invólucros à prova de violação, e a implementação de medidas de segurança de *hardware*, como o uso de chips *Trusted Platform Module* (TPM) para proteger credenciais armazenadas (ver: ISO/IEC 11889-1, Trusted Computing Group).

4.2.10 Complexidade no gerenciamento de atualizações e configurações

Desafio: gerenciar a configuração e atualização de uma grande quantidade de dispositivos IoT é complexo, aumentando a probabilidade de falhas e brechas de segurança.



Solução: utilização de soluções automatizadas de gestão de *patches* e configuração, que garantam que todos os dispositivos estejam atualizados com as últimas correções de segurança e configurados de acordo com as melhores práticas.

4.2.11 Ataques à cadeia de suprimento

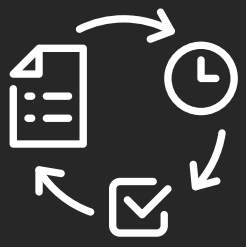
Desafio: os ataques à cadeia de suprimentos de dispositivos e sistemas de IoT estão se tornando cada vez mais preocupantes, pois os dispositivos IoT envolvem vários componentes de *hardware* e software, muitas vezes fabricados ou desenvolvidos por terceiros.

Soluções:

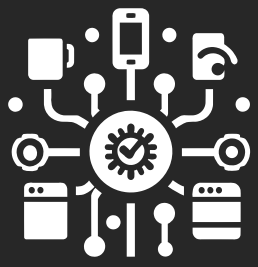
- **Geral – auditorias de segurança** e **políticas de *due* diligence rigorosas**: para a seleção de fornecedores, garantindo que eles sigam padrões de segurança reconhecidos, conjugadas com a adoção de **programas de avaliação de riscos da cadeia de suprimentos** que incluam monitoramento contínuo.
- ***Hardware* – certificações rigorosas e verificações de integridade**: implementação de **certificações rigorosas** para fornecedores de *hardware*, adoção de **verificações de integridade** dos componentes ao longo da cadeia de fornecimento e parcerias com fornecedores confiáveis.

- ***Hardware* – uso de selos de segurança e criação de trilhas de auditoria**: durante o transporte e monitoramento da cadeia logística, bem como a adoção de ***blockchain*** para rastrear cada etapa do transporte e assegurar a integridade dos dispositivos.
- ***Software* – políticas de segurança** que garantam a validação de fornecedores e a proteção das cadeias de distribuição de *software*.
- ***Software* – assinaturas digitais, verificação criptográfica e verificação de integridade de *software***: para garantir que apenas *firmware* autenticado e não modificado seja carregado em dispositivos IoT.
- ***Software* – políticas de verificação rigorosa de software de código aberto**, incluindo análise de código, monitoramento contínuo de vulnerabilidades conhecidas e **auditorias de segurança** periódicas.
- ***Software* – medidas de proteção em servidores de atualização** e monitoramento contínuo do processo de distribuição de atualizações.
- **Usuários e instalações – programas de conscientização de segurança** para funcionários, **políticas de acesso privilegiado**, e **monitoramento contínuo**: para detectar comportamentos suspeitos, conjugados com o estabelecimento de processo de **controle de acesso restrito** nas áreas sensíveis da cadeia de produção.

4.3 Normas e Iniciativas de Regulação:



- **Decreto nº 9.854, de 25 de junho de 2019**: institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas.



- **ISO/IEC 27400:2022 (en)**: provê diretrizes sobre riscos, princípios e controles para segurança e privacidade de soluções de IoT.
- **ISO/IEC 30141:2024 (en)**: fornece uma arquitetura de referência para IoT padronizada usando um vocabulário comum, designs reutilizáveis e melhores práticas do setor.
- **ISO/IEC 30162:2022 (en)**: requisitos de compatibilidade e modelo para dispositivos em sistemas industriais de internet das coisas (IIoT, na sigla em inglês).

- **ISO/IEC 30179:2023 (en)**: fornece uma visão geral e requisitos gerais de sistemas IoT para monitoramento ambiental ecológico. É voltada a sistemas de IoT para monitoramento de entidades naturais, tais como ar, água, solo e organismos vivos.
- **ISO/IEC JTC 1/SC 41** *Internet of Things and Digital Twin*: é um subcomitê de padronização da ISO e da IEC que serve como foco do programa de padronização do JTC 1 nas áreas de IoT e Digital *Twin*, incluindo suas tecnologias correlatas, e fornece orientação ao JTC 1, IEC, ISO e outras entidades que desenvolvam aplicações relacionadas a essas tecnologias.

- **ENISA Guidelines for Securing the Internet of Things**: elaborado com a contribuição de especialistas, o guia define diretrizes para proteger a cadeia de suprimentos de IoT em todo o seu ciclo de vida, desde os requisitos e o projeto até a entrega para uso final, manutenção e descarte. Seu público alvo são fabricantes, desenvolvedores, integradores e partes interessadas envolvidas na cadeia de suprimentos.

- **NISTIR 8259 Series – NIST Cybersecurity for IoT Program**: série de relatórios que fornece orientação a fabricantes e seus terceiros para concepção, projeto, desenvolvimento, teste, venda e suporte de dispositivos de IoT em todo o seu espectro de clientes.

- **H.R.1668 – IoT Cybersecurity Improvement Act of 2020 (EUA)**: exige que o NIST e o *Office of Management and Budget* (OMB) dos EUA tomem medidas específicas para aumentar a segurança cibernética para dispositivos de IoT, bem como que o NIST desenvolva e publique padrões e diretrizes para o governo federal sobre o uso e o gerenciamento apropriados de dispositivos de IoT de propriedade ou controlados por órgãos e entidades e conectados a sistemas de informação de propriedade ou controlados por estes, incluindo requisitos mínimos de segurança da informação para gerenciar riscos de segurança cibernética associados a tais dispositivos.

- GSI/PR: tem acompanhado desde 2019 as discussões do tema nos organismos e grupos de trabalho e da legislação, nacionais e internacionais, com vistas à eventual elaboração de norma com diretrizes de segurança da informação e cibersegurança para uso de soluções IoT.

4.4 Conclusões

A Internet das Coisas está transformando a forma como interagimos com o mundo ao nosso redor, proporcionando eficiência e novas funcionalidades – é onde o mundo digital toca o mundo físico.

No entanto, essa transformação traz desafios de gestão e riscos significativos para a cibersegurança, exigindo uma abordagem regulatória robusta e equilibrada para proteger dados e garantir a segurança dos dispositivos, sem causar ônus desnecessário às partes envolvidas.

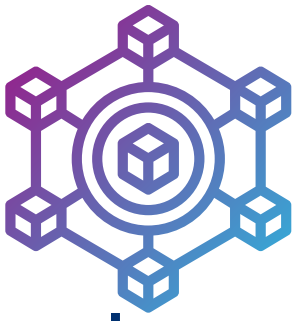
Esses desafios evidenciam a necessidade de estratégia e políticas nacionais de IoT com objetivos, metas e ações abrangentes e proativos para, por um lado, aproveitar os benefícios da IoT e, por outro lado, minimizar riscos associados, proteger o ecossistema IoT, estabelecer a regulamentação realmente necessária, com normas claras e aplicáveis, usar tecnologias adequadas à cada situação, aplicar as melhores práticas de desenvolvimento e realizar ações de conscientização dos usuários.

5. *BLOCKCHAIN* E TECNOLOGIAS CORRELATAS

5.1 Definição de *Blockchain*

Blockchain – base de dados que mantém um conjunto de registros que crescem continuamente. Novos registros são apenas adicionados à cadeia existente, sem que nenhum registro seja apagado.

[Portaria GSI/PR nº 93, de 18 de outubro de 2021. Glossário de Segurança da Informação]



Blockchain: livro-razão distribuído com blocos confirmados organizados em uma cadeia sequencial única encadeada por meio de *links* criptográficos. *Blockchains* são projetados para serem resistentes à adulteração e para criar registros contábeis finais, definitivos e imutáveis.

Sistema DLT (*Distributed Ledger Technology*), **sistema de livro-razão distribuído, sistema de tecnologia de livro-razão distribuído**: sistema que implementa um livro-razão distribuído.

Sistema *blockchain*: sistema que implementa a *blockchain*. Um sistema *blockchain* é um tipo de sistema DLT.

[tradução livre da definição da ISO/IEC 27400:2022(en)]

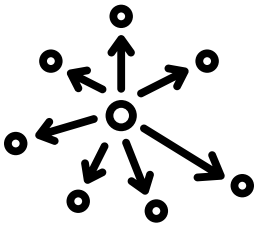
5.2 Desafios da tecnologia blockchain para a Segurança da Informação e a Cibersegurança

A **tecnologia *blockchain*** oferece várias vantagens em termos de segurança e transparência, mas também apresenta desafios que precisam ser enfrentados para garantir sua confiabilidade e segurança no contexto de **segurança da informação** e **cibersegurança**. Abaixo estão os principais desafios e suas respectivas soluções:

5.2.1 Ataques de 51% (controle da rede)

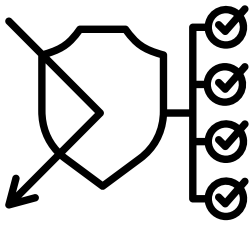
Desafio: um ataque de 51% ocorre quando um único minerador ou grupo de mineradores controla mais da metade do poder de processamento da rede *blockchain*. Isso permitiria ao atacante reescrever partes da *blockchain*, reverter transações ou criar transações duplicadas (*double spending*).

Solução: redes *blockchain* devem garantir que o poder de processamento seja suficientemente descentralizado, utilizando protocolos de consenso alternativos, como *Proof of Stake (PoS)*, que reduzem a dependência de poder computacional, ou *Proof of Authority (PoA)*, que exige uma camada de confiança entre validadores.



5.2.2. Vulnerabilidades em *smart contracts*

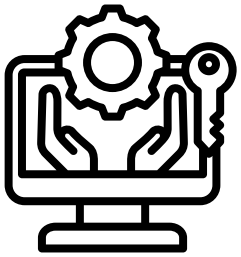
Desafio: *smart contracts* são scripts executados automaticamente na *blockchain*. Como são imutáveis após sua implantação, qualquer vulnerabilidade no código pode ser explorada por atacantes, como ocorreu no caso da DAO em 2016.



Solução: auditorias de segurança rigorosas no código dos *smart contracts* antes da implantação. Utilização de **ferramentas de verificação formal** e **testes de penetração** para identificar e corrigir vulnerabilidades antes de qualquer uso em produção. Implementar também contratos com **funcionalidades de atualização**, desde que balanceadas com segurança.

5.2.3. Chaves privadas comprometidas

Desafio: a posse de **chaves privadas** garante o controle total sobre os ativos em uma *blockchain*. Se essas chaves forem perdidas ou roubadas, os ativos não podem ser recuperados, e o atacante pode ter acesso irrestrito à conta.



Solução: implementar **melhores práticas de gestão de chaves**, como a utilização de *hardware wallets* para armazenar chaves privadas fora de ambientes conectados à internet. Outras práticas incluem **multifator de autenticação** (MFA) e **esquemas de chaves múltiplas** (multi-sig), onde várias chaves são necessárias para autorizar uma transação.

5.2.4. Ataques de *phishing* e engenharia social

Desafio: atacantes podem usar ***phishing*** ou outras técnicas de **engenharia social** para induzir vítimas a revelar suas chaves privadas ou credenciais de acesso, permitindo o roubo de ativos.

Solução: campanhas de **conscientização e educação sobre cibersegurança** para usuários de *blockchain*. Ferramentas de **autenticação forte** e interfaces de usuário que evitem a exposição direta de chaves privadas. Usar **segregação de funções**, onde uma única parte não tem controle total sobre transações críticas.

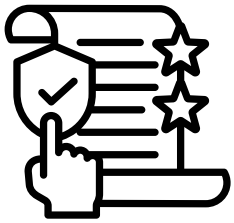
5.2.5. Escalabilidade e desempenho

Desafio: o aumento no número de transações pode sobrecarregar a rede *blockchain*, levando a tempos de confirmação mais longos e aumentando o risco de falhas de desempenho que afetam a segurança. Redes lentas podem também ser alvo de ataques de negação de serviço (DoS).

Solução: implementação de soluções de **escalabilidade**, como *sharding* (fragmentação da *blockchain*), *sidechains* (cadeias laterais que processam transações secundárias) e protocolos de Layer-2 (p.ex.: *Lightning Network*, *Rootstock*, *Stacks* e *Liquid Network*). Essas tecnologias ajudam a aumentar o desempenho sem comprometer a segurança da rede principal.

5.2.6. Segurança de redes descentralizadas

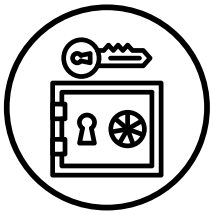
Desafio: redes *blockchain*, por serem descentralizadas, não possuem uma entidade central responsável pela segurança, tornando-as mais vulneráveis a erros de configuração, vulnerabilidades ou ataques coordenados por vários agentes.



Solução: estabelecimento de **normas e padrões de segurança** que todos os participantes da rede devem seguir. **Consensos híbridos** podem ser explorados, combinando elementos de descentralização com governança centralizada, como comitês de validadores com responsabilidade de supervisão da segurança.

5.2.7. Ataques Sybil e Eclipseas

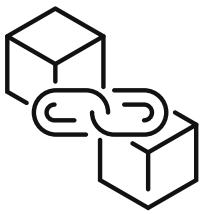
Desafio: em ataques Sybil, um atacante cria múltiplos nós falsos para obter controle da rede e eventualmente pode evoluir para um ataque de 51%, enquanto em ataques Eclipse, o atacante isola um nó específico de interagir com outros nós legítimos, controlando todas as suas interações.



Solução: limitar a criação de novos nós por meio de mecanismos de *Proof of Work* (PoW) ou ***Proof of Stake (PoS)***. Implementar **protocolos de resistência a Sybil**, como exigir um certo nível de reputação ou participação financeira para que novos nós possam se juntar à rede.

5.2.8. Privacidade dos dados

Desafio: a transparência do *blockchain*, que permite a verificação pública de transações, pode comprometer a **privacidade dos usuários**, já que dados financeiros ou pessoais podem ser rastreados e analisados.
Contudo, esse desafio está ligado a uma característica essencial das criptomoedas que vai de encontro à crescente pressão regulatória mundial, em especial para evitar a lavagem de dinheiro e que, em geral, grupos criminosos viabilizem suas operações por meio desses ativos digitais.



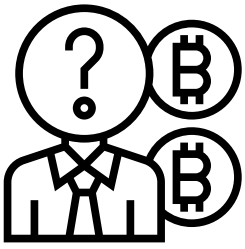
Solução: por um lado, utilização de ***blockchains* com foco em privacidade**, tais como Monero, Zcash e Horizen, que aplicam tecnologias como **criptografia de chaves de uso único e provas de conhecimento zero** (*Zero-Knowledge Proofs*), permitindo transações sem expor detalhes dos envolvidos. *Mixers* e *tumbler services* também podem ofuscar os detalhes das transações.

Por outro lado, as moedas de privacidade exemplificadas correm o risco de sofrerem cada vez mais restrições ou mesmo serem excluídas das grandes corretoras de criptomoedas, tais como a Binance e a OKX, em face das pressões regulatórias (ver em: Livecoins, Portal do Bitcoin [2023], Portal do Bitcoin [2024]). Pelas razões supracitadas, os *mixers* e *tumbler services* também sofrem pressões regulatórias (ver em: *Cointelegraph* Brasil, Wikipedia – *Cryptocurrency* tumbler).

5.2.9. Dependência de pseudoanônimos

Desafio: embora endereços *blockchain* sejam pseudoanônimos, ainda é possível vincular transações a identidades reais por meio de análise de padrões de transações ou vazamentos de dados externos.

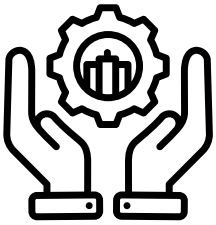
Ver aspecto controverso desse desafio no item anterior (6.2.8 Privacidade de Dados).



Solução: melhorias na anonimização de transações, como o uso de endereços temporários, e a combinação de transações para obscurecer padrões. Adotar **melhores práticas de anonimato** para proteger a identidade dos usuários fora da *blockchain* (p.ex.: não reutilizar endereços e minimizar a vinculação com serviços centralizados).

5.2.10. Governança descentralizada e *hard forks*

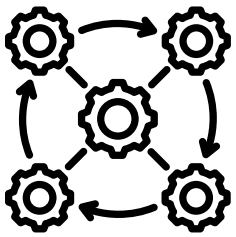
Desafio: a falta de uma governança clara pode resultar em conflitos entre membros da comunidade, levando a *hard forks*, que são divisões da *blockchain* original. *Hard forks* podem criar **fragmentação** na rede e vulnerabilidades de segurança, como ataques de repetição (***replay attacks***), onde transações válidas em uma cadeia podem ser repetidas na outra.



Solução: criação de mecanismos de governança bem definidos, como votação *on-chain* ou Organizações Autônomas Descentralizadas (DAOs), para decisões sobre mudanças importantes. Proteção contra ataques de repetição, implementando assinaturas exclusivas para cada cadeia após um *hard fork*.

5.2.11. Riscos de interoperabilidade

Desafio: Diferentes *blockchains* podem ter protocolos, formatos de dados e regras distintas, dificultando a **interoperabilidade** entre cadeias e a troca segura de informações ou ativos. Isso pode criar vulnerabilidades entre redes ao usar pontes inseguras.



Solução: Adoção de protocolos de interoperabilidade padrão, como Cosmos ou Polkadot, que facilitam a comunicação segura entre diferentes *blockchains*. Utilização de **tecnologias** *cross-chain*, como *atomic swaps*, que garantem a troca de ativos entre cadeias sem confiar em intermediários centralizados.

5.2.12. Composição maliciosa de aplicativos descentralizados (DApps)

Desafio: Aplicativos Descentralizados (DApps) frequentemente se compõem, interagindo entre si. Isso pode levar a vulnerabilidades quando um DApp confiável interage com outro DApp malicioso, comprometendo a segurança da transação.

Solução: implementação de **ferramentas de *sandboxing*** para DApps e **limitação de permissões** de interação entre diferentes contratos. **Auditorias regulares** e verificação formal de contratos antes da interação entre diferentes DApps.

Esses desafios refletem a complexidade inerente à tecnologia *blockchain*, que, embora poderosa, exige **medidas de segurança avançadas e boas práticas de desenvolvimento** para garantir que seja implementada de maneira segura e eficaz.

