

RELATÓRIO TÉCNICO - VERSÃO 03

USO DO VOTO ONLINE EM ELEIÇÕES DA UFSCAR

CONTEÚDO

Resumo

Seção 1- A Comunidade Quer o Voto Online?

A Vontade da Comunidade sobre o Uso do Voto Online nas Eleições da UFSCar

Seção 2 – É Tecnicamente Possível?

Condições Técnicas para Uso do Voto Online na UFSCar: o Sistema Helios Voting

Seção 3 – É Seguro?

Condições de Segurança para o Uso de Voto Online em Eleições na UFSCar

Seção 4 – É Juridicamente Possível?

Análise Legal e de Regimentos Internos

Anexo: PARECER n. 00082/2018/CONS/PFFUFSCAR/PGF/AGU

O Conselho de Administração da UFSCar, através do ATO COAD 402, de 26/06/2018, constituiu “Comissão Técnica para elaborar estudo sobre métodos e ferramentas para votação eletrônica, e coordenar consulta pública visando identificar a opinião da comunidade UFSCar acerca da implantação de voto eletrônico no âmbito da UFSCar”. Este Relatório técnico apresenta os resultados dos estudos e encaminhamentos realizados até o momento.

Comissão Técnica Voto Online - Ato COAD 402

Profa. Dra. Marilde Terezinha Prado Santos (Presidente), Prof. Dr. Paulo Matias, Dr. Erick Lazaro Melo, Prof. Dr. Ednaldo Brigante Pizzolato, Prof. Dr. Roberto Ferrari (colaborador).

UFSCar, 31 de agosto de 2018

Resumo

A Comissão Técnica nomeada pelo Conselho de Administração da UFSCar realizou Consulta Pública visando identificar a opinião da comunidade sobre a adoção do voto online nas eleições da UFSCar. A Consulta foi realizada entre os dias 20 e 24 de agosto de 2018. Oitenta por cento (80%) dos docentes que participaram da Consulta se disseram favoráveis ao voto online. Entre os estudantes de graduação que participaram da Consulta os favoráveis ao voto online foram 77,8%. Na pós graduação, 85,3% dos que participaram se disseram a favor do voto online, e nos técnico-administrativos, 70,1% dos respondentes são favoráveis ao voto online. A média simples, sem qualquer ponderação, entre todas as categorias indica que 78,1% dos votantes são a favor do voto online nas eleições da UFSCar. A consulta não teve caráter deliberativo; apenas buscou "identificar a opinião da comunidade" (Ato CoAd 402). Para realizar a Consulta, utilizou-se a ferramenta Helios Voting - um sistema de código aberto, desenvolvido em Harvard, que proporciona rastreabilidade, auditoria e privacidade através de técnicas criptográficas; e vem sendo utilizado em eleições em diversas instituições, como USP, UNICAMP, Princeton e Harvard. O Helios Voting foi instalado na UFSCar e testado em uma Votação para Escolha do Logotipo do CCET, e na Consulta sobre Voto Online já mencionada. A identificação dos eleitores foi realizada através do próprio número UFSCar e senha UFSCar. Para analisar a viabilidade jurídica do uso do voto online nas eleições da UFSCar, esta Comissão Técnica estudou a legislação, os regimentos internos, e realizou Consulta Específica à PF-UFSCar inquirindo sobre a viabilidade jurídica de utilizar voto online nas eleições da UFSCar, à luz do Decreto 8.539/2015. O PARECER n.082/2018/CONS/PFFUFSCAR / PGF / AGU, em seu artigo 28, conclui: "Do exposto, do ponto de vista jurídico não nos parece haver impossibilidade de realização de eleição eletrônica ou online para representantes de quaisquer dos conselhos superiores da UFSCar". **Assim, considerando a vontade da Comunidade UFSCar, claramente expressa na Consulta, considerando a viabilidade técnica e condições de segurança obtidos com a instalação e testes realizados, e considerando a possibilidade jurídica, conforme disposto no Parecer 082/2018 PF-UFSCar, esta comissão recomenda que a UFSCar adote o voto online em suas eleições, com a perspectiva de maior facilidade e menor risco no processo de apuração, maior flexibilidade quanto a local e modo de votação, provável aumento da participação e consequente aprimoramento da democracia. Como encaminhamentos, sugere-se a elaboração e aprovação de edital prevendo explicitamente o uso do voto online.**

Seção 1- A Comunidade Quer o Voto Online?

A Vontade da Comunidade sobre o Uso do Voto Online nas Eleições da UFSCar

1.1- Descrição da Consulta

Com o propósito de verificar se a Comunidade UFSCar é favorável ou não ao uso de voto online nas eleições da UFSCar, estudantes, servidores docentes e técnico-administrativos dos 4 campi foram convidados a responder a **questão**:

"Caso as condições técnicas e de segurança sejam adequadas, você é favorável ao uso do voto online em eleições na UFSCar"?

Ao apresentar a ressalva "caso as condições técnicas e de segurança sejam adequadas", a Consulta procurou identificar se a comunidade é conceitualmente favorável ao voto online. As condições técnicas e de segurança serão abordadas nas seções 2 e 3 deste Relatório Técnico.

Para responder os eleitores tinham as seguintes **opções de respostas**:

- () A favor do voto online
- () Contra o voto online

Tanto a questão quanto as opções de voto podem ser observadas na Figura 1. Em outras eleições ou votações, é possível oferecer uma quantidade maior de opções de candidatos ou respostas, é possível possibilitar que o eleitor marque mais de uma opção, e é possível também incluir uma opção para branco - nulo, caso desejado.

Figura 1: Cabine de Votação Mostrando a Questão e as Opções de Voto

Caráter da Consulta: Esta Consulta **não possui caráter deliberativo**. Conforme indicado pela redação do ATO COAD 402 o caráter da Consulta foi "**identificar a opinião da Comunidade**". Os resultados desta Consulta poderão servir de subsídio para as instâncias competentes para decidir sobre a adoção do voto online.

1.2- Metodologia Adotada

Período: A eleição ocorreu do dia 20/08/2018 as 16:00h até o dia 24/08/2018 as 9:30h.

Cabines de Votação: foram criadas 4 cabines de votação - para (1) estudantes de graduação, (2) estudantes de pós-graduação, (3) servidores docentes, e (4) servidores técnico-administrativos. A estratificação da consulta nas quatro categorias permitiu uma análise dos resultados de modo também estratificado por categorias.

Eleitores só podem acessar a cabine de votação da categoria a qual pertencem. Os *links* para as quatro cabines de votação são:

- Docentes: <https://votacao.ufscar.br/helios/e/voto-online-docentes/vote>
- Estudantes de Graduação: <https://votacao.ufscar.br/helios/e/voto-online-grad/vote>
- Estudantes de pós-graduação: <https://votacao.ufscar.br/helios/e/voto-online-pos/vote>
- Técnico-administrativos: <https://votacao.ufscar.br/helios/e/voto-online-tas/vote>

Listas de Eleitores: A formação das listas de eleitores: as listas de eleitores foram criadas a partir dos cadastros da Secretaria de Informática - SIN, da UFSCar. Eleitores que pertencem a mais que uma categoria foram incluídos na categoria com menor número total de eleitores, para dar a cada eleitor o maior peso possível para seu voto.

O universo de eleitores selecionado para cada uma das categorias é apresentado na Tabela 1.

	Universo de Eleitores
Docentes	1.321
Estudantes de Graduação	13.119
Estudantes de Pós-Graduação	4.161
Técnico-Administrativos	1.007

Tabela 1: Universo de Eleitores para Cada uma das Categorias

Divulgação: A divulgação da consulta ocorreu de duas maneiras: (1) divulgação de notícia, enviada através do veículo InfoRede (email) enviado nos dias 21, 22 e 23/08/2018, informando os *links* para as 4 cabines de votação; e (2) envio de email individual pelo próprio sistema de votação, a cada eleitor que ainda não havia votado no dia 22/08/2018, informando seu login, *link* para sua cabine de votação, e orientações para recuperação de sua senha, caso houvesse necessidade.

Processo de Votação: Para que pudesse votar, cada eleitor deveria acessar o *link* de sua cabine de votação, e comprovar sua identidade ao fornecer como login seu número UFSCar (Figura 2), e a senha que utiliza nos sistemas integrados da UFSCar (SIGA, SAGUI, WIFI EDUROAM).

Número UFSCar

Senha

Conectar

Figura 2: Acesso à Cabine de Votação com *Login* e Senha dos Sistemas UFSCar

O eleitor seria então direcionado à Cabine de votação e passaria por 3 passos: (1) selecionar a opção - a favor ou contra o voto online; (2) verificar se a opção selecionada estava correta, e (3) depositar efetivamente o voto na urna (Figura 3).

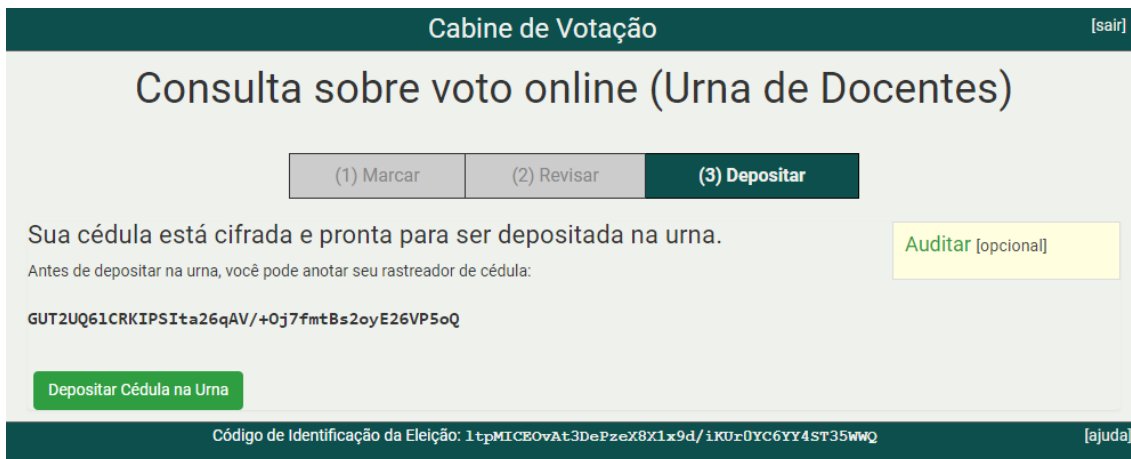


Figura 3: Terceiro passo na Cabine de Votação - Depositar a Cédula na Urna

Alteração do Voto / Repetição do Voto: foi permitido, a cada eleitor, alterar seu voto quantas vezes fosse necessário. Bastava, para isso, que o eleitor votasse novamente. Foi considerado como válido somente o último voto depositado por cada eleitor. A possibilidade de votar várias vezes, visando alterar seu voto, foi informada no email individual enviado a cada eleitor.

Apelidos e Rastreador das Cédulas: A cada eleitor foi designado um "apelido", informado apenas ao eleitor. Aos eleitores que votaram foi designado um código rastreador da cédula. Através de uma lista de votantes divulgada publicamente é possível que cada eleitor busque seu apelido e o seu rastreador da cédula, para se certificar de que seu voto está sendo / foi computado (Figura 4).

Eleitores 1 - 50 (of 1321) próximo 50

Pseudônimo	Rastreador da Cédula
V1	—
V10	—
V100	—
V1000	—
V1001	—
V1002	—
V1003	—
V1004	—
V1005	NZDABMhefFWc5VjgOpjPAzNtfM1qQLHG4K0/ww8tMBs
V1006	—
V1007	—
V1008	43M485+SyXn/SBgLB2R6wxP93xJD67mFX8gcywrwE3U
V1009	ByugqJwFBpC7N77FEXBGcGn5tlcb/zAaLUU7dt85SB4

Figura 4: Lista Parcial de Votantes, Indicando Apelidos, e Rastreadores dos Que Votaram

1.3- Resultados Obtidos

A Tabela 2 apresenta os resultados da Consulta. O percentual de participação na Consulta foi de 29,6% na categoria docente, 11% nos estudantes de graduação, 8% nos estudantes de pós-graduação, e 33,3% nos servidores técnico administrativos.

	Total de Eleitores	Total de Votantes	% de Participação	A Favor do Voto Online		Contra o Voto Online	
				Total a Favor	%	Total Contra	%
Docentes	1.321	391	29,6%	313	80,0%	78	19,9%
Estudantes - Graduação	13.119	1.444	11,0%	1.123	77,8%	321	22,2%
Estudantes - Pós-Graduação	4.161	334	8,0%	285	85,3%	49	14,7%
Técnico-Administrativos	1.007	335	33,3%	235	70,1%	100	29,8%
Total Geral	19.608	2.504	12,8%	1.956	78,1%	548	21,9%

Tabela 2: Resultados da Consulta em Valores Absolutos e Percentuais

Oitenta por cento (80%) dos docentes que participaram da Consulta se disseram favoráveis ao voto online. Entre os estudantes de graduação que se manifestaram na Consulta, os favoráveis ao voto online foram 77,8%. Na pós-graduação, 85,3% dos que participaram da Consulta se disseram a favor do voto online, e nos técnico-administrativos, 70,1% dos votantes são favoráveis ao voto online. A média simples, sem qualquer ponderação, entre todas as categorias indica que 78,1% dos votantes são a favor do voto online nas eleições da UFSCar. As Figuras 5 a 9 ilustram esses resultados.

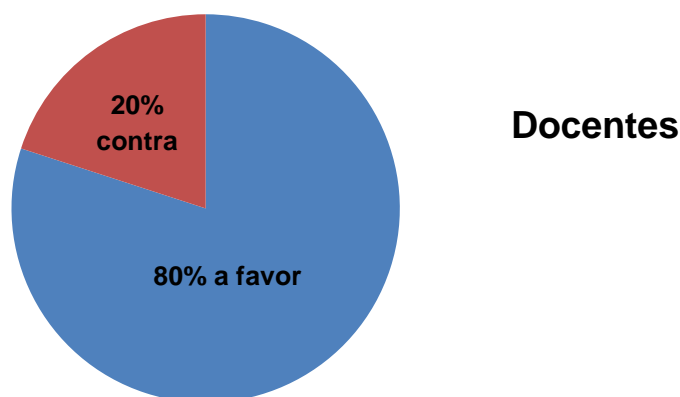


Figura 5: Resultados Percentuais na Categoria Servidores Docentes

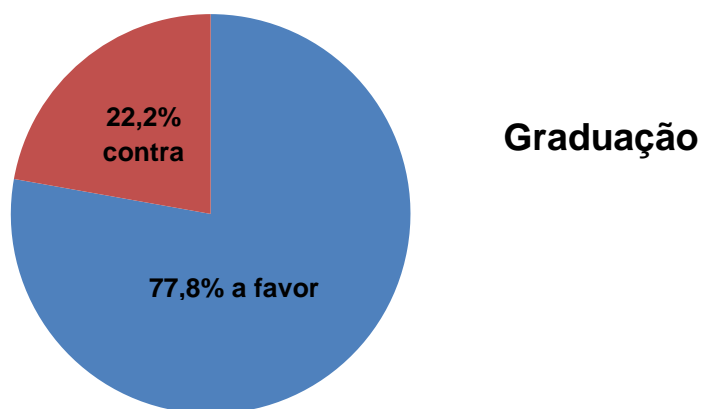


Figura 6: Resultados Percentuais na Categoria Estudantes de Graduação

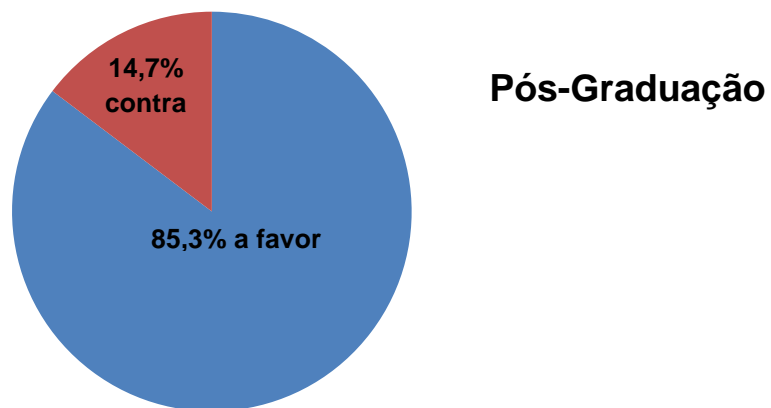


Figura 7: Resultados Percentuais na Categoria Estudantes de Pós-Graduação

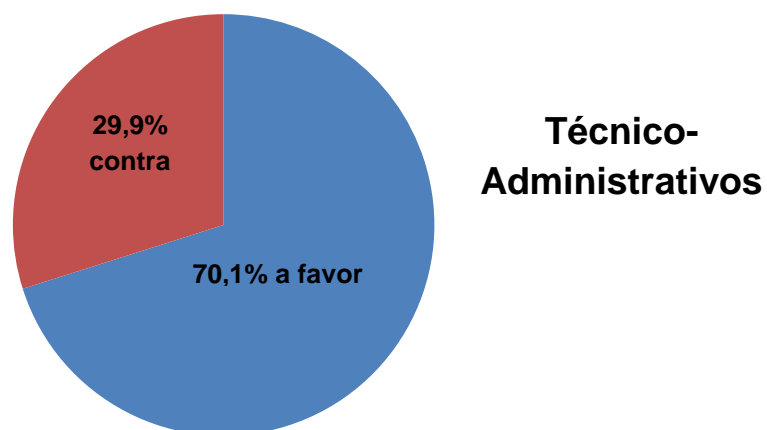


Figura 8: Resultados Percentuais na Categoria Servidores Técnico-Administrativos

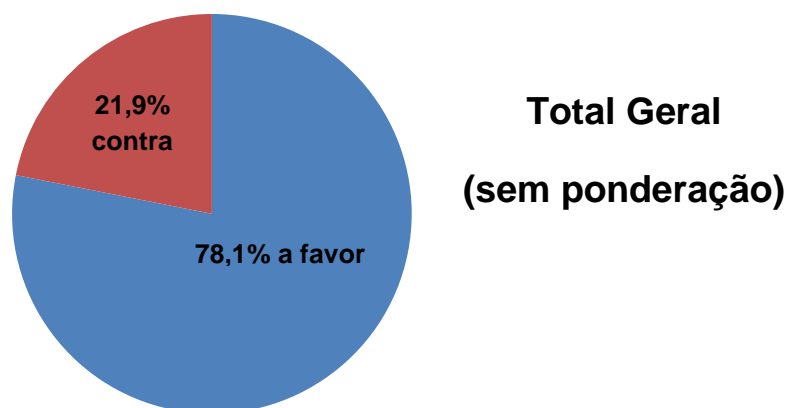


Figura 9: Resultados Percentuais - Total Geral - Sem Ponderação

1.4- Análise dos resultados

Os resultados indicam que a maioria da Comunidade UFSCar gostaria que fosse utilizado o voto online nas eleições da UFSCar, com percentuais a favor variando de 70,1% a 85,3% a depender da categoria.

Comparando os percentuais de participação na presente Consulta com os percentuais de participação nas últimas eleições para representantes discentes aos Conselhos Superiores, é possível supor que a adoção de voto online aumentaria o percentual de participação nas eleições, em especial nas categorias de estudantes de graduação e pós-graduação (Tabela 3).

	Votaram na Consulta sobre o Uso de Voto Online	Votaram na Eleição para Representantes 2016	Votaram na Eleição para Representantes 2017 (cancelada)
Estudantes - Graduação	1.444	498	810
Estudantes - Pós-Graduação	334	47	166

Tabela 3: Comparação do Total de Votantes na Consulta sobre Voto Online com as Eleições para Representantes Discentes em 2016 e 2017

Parte II – É Tecnicamente Possível?

Condições Técnicas para Uso do Voto Online na UFSCar: o Sistema Helios Voting

O Sistema Helios Voting

Helios Voting - <https://heliosvoting.org/> - é um sistema de votação online que proporciona que as eleições sejam seguras (criptografia), rastreáveis (cada voto gera um token), e auditáveis (código e especificações abertas podem ser auditados). Naturalmente, proporciona privacidade quanto ao voto de cada eleitor.

Quem Já Utiliza o Helios Voting

O Helios Voting foi desenvolvido em Harvard, e tem sido utilizado em eleições de diversas instituições como Universidade de São Paulo - USP (<http://www.sti.usp.br/novo-servico-de-votacao-da-universidade-de-sao-paulo/>), Universidade de Campinas - UNICAMP (<https://www.ccuec.unicamp.br/ccuec/noticias/2015/12/22/ccuec-disponibiliza-sistema-automatizado-para-eleicoes-e-consultas-na-unicamp>), Universidade Federal de Santa Catarina (<http://e.ufsc.br/e-democracia/>), Universidade Federal da Grande Dourados (<https://votacao.ufgd.edu.br/>), Instituto Federal de Rondônia (<http://consulta.ifro.edu.br/sistemas-de-votacao-online-helios/>), Instituto Federal de Santa Catarina (<http://dtic.ifsc.edu.br/sistemas/sistema-de-votacao-on-line-helios/>), Instituto Federal Fluminense (<http://portal1.iff.edu.br/reitoria/noticias/sistema-de-votacao-online-do-iffuminense-garante-rapidez-e-seguranca-dos-processos-eleitorais>), Katholieke Universiteit Leuven (<https://www.kuleuven.be/rectorverkiezing/english>), Princeton (<https://princeton.heliosvoting.org/>) e Harvard (<https://helios.law.harvard.edu/>). A Universidade de São Paulo já realizou mais de 1200 eleições através do Helios Voting (<https://jornal.usp.br/institucional/usp-implanta-sistema-inedito-de-votacao-eletronica/>).

Helios Voting na UFSCar

É possível utilizar o Helios Voting em seu próprio servidor, mas como o código é aberto, também é possível instalar o Helios Voting, e adaptá-lo, de acordo com as necessidades do usuário. A Secretaria de Informática - SIn da UFSCar instalou os Helios Voting em um servidor na UFSCar, e adaptou-o para o número UFSCar e senha UFSCar possam ser utilizados na autenticação dos usuários. Esta instalação do Helios Voting na UFSCar pode ser acessada no link: votacao.ufscar.br

Como Funciona uma Eleição com o Helios Voting UFSCar

1. É possível designar uma **Comissão Eleitoral** no Sistema. A Comissão Eleitoral poderá definir, acompanhar e rastrear todo o processo;
2. **Cria-se uma votação**, e é definindo o **período de votação**;

3. A **Comissão Eleitoral insere no Sistema a lista de votantes** que, uma vez fechada, não poderá mais ser alterada. Isso garante que nenhum eleitor indevido poderá participar do processo;
4. Comissão Eleitoral e fiscais podem fazer **testes preliminares no sistema** para verificar se está funcionando de forma adequada;
5. **Comissão Eleitoral lacra as urnas** antes do início do período das eleições;
6. Iniciado o período de votação, **os(as) eleitores(as) podem votar de qualquer lugar do mundo com qualquer dispositivo**; podem inclusive votar várias vezes, alterando seu voto, mas somente a última cédula virtual depositada na urna virtual será computada;
7. **A comprovação da identidade do(a) eleitor(a) é feito com login (número UFSCar) e senha da própria UFSCar**, e o *link* de acesso ao local de votação pode ser divulgado publicamente, e também de modo individual, a cada eleitor;
8. As **informações dos votos transitarão de forma cifrada** entre o dispositivo de votação (computador, celular, tablet) e o banco de dados da SIn-UFSCar e serão **armazenadas de também de forma cifrada** (ou seja, **ninguém conseguirá decifrar ou alterar essa informação**);
9. Cada eleitor(a) pode consultar as propostas dos candidatos no momento da votação;
10. **Depois votar, o(a) eleitor(a) recebe um token de garantia** que o voto foi depositado na urna e será computado;
11. Ao depositar o voto na urna (*click* de um *mouse*), **uma lista de presença é assinada eletronicamente**;
12. A **lista dos eleitores e a lista dos votantes é divulgada publicamente**. Os **nomes dos eleitores podem ser trocados por apelidos** que só o eleitor conhecerá. Assim, cada eleitor poderá verificar se seu voto está na lista de votantes e, portanto, sendo computado;
13. Após o término do período de votação, **a Comissão Eleitoral abre as urnas** e o **processo de apuração é feito de forma instantânea** (sem necessidade de transporte e nem de armazenamento de urnas);
14. É possível **verificar se a contabilidade dos votos corresponde a quantidade de assinaturas da lista de votantes**;
15. O processo de **criptografia** utilizado pelo Helios Voting **garante**: a) **que os votos não possam ser alterados no banco de dados sem que ocorra alteração dos códigos de rastreamento, detectável por auditoria** e b) **que todos os votos das urnas virtuais são computados**;
16. A Comissão Eleitoral gera relatório final com o resultado das eleições.

Exemplo: Votação para Escolha do Logotipo do CCET

Uma eleição foi criada para subsidiar a escolha do logotipo do Centro de Ciências Exatas e Tecnologia - CCET da UFSCar. A cédula ofereceu 5 opções de logotipo - p1, p2, p3, p4 e p5 - que podiam ser visualizados se o usuário acionasse a opção "mais informações" ao lado de cada opção. Também era oferecida a opção "não gostei de nenhuma das propostas" (Figura 10).

[sair]

Logotipo CCET (Urna dos Docentes)

(1) Marcar
(2) Revisar
(3) Depositar

Com qual opção você mais se identifica? (Lembramos que a cor institucional do CCET é o vermelho e a proposta vencedora terá as suas convertidas em tons de vermelhos)
questão 1 de 1 – você deve marcar no mínimo 1 e no máximo 1

- P1 [\[mais informações\]](#)
- P2 [\[mais informações\]](#)
- P3 [\[mais informações\]](#)
- P4 [\[mais informações\]](#)
- P5 [\[mais informações\]](#)
- Não gostei de nenhuma das propostas

Próximo passo

Código de Identificação da Eleição: 7SvGp11KOW6aRdCpN1M/EZGE68FbWY40ENW9gSyED3M [ajuda]

Figura 10: Resultados Percentuais - Total Geral - Sem Ponderação

Após o eleitor escolher sua opção e votar, recebe uma confirmação e um código, para rastreamento de seu voto (Figura 11).

Logotipo CCET (Urna dos Docentes)

Parabéns, seu voto foi **depositado com sucesso!**

O número do rastreador da sua cédula é: /YstUNA6xNMDnzdZnIAUMHDYqYOHHP/3QJLjHzBr63I

Você foi desconectado. Por favor, para sua segurança, feche seu navegador.

Figura 11: Confirmação de Voto e Código para Rastreamento - Logo do CCET

Para a escolha do Logo do CCET foram criadas 4 urnas: docentes, técnico administrativos (TAs), (estudantes da) Graduação e (estudantes da) Pós-Graduação.

Logotipo CCET (Urna dos Docentes)

por Paulo Matias

Logotipo CCET (Urna da Graduação)

por Paulo Matias

Logotipo CCET (Urna da Pós-Graduação)

por Paulo Matias

Logotipo CCET (Urna dos TAs)

por Paulo Matias

Figura 12: Urnas - Logo do CCET

Resultados da Votação para Escolha do Logo do CCET permanecem públicos, no [link votacao.ufscar.br](http://linkvotacao.ufscar.br).

Exemplo: Consulta sobre Voto Online

Um outro exemplo da utilização do Helios Voting UFSCar foi a própria consulta sobre voto online, já descrita na Seção 1 deste Relatório Técnico. Na Seção 1 foram apresentados a pergunta, as opções de resposta (a favor ou contra o voto online nas eleições da UFSCar), a lista de eleitores (apelidos) e votantes, com seus respectivos códigos rastreadores.

Resultados desta Consulta sobre Voto Online permanecem públicos, no [link votacao.ufscar.br](http://linkvotacao.ufscar.br).

Exemplo: Modelagem de uma Eleição para Representantes nos Conselhos Superiores

Para a realização de eleição de representantes dos discentes, técnico-administrativos e docentes no Conselho Universitário, poderiam ser criadas urnas separadas para:

- Eleição de Representantes dos discentes - graduação;
- Eleição de Representantes dos discentes - pós-graduação;
- Eleição de Representantes dos Servidores técnico administrativos;
- Eleição de Representantes dos Servidores Docentes
- Eleição de Representantes dos Servidores Docentes - associados;
- Eleição de Representantes dos Servidores Docentes - adjuntos;

- Eleição de Representantes dos Servidores Docentes - EBTT, Auxiliares e Assistentes.

Analogamente, para cada um dos demais Conselhos Superiores da UFSCar.

As cédulas poderiam indicar os nomes de cada um dos candidatos, bem como a unidade / curso, campus, e ainda, caso desejado, um *link* para suas propostas (como ocorreu na Votação para Escolha do Logo do CCET).

Parte II – É Seguro?

Condições de Segurança para o Uso de Voto Online em Eleições na UFSCar

A segurança do Helios Voting, bem como de sua instalação na UFSCar, é baseada nos seguintes princípios:

- A lista de votantes é definida, conferida e auditada por uma Comissão Eleitoral, e pode ser verificada publicamente também; A cada voto é atribuído um código rastreador, atrelado univocamente à cédula e que garante que o voto não foi alterado. Cada eleitor pode verificar se seu voto está sendo computado; É possível verificar se o total de votos corresponde à lista de votantes, por exemplo (Figura 13);
- A identificação dos usuários é feita por login e senha utilizados nos próprios sistemas da UFSCar - sistema de matrícula e digitação de notas, por exemplo (Figura 14);
- As informações dos votos transitam de forma cifrada, e são armazenadas de forma cifrada, o que impede a quebra do sigilo do voto mesmo que os pseudônimos sejam divulgados;
- O código fonte do sistema é totalmente aberto, e pode ser verificado por qualquer pessoa com conhecimento em programação;
- Pela lista de votantes é possível garantir que todos os votos estão sendo computados; pelos rastreadores de cédula embutidos nessa lista é possível garantir que os votos não serão alterados, pela criptografia é possível garantir o sigilo do voto; pelo código aberto é possível verificar que os cálculos estão sendo feitos corretamente e não estão sendo adulterados;
- Pela lista de eleitores em combinação com o login e senha pode ser garantido que somente os eleitores (membros da comunidade UFSCar) que estão na lista de votantes, poderão efetivamente votar;
- Uma Comissão Eleitoral, designada formalmente no Sistema, poderá acompanhar, avaliar, e nortear todo o processo: lista de eleitores, fechamento de urnas, apuração, etc.

Algumas destas características de segurança não podem ser obtidas nem em votações em papel, nem em votações nas urnas eletrônicas utilizadas no Brasil.

Eleitores 1 - 50 (of 1321) [próximo 50](#)

Pseudônimo	Rastreador da Cédula
V1	—
V10	—
V100	—
V1000	—
V1001	—
V1002	—
V1003	—
V1004	—
V1005	<i>NZDABMhefFWc5VjgOpjPAzNtfM1qOLHG4K0/ww8tMBs</i>
V1006	—
V1007	—
V1008	<i>43M485+SyXn/SBgLB2R6wxP93xJD67mFX8gcywrwE3U</i>
V1009	<i>ByugqJwFBpC7N77FEXBGcGn5tlcb/zAaLUU7dt85SB4</i>

Figura 13: Exemplo de Lista Indicando Apelidos, e Rastreadores dos Que Votaram



[Início](#) [Desconectar](#) [Ajuda](#)

Número UFSCar

Senha

Figura 14: Acesso à Cabine de Votação com Login e Senha dos Sistemas UFSCar

Um conjunto de dúvidas foi respondido, com a participação especial do Prof. Dr. Paulo Matias, docente da UFSCar, colaborador da Secretaria de Informática - SIn UFSCar, um dos responsáveis pela instalação do Helios Voting na UFSCar. O Prof. Paulo Matias é especialista

na área de segurança de votações. Foi convidado pelo TSE para participar de teste de segurança das urnas eletrônicas.

O que garante que meu voto não será alterado por um invasor, ou mesmo pelo pessoal interno da SIn?

Quando você vota no Helios, ele lhe informa um código chamado "rastreador de cédula", que nada mais é que uma versão cifrada do seu voto. O seu "rastreador de cédula" fica público, assim como o de todos os eleitores. Assim, você pode conferir, ao final da votação, que o seu "rastreador" permanece igual ao que era no momento em que você depositou o voto.

Quando a comissão abre as urnas, a soma de todos os "rastreadores de cédula" é decifrada. O método que o Helios utiliza para cifragem permite que o cálculo dessa soma seja auditado publicamente, com garantias criptográficas de que ele está correto.

Dessa forma, o "rastreador de cédula" funciona como um comprovante de que o seu voto realmente foi depositado e de que foi corretamente contabilizado na apuração. Na literatura sobre votação eletrônica, esse processo é chamado de "verificação fim-a-fim", porque não depende da segurança do sistema que está no meio, ou seja, do servidor que hospeda o site. Esse mecanismo faz com que o Helios forneça garantias no quesito de integridade dos votos que não existem, por exemplo, na urna eletrônica brasileira.

Existem outros sistemas de votação on-line? Por que a escolha pelo Helios?

O Helios é um sistema verificável fim-a-fim, totalmente livre e de código aberto. Existem vários outros sistemas. Alguns deles são verificáveis fim-a-fim, já outros dependem de confiança na proteção do servidor que hospeda o site. Por exemplo, o sistema Safevote (<http://safevote.com>) permite verificação fim-a-fim, no entanto é um produto de código fechado e exige a compra de licenças. Outros sistemas, como o SigEleição (<https://sigeleicao.ufrn.br>), da UFRN, e o ElectionBuddy (<https://electionbuddy.com>), de uma empresa chamada RightLabs, também são usados por algumas instituições, mas não permitem verificação fim-a-fim, portanto julgamos que não atenderiam os critérios de segurança para a UFSCar.

Se o "rastreador de cédula" é público, a escolha que eu fiz na votação também ficará pública? Trata-se de votação por aclamação?

Não, o "rastreador de cédula" é cifrado, e só pode ser decifrado reunindo todas as chaves de apuração cadastradas no sistema Helios. Quando a urna é aberta, cada chave é utilizada em uma etapa de decifração que obrigatoriamente embaralha os votos fornecidos como entrada. Assim, é possível verificar que a decifração está correta, mas não a ordem original de quem votou em quem.

Quem ainda não votou vai aparecer sem "rastreador de cédula" na lista de votantes. Isso não revela quem já votou e quem ainda não votou?

O Helios pode ser configurado para que cada eleitor seja identificado apenas por um pseudônimo (apelido) na lista pública de eleitores / votantes, evitando que os candidatos abordem os eleitores que ainda não votaram ("boca de urna direcionada").

O Helios é impossível de ser atacado?

Não. O Helios foi proposto em um artigo científico [1] publicado em 2008 no congresso USENIX, um dos mais importantes da área de segurança. Desde então, vários trabalhos da literatura têm proposto ataques contra o Helios. No entanto, todos os ataques propostos até o momento foram corrigidos ou mitigados pelos desenvolvedores.

Por exemplo, um dos ataques propostos na literatura [2] consistia em desenvolver um software malicioso especialmente projetado para desviar votos em uma certa votação. Esse software era instalado no computador dos eleitores por meio de técnicas tradicionais de infecção utilizadas por vírus e outros tipos de software malicioso. Por mais que esse ataque tenha elevado grau de complexidade, os desenvolvedores do Helios introduziram um recurso de auditoria da cédula para mitigá-lo, permitindo que o eleitor faça o cálculo da versão cifrada do voto em vários computadores diferentes, com a finalidade de conferir o resultado caso suspeite que seu computador possa estar infectado.

Se alguém ficar me observando enquanto eu voto, o Helios protege o sigilo do voto?

O Helios protege o sigilo da melhor forma que se considera ser possível para uma votação online. Ele permite que o eleitor troque o voto quantas vezes quiser até o final da votação, sendo que apenas a última escolha feita pelo eleitor vale para a apuração.

O sistema permite ao usuário votar mais de uma vez. Isso significa que um mesmo eleitor pode depositar vários votos na urna?

Não. Apenas o último voto é efetivamente computado. Funciona como uma urna em que você pode apertar o botão CORRIGE a qualquer momento, durante todo o período designado para votação.

Como o sigilo do voto é garantido? Não é possível, a partir do rastreador de cédula, saber em quem uma determinada pessoa votou?

O sigilo é garantido pois o voto é cifrado. Não é possível identificar o voto a partir do rastreador.

Esse sistema foi desenvolvido pela SIn? Quem o utiliza?

Foi desenvolvido por Ben Adida, inicialmente durante seu pós-doutorado e depois como membro do corpo docente em Harvard. O código é aberto; a SIn fez uma instalação local do sistema. O Helios é utilizado, por exemplo, pela USP, Unicