

Resposta aos apontamentos/questionamentos realizados pela Associação dos Municípios Alagoanos (AMA) em 16/02/2024

Este documento visa elucidar os temas apresentados pela Associação dos Municípios Alagoanos – AMA, através do requerimento enviado à CNM e que tivemos conhecimento através de solicitação realizada pela Comissão Eleitoral no dia 16 de fevereiro de 2024 da qual se referem ao sistema de votação.

O formato que utilizaremos para a elaboração de nossa resposta e/ou explicação será a cópia do trecho descrito no requerimento com uma numeração adaptada para as finalidades deste documento e, logo abaixo e em letra destacada com negrito, a nossa resposta e/ou explicação.

Apontamentos, questionamentos, respostas e/ou explicações

1. ... Voto secreto em meio eletrônico via internet, sem mencionar a fiscalização, por parte das Chapas concorrentes, da veracidade das informações coletadas pela empresa; e ...

R.: O calendário eleitoral divulgado no site define a data de 26/02/2024 para a realização de Reunião com as chapas inscritas para apresentação e esclarecimento de dúvidas relativas ao sistema de votação eletrônico.

2. ... o controle das “senhas individuais”, sem mencionar a segurança do envio e recebimento ...

R.: Idem resposta 1

3. ... Como primeiro ponto a evidenciar a ausência segurança e transparência no sistema de votação, em que pese esteja sendo utilizado serviço de DNS internacional (CloudFlare) que mascara a real localização geográfica do banco de dados da aplicação de votação, por meio de serviços como censys e crt.sh é possível constatar que o sistema se encontra hospedado em servidores localizados nos Estados Unidos da América, Provo, estado de Utah ...

R: A solução de firewall de aplicação (WAF) adotada para mitigar ataques é a solução chamada Cloudflare, responsável por inibir o maior ataque DDoS da história (vide: <https://olhardigital.com.br/2023/10/11/seguranca/google-amazon-e-cloudflare-neutralizam-o-maior-ataque-ddos-da-historia>), e também responsável por inibir um ataque DDoS com mais de 30 milhões de tentativas e 1TB de dados em eleição realizada pela empresa provedora do sistema eleitoral utilizado na CNM (Beevoter) em outra eleição (vide: <https://www.baguete.com.br/noticias/29/11/2021/beevoter-resolve-previa-do-psdb>).

Esta solução (Cloudflare) protege integralmente a infraestrutura, desde os acessos aos registros de DNS e por isso a constatação evidenciada.

A solução de votação adotada pela CNM está hospedada em servidores fora do país, a saber na infraestrutura da *Microsoft* chamada *Azure* que é utilizada por inúmeros grandes clientes do Brasil, dentre eles a *Justiça Federal*, o *Metrô de São Paulo*, o *Ministério da Economia* e a *Secretaria*

de Estado de Fazenda do Rio de Janeiro (vide: https://customers.microsoft.com/pt-br/search?sq=&ff=story_industry_friendlyname%26%3EGovernment%26%26story_product_categories%26%3ECloud%20Platform&p=0&so=story_publish_date%20desc) e não há na legislação brasileira nenhum impedimento em adotar o uso de servidores fora do Brasil. A Lei n. 9.504/97 mencionada no questionamento restringe apenas a veiculação de propaganda eleitoral da eleição brasileira realizada pelo TSE/TRE em ambiente fora do país, mas não determina o uso de infraestrutura para a realização de eleições eletrônicas fora deste escopo.

4. ... O segundo ponto diz respeito à total ausência de conformidade do sistema eletrônico de votação com a Lei n. 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), inexistindo na aplicação qualquer menção à política de tratamento de dados, privacidade e segurança, muito menos existe a indicação do encarregado pelo tratamento de dados pessoais (DPO), conforme exige o art. 41 da referida lei. Nem mesmo no sítio eletrônico da empresa responsável pelo sistema (beevoter.com) é possível localizar quaisquer informações relativas ao tratamento de dados, privacidade e/ou segurança da aplicação...

R: É importante o destaque que, até o presente momento, nenhuma informação de candidatos ou eleitores foi carregada ao site, sendo este sítio apenas informativo até a data da redação desta resposta.

No momento da carga dos dados dos eleitores e dos candidatos, é prevista a divulgação das informações solicitadas e a disponibilização de um canal de atendimento (POSSO AJUDAR) que permitirá aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, receber comunicações da autoridade nacional e adotar providências e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares, conforme preconiza o Art. 41 da lei de n. 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).

5. ... O terceiro aspecto que chama atenção é a existência de duplicidade do sistema na internet, o qual se encontra disponível nos seguintes endereços: ...

R: A afirmação da duplicidade do sistema na internet foi equivocada da forma que foi apresentada pela AMA. A infraestrutura que suporta a eleição é composta de um conjunto de elementos, alguns redundantes para suportar balanceamento de carga e tolerância a falhas, mas todos se comportam de forma a garantir um ambiente único e controlado, sem haver a tal diluição de votos entre sistemas ou discrepância de dados em geral apontadas pela AMA.

A utilização de dois (ou mais) endereços URL, conforme descrito pela AMA, e configurados para um mesmo servidor é uma característica técnica que não causa os efeitos apontados e tão pouco implica na existência de duplicidade de banco de dados como foi afirmado.

6. ... A quarta vulnerabilidade já identificada, talvez a mais grave, é a ausência de validação dos campos “CPF/CNPJ” e “senha” no ambiente de simulação do voto. Mesmo o sistema informando que a simulação ocorrerá pelo preenchimento do CPF ou CNPJ da prefeitura, além da senha recebida por e-mail ou SMS, o que se verifica é a total ausência de validação desses campos...

R: O ambiente de simulação de votos foi proposto no site como forma de possibilitar uma experiência do preenchimento da cédula de votação antes do dia da eleição e não faz NENHUMA verificação de autenticidade do eleitor, até porque a base de dados contendo o colégio eleitoral e

os respectivos CPFs e CNPJs não foram carregados para o sistema até o momento da elaboração desta resposta. Esta ferramenta de votação simulada permite o acesso sem a necessidade de preenchimento das informações de CPF/CNPJ e senha (ou com a possibilidade de se preencher qualquer informação a critério do usuário). O campo foi disponibilizado apenas para conhecimento da interface de usuário pelos eleitores.

O ambiente de votação REAL, disponibilizado apenas no dia 01 de março de 2024, fará a verificação da identidade fornecida pelo eleitor confrontando-a com a relação de eleitores (colégio eleitoral) disponibilizada pela CNM e impossibilitando que CPFs ou CNPJs inválidos possam votar, garantindo também que não seja possível votar mais de uma vez.

7. ... A quinta inconsistência verificada no sistema diz respeito à ausência de transparência acerca de qual empresa, de fato, desenvolveu e é responsável pelo sistema de votação. O domínio no qual foi hospedada a aplicação (eleicoes2024cnm.com.br) possui como titular a empresa DGB SOLUÇÕES DE TEC. DA INF. LTDA, cujo responsável é o Sr. DOUGLAS GOMES BATISTA, conforme informações públicas disponíveis no registro.br...

R: Com relação ao questionamento, cabe destaque que a empresa DGB SOLUÇÕES DE TEC. DA INF. LTDA de responsabilidade do Sr. DOUGLAS GOMES BATISTA é a signatária do contrato de prestação de serviços de sistema eleitoral junto a CNM, e a marca BeeVoter, registrada no INPI em nome de UBIRATAN DE ALMEIDA ELIAS e membro da citada empresa, faz parte dos ativos da empresa DGB SOLUÇÕES DE TEC. DA INF. LTDA e refere-se ao nome do produto e da área exclusiva ao desenvolvimento de sistemas eleitorais da empresa. A aquisição do domínio exclusivo para a realização da eleição foi prevista no objeto da contratação e é certo que seria feito em nome da empresa responsável pelo contrato.

8. ...A sexta inconsistência, por sua vez, revela a utilização de certificados de segurança gratuito no servidor do aplicativo de votação, revelando a baixa ou inexistente preocupação com a segurança do sistema...

R: A garantia da segurança de certificados digitais SSL não se dá pelo fato do certificado ser ou não gratuito e não há nenhum risco de segurança no uso desta prática. A garantia dos certificados SSL se dá pelos acordos firmados entre os fabricantes de navegadores e os provedores de certificados digitais, pelos algoritmos criptográficos utilizados no certificado digital e pelos processos de verificação de propriedade de domínio destes fabricantes.

A solução adota os certificados digitais da empresa Let's Encrypt (<https://letsencrypt.org/pt-br/about>) com algoritmo de assinatura X9.62 ECDSA/SHA 384, o que garante que a solução será aceita por diversos navegadores e que seus processos de verificações são seguros (<https://letsencrypt.org/how-it-works>) e que a comunicação dos dados entre o equipamento do eleitor e os servidores seja feito de forma encriptada e que o endereço do site acessado é de propriedade da empresa contratada, sem nenhuma falha na segurança do sistema.

9. ...Com relação aos pedidos:
 - a. Utilização de provedor de serviço de internet estabelecido no Brasil...

R: Não existe em nosso contrato ou na legislação vigente a exigência do serviço de internet estabelecido no Brasil.

- b. ...Conformidade da aplicação com Lei n.13.709/2018 (Lei Geral de Proteção de Dados – LGPD), com a disponibilização da política de tratamento, privacidade e segurança dos dados depositados no sistema...

R: Será disponibilizado no site a política de tratamento, privacidade e segurança dos dados depositados no sistema.

- c. ...Esclarecimento sobre quais empresas e profissionais estão envolvidas no processo eletrônico de votação...

R: As únicas pessoas técnicas envolvidas diretamente no processo eletrônico de votação por parte da DGB, e todas membro da direção da empresa são:

- **Ubiratan de Almeida Elias (responsável pelo desenvolvimento do sistema e gestão do contrato);**
- **Douglas Gomes Batista (responsável pela infraestrutura);**
- **Humberto Gomes de Lima (responsável pela operação do sistema);**
- **Giselle Pimenta (responsável pela gestão do cliente).**

- d. ...Utilização de sistema que garanta a inviolabilidade e segurança do voto, permitindo o acesso prévio do código fonte do sistema aos técnicos indicados pela entidade requerente para análise e auditoria...

R: É previsto no calendário eleitoral a apresentação do sistema, no dia 26 de fevereiro de 2024, para técnicos qualificados, onde serão apresentadas as inúmeras ferramentas criptográficas que garantem a inviolabilidade e segurança do voto, bem como demais características de segurança. A verificação do código fonte do sistema poderá ser feita em ambiente controlado, apenas diante dos técnicos da DGB, com a exigência da assinatura de um acordo de não divulgação e sem a possibilidade de remoções, alterações, cópias, fotografias ou qualquer outro meio que possa expor seu conteúdo publicamente ou ferir o segredo industrial da DGB.

- e. ... No processo de análise e auditoria que a empresa responsável pelo sistema preste os seguintes esclarecimentos quanto ao banco de dados da aplicação: ...

- i. ... O que garante a atomicidade? ...

R: A solução utiliza-se de gerenciador de banco de dados SQL hospedada na infraestrutura do Azure (vide: <https://azure.microsoft.com/en-us/products/azure-sql>) e as operações que exigem atomicidade, como por exemplo o voto, são realizadas em transação de banco de dados em Stored Procedures;

- ii. ...O que garante a consistência? ...

R: Uma apresentação detalhada da solução, inclusive com a apresentação de nosso modelo de dados, a ser realizada no dia 26 de fevereiro de 2024 de acordo com o

calendário eleitoral, permitirá evidenciar as relações de consistência existentes entre os artefatos de dados para as inúmeras ações no sistema;

iii. ...O que garante o Isolamento? ...

R: A garantia do Isolamento se dá pelo uso correto de "locks" impossibilitam a interferência de atos praticados de forma concorrente, acrescentando que alguns destes "locks" são implementados em Stored Procedures complexas, como por exemplo o ato de verificar a existência de votos anteriores e registro de voto (em transação atômica), e alguns em camada de aplicação, como a inserção de logs de servidores.

iv. ...O que garante a durabilidade? ...

R: A infraestrutura de banco de dados que suporta a eleição (vide: <https://azure.microsoft.com/en-us/products/azure-sql>) provê o uso de plataforma tolerante a falha e com balanceamento de carga, suportando um volume de transações muito maior do que o exigido pelo sistema de votação e com a garantia de disponibilidade superior à 99.995% (vide: <https://azure.microsoft.com/en-us/blog/understanding-and-leveraging-azure-sql-database-sla>), sendo hoje a solução de banco de dados mais robusta para aplicações de missão crítica encontrada no mercado.

10. ...Para garantir a integridade e segurança do processo de votação, permitindo completa auditoria de todas as fases do processo que sejam disponibilizados os seguintes dados/informações:...

As respostas abaixo referem-se às capacidades do sistema em produzir as informações, no entanto destaca-se que a disponibilização das informações a que nos referimos restringe a entrega dos artefatos exclusivamente a CNM, onde o repasse destas informações a pessoas externas ficará sob decisão e responsabilidade da CNM.

a. ...Registros de log de operação, contendo Data, Hora, IP, Navegador, Localização (Cidade/UF), páginas acessadas, operações e decisões dentro do sistema...

R: O sistema armazena log das operações realizadas contendo Data, Hora, IP, navegador, operações, decisões dentre outras informações. As informações de Localização-Cidade/UF não fazem parte do pacote HTTP e conseqüentemente não são registradas nos logs e o sistema opera de forma SPA-Single Page Application, ou seja, não contempla a "troca de páginas" e não há a necessidade de registro de páginas acessadas;

b. ...Registro de log de acesso, contendo quem acessou, quantidade de acessos únicos por IP ou usuário (CPF), de modo a permitir a comparação entre o número de acessos e a quantidade de votos lançados no sistema por usuário...

R: Os registros de logs mencionados na resposta anterior permitem a verificação dos itens solicitados.

c. ...Quem tem acesso ao banco de dados? ...

R: Apenas as pessoas qualificadas da empresa (previamente relacionadas na resposta 9.c) detêm permissão de acesso ao banco de dados, e somente a partir de ambientes autorizados através de firewall de segurança.

Acrescenta-se que os mecanismos de segurança adotados dentro do sistema permitem a garantia da integridade de seus dados sem a fragilidade de eventuais acessos de administradores de banco de dados, no entanto, como forma a preservar o sigilo do voto de forma inequívoca, as logs de acesso ao banco de dados são desativadas.

d. ...A equipe de TI que terá acesso aos dados possui termos assinados para garantia da conduta ética para sigilo? ...

R: O contrato firmado com a CNM prevê cláusula de sigilo das informações e a equipe de TI que terá acesso aos dados (previamente relacionadas na resposta 9.c) é composta exclusivamente por membros da diretoria da empresa. Nenhum acesso a dados da CNM é concedido à funcionários da DGB ou terceiros.

e. ...O log de acesso é auditável? ...

R: As logs são armazenadas no sistema de forma análoga a tecnologia Blockchain, onde o conteúdo de cada log mais a assinatura da respectiva log anterior é assinada digitalmente por chave privada residente exclusivamente na memória do servidor, garantindo a impossibilidade de modificação de seu conteúdo, inserção de novas logs ou remoção de log sem que isso cause inconsistência criptográfica. Ao final do processo todas as logs serão entregues à CNM com os respectivos criptogramas de forma que possam ter sua verificação de integridade criptográfica efetuadas fora do sistema, por programas elaborados por terceiros;

f. ...Quem terá acesso aos dados de votação discriminando quem votou, ou quem terá poder de escolher no universo de dados, uma amostragem para validar a votação externamente?
...

R: O acesso aos dados durante o período de votação é restrito aos integrantes da empresa DGB (previamente relacionadas na resposta 9.c) e disponibilizados para a equipe de atendimento da CNM ao eleitor com caráter exclusivo de apoiar o eleitor na dificuldade técnica da realização de seu voto. Durante o período de votação é previsto o envio de mensagens (e-mail e/ou SMS) para os eleitores que não tenham votado, lembrando-os e convidando a participar da votação.

Sem nada mais a esclarecer e certo de tê-los atendido, Brasília, 18 de fevereiro de 2024.