4º Webinário de Segurança da Informação

24 setembro

das 14h30 às 17h30 - ON-LINE

Panorama da regulação de tecnologias emergentes no cenário da cibersegurança global

Coordenação-Geral de Gestão de Segurança da Informação – CGGSI

1. Estrutura da apresentação

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

Cada um desses títulos está assim dividido :

- Definição conceitual à luz da legislação e/ou das normas
- Desafios para a SI e a cibersegurança e respectivas soluções
- Legislação e normas nacionais e internacionais
- Conclusões

2. Inteligência Artificial (IA): o que é e suas implicações para a SI

2.1 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]

2. Inteligência Artificial (IA): o que é e suas implicações para a SI

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

Desafio: **ameaças automatizadas** (*ransomware*, *phishing*, DDoS) e **ataques avançados**
Soluções: IA defensiva; sistemas de detecção de intrusões baseados em IA; análise comportamental

---

Desafio: manipulação de dados e modelagem adversária (p.ex.: ***data poisoning***)
Soluções: treinamento robusto; validação de dados; defesa adversária

---

Desafio: **privacidade dos dados** X volume de dados, velocidade e vulnerabilidade
Soluções: anonimização e pseudonimização de dados; técnicas de IA com preservação de privacidade (IA federada e aprendizado criptográfico); conformidade com regulamentações

---

Desafio: **exploração de vulnerabilidade** de IA
Soluções: auditoria de modelos; transparência e interpretabilidade; monitoramento contínuo

---

Desafio: IA como uma **caixa-preta** (falta de transparência)
Soluções: *Explainable AI* (*XAI*); revisões de conformidade

Desafio: uso malicioso de IA em **ciberespionagem**
Soluções: IA de contrainteligência; treinamento e conscientização de funcionários; sist. de monitoramento avançados

---

Desafio: ***deepfakes*, desinformação e manipulação**
Soluções: tecnologias e processos de verificação de autenticidade; educação e conscientização; canais para denúncias; autenticação baseada em *blockchain*; p/manipulação conjugar diretrizes éticas, técnicas, regulação e fiscalizar

---

Desafio: **viés e discriminação**
Soluções: auditoria de dados; políticas de IA ética e responsabilidade; diversificação de equipes

---

2. Inteligência Artificial (IA): o que é e suas implicações para a SI

2.3 Normas e Iniciativas de Regulação

Estratégia Brasileira de Inteligência Artificial – EBIA (2021) **[em revisão]**

Plano Brasileiro de Inteligência Artificial 2024-2028 – IA para o Bem de Todos

Resolução CNJ Nº 332, de 21 de agosto de 2020, e Portaria CNJ Nº 271, de 4 dezembro de 2020

ABNT NBR ISO/IEC 22989:2023: **terminologia** para IA **e conceitos** no campo de IA

ISO/IEC 23053:2022 (en): estrutura de IA e ML para sistemas de uso genérico. Para todos os tipos e tamanhos de orgs.

ABNT NBR ISO/IEC 23894:2023: **gestão de riscos** de IA para orgs. que desenvolvem, produzem, implantam ou usam

ISO/IEC TR 24368:2023 (en): visão geral de alto nível das preocupações éticas e sociais relacionadas à IA

ABNT NBR ISO/IEC 38507:2023: **governança** do uso de IA em orgs, princípios e estruturas p/integração de **IA responsável**

ABNT NBR ISO/IEC 42001:2024: **requisitos e orientações para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de IA no contexto de uma organização** (DIS: 42005, impactos; e 42006, auditoria)

ISO/IEC JTC 1/SC 42: **subcomitê do Comitê Técnico Conjunto ISO/IEC JTC 1 da ISO e da IEC** que desenvolve e facilita o desenvolvimento de padrões internacionais, relatórios técnicos e especificações técnicas nas áreas de IA e *big data*

ENISA Multilayer Framework for Good Cybersecurity Practices for AI: estrutura escalável para orientar autoridades nacionais de cibersegurança e partes interessadas em IA

EU AI Act **(UE, 2024)**: **regula o uso de IA com base em níveis de risco. '1ª lei abrangente sobre IA no mundo'**

ENISA Cybersecurity of AI and Standardisation: relatório c/visão geral sobre normas relacionadas à cibersegurança de IA

National Artificial Intelligence Initiative Act **(EUA, 2020)**: visa liderança em P&D, benefício do povo e força de trabalho

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence **(EUA, 2023)**

NIST AI 600-1 Risk Management Framework **(EUA, 2024)**: estrutura de gestão de riscos em IA; em parte, responde à EO

Projeto de Lei nº 2338, de 2023: **do Congresso Nacional** (iniciou no Senado), **dispõe sobre o uso da IA**

2. Inteligência Artificial (IA): o que é e suas implicações para a SI

2.4 Conclusões

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**.

3. Computação em nuvem: definição e seus desafios regulatórios

3.1 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.

3. Computação em nuvem: definição e seus desafios regulatórios

3.2 Desafios da Computação em Nuvem para a Segurança da Informação e a Cibersegurança (parte 1 de 2)

Desafio: **perda de controle sobre dados**
Soluções: criptografia de ponta a ponta; fazer provedor cumprir certificações e práticas de segurança (ex. ISO 27001), gestores públicos observarem normas (IN GSI 5/2021 e Prt SGD 5.950/2023) e órgãos adotarem normas internas e boas práticas de controle de acesso (Modelo de Política e Gestão de Controle de Acesso da SGD)

Desafio: violação de dados (***data breaches***)
Soluções: autenticação multifator (MFA), criptografia robusta e políticas de controle de acesso com base em identidade (IAM), monitoramento contínuo da atividade na nuvem com ferramentas de detecção de intrusão

---

Desafio: **segurança de API e interfaces** X ataques e usos indevidos
Soluções: práticas seguras de desenvolvimento, autenticação robusta, criptografia TLS e limitação de taxa de requisições; testes de penetração regulares; boas práticas e recomendações do GSI e da SGD (OSIC 10/23, Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para APIs)

Desafio: **conformidade e regulamentações**, em especial LGPD e normas ANPD e, se for o caso, GDPR
Soluções: avaliar se provedor cumpre regulamentações e oferece ferramentas de conformidade; auditorias para aferir conformidade às normas da ANPD e às IN GSI 5/2021 e a Prt SGD 5.950/2023

Desafio: **gerenciamento de identidades e acessos**
Soluções: princípio do menor privilégio (PoLP); se informações classificadas, conjugar c/ princípio *need to know;* integrar sistemas de IAM (*Identity and Access Management*) com políticas de auditoria e revisão contínua de acessos

---

Desafio: **ambientes multinuvem e híbridos** X complexidade na gestão de segurança
Soluções: soluções de gestão de segurança unificadas (ex. SIEMs) p/centralizar monitoramento e resposta a incidentes; políticas consistentes para toda a infraestrutura de nuvem (IN GSI 5/2021)

3. Computação em nuvem: definição e seus desafios regulatórios

3.2 Desafios da Computação em Nuvem para a Segurança da Informação e a Cibersegurança (parte 2 de 2)

Desafio: **falhas no isolamento de dados** (*multitenancy*)
Soluções: provedores c/ fortes mecanismos de isolamento (ex. virtualização segura e segmentação de rede); ambientes dedicados ou VPC p/ maior separação dos dados e, se requisitos e riscos exigirem, até mesmo separação física

---

Desafio: **disponibilidade e continuidade** de negócios
Soluções: planos robustos de recuperação de desastres e continuidade de negócios; *backups* automatizados e distribuídos geograficamente. Garantir que SLA do provedor atenda às necessidades de disponibilidade

---

Desafio: **ataques internos** (*insider threats*)
Soluções: controle de acesso baseado em função (*Role-Based Access Control – RBAC*); monitorar atividades de usuários internos c/ ferramentas de auditoria contínua; políticas *zero trust*: cada acesso é constantemente verificado

---

Desafio: **falta de transparência** no provedor sobre a gestão de segurança e a localização de dados
Soluções: contratos claros c/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

---

Desafio: **ataques** distribuídos de negação de serviço (**DDoS**)
Soluções: soluções de defesa DDoS (ex. WAF); sistemas de detecção de intrusões (IDS/IPS); distribuição de tráfego em diferentes regiões c/ uso de CDNs e balanceadores; políticas de limitação de taxa e monitoramento constante

---

Desafio: **serviços em nuvem fornecidos a partir de país estrangeiro** X localização dos dados
Soluções: seguir IN GSI 5/2021,art. 18, quanto à hospedagem de dados, metadados, informações e conhecimento produzidos e custodiados pela APF. GSI e ABIN estudam opções p/informação classificada (idem, art. 17, II).

3. Computação em nuvem: definição e seus desafios regulatórios

3.3 Normas e Iniciativas de Regulação

IN GSI 5/2021: **requisitos mínimos de SI p/ uso de soluções de nuvem pelos órgãos e pelas entidades da APF**

Prt SGD 5.950/2023: **modelo de contratação de software e de serviços de nuvem**, no âmbito dos **órgãos e entidades** integrantes **do SISP** do Poder Executivo Federal

Resolução CMN 4.893/2021 (Bacen): política de segurança cibernética e requisitos para a contratação de serviços de nuvem a serem observados pelas instituições autorizadas a funcionar pelo Bacen

ABNT NBR ISO/IEC 17788: visão geral de computação em nuvem, termos e definições

ABNT NBR ISO/IEC 27017: **Código de prática para controles de SI com base NBR ISO/IEC 27002 para serviços em nuvem**; diretrizes para os controles de SI aplicáveis à prestação e utilização de serviços em nuvem; diretrizes adicionais para implementação de controles relevantes especificados na NBR ISO/IEC 27002; controles adicionais com diretrizes de implementação relacionadas a serviços em nuvem; aplicável para provedores e clientes

ABNT NBR ISO/IEC 27018:2021: objetivos de controle, controles e diretrizes para **proteção de dados pessoais em nuvem** pública, de acordo com a NBR ISO/IEC 29100 (Estrutura de Privacidade para o tratamento de DP),

General Data Protection Regulation – GDPR/EU: regras da UE relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

Cloud Act: **(EUA, 2018)**: dispõe que um **provedor de serviço de comunicação eletrônica ou serviço de computação remota 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 (ex. metadados), **pertencentes a um cliente ou assinante**, independentemente de a comunicação ou registro estar localizado **dentro ou fora dos EUA**.

3. Computação em nuvem: definição e seus desafios regulatórios

3.4 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.

4. Computação quântica e criptografia pós-quântica: impactos esperados e necessidades de regulação

4.1 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.

4. Computação quântica e criptografia pós-quântica: impactos esperados e necessidades de regulação

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

Desafio: **quebra da criptografia assimétrica** (ex. RSA e ECC poderiam ser quebrados com o *Shor's algorithm*)
Soluções: criptografia pós-quântica; adoção gradual

Desafio: **ataques a sistemas de criptografia simétrica**
Soluções: aumento do tamanho das chaves (ex. chaves AES de 256 bits são consideradas seguras contra ataques quânticos baseados no algoritmo de Grover); criptografia híbrida (algoritmos pós-quânticos + clássicos)

Desafio: **quebra de assinatura digital** (ex. *blockchain* e autenticação de identidades usam criptografia assimétrica)
Soluções: esquemas de assinatura digital pós-quânticos (ex. os *hash-based* do NIST); esquemas de assinaturas *hash-based* baseado em árvores Merkle; atualização das atuais infraestruturas p/suportar assinaturas pós-quânticas

---

Desafio: **riscos para a infraestrutura de chaves públicas** (ex. HTTPS, VPNs, e-mails criptografados, assinaturas digitais)
Soluções: redesenho da ICP para suportar algoritmos pós-quânticos e novos métodos de distribuição e gerenciamento de chaves; Distribuição Quântica de Chaves (QKD)

Desafio: **ataques intermediários e persistência de dados** (risco a dados classificados; *store now, decrypt later* – SNDL)
Soluções: criptografia pós-quântica imediata, prioridade para dados classificados, pessoais e sensíveis; segurança de dados transmitidos por meio do uso imediato de criptografia híbrida ou algoritmos pós-quânticos

---

Desafio: **impacto em sistemas que usam tecnologia *blockchain***
Soluções: *blockchain* pós-quântico (integração de criptografia pós-quântica nos algoritmos de verificação); atualização das chaves existentes c/migração planejada e executada antes do futuro quântico.

Desafio: **desafios operacionais e de implementação**
Soluções: planejamento da transição; testes e validação do nível de segurança e funcionamento eficiente

---

4. Computação quântica e criptografia pós-quântica: impactos esperados e necessidades de regulação

4.3 Normas e Iniciativas de Regulação

IN GSI 3/2013: **parâmetros e padrões mínimos dos recursos criptográficos** baseados em algoritmos de Estado para criptografia (em processo de revisão)

Comissão Europeia – Recomendação C(2024) 2393: roteiro de transição p/ a criptografia pós-quântica

ISO/IEC 4879:2024 (en): define termos comumente usados no campo da computação quântica

ISO/IEC DIS 23837-1 (en): **requisitos de segurança, métodos de teste e avaliação para Distribuição Quântica de Chaves (QKD)** tendo como referência a ISO/IEC 15408 (critérios de avaliação para SI)

ISO/IEC 18033 (en): trata de algoritmos de criptografia no âmbito da SI 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: GT estabelecido pelo Comitê Técnico Conjunto ISO/IEC JTC 1 para servir como ponto focal na padronização em computação quântica; e desenvolver e manter uma lista de normas

NIST Post-Quantum Encryption Standards (**EUA, 2024**): 3 primeiros **padrões p/criptografia pós-quântica**

ITU-T FG-QIT4N Focus Group on Quantum Information Technology for Networks (QIT): grupo focal que forneceu de 2019 a 2021 uma plataforma colaborativa para pré-padronização da *QIT*.

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.

4. Computação quântica e criptografia pós-quântica: impactos esperados e necessidades de regulação

4.4 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.

5. Internet das Coisas (IoT): riscos e desafios específicos de segurança

5.1 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)]

5. Internet das Coisas (IoT): riscos e desafios específicos de segurança

5.2 Desafios da Internet das Coisas para a Segurança da Informação e a Cibersegurança (parte 1 de 2)

Desafio: **diversidade de dispositivos e heterogeneidade** X dificuldade de aplicação de medidas de segurança
Soluções: padrões de segurança universais; protocolos de comunicação interoperáveis; estimular fabricantes a seguirem melhores práticas (ex. atualizações automáticas de *firmware;* certificações de segurança p/ dispositivos IoT)

Desafio: **baixa capacidade computacional dos dispositivos IoT**
Soluções: uso de criptografia leve e protocolos de autenticação simplificados; soluções *Edge Computing*

Desafio: **atualizações de segurança inadequadas**
Soluções: políticas de ciclo de vida para dispositivos IoT, exigir atualizações de *firmware* contínuas; negociar extensão do suporte; regulamentações governamentais que obriguem suporte de longo prazo caso a caso

---

Desafio: **autenticação fraca**
Soluções: autenticação multifator (MFA) e protocolos de autenticação robustos (ex. OAuth 2.0) ou certificados digitais; incentivar o uso de senhas fortes e a imediata mudança das senhas padrão

---

Desafio: **ataques distribuídos** (DDoS) usando dispositivos IoT como *bots* em redes (*botnets*)
Soluções: *firewalls* para IoT; redes segmentadas para isolar ativos críticos; e sistemas de detecção de anomalias

---

Desafio: **privacidade de dados**
Soluções: criptografia de ponta a ponta; conformidade com regulamentações de privacidade; garantir que os usuários possam gerenciar o consentimento sobre o que está sendo coletado nos dispositivos IoT

Desafio: **falta de visibilidade e monitoramento** dos dispositivos IoT conectados à rede da organização
Soluções: ferramentas de gestão de dispositivos c/ descoberta automática e o monitoramento contínuo dos dispositivos conectados; soluções de *Security Information and Event Management* (SIEM) p/ centralizar os *logs* de eventos

---

5. Internet das Coisas (IoT): riscos e desafios específicos de segurança

5.2 Desafios da Internet das Coisas para a Segurança da Informação e a Cibersegurança (parte 2 de 2)

Desafio: **comunicação insegura** (protocolos inseguros, transmissão sem criptografia ou autenticação inadequada)
Soluções: protocolos de comunicação seguros (ex. TLS/SSL) para a transmissão de dados; VPN para proteger a comunicação entre dispositivos e servidores centrais

---

Desafio: **ataques físicos**, em especial nas áreas públicas
Soluções: técnicas de proteção física (ex. invólucros à prova de violação); medidas de segurança de *hardware* (ex. chips *Trusted Platform Module* – TPM) p/ proteger credenciais (ver: ISO/IEC 11889-1, Trusted Computing Group)

Desafio: **complexidade no gerenciamento de atualizações e configurações** ante a grande quantidade de dispositivos
Soluções: soluções automatizadas de gestão de *patches* e configuração

---

Desafio: **ataques à cadeia de suprimento**
Soluções: **Geral – auditorias de segurança e políticas de *due diligence* rigorosas**: para selecionar fornecedores, garantir que sigam padrões de segurança e adotem programas de avaliação de riscos e monitoramento contínuo
***Hardware* – certificações rigorosas e verificações de integridade**: para fornecedores de *hardware*, adoção de verificações de integridade dos componentes ao longo da cadeia e parcerias com fornecedores confiáveis
***Hardware* –selos de segurança e trilhas de auditoria**: durante o transporte e monitoramento da cadeia logística; adoção de *blockchain* p/ rastrear cada etapa do transporte e assegurar a integridade dos dispositivos
Software – políticas de segurança para 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 da distribuição de atualizações
Usuários e instalações – programas de conscientização de segurança para funcionários, **políticas de acesso privilegiado**, e **monitoramento contínuo** para detectar comportamentos suspeitos; controle de acesso restrito nas áreas sensíveis da cadeia

5. Internet das Coisas (IoT): riscos e desafios específicos de segurança

5.3 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): **diretrizes sobre riscos, princípios e controles para segurança e privacidade de soluções de IoT**

ISO/IEC 30141:2024 (en): 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)**

ISO/IEC 30179:2023 (en): 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**: subcomitê da ISO e da IEC que serve como **ponto focal na padronização de IoT** e Digital Twin e suas tecnologias correlatas.

ENISA Guidelines for Securing the Internet of Things: diretrizes para **proteger a cadeia de suprimentos de IoT** em todo o ciclo de vida, desde requisitos e projeto até entrega para uso final, manutenção e descarte. Público alvo amplo

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

IoT Cybersecurity Improvement Act of 2020 (**EUA, 2020**): 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

GSI/PR: desde 2019 acompanhado discussões do tema nos organismos e grupos de trabalho e a evolução da legislação, nacionais e internacionais, com vistas à eventual elaboração de norma com diretrizes de segurança da informação

5. Internet das Coisas (IoT): riscos e desafios específicos de segurança

5.4 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.

6. *Blockchain* e tecnologias correlatas

6.1 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 22739:2020(en)]

6. *Blockchain* e tecnologias correlatas

6.2 Desafios da tecnologia *blockchain* para a Segurança da Informação e a Cibersegurança (parte 1 de 2)

Desafio: **ataques de 51%** (Controle da Rede)
Soluções: 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

---

Desafio: **vulnerabilidades em *Smart Contracts***
Soluções: **auditorias de segurança rigorosas** no código dos *smart contracts* antes da implantação; uso de **ferramentas de verificação formal** e **testes de penetração** para identificar e corrigir vulnerabilidades antes do uso em produção; implementar contratos com **funcionalidades de atualização**, desde que balanceadas com segurança

---

Desafio: **chaves privadas comprometidas**
Soluções: **melhores práticas de gestão de chaves** (ex. uso de *hardware wallets* para armazenar chaves privadas sem conexão à internet); **multifator de autenticação** (MFA); e **esquemas de chaves múltiplas** (*multi-sig*)

Desafio: **ataques de *phishing* e engenharia social**
Soluções: campanhas de **conscientização e educação sobre cibersegurança** para usuários; ferramentas de **autenticação forte**; interfaces de usuário que **evitem exposição direta de chaves privadas**; e **segregação de funções**

Desafio: **escalabilidade e desempenho**
Soluções: soluções de **escalabilidade**, como *sharding* (fragmentação da *blockchain*), *sidechains* (cadeias laterais que processam transações secundárias) e protocolos de Layer-2 (ex. Lightning Network, Rootstock, Stacks)

Desafio: **segurança de redes descentralizadas**, suscetíveis a erros de config., vulnerabilidades ou ataques coordenados
Soluções: **normas e padrões de segurança** para todos; **consensos híbridos**, combinando elementos de descentralização com governança centralizada (ex. comitês de validadores c/ responsabilidade de supervisão da segurança

---

6. *Blockchain* e tecnologias correlatas

6.2 Desafios da tecnologia *blockchain* para a Segurança da Informação e a Cibersegurança (parte 2 de 2)

Desafio: **ataques Sybil**, um atacante cria múltiplos nós falsos, **e Eclipse**, o atacante isola um nó específico
Soluções: 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** (ex. exigir certo nível de reputação ou participação financeira)

Desafio: **privacidade de dados,** característica essencial das criptomoedas x crescente pressão regulatória mundial
Soluções: ***blockchains* com foco em privacidade** (ex. Monero, Zcash e Horizen), que usam 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

---

Desafio: **dependência de pseudônimos**
Soluções: **melhorias na anonimização de transações** (ex. endereços temporários, combinação de transações para obscurecer padrões); **melhores práticas de anonimato** para proteger a identidade dos usuários fora da *blockchain* (ex.: não reutilizar endereços e minimizar a vinculação com serviços centralizados)

Desafio: **governança descentralizada e *hard forks***
Soluções: mecanismos de governança bem definidos (ex. votação *on-chain* ou DAOs - Organizações Autônomas Descentralizadas) p/decisões sobre mudanças importantes; proteção contra ataques de repetição, implementando assinaturas exclusivas para cada cadeia após um *hard fork*

Desafio: **risco de interoperabilidade**
Soluções: **protocolos de interoperabilidade padrão** (ex. Cosmos ou Polkadot); **tecnologias** *cross-chain* (ex. *atomic swaps*) que garantem a troca de ativos entre cadeias sem confiar em intermediários centralizados

---

Desafio: **composição maliciosa de aplicativos descentralizados (DApps)**
Soluções: **ferramentas de *sandboxing*** para Dapps; **limitação de permissões** de interação entre diferentes contratos; **auditorias regulares** e verificação formal de contratos antes da interação entre diferentes DApps

6. *Blockchain* e tecnologias correlatas

6.3 Normas e Iniciativas de Regulação (parte 1 de 2)

- Lei nº 14.478/2022: **diretrizes** a serem observadas na **prestação de serviços de ativos virtuais** e na regulamentação das prestadoras de serviços de ativos virtuais; **prevê crimes c/ o uso de ativos virtuais**
- Decreto nº 11.563/2023: regulamenta a Lei nº 14.478/2022, estabelece **competências ao Bacen**
- 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
- 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.
- 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
- ISO/TR 23244:2020(en): relatório técnico c/ visão geral da privacidade e da proteção de informações de identificação pessoal aplicadas a sistemas *blockchain* e tecnologias de livro-razão distribuído (DLT)

6. *Blockchain* e tecnologias correlatas

6.3 Normas e Iniciativas de Regulação (parte 1 de 2)

- 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
- ISO/TS 23635:2022(en): especificação técnica com princípios orientadores e **estrutura p/ a governança de sistemas *blockchain* e DLT**, e 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
- 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
- IEEE 2140.1-2020: requisitos gerais para negociação de criptomoedas; aborda a autodisciplina e a ética profissional das plataformas de troca de criptomoedas, e a relevância entre elas e p/ as carteiras
- IEEE 2140.2-2021: **gerenciamento de segurança para ativos criptográficos** de clientes em corretoras de criptomoedas
- IEEE 2140.5-2020: estrutura de serviço de custódia para criptomoedas e ativos simbólicos.
- ANSI ASC X9 TR 54-2021 - Blockchain Risk Assessment Framework: fornece estrutura para executar **avaliações de risco operacional** em sistemas e aplicações *blockchain* dentro de uma rede distribuída
- EU Crypto-Assets Regulagion (MiCA) (**UE, 2023**): regras de mercado para criptoativos na UE

6. *Blockchain* e tecnologias correlatas

6.4 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.

Eng. Eletric. Eletron. Victor Hugo da Silva Rosa, Dr.
Coordenador-Geral / Diretor substituto

Coordenação-Geral de Gestão de Segurança da Informação – CGGSI
Departamento de Segurança da Informação – DSI
Secretaria de Segurança da Informação e Cibernética – SSIC
Gabinete de Segurança Institucional da Presidência da República – GSI/PR