5.3 Normas e Iniciativas de Regulação:

- **Lei nº 14.478, de 21 de dezembro de 2022**: dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições.
- **Decreto nº 11.563, de 13 de junho de 2023**: regulamenta a Lei nº 14.478, de 2022, para estabelecer competências ao Banco Central do Brasil.
- **Banco Central do Brasil - Confira os próximos passos da regulação dos criptoativos e dos prestadores de serviços de ativos virtuais**: notícia de maio de 2024 do sítio do Banco Central do Brasil.
- **SERPRO – Como o governo federal usa o blockchain?** Matéria de janeiro de 2023 do SERPRO que traz uma breve história do *blockchain* e cenários de uso da tecnologia no setor governamental, incluindo as iniciativas do Serpro na área.
- **ACÓRDÃO 1613/2020 – TCU PLENÁRIO**: levantamento com o objetivo de identificar áreas de aplicação de *blockchain* e de livros-razão distribuídos (DLT) no setor público, seus principais riscos e fatores críticos de sucesso, além dos desafios para o controle. Determinou ao então Ministério da Economia, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público que atentem, em seu âmbito e nos órgãos e entidades sob sua supervisão, para a necessidade de realizar estudo de viabilidade e de verificar desafios, riscos e oportunidades dessas tecnologias.

- **ISO/TC 307**: comitê técnico da ISO responsável por desenvolver padrões internacionais para *blockchain* e tecnologias de livro-razão digital distribuído, incluindo segurança e governança.
- **ISO/IEC 22739:2024(en)**: define termos básicos relacionados a tecnologias de *blockchain* e de livro-razão distribuído para esclarecer o significado de termos e conceitos usados em outros documentos dentro do domínio dos padrões ISO/TC 307. Aplica-se a todos os tipos de organizações (p.ex.: empresas comerciais, agências governamentais, organizações sem fins lucrativos). O público-alvo inclui, entre outros, acadêmicos, arquitetos de soluções, clientes, usuários, desenvolvedores de ferramentas, reguladores, auditores e organizações de desenvolvimento de normas (SDO, na sigla em inglês).
- **ISO/TR 23244:2020(en)**: relatório técnico que provê uma visão geral da privacidade e da proteção de informações de identificação pessoal aplicadas a sistemas *blockchain* e tecnologias de livro-razão distribuído (DLT, na sigla em inglês).
- **ISO/TR 23455:2019(en)**: relatório técnico que fornece uma visão geral dos contratos inteligentes (*smart contracts*) em sistemas *blockchain* e DLT, descrevendo o que são esses contratos e como funcionam. Também discute métodos de interação entre vários contratos inteligentes. O relatório se concentra nos aspectos técnicos dos contratos inteligentes. Contratos inteligentes para uso e aplicações juridicamente vinculativas são apenas brevemente mencionados no relatório.
- **ISO/TS 23635:2022(en)**: especificação técnica (TS) que provê princípios orientadores e uma estrutura para a governança de sistemas *blockchain* e DLT, bem como orientações para o cumprimento dessa governança, incluindo contextos regulatórios e de risco que dão amparo ao uso eficiente, eficaz e aceitável de sistemas DLT.
- **ISO/TR 23576:2020(en)**: relatório técnico que discute as ameaças, riscos e controles relacionados a: sistemas que fornecem serviços de custódia de ativos digitais e/ou serviços de câmbio aos seus clientes (consumidores e empresas) e gestão da segurança quando ocorre um incidente; e informações sobre ativos (incluindo a chave de assinatura do ativo digital) gerenciadas por um custodiante de ativos digitais. O relatório é dirigido aos custodiantes de ativos digitais que gerenciam chaves de assinatura associadas a contas de ativos digitais, situação em que se aplicam certas recomendações específicas. Não fazem parte do escopo desse relatório: controles básicos de segurança de sistemas *blockchain* e DLT; iscos comerciais dos custodiantes de ativos digitais; segregação dos ativos dos clientes; questões de governaça e gestão.
- **IEEE *Blockchain Technical Community***: colabora com a IEEE *Standards Association* (IEEE SA) para desenvolver e aprimorar os padrões relacionados à *blockchain*. Na página da Comunidade há *links* para dezenas de normas da IEEE em desenvolvimento e publicadas sobre o assunto. Há também *links* para eventos e conferências e outras comunidades que tratam do assunto em setores específicos, como agricultura, saúde e indústria farmacêutica.
- **IEEE 2140.1-2020**: norma para requisitos gerais para negociação de criptomoedas. Aborda a autodisciplina e a ética profissional das plataformas de troca de criptomoedas, bem como a relevância entre elas e para as carteiras de criptomoedas. Também são tratados a lógica de negócios do mercado de criptomoedas, os procedimentos operacionais e os programas de autenticação de usuários. Além disso, trata de uma categoria técnica de requisitos, incluindo terminologias, estrutura arquitetônica básica, indicadores-chave, e especificações de interface do usuário final.

- **IEEE 2140.2-2021**: norma para gerenciamento de segurança para ativos criptográficos de clientes em corretoras de criptomoedas. Nela são definidos requisitos para múltiplos aspectos de gestão de segurança para ativos criptográficos de clientes em corretoras de criptomoedas, como identificação de usuários usando autenticação multifatorial, proteção priorizada de ativos de clientes sob circunstâncias imprevistas e ética profissional de operação para plataformas de negociação de criptomoedas.
- **IEEE 2140.5-2020**: norma que define uma estrutura de serviço de custódia para criptomoedas e ativos simbólicos. Esta estrutura inclui a arquitetura técnica de referência do custodiante, a descrição da lógica de negócios, os modelos de negócios de serviços de custódia, os critérios de avaliação de ativos digitais, os modelos de procedimentos operacionais e os modelos de suporte a requisitos regulatórios.
- **ANSI ASC X9 TR 54-2021 - *Blockchain Risk Assessment Framework***: relatório técnico que fornece uma estrutura para executar avaliações de risco operacional em sistemas e aplicações *blockchain* dentro de uma rede distribuída. Os riscos operacionais incluem as áreas de tecnologia da informação (TI) e segurança da informação (SI). TI inclui interoperabilidade, resiliência, acessibilidade e manutenção de *software*. SI inclui integridade de dados, confidencialidade, autenticação, autorização e responsabilidade (capacidade de registro). O relatório traz alguns aspectos dos riscos da aplicação, incluindo precisão dos dados, controle de versão, compatibilidade com versões anteriores e outras funções de usabilidade.
- **EU *Crypto-Assets Regulagion* (MiCA)**: instituiu em junho de 2023 regras de mercado para criptoativos na UE. O regulamento abrange criptoativos que não são atualmente regulamentados pela legislação existente na UE em matéria de serviços financeiros. As principais disposições aplicáveis aos que emitem e comercializam criptoativos (incluindo *tokens* de referência de ativos e *tokens* de moeda eletrônica) abrangem a transparência, a divulgação, a autorização e a supervisão das transações. Esse novo quadro jurídico apoiará a integridade do mercado e a estabilidade financeira, regulando as ofertas públicas de criptoativos e garantindo que os consumidores estejam mais bem informados sobre os riscos associados.

5.4 Conclusões

Blockchain e tecnologias correlatas têm o potencial de revolucionar vários setores ao oferecer segurança, transparência e eficiência de processos, principalmente naqueles que geram produtos digitais com prazos de validade curtos, tais como bilhetes e cartões de embarque aéreos, ferroviários e rodoviários, ingressos para espetáculos e outros dessa natureza.

No entanto, os riscos de cibersegurança e a complexidade associada aos sistemas *blockchain* exigem uma abordagem regulatória cuidadosa para garantir a integridade dos sistemas e a proteção dos dados, ao mesmo tempo que impedem, no caso das criptomoedas, o uso desses ativos digitais para lavagem de dinheiro ou viabilização da operação de grupos criminosos.

A criação de padrões e regulamentações robustas é fundamental para maximizar os benefícios de sistemas *blockchain* e de outros sistemas DLT, mantendo a confiança dos usuários e mitigando possíveis vulnerabilidades.

TLP:CLEAR