REVISTA DCS
FUNDADA EN 2000

VULNERABILIDADE ALGORÍTMICA E GOVERNANÇA ELEITORAL: QUANDO A URNA ACEITA O ERRO

ALGORITHMIC VULNERABILITY AND ELECTORAL GOVERNANCE: WHEN THE VOTING MACHINE VALIDATES AN ERROR

VULNERABILIDAD ALGORÍTMICA Y GOBERNANZA ELECTORAL: CUANDO LA URNA ADMITE EL ERROR

Ary Jorge Aguiar Nogueira[1]

DOI: 10.54899/dcs.v23i87.4234
Recibido: 14/01/2026| Aceptado: 19/01/2026| Publicación en línea: 04/02/2026.

RESUMO

O artigo analisa a vulnerabilidade algorítmica no processo de justificativa eleitoral no Brasil, com foco na validação do número de inscrição pela urna eletrônica. Adota-se uma abordagem mista, de natureza exploratória e hipotético-dedutiva, combinando análise matemática e revisão bibliográfica. Sob a perspectiva da governança eleitoral e da integridade administrativa, examina-se a robustez do algoritmo Módulo 11, base da formação do Título de Eleitor, através de simulações fundamentadas na Aritmética Modular e no Princípio da Casa dos Pombos. Os resultados indicam que, embora o sistema seja seguro na prevenção de erros simples, a troca simultânea de dois dígitos pode desencadear "colisões de hash" matematicamente válidas em aproximadamente 8% dos casos. Diante da ocorrência da "justificativa cega" por ausência de confirmação visual do nome da pessoa requerente pós-digitação, conclui-se que tais colisões representam um risco residual relevante à confiança social na integridade eleitoral, exigindo a implementação de camadas secundárias de verificação na governança.

Palavras-chave: Governança Eleitoral. Integridade Eleitoral. Aritmética Modular. Urna Eletrônica. Colisão de Hash.

ABSTRACT

This article analyzes algorithmic vulnerability in Brazil's electoral justification process, focusing on the validation of voter registration numbers by the electronic voting machine. A mixed-methods approach is adopted, exploratory and hypothetico-deductive in nature, combining mathematical analysis and literature review. From the perspective of electoral governance and administrative integrity, the robustness of the "Module 11" algorithm, the basis for generating the Voter ID number, is examined through simulations grounded in Modular Arithmetic and the Pigeonhole Principle. The results indicate that, although the system is secure against simple errors, the simultaneous swapping of two digits can trigger mathematically valid "hash collisions" in approximately 8% of cases. Given the occurrence of "blind justification," due to the absence of visual confirmation of the voter's name after number entry, such collisions are found to pose

[1] Doutor em Teoria e Filosofia do Direito, Universidade de São Paulo (USP), São Paulo, São Paulo, Brasil.
E-mail: aryjorge@alumni.usp.br Orcid: https://orcid.org/0000-0003-4914-3929

a relevant residual risk to public trust in electoral integrity, requiring the implementation of secondary verification layers within governance procedures.

Keywords: Electoral Governance. Electoral Integrity. Modular Arithmetic. Voting Machine. Hash Collision.

RESUMEN

Este artículo analiza la vulnerabilidad algorítmica en el proceso de justificación electoral en Brasil, centrándose en la validación del número de inscripción electoral por parte de la urna electrónica. Se adopta un enfoque de métodos mixtos, de carácter exploratorio e hipotético-deductivo, que combina el análisis matemático con la revisión bibliográfica. Desde la perspectiva de la gobernanza electoral y la integridad administrativa, se examina la robustez del algoritmo "Módulo 11", base para la generación del título de elector, mediante simulaciones fundamentadas en la Aritmética Modular y el Principio del Palomar. Los resultados indican que, si bien el sistema es seguro frente a errores simples, el intercambio simultáneo de dos dígitos puede dar lugar a "colisiones de hash" matemáticamente válidas en aproximadamente el 8% de los casos. Dada la ocurrencia de la "justificación ciega", debido a la ausencia de confirmación visual del nombre del elector tras la introducción del número, se concluye que tales colisiones representan un riesgo residual relevante para la confianza pública en la integridad electoral, lo que exige la implementación de capas de verificación secundaria en los procedimientos de gobernanza.

Palabras clave: Gobernanza Electoral. Integridad Electoral. Aritmética Modular. Urna Electrónica. Colisión de Hash.

INTRODUÇÃO

Todos os anos milhões de pessoas vão às urnas no Brasil, uma das maiores democracias do mundo em número de eleitores registrados. Uma operação de tão grande porte traz imensos desafios logísticos e de manutenção da estabilidade institucional, num cenário global cada vez mais instável.

O Brasil é uma referência mundial em informatização do processo eleitoral e as urnas eletrônicas são apenas a ponta do imenso iceberg de procedimentos eleitorais que se beneficiam da tecnologia.

A pergunta de pesquisa deste artigo diz respeito ao processo de justificativa por ausência às urnas: qual é a chance de alguém que trabalha nas mesas receptoras de votos/justificativas, ao

digitar o número de inscrição eleitoral de uma pessoa que está justificando a ausência às urnas, acabar registrando o título de outrem? Uma questão adicional se coloca: qual seria o número mínimo de dígitos equivocados para ocorrer este fenômeno?

Como é sabido, o voto no Brasil é obrigatório e há uma série de sanções que o absenteísmo traz: o pagamento de uma multa no valor de R$3,51 por cada turno ausente; suspensão de salários no serviço público; proibição de matrícula em estabelecimento de ensino oficial; impedimento de obter ou renovar passaporte; vedação à obtenção de empréstimos em bancos públicos; impossibilidade de participação em licitações e até mesmo a suspensão do CPF, nos casos em que a ausência é persistente.

