UNIVERSIDADE ESTADUAL DO CEARÁ
AV. DR. SILAS MUNGUBA, 1700
CAMPUS DO ITAPERI, FORTALEZA, CEARÁ

# PARECER

Assunto: Avaliação de Sistema Eletrônico de Votação para eleições remotas para Ouvidor da Fundação Universidade Estadual do Ceará - FUNECE.

No dia 19 de outubro de 2021 reuniu-se esta comissão, designada através da Portaria Nº 719/2021-FUNECE, para emitir o Parecer Técnico sobre Sistemas de Eleições Remotas para ser utilizado na eleição de Ouvidor da Fundação Universidade Estadual do Ceará - FUNECE.

Apesar de existirem no mundo diversos sistemas abertos ou proprietários para a realização de eleições remotas, esta comissão se deteve em analisar o sistema implantado pelo DETIC/UECE, o Helios Voting System, sistema de código aberto colaborativo inicialmente desenvolvido por Ben Adida.

O processo consistiu em realizar reuniões desta comissão com a Comissão Eleitoral e DETIC/UECE para levantar os requisitos do processo eleitoral e das características técnicas do sistema. Após essas reuniões, esta comissão se reuniu para preparar este parecer fundamentado com as respectivas justificativas e algumas sugestões operacionais para melhorar a segurança do processo.

## Requisitos desejáveis para um sistema de Votação Eletrônica

Inicialmente citamos alguns requisitos desejáveis para um sistema de votação eletrônica.[1] São requisitos usuais em eleições presenciais tradicionais no qual um sistema eletrônico deve incorporar algum mecanismo que possa garantir esses requisitos.

Igualdade: todos os eleitores aptos devem ter o direito de votar. Um voto deve vincular a apenas um candidato e ninguém pode votar em mais de um candidato.

Autenticidade: apenas os eleitores aptos podem votar.

[1] Ghassan Z.,Qadah Rani Taha. *Electronic voting systems: Requirements, design, and implementation.* Computer Standards & Interfaces Volume 29, Issue 3, pp 376-386, March 2007.

Segurança: em todo o processo de votação, desde a escolha do candidato pelo eleitor até a finalização da apuração, o voto não pode ser adulterado ou violado.

Integridade: uma vez que o eleitor deu um voto, não é permitida nenhuma alteração neste voto. Além disso, todos os votos válidos devem ser contados, ao passo que todos os votos inválidos não devem ser contados.

Privacidade: depois de emitir um voto, ninguém deve poder vincular o eleitor a seu voto.

Auditoria: para garantir a confiabilidade de qualquer eleição é necessário permitir uma auditoria dos votos caso ocorra um questionamento.

Coerção: garantir que o eleitor possa votar sem ser coagido.

Recursos humanos e infraestrutura: garantir recursos que possibilitem ao sistema funcionar de forma satisfatória para prover a acreditação do processo.

## Histórico do Sistema Helios

O sistema Helios Voting System Helios é um software aberto criado em 2009 com Licença Open Source Apache 2.0[2]. O software é originário da tese de doutorado (PhD) de Ben Adida no MIT Cryptography and Information Security Group, defendida em 2006. Ben Adida é fundador e atual presidente da Voting Works, organização não governamental com objetivo de desenvolver sistemas de votação abertos e seguros (https://voting.works/). O software Helios possui uma comunidade bastante ativa e está disponível sem custo em https://github.com/benadida/helios-server. A Voting Works é responsável pela manutenção e evolução do sistema Helios.

O sistema Helios foi desenvolvido na linguagem Python e JavaScript com servidor Django e apresenta uma interface simples e intuitiva (lista de opções em página HTML). O foco desse sistema é a segurança e tem sido usado como referência em trabalhos acadêmicos sobre segurança de votação eletrônica.

Existe uma versão do Helios traduzida para o português e com suporte a Lightweight Directory Access Protocol (LDAP) desenvolvida pelo IFSC e disponível em https://github.com/ifsc/helios-server. Ressaltamos que todos os sistemas acadêmicos e administrativos da UECE utilizam autenticação LDAP.

[2] Adida, Ben. Helios: Web-based Open-Audit Voting.USENIX security symposium. Vol 17, pp 335-348, 2008.

Algumas instituições de ensino superior que utilizam do Helios Voting são: USP, UFSCar, IFMG, IFNMG, IFTM, IFSC, UFSC, UTFPR, UFPEL, IFRS, IFMA, UFMT, UNB.

O sistema Helios customizado foi utilizado de forma satisfatória na UECE sem ter sido registrado nenhum incidente nas eleições de Coordenadores dos cursos de graduação em junho/2021. Neste período foram realizadas 74 eleições simultâneas durante quatro dias com um total de 10.290 votos.

## Igualdade

O sistema Helios oferece esse requisito, isto é, todos os eleitores aptos podem votar e cada eleitor apenas pode votar em um candidato. A literatura mostra que eleições com voto facultativo na modalidade on-line apresentam menor taxa de abstenção devido a facilidade de votar, melhorando a igualdade do sistema.

Ressaltamos que estamos considerando que todos os eleitores possuem um equipamento adequado para realizar seu voto, seja computador próprio ou telefone celular.

Quanto à acessibilidade, a interface simples enxuta do sistema Helios possibilita ao eleitor votar a partir de qualquer equipamento, seja computador, tablet ou telefone celular. O voto é uma página web simples com fundo branco no qual o eleitor deve marcar o candidato escolhido (é possível configurar para aceitar votos em mais de um candidato). O voto em uma tela pequena (celular) fica bem nítido e legível, mas melhora significativamente ao deitar o telefone (tela horizontal). A autenticação do voto é realizada após a escolha para garantir que seja depositado na urna apenas votos dos eleitores aptos.

Concluindo, a interface do sistema Helios favorece a avaliação sob o aspecto de garantia de igualdade de voto, permitindo a maior participação dos eleitores.

## Autenticidade

O sistema Helios implementa vários mecanismos para verificar a autenticidade e permitir que apenas os eleitores aptos possam votar.

O sistema Helios oferece três formas diferentes de autenticação, (1) através do envio de um e-mail ao eleitor com o login e uma senha aleatória, (2) autenticação pelo protocolo OAuth com provedores externos como Google ou Facebook, e (3) através do protocolo LDAP (contribuição do IFSC). O processo de autenticação ocorre apenas na hora de depositar o voto na urna utilizando uma dessas formas.

Qualquer uma dessas formas atende ao requisito de autenticação. A escolha deverá recair sobre a forma mais fácil de ser implementada pelo DETIC.

## Segurança

A segurança talvez seja o ponto mais importante para analisar um sistema de votação. Um sistema inseguro é vulnerável a fraudes e, caso seja de conhecimento de todos, pode desacreditar todo o processo eleitoral. É necessário que em todo o processo de votação, desde a escolha do candidato pelo eleitor até a finalização da apuração, o voto não possa ser adulterado nem violado. Outro ponto importante da segurança é garantir que o código executável do sistema de votação não possa ser alterado durante o processo de votação.

O sistema Helios utiliza dois mecanismos de criptografia. O primeiro mecanismo é a criptografia Transport Layer Security (TLS) utilizada entre o browser do equipamento do eleitor e o servidor de eleição. No entanto, esse mecanismo é praticamente obrigatório pois atualmente toda a comunicação na Internet utiliza o protocolo Hyper Text Transfer Protocol Secure (HTTPS). O segundo mecanismo de criptografia usada pelo Helios é a criptografia Homomórfica em Mixnets, técnica que permite operar dois valores criptografados (eleitor e voto) e ao decriptografar somente o resultado desejado será conhecido (voto), sem associar com o operando original (eleitor). Esse mecanismo é importante pois garante que o conteúdo do voto seja preservado corretamente na apuração sem correlacionar com o eleitor que depositou o voto. A criptografia homomórfica é realizada no browser do eleitor mediante um programa JavaScript e somente é decriptografado mediante a chave do administrador da eleição no servidor. Esse mecanismo, junto com outros mecanismos de auditoria, garantem o sigilo do voto desde o browser do eleitor até o servidor onde será apurado o resultado, impedindo vincular o voto ao eleitor. Apesar de impedir vincular o voto em seu formato final a um eleitor, é possível o eleitor provar como votou usando valores publicados em um Bulletin board. O sistema Helios utiliza a técnica de Mixnets, que consiste em criptografar e embaralhar seguidas vezes o voto para melhorar a segurança e dificultar a identificação do voto e do eleitor. O algoritmo de chave assimétrica com capacidade homomórfica utilizada é o ElGamal Exponencial. O sistema Helios é escrito em linguagem Python interpretada e o código fonte fica legível no servidor, possibilitando que qualquer pessoa com acesso ao sistema possa alterá-lo. Isso pode ser evitado caso seja definido um procedimento de verificação de integridade do código do sistema (por exemplo, MD5 ou SHA-256) para garantir que o código não foi alterado durante todo o processo de eleição.

O sistema Helios, no entanto, permite a utilização de ataque do tipo Homem no meio (man-in-the-middle), basta criar uma página semelhante ao voto redirecionada por um e-mail (phishing) que coleta todos os usuários e senhas. Mediante usuário e senha, um atacante pode votar em um candidato sem conhecimento do eleitor que considera que votou corretamente.

Acerca da segurança, o sistema Helios apresenta vantagens substanciais. Por ser um sistema concebido por pesquisadores em segurança, ter o código aberto e ser bastante testado pela comunidade acadêmica em várias partes do mundo, podemos dizer que é um sistema onde se considerou bastante os aspectos de segurança. O uso de criptografia assimétrica ElGamal com propriedades homomórficas apresenta características desejáveis a um sistema eleitoral.

Finalizando o aspecto de segurança, todos sabemos que uma corrente é tão forte quanto seu elo mais fraco. Procedimentos e metodologias de segurança que vão desde equipamentos do usuário passando por todos os equipamentos de comunicação até os servidores da UECE, devem ser propostos e implementados para garantir o processo de eleição. Não basta o sistema mais seguro do mundo se houver erros de procedimento e operação do sistema. Envolve pessoal altamente qualificado em segurança, como também, o sistema deve ser implementado e oferecido com garantias de disponibilidades.

## Integridade

Integridade de um voto é garantir que o sistema não permita a alteração do conteúdo de um voto que o eleitor depositou na urna. Além disso, deve-se garantir que todos os votos válidos devem ser contabilizados e todos os votos inválidos não devem ser contados. A integridade de informação geralmente é obtida com o uso de algoritmos de resumo (Hash).

O sistema Helios utiliza o algoritmo SHA-1 em várias etapas do processo, desde a criação do voto no computador do eleitor até a apresentação do resultado final. Cada etapa é acompanhada pela geração de um hash que é armazenado e exibido publicamente pelo Bulletin board.

Podemos afirmar que o sistema Helios apresenta funcionalidades para garantir a integridade do voto. Devemos ressaltar que todos os mecanismos de auditoria pelo eleitor e auditoria via provas de transformação na Mixnet permitem provar a integridade do processo de votação do Helios, sendo sua maior contribuição científica.

## Privacidade

Uma das características de qualquer sistema democrático é garantir o sigilo da escolha de cada eleitor através do voto secreto, seja ele em papel ou eletrônico. Para se garantir realmente uma eleição democrática é necessário que todos os eleitores tenham certeza que o seu voto não será violado. Essa característica é de suma importância para os sistemas de votação eletrônica pois, como é sabido, todo computador é previsível (um computador somente gera valores pseudo-aleatórios).

Em um sistema de votação remota não é possível garantir a privacidade do local e ambiente físico onde o eleitor vai votar. Assim, na avaliação de um sistema de votação remota deve ser considerado verificar a facilidade do sistema permitir a identificação dos eleitores.

O sistema Helios criptografa o voto no equipamento do eleitor, e o voto transita pela rede e pela memória e banco de dados do servidor totalmente criptografado. O uso da criptografia homomórfica garante que após a apuração, perde-se o registro do eleitor, restando apenas a contabilização dos votos. O uso de criptografia homomórfica ElGamal e utilização de Mixnets torna o sistema Helios significativamente íntegro na questão de privacidade dos votos.

## Auditoria

A auditoria de uma eleição eletrônica sem que sejam identificados os eleitores é um dos pontos mais sensíveis em qualquer sistema. Auditoria e sigilo do voto viajam em direções opostas, a cada funcionalidade de auditoria prejudica o sigilo e vice-versa. Por isso, a funcionalidade de auditoria é bastante difícil para um sistema de votação eletrônico, e mais difícil ainda quando é realizada na modalidade remota.

O sistema Helios incorporou ferramentas de auditoria desenvolvidos pela Universite Catholique de Louvain. Basicamente, cada eleitor pode opcionalmente verificar o voto criptografado e caso esteja correto ele marca que está OK. Esta marca é pública no Bulletin board e caso um percentual de eleitores confirmarem o voto (de consenso entre os eleitores), a eleição é considerada válida. Existem várias outras ferramentas que verificam se as reencriptações homomórficas e misturas das mixnets foram executadas corretamente. Vale lembrar que o primeiro artigo publicado sobre o Helios ressalta a característica dele poder ser publicamente auditado.

Sobre este ponto, o sistema Helios possui a funcionalidade de auditoria. Sendo essa funcionalidade imprescindível para qualquer sistema eleitoral confiável, é uma das grandes contribuições do sistema Helios.

## Coerção

Um sistema de votação remota oferece a facilidade que o eleitor votar em qualquer lugar. Porém essa facilidade possibilita que o eleitor possa sofrer coerção para votar em um determinado candidato, o que não ocorre em uma sala de votação pública e fiscalizada por todas as chapas em uma eleição presencial tradicional. Mas ainda mais grave do que a possibilidade de coerção é a possibilidade de venda de voto, particularmente em uma eleição onde o eleitor aparentemente não tem muito a perder.

O próprio idealizador do sistema Helios reconhece a possibilidade de coerção, e venda de votos, colocando claramente como premissa que tal sistema só deveria ser utilizado para eleições onde a coerção ou venda de votos fossem tolerados (low-coercion system).

O sistema Helios implementa uma funcionalidade de permitir que o eleitor possa votar várias vezes durante o período da eleição e considerar apenas o último voto, desconsiderando todos os demais. Assim, se um eleitor for coagido a votar em um candidato (e mandar uma foto do voto, por exemplo), pode posteriormente votar novamente no candidato que desejar (sobrescrever sobre o mesmo registro anterior). No entanto, na tela do Bulletin Board a chave do voto referente a esse eleitor muda, indicando que o eleitor alterou o voto.

Para evitar a identificação do eleitor que voto mais de uma vez, recomendamos que a lista temporária de votantes seja conhecida apenas pela comissão eleitoral e que a apenas seja divulgada após o encerramento do pleito a lista final com a chave dos votos.

## Recursos humanos e infraestrutura

É importante lembrar que um sistema de votação eletrônica apresenta muitas características diferentes de uma eleição tradicional, exigindo cuidados distintos. Qualquer falha que ocorra, por menor que seja, pode comprometer todo o processo eleitoral. Nos últimos anos ocorreram várias eleições, como UFMT, UFPI e UTFPR, onde foram utilizados o sistema Helios ou outros, e que sofreram questionamentos jurídicos acerca dos resultados em virtude da ocorrência de interrupções e falhas que não impactasse no resultado.

Sendo assim, além da seleção de um sistema computacional tecnicamente bom e seguro, devemos nos preocupar em questões da infraestrutura de TIC, a saber:

- Manter energia estável durante todo o pleito. É necessário que o suporte de energia redundante (nobreak e gerador) seja garantido durante todo o período de realização da eleição.
- Garantir redundância do sistema em, pelo menos, quanto ao banco de dados.
- Garantir sistema para substituição de sistema em falha e redirecionar as requisições para um servidor operacional, possivelmente utilizando um balanceador de carga.

## Parecer e Recomendações

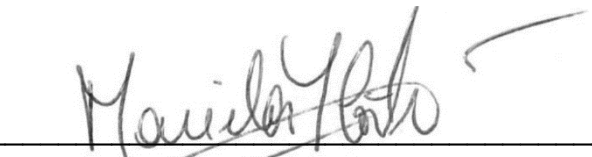
Perante os fatos aqui relatados, esta comissão deliberou que o sistema Helios apresenta características de segurança e privacidade necessárias para realização de

eleições eletrônicas remotas para Ouvidor da Fundação Universidade Estadual do Ceará - FUNECE.

Para garantir um processo eleitoral seguro e integro, sugerimos algumas recomendações:

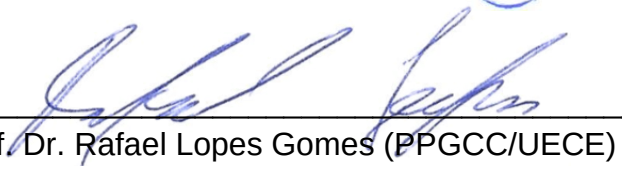
- Não permitir a inclusão de novos eleitores durante o período de eleição (quando os eleitores poderão depositar o voto) devido ao fato de não garantir lisura do processo e possíveis recursos. Como não é possível implementar o voto em separado em uma eleição remota, qualquer quebra no procedimento poderá expor fragilidades no sistema. Como não é possível identificar o voto depositado, será necessário realizar uma nova eleição caso um voto em separado não seja considerado válido. Deve ser estabelecido no edital um prazo máximo para inclusão de novos eleitores na lista de eleitores (após a comprovação) e vetar qualquer inclusão posterior;
- Configurar a possibilidade que o eleitor possa votar várias vezes, sendo considerado apenas o último voto. Essa metodologia evita o problema de coerção na eleição.
- Aculturamento da comunidade sobre a possibilidade de coerção e venda de votos. Informar os eleitores da possibilidade que ele pode votar novamente, valendo apenas o último voto;
- Disponibilização de material multimídia a fim de orientar os eleitores na utilização e funcionalidades do sistema Helios, mitigando possíveis dificuldades de utilização do sistema ao decorrer das eleições.

É o parecer.



Profa. Dra. Mariela Inés Cortes (PPGCC/UECE) - Presidente

Prof. Dr. Marcial Porto Fernandez (PPGCC/UECE) - Membro



Prof. Dr. Rafael Lopes Gomes (PPGCC/UECE) - Membro