A justificativa por ausência às urnas é um procedimento que evita que o eleitorado ausente sofra as mencionadas sanções e pode ser realizada de várias formas. Até 60 dias após cada turno, pode ser apresentado um pedido por meio do Sistema Justifica, na plataforma *on line* dos Tribunais Regionais Eleitorais e do TSE, ou de forma presencial, nos cartórios eleitorais.

O principal inconveniente da justificativa pós-eleições é a necessidade de apresentação de alguma documentação para o deferimento, o que torna o processamento mais demorado e condicionado ao crivo judicial.

Caso seja escolhida a opção de realizar a justificativa no dia da eleição, esta poderá ocorrer por meio do aplicativo e-Título, que utiliza a ferramenta de geolocalização do celular para conferir a ausência ao domicílio eleitoral. Há também a possibilidade de realização em qualquer local de votação, entregando o requerimento preenchido nas Mesas Receptoras de Justificativa ou de Votação, apresentando documento com foto.

Neste último caso, os números que compõem a inscrição eleitoral são digitados no microterminal da urna, a qual registrará o dado para posterior remessa digital, junto com os resultados. Assim, se for digitado um número de inscrição que passe pelo crivo do algoritmo de validação do título, a urna aceitará inicialmente a justificativa, que poderá, ou não ser validada na etapa posterior de processamento[2].

Estudos empíricos com base matemática e estatística, ainda constituem exceções no campo do direito (Nogueira, 2023). A pesquisa pretende suprir parte desta lacuna.

[2] Um caso bastante comum de não aceitação da justificativa durante o processamento ocorre quando a pessoa vota no mesmo município no qual está apresentando a justificativa. Como a urna opera de forma *off line*, não há como identificar no momento da digitação dos dados que aquela inscrição eleitoral pertence àquele município. Aqui é uma clara falha humana, pois quem recebe a justificativa teria acesso a essa informação, seja perguntando à pessoa requerente, seja observando os dados de seu título.

O artigo adota uma abordagem mista, de natureza exploratória e hipotético-dedutiva, combinando a simulação algorítmica de verificação de dados com a revisão bibliográfica focada na teoria da governança eleitoral.

O percurso metodológico foi estruturado em três etapas distintas: a decomposição do algoritmo de verificação da inscrição eleitoral, a simulação de cenários de erro (colisões) e a análise contextual da integridade do processo.

Importante salientar que as simulações de inscrições eleitorais utilizaram o estado do Amapá como base, a fim de se prevenir o risco de geração de um número já atribuído a alguém. Como aquele estado conta com um dos menores eleitorados do país, superando apenas Roraima, foi possível gerar inscrições que não pertencem a nenhuma pessoa. Optou-se por aquele em detrimento deste meramente por uma questão de ordem alfabética.

Embora tenha identificado uma vulnerabilidade algorítmica relevante no sistema de justificativa eleitoral, este estudo apresenta limitações inerentes à sua abordagem metodológica. Em primeiro lugar, a análise restringiu-se ao cenário de erro simultâneo de dois dígitos, não explorando padrões mais complexos ou frequentes de erro humano, como trocas de três ou mais dígitos ou erros sistemáticos associados à disposição do teclado.

Outra limitação reside na natureza teórico-estatística do estudo, que não analisou dados empíricos de justificativas com erro real, nem avaliou em profundidade os eventuais mecanismos de pós-processamento existentes no Tribunal Superior Eleitoral que poderiam mitigar colisões após a eleição.

Por fim, a pesquisa não mensurou o impacto operacional concreto das colisões na logística eleitoral, aspecto que demandaria cooperação institucional para acesso a dados administrativos. Tais limitações, contudo, não invalidam a robustez das evidências matemáticas apresentadas e sinalizam caminhos para investigações futuras mais abrangentes e aplicadas.

A pesquisa encontra-se dividida em três seções, além desta introdução e das considerações finais. Na primeira seção, é discutida a relação entre governança e integridade eleitorais, bem como é realizada a análise descritiva da estrutura de formação do número da Inscrição Eleitoral, conforme estabelecido pela Lei n.º 6.996/1982 e regulamentado pela Resolução TSE n.º 23.659/2021.

A seção seguinte testa a robustez do algoritmo frente a erros de digitação, utilizando o conceito matemático de "colisão de hash[3]" e o Princípio da Casa dos Pombos, investigando-se a

[3] Este trabalho utiliza o termo “colisão de hash” em seu sentido lato, referindo-se à ocorrência de entradas distintas

probabilidade de validação de inscrições espúrias decorrentes da alteração simultânea de dois dígitos.

Por fim, a terceira seção busca contextualizar a relevância estatística e política dessa vulnerabilidade matemática.

GOVERNANÇA ELEITORAL E O NÚMERO DO TÍTULO DE ELEITOR NO BRASIL

As eleições estão na base das democracias contemporâneas. Embora sejam fenômenos originalmente independentes, o exercício do voto e a consolidação da democracia dificilmente conseguem ser dissociados no século XXI. Há quem aponte, inclusive, que eleições bem administradas seriam um pré-requisito para a democracia (Pastor, 1999; Birch, 2011; Norris; 2014).

A noção de que eleições envolveriam mais que o simples ato de votar é algo bastante consolidado na Literatura (Cox, 1997; Lijphart, 1994; Taagepera; Shugart, 1989). Entretanto, o conceito de governança eleitoral, como o conjunto de atividades que cria e mantém o quadro institucional em que se realizam as votações e a competição eleitoral, consolidou-se apenas nos anos 2000 (Mozaffar & Schedler, 2002). Resguardam-se, portanto, a certeza quanto aos procedimentos e a incerteza quanto aos resultados eleitorais.

A governança eleitoral operaria então, em três níveis distintos: *rule making*, *rule application* e *rule adjudication*. O primeiro nível envolveria o desenho das regras básicas do jogo eleitoral. Já o segundo, a implementação dessas regras para organizar o jogo. Por fim, adjudicação diz respeito à resolução das disputas que surgem no corpo da competição eleitoral (Mozaffar & Schedler, 2002).

Normalmente, os três níveis não costumam estar sob a tutela de um mesmo órgão. O *rule making*, geralmente, vincula-se às Constituições e aos Códigos Eleitorais, estando, portanto, na esfera legislativa. Os demais níveis podem ou não se encontrar sob a administração de um único órgão. Em alguns países, a administração do processo eleitoral e a adjudicação de conflitos podem ser conduzidos por órgãos diferentes, enquanto em outros, a mesma instituição desempenha as duas funções (Tarouco, 2014).

O Organismo Eleitoral do Brasil opera nos três níveis, participando do *rule making* em

que produzem o mesmo resultado numa função de mapeamento de tamanho fixo. Tecnicamente, o algoritmo Módulo 11 atua como uma função de *hash* não-criptográfica (checksum).

conjunto com o Legislador, por meio da edição de Resoluções; implementando as regras (*rule application*) e decidindo o contencioso (*rule adjudication).*

A literatura aponta que a administração das eleições por órgãos percebidos pelas pessoas como independentes, imparciais e competentes pode não apenas ajudar na resolução de problemas administrativos, como conferir legitimidade aos pleitos (Pastor, 1999).

Nesse sentido, a integridade eleitoral surge como uma necessidade da boa governança. Integridade aqui, não é apenas uma questão de ter leis justas (*rule making*), mas depende de forma crucial da qualidade da implementação (*rule application*), através de redes de governança complexas (James, 2019).

O uso de recursos tecnológicos, como o processamento eletrônico de dados e a identificação biométrica, destaca-se na governança eleitoral brasileira, permitindo agilizar a totalização dos resultados e mitigar fraudes tradicionais, como a falsidade ideológica no momento da votação.

Contudo, a importância da tecnologia para a integridade eleitoral não reside apenas na sua eficiência operacional, mas na sua capacidade de oferecer "certeza institucional" através de procedimentos padronizados e auditáveis.

A introdução da tecnologia, especialmente após a Pandemia da COVID 19, possibilitou novos vetores de ataques, o que exige o desenvolvimento de outras competências pelos Organismos Eleitorais. A governança eleitoral agora inclui obrigatoriamente a gestão de riscos algorítmicos (Garnett, H. A., & James, T. S., 2020).

A integridade eleitoral não deve ser medida unicamente pela ausência de fraudes nos resultados, mas pela segurança e qualidade administrativas de todo o ciclo eleitoral (Norris, 2014). Se a governança falha em garantir a precisão procedimental pode acabar transformando um erro técnico residual em um passivo de integridade, comprometendo a cadeia de custódia da participação eleitoral.

Nesse sentido, a legitimidade democrática depende da capacidade do sistema de responder ao “ceticismo informado” (a desconfiança baseada em falhas reais) com transparência e verificação, a fim de evitar o “cinismo corrosivo” (descrença infundada), que pode fragilizar o contrato de confiança entre quem vota e a autoridade eleitoral (Norris, 2022).

O desafio dos Organismos Eleitorais passa, então, pela gestão de risco adaptativa (Garnett, H. A., & James, T. S., 2020), que é a capacidade de a administração eleitoral identificar e neutralizar vulnerabilidades emergentes em tempo real, superando a rigidez dos protocolos fixos.

Ao contrário da conformidade legal pura, que foca apenas o passado (regras escritas), a gestão adaptativa olha para o futuro (ameaças prováveis), exigindo que mecanismos de segurança adicionais sejam acionados paralelamente, sempre que a proteção primária se mostrar insuficiente diante de novos cenários operacionais.

A utilização do processamento eletrônico de dados nos serviços eleitorais foi autorizada pela Lei n.º 6.996, de 07 de junho de 1982, regulamentada atualmente pela Resolução TSE n.º 23.659, de 26 de outubro de 2021. Conforme previsto no artigo 36 da mencionada Resolução, a atribuição do número de inscrição eleitoral é realizada automaticamente pelo sistema, resultando em uma cadeia numérica composta por doze algarismos.

A estrutura desse identificador é formada de três componentes funcionais: os oito dígitos iniciais correspondem ao número sequencial da inscrição, seguidos por dois algarismos que representam o código da Unidade da Federação (UF) de origem, que vão de 01 (São Paulo) a 28 (Exterior) e dois dígitos verificadores.

A validação da integridade da sequência numérica inicial (número sequencial e Unidade da Federação) é assegurada pelos dígitos verificadores, os quais são determinados mediante a aplicação de um algoritmo no "Módulo 11".

A verificação opera em uma lógica de dependência em cascata, com o primeiro dígito incidindo sobre o segmento sequencial, enquanto o segundo utiliza como base de cálculo o código da Unidade da Federação, acrescido do primeiro dígito verificador previamente obtido.

O exemplo a seguir simula a atribuição de um número de inscrição eleitoral do Amapá, cujo número sequencial é "12345678". O Título de Eleitor possui 12 dígitos, organizados da seguinte forma: $d_1d_2d_3d_4d_5d_6d_7d_8\ u_1u_2\ v_1v_2$

- d_1 ... d_8: Número sequencial (identificação do eleitor).
- u_1u_2: Código da Unidade da Federação (UF). Ex: SP=01, AP=25.
- v_1v_2: Os Dígitos Verificadores.

Passo 1: Cálculo do Primeiro Dígito Verificador (DV_1)

O cálculo é feito sobre os 8 dígitos do sequencial. Multiplica-se cada dígito pelos pesos de 2 a 9 (da esquerda para a direita). Matematicamente, segue-se a seguinte fórmula:

$$S_1 = \sum_{i=1}^{8} (di \,.\, xi) \qquad (1)$$

onde

xi é o peso correspondente à posição (2, 3, 4... 9).

1. Multiplicação pelos pesos:

- 1 . 2 = 2
- 2 . 3 = 6
- 3 . 4 = 12
- 4 . 5 = 20
- 5 . 6 = 30
- 6 . 7 = 42
- 7 . 8 = 56
- 8 . 9 = 72

2. Soma dos resultados: 2 + 6 + 12 + 20 + 30 + 42 + 56 + 72 = 240
3. Cálculo do Resto (Módulo 11): Divide-se a soma por 11 e pega-se o resto.

240/ 11 = 21 com resto 9.

(Cálculo: 21 . 11 = 231; 240 - 231 = 9)

Resultado do DV1: Como o resto é 9, o primeiro dígito verificador é 9.

Importante: Na aritmética modular completa (ou pura), o resto pode ser 10. Como não podemos escrever "10" em um único dígito, a regra do TSE determina:

- Se $v_1 = 10$, então considera-se 0.

Passo 2: Cálculo do Segundo Dígito Verificador (DV_2)

O cálculo é feito sobre o código da UF do Amapá (25) seguido pelo DV_1 do Passo 1 (9). Os pesos fixos são 7, 8 e 9.

$S_2 = (u_1 . 7) + (u_2 . 8) + (v_1 . 9)$ (2)

1. Multiplicação pelos pesos:

- 2 (1º dígito UF) . 7 = 14
- 5 (2º dígito UF) . 8 = 40

- 9 (DV_1 calculado) . 9 = 81

2. Soma dos resultados: 14 + 40 + 81 = 135
3. Cálculo do Resto (Módulo 11): Dividimos a soma por 11 e pegamos o resto.

A Congruência: $v_2 \equiv S_2 \pmod{11}$

135 / 11 = 12 com resto 3. (Cálculo: 12 . 11 = 132; 135 - 132 = 3)

Resultado do DV_2: Como o resto é 3, o segundo dígito verificador é 3.

Resultado: Combinando todas as partes (Sequencial + UF + DVs), o Título de Eleitor simulado é 12345678 25 93, sendo:

- 12345678: Número Sequencial
- 25: Amapá
- 93: Dígitos Verificadores

A formação dos dígitos verificadores do Título de Eleitor é um exemplo prático da aplicação da Aritmética Modular.

ARITMÉTICA MODULAR

Na aritmética modular, também chamada de "aritmética do relógio", os números "dão a volta" e reiniciam a contagem ao atingir um determinado valor limite, denominado módulo. A analogia mais comum é o relógio de 12 horas: se são 10 horas e adicionamos 5 horas, podemos dizer que são 15 horas e também, que são 3 horas da tarde. Isso ocorre porque, ao ultrapassar o módulo 12, o ciclo recomeça.

Matematicamente, o foco da aritmética modular não é o resultado da divisão, mas sim o resto. A operação $A \pmod{N}$ pergunta: "qual é a sobra quando dividimos A por N?". Por exemplo, 14 (mod 12) = 2, porque 14 dividido por 12 resulta em 1 com resto 2.

Quando dois números diferentes deixam o mesmo resto ao serem divididos pelo módulo, dizemos que eles são congruentes. Assim, no relógio, 2 e 14 são congruentes no módulo 12 [$2 \equiv 14 \pmod{12}$] [4].

A aritmética modular confere previsibilidade a ciclos matemáticos, podendo ser melhor compreendida em problemas que envolvam calendários. Por exemplo, se hoje é uma segunda-feira, qual será o dia da semana daqui a 357 dias?

Com a utilização da aritmética modular, observa-se que será igualmente uma segunda-

[4] Lê-se: dois é congruente a quatorze no módulo doze.

feira, pois 357 ≡ 0 (mod 7), ou seja, 357 é congruente a zero no módulo 7. Os dias da semana constituem um conjunto formado por apenas 7 elementos. Dividindo-se 357 por 7, obtém-se resto zero. Isso significa que o ciclo temporal “deu a volta” e colidiu com seu início após 51 semanas.

A estrutura da aritmética modular encontra-se na base da segurança digital e dos sistemas de verificação. Como o conjunto de resultados possíveis é finito (de 0 até N - 1), pode-se manipular números infinitamente grandes dentro de um espaço controlado.

No caso do Título de Eleitor, o uso do módulo 11 transforma a soma complexa dos dígitos do documento em um único número de verificação (entre 0 e 10), criando uma "impressão digital" matemática que valida a integridade da sequência numérica.

A aritmética modular é a "espinha dorsal" dos algoritmos de verificação (como CPF, CNPJ, Título de Eleitor e cartões de crédito) por três razões fundamentais: redução cíclica, sensibilidade a erros e propriedades algébricas dos números primos.

REDUÇÃO E PADRONIZAÇÃO (EFEITO “FUNIL”)

A função mais óbvia da aritmética modular é transformar um número de qualquer tamanho (uma soma que pode chegar a 300, 500, etc.) em um conjunto finito e previsível de resultados, como uma espécie de funil.

- O Problema: Se somássemos os dígitos de um documento usando aritmética comum, o resultado poderia ter 1, 2 ou 3 dígitos. Isso ocuparia espaço variável no banco de dados.
- A Solução Modular: Ao aplicar módulo n, garantimos que o resultado (o resto) esteja sempre entre 0 e n-1.

No caso do Título de Eleitor (Módulo 11), o resultado é forçado a ser um número entre 0 e 10. Isso permite condensar toda a informação do documento em apenas um dígito (com a regra de tratar o 10 como 0).

DETECÇÃO DE ERROS HUMANOS (TRANSPOSIÇÃO E SUBSTITUIÇÃO)

Os erros mais comuns que humanos cometem ao digitar números são:

1. Substituição: Trocar um número por outro (ex: digitar 4 em vez de 5).
2. Transposição: Inverter números vizinhos (ex: digitar 12 em vez de 21).

A aritmética comum (apenas somar os números) falha miseravelmente na transposição.

- *Soma simples:* 1 + 2 = 3 e 2 + 1 = 3. O erro passa despercebido.

A Aritmética Modular Ponderada (usando pesos e módulo) resolve isso. Cada posição tem um "peso" diferente na multiplicação (no Título, os pesos variam de 2 a 9), e o resultado analisado sob um módulo identifica a ocorrência de um erro:

- (1 . 2) + (2 . 3) = 8
- (2 . 2) + (1 . 3) = 7
- $8 \not\equiv 7 \pmod{11}$[5]

O sistema percebe a inversão imediatamente, diante da ausência de congruência.

POR QUE MÓDULO 11?

Esta é a razão matemática mais profunda, pois a escolha do módulo 11 no Título de Eleitor não é arbitrária. A vulnerabilidade dos sistemas de verificação reside, fundamentalmente, na estrutura algébrica utilizada. Para que um algoritmo de dígito verificador opere como um sistema matematicamente robusto, tecnicamente, um Corpo Finito[6] (ou *Galois Field*), é essencial que o módulo da operação seja um número primo (Gallian, 2010).

Em sistemas decimais, nos quais os *inputs* variam de 0 a 9, o uso do Módulo 10 (um número composto) impediria a formação de um corpo, introduzindo divisores de zero que causam "cegueira" algorítmica.

A segurança matemática "perfeita" para a base 10 exige a adoção do primo imediatamente superior, ou seja, o Módulo 11. A utilização do Módulo 10, que não é primo, criaria "buracos" na verificação. Certas multiplicações e trocas de dígitos resultariam em zero (congruência) indevidamente, deixando erros passarem. Matematicamente, o módulo 11 seria superior ao módulo 10 (Faria, Pinto & Pedroza, 2017).

Como o 11 é o primeiro número primo logo após o 10, garante-se que cada dígito (de 0 a 9) tenha um comportamento único e previsível quando multiplicado pelos pesos. Isso garante que a totalidade dos erros de digitação de um único dígito sejam detectados, bem como as transposições de dígitos adjacentes (trocar *ab* por *ba*).

Cabe aqui uma ressalva importante acerca da utilização Módulo 11: a literatura aponta a

[5] Lê-se: oito não é congruente a sete no módulo onze.
[6] Um corpo finito constitui uma estrutura algébrica com um número limitado de elementos na qual as operações de adição, subtração, multiplicação e divisão (por elementos não nulos) são bem definidas e livres de anomalias aritméticas, como os divisores de zero (Gallian, 2010).

diferença entre uma versão completa (pura), na qual o resto 10 gera um dígito verificador representado por um caractere especial, geralmente a letra “X”, como acontece no ISBN de livros antigos ou em matrículas internacionais e a versão restrita, que força o dígito verificador a ser “0”, quando o resto for 10.

A adoção do Módulo 11 restrito na formação da inscrição eleitoral introduz uma taxa de falha que não existiria em sua versão pura. Este percentual de erro constitui o que neste artigo é chamado de colisão, tema da seção a seguir .

ANATOMIA DE UM ERRO: A LÓGICA DA COLISÃO

Uma colisão de hash ocorre quando duas informações de entrada distintas (como dois arquivos diferentes, duas senhas ou dois números de Título de Eleitor) produzem exatamente o mesmo resultado de saída (o mesmo código ou dígito verificador) após passarem por uma função matemática.

Conforme observado nas seções anteriores, a escolha pelo Módulo 11 na formação dos dígitos verificadores garante que seja impossível o erro de digitação de um único dígito produzir uma inscrição eleitoral válida. Da mesma forma, o risco de transposição também é afastado e a inversão de dígitos adjacentes não produz um título válido.

No entanto, resta a dúvida quanto à troca de mais de um dígito. Ou seja, se inadvertidamente forem digitados erroneamente dois números diferentes ao registrar um pedido de justificativa, qual é a chance de acertar um outro título de eleitor válido?

Podemos estabelecer o limite determinístico de qualquer função de alocação por meio do Princípio da Casa dos Pombos, utilizando a analogia do modelo de “Bolas e Urnas” (Mitzenmacher & Upfal, 2017). Ao se distribuírem m bolas em n urnas, a existência de pelo menos uma urna contendo duas ou mais bolas é uma certeza matemática sempre que $m > n$.

Porém, mesmo antes de se atingir esse limite de saturação, a probabilidade de ocupação múltipla cresce de forma não linear, o que desafia a intuição sobre a capacidade de armazenamento e distinção de sistemas discretos (Mitzenmacher & Upfal, 2017).

A troca de dois dígitos na inscrição eleitoral permitiria a formação de 100 combinações numéricas diferentes. Pelo Princípio da Casa dos Pombos, se temos 100 pares de dígitos e 11 restos possíveis (no Módulo 11), a distribuição será:

$\frac{100}{11} = 9{,}09$

Isso significa que, em média, para qualquer resto que o cálculo exija, existirão 9 pares de dígitos válidos, sendo 1 desses pares o título original e as 8 demais “colisões” – combinações falsas que geram o mesmo Dígito Verificador.

Equacionando o problema da alteração de apenas dois dígitos do título, nas posições com pesos *A* e *B*:

- Sejam x e y os dígitos originais nessas posições.
- Sejam x' e y' os novos dígitos.
- O restante dos dígitos e seus pesos somados resultam em uma constante K.

Para que os Dígitos Verificadores (DVs) permaneçam idênticos, a soma ponderada dos novos dígitos deve ter o mesmo resto (Módulo 11) que a soma original.

$$A \cdot x' + B \cdot y' + K \equiv S_{original} \pmod{11} \qquad (3)$$

Isso se simplifica em uma congruência linear com duas variáveis:

$$A \cdot x' + B \cdot y' \equiv C \pmod{11} \qquad (4)$$

onde

C é o valor alvo necessário para manter o DV.

No caso simulado, há 9 pares de resultados (x', y') que satisfazem a equação.

- 1 desses pares é o título original.
- 8 são as "colisões".

Ao variar dois dígitos (x' e y'), cada um pode ir de 0 a 9. Tem-se, portanto, uma grade de 10 x 10 = 100 pares possíveis de dígitos (00, 01, ..., 99).

O algoritmo "espreme" essas 100 combinações através do Módulo 11. O resultado dessa conta só pode ser um número inteiro entre 0 e 10 (11 possibilidades[7]).

O sistema do Título de Eleitor valida, então, o número com base no resto da divisão da

[7] Na verdade, 10 possibilidades porque o resto 10 é convertido em 0.

soma ponderada (S) por 11.

- Se é digitado o número certo, a soma S tem um certo resto.
- Se é digitado algo errado, a nova soma S' só será considerada "válida" se ela tiver o mesmo resto da soma original.

Para que S e S' tenham o mesmo resto, a diferença entre eles (ΔS) precisa ser um múltiplo de 11.

Exemplo numérico:

- Imagine-se que a soma original correta é $S = 25$. O resto de 25 dividido por 11 é 3.
- Comete-se um erro de digitação e a nova soma é $S' = 47$. O resto de 47 dividido por 11 também é 3.
- Como os restos são iguais, o sistema não detecta o erro.

Aplicando-se a fórmula:

$$\Delta S = S' - S = 47 - 25 = 22 \qquad (5)$$

O número 22 é um múltiplo de 11? Sim. Portanto, $22 \equiv 0 \pmod{11}$. A condição foi satisfeita, e o erro passou despercebido.

No exemplo hipotético anterior, o título original era 12345678 25 93. A troca de dois dígitos neste número de inscrição gera um total de 8 “colisões”, conforme pode ser observado a seguir:

Tabela 1

Simulação das colisões.

Inscrições	***S'***	***S***	**$\Delta S = S' - S$**
123456 **64** 25 93	196	240	44
123456 **50** 25 93	152	240	88
123456 **47** 25 93	207	240	33
123456 **33** 25 93	163	240	77
123456 **16** 25 93	174	240	66
123456 **02** 25 93	130	240	110
123456 **95** 25 93	229	240	11
123456 **81** 25 93	185	240	55

Fonte: Elaboração própria (2025).

Observe-se que os ΔS de todas as colisões são formados por números múltiplos de 11, tornando-se, portanto, indetectáveis pelo algoritmo utilizado para checar os títulos.

Nas eleições de 2024, o Brasil contava com um eleitorado apto de 155.912.680, dos quais 122.115.555 compareceram para votar. O total de justificativas apresentadas foi de 7.489.096. (TSE, s.d.). Num universo amostral tão grande, a probabilidade de 8% de colisões em caso de erro na digitação de dois números é bastante significativa e não pode ser descartada pelos responsáveis pela governança eleitoral brasileira.

É evidente que o risco está sendo calculado considerando-se a ocorrência de erros aleatórios. De fato, seres humanos tendem a cometer erros diferentes, seja realizando transposições (inversão de números) ou erros de proximidade física (digitar 4 ao invés de 5 num teclado). Nesse sentido, a utilização do Módulo 11 na verificação seria capaz de mitigar o risco.

Porém, apesar da robustez do algoritmo, a literatura especializada em matemática computacional (Faria, Pinto & Pedroza, 2017) aponta que a variante "restrita" (que converte o resto 10 em 0), utilizada pela Justiça Eleitoral, possui pontos cegos documentados, falhando na detecção de certos tipos de erros de dupla digitação e os cálculos anteriores confirmam esta afirmação.

Questões empíricas advogam, ainda, em favor das "colisões" não intencionais. Há um imenso contingente no eleitorado que porta títulos antigos, cujos números muitas vezes são quase irreconhecíveis. Além disso, milhares de requerimentos de justificativa são preenchidos manualmente, trazendo o complicador da caligrafia.

Com a implantação da identificação biométrica, tornou-se praticamente impossível que alguém vote no lugar de outra pessoa. Porém, a forma como é estruturada a justificativa eleitoral deixa brecha para que colisões sejam inadvertidamente registradas em nome de pessoas que votaram.

Cada urna opera como uma ilha e isso é fundamental para garantir a segurança da votação. Porém, o recebimento dos pedidos de justificativa por ausência às urnas durante o dia de votação abre a possibilidade de registro simultâneo com o voto, caso haja equívoco na digitação (as colisões).

Eleições íntegras não são apenas aquelas onde não há fraude na contagem dos votos (foco no resultado), mas aquelas que obedecem a padrões internacionais durante todo o ciclo eleitoral, ou seja, também nos processos e procedimentos (Norris, 2014).

Em essência, é preciso olhar tanto para o processo quanto para o resultado para avaliar o quadro completo da qualidade da eleição (Elklit & Reynolds, 2005), pois a confiabilidade processual e a certeza administrativa são vitais para a legitimidade democrática,

independentemente da incerteza quanto aos resultados (Mozaffar & Schedler, 2002).

A vulnerabilidade transcende a curiosidade aritmética e atinge o núcleo da "eficácia administrativa" (Elklit & Reynolds, 2005). Considerando que as urnas operam desconectadas de um banco de dados nacional durante o pleito (e assim precisa ser mesmo), a validação de um título de eleitor (inclusive de outra unidade federativa), baseia-se exclusivamente no algoritmo de verificação, sem a possibilidade de confirmação visual do nome da pessoa eleitora pelos membros da mesa após a digitação (justificativa cega).

Cabe aqui salientar que o *design* institucional atual só permite a justificativa cega, caso a opção seja realizar o pedido nos locais de votação. Como a urna opera de maneira *off line*, não há como realizar a checagem que permitiria ver o nome da pessoa requerente no microterminal. A urna apenas valida o algoritmo da inscrição eleitoral e guarda o dado para posterior batimento.

O fato é que um sistema que permite colisões matemáticas indetectáveis no *front-end* (na urna) falha na eficácia preventiva, transferindo o custo do erro para a fase de *rule adjudication* (resolver o problema depois).

Nesse cenário, uma colisão de hash decorrente de erro de digitação não é apenas um dado estatístico, mas um erro administrativo validado pelo sistema, que só será detectado na etapa de processamento posterior, podendo gerar incerteza institucional, especialmente quando registra justificativa por ausência às urnas para alguém que votou.

Já existem protocolos que, em tese, mitigariam o risco de registro justificativa em favor de alguém que votou, porém, são totalmente dependentes da ação humana (passíveis de erro). O treinamento do pessoal temporário convocado para as eleições inclui recomendações acerca do cuidado na digitação dos números de inscrição, além da conferência das informações com os documentos apresentados.

A qualidade da implementação das regras na ponta da linha (neste caso, a interface entre trabalhadores de mesas receptoras de votos/justificativas e a máquina) segue determinante para a integridade percebida do ciclo eleitoral (James, 2019).

As colisões são um fenômeno estatisticamente possível, mas a pouca prática jurídica com números pode fazer com que o fenômeno seja percebido como um tipo de fraude pelos responsáveis pela governança eleitoral. Estatisticamente, o registro de justificativa em favor de alguém que votou pode ser meramente decorrência de um erro não intencional.

Em teoria, as recomendações atuais dariam conta de evitar as colisões, pois envolvem a checagem dos documentos da pessoa requerente e o apoio de uma segunda pessoa (alguém lê o

número de inscrição e a digitação é feita por outro integrante da mesa). Porém, persiste o risco de falha humana.

Cabe lembrar que a implementação das eleições depende de um imenso contingente de pessoal temporário, que opera em condições de estresse (filas, calor, pressão). Nesse cenário, a probabilidade de erros de digitação aumenta, tornando a vulnerabilidade matemática um problema real na gestão dos recursos humanos eleitorais.

Junte-se a tudo isso o fato de que a sociedade brasileira apresenta de forma consistente e persistente baixos níveis de alfabetização matemática, com 73% dos estudantes brasileiros de 15 anos não atingindo sequer o nível 2 de proficiência (OCDE, 2023) e têm-se um campo fértil para a desinformação. Afinal, o ser humano desconfia daquilo que não conhece.

No entanto, uma certa dose de ceticismo informado (Norris, 2022) é algo crucial para o fortalecimento da integridade, pois a capacidade de verificação fomenta a confiança nas eleições. Num momento em que a manutenção da credibilidade da governança eleitoral brasileira enfrenta desafios de vulto (Crespo & Peixoto, 2024), nunca foi tão importante assegurar que não pairem dúvidas acerca do processo eletrônico de votação.

CONSIDERAÇÕES FINAIS

A pesquisa parte de uma dúvida quanto à possibilidade de ser registrado um pedido de justificativa por ausência às urnas em nome de uma pessoa diferente, que pode ter votado, inclusive. Em caso positivo, qual seria o número mínimo de dígitos equivocados para validar o erro?

O que um cientista faz quando tem uma dúvida? Realiza um experimento. E embora as ciências sociais aplicadas não tenham as mesmas características das ciências duras, ainda é possível usar a falseabilidade científica num trabalho teórico, realizando-se um experimento mental.

A análise da arquitetura aritmética do Título de Eleitor mostra um sistema projetado com elegância para garantir a integridade dos dados em um cenário de processamento em massa. A escolha do Módulo 11 não é acidental; ela oferece uma barreira matemática praticamente invencível para os erros humanos mais triviais, garantindo a detecção das transposições de dígitos adjacentes e erros de substituição única. Ou seja, a possibilidade de ser errar um único dígito e acabar acertando uma inscrição eleitoral válida é nula.

Contudo, a segurança do algoritmo não é absoluta. A demonstração do fenômeno das colisões apresenta uma vulnerabilidade residual estatisticamente relevante: a alteração de dois dígitos, de forma acidental, carrega uma probabilidade de aproximadamente 8% de gerar um dígito verificador válido, em razão da aplicação do Princípio da Casa dos Pombos sobre o espaço finito de restos.

Lembrando, a cada 100 possíveis erros de digitação, serão gerados nove títulos matematicamente válidos, dos quais, oito podem ser considerados “colisões”, ou seja, diferentes da inscrição original, porém com os mesmos dígitos verificadores.

Este dado teórico ganha contornos críticos quando confrontado com a realidade operacional das eleições brasileiras. Considerando o pleito de 2024, no qual foram processadas mais de sete milhões de justificativas, a margem de erro permitida pelas colisões deixa de ser uma curiosidade matemática para se tornar um ponto de atenção na governança eleitoral.

A persistência de títulos antigos com numeração pouco legível e o preenchimento manual de formulários de justificativa amplificam o risco de que erros de dupla digitação passem pelo filtro primário do algoritmo.

As urnas eletrônicas são configuradas para trabalharem *off line*, condição fundamental para a segurança da votação. Porém, isso também abre a possibilidade de registro de pedidos de justificativa desde que o número de inscrição digitado passe pelo crivo algorítmico.

Embora a aritmética modular seja uma "espinha dorsal" eficiente para a validação cadastral, ela não consegue individualmente garantir a integridade do processo. A existência de colisões matematicamente indetectáveis reforça a necessidade de camadas secundárias de verificação para mitigar os riscos que a matemática, por sua natureza, não pode eliminar sozinha.

A Justiça Eleitoral não divulga publicamente informações acerca do número de colisões a cada pleito, o que dificulta a aferição do quanto essa possibilidade teórica se traduz num problema efetivo. Tampouco há estudos que busquem identificar o impacto das colisões na percepção de integridade eleitoral.

A confiabilidade dos resultados é apenas uma parte pequena da integridade eleitoral. Por sua vez, uma parcela importante do que se entende como eleições íntegras diz respeito à confiabilidade dos processos.

O algoritmo é robusto, mas a supervisão humana e procedimental permanece indispensável para garantir a confiança no processo. Uma integração ser humano/máquina parece ser o melhor cenário. Não basta ser íntegra, a eleição também precisa parecer assim.

REFERÊNCIAS

Birch, S. (2011). *Electoral malpractice*. Oxford University Press.

Brasil. (1982, 7 de junho). *Lei n.º 6.996, de 7 de junho de 1982*. Dispõe sobre a utilização de processamento eletrônico de dados nos serviços eleitorais e dá outras providências. Presidência da República. http://www.planalto.gov.br/ccivil_03/leis/l6996.htm

Brasil. Tribunal Superior Eleitoral. (2021, 26 de outubro). *Resolução n.º 23.659, de 26 de outubro de 2021*. Dispõe sobre a gestão do Cadastro Eleitoral e sobre os serviços eleitorais que lhe são correlatos.

Cox, G. W. (1997). *Making votes count: Strategic coordination in the world's electoral systems*. Cambridge University Press.

Crespo, R. A., & Peixoto, V. de M. (2024). Governança eleitoral e sua credibilidade institucional: Uma análise do caso brasileiro. *Revista Direitos Fundamentais & Democracia, 29*(3), 114–141. https://doi.org/10.25192/ISSN.1982-0496.RDFD.V.29.III.2669

Elklit, J., & Reynolds, A. (2005). A framework for the systematic study of election quality. *Democratization, 12*(2), 147–162.

Faria, L., Pinto, P. E. D., & Pedroza, N. (2017). Optimal Check Digit Systems Based on Modular Arithmetic. *TEMA (São Carlos), 18*(1), 105-125.

Gallian, J. A. (2010). *Contemporary Abstract Algebra* (7.ª ed.). Cengage Learning.

Garnett, H. A., & James, T. S. (Eds.). (2020). *Cyber Elections in the Digital Age: Threats and Opportunities of Election Technology*. Routledge.

James, T. S. (2019). *Comparative electoral management: Networks, performance and instruments*. Routledge.

Lijphart, A. (1994). *Electoral systems and party systems: A study of twenty-seven democracies, 1945-1990*. Oxford University Press.

Mitzenmacher, M., & Upfal, E. (2017). *Probability and computing: Randomized algorithms and probabilistic analysis* (2.ª ed.). Cambridge University Press.

Mozaffar, S., & Schedler, A. (2002). The comparative study of electoral governance: Introduction. *International Political Science Review, 23*(1), 5–27.

Nogueira, A. J. A. (2023). Statistical methods and electoral integrity: The 2022 Brazilian elections. *Beijing Law Review, 14*(2), 727–738. https://doi.org/10.4236/blr.2023.142039

Norris, P. (2014). *Why electoral integrity matters*. Cambridge University Press.

Norris, P. (2022). *In Praise of Skepticism: Trust but Verify*. Oxford University Press.

OECD. (2023). *PISA 2022 results: Factsheets Brazil*. OECD Publishing. https://www.oecd.org/publication/pisa-2022-results/

Pastor, R. A. (1999). The role of electoral administration in democratic transitions: Implications for policy and research. *Democratization, 6*(4), 1–27.

Taagepera, R., & Shugart, M. S. (1989). *Seats and votes: The effects and determinants of electoral systems*. Yale University Press.

Tarouco, G. (2014). Governança eleitoral: Modelos institucionais e legitimação. *Cadernos Adenauer, 15*(1), 229–243.

Tribunal Superior Eleitoral. (s.d.). *Estatísticas do eleitorado*. Reccuperado em 26 de janeiro de 2026, de https://sig.tse.jus.br/ords/dwapr/r/seai/sig-eleicao-eleitorado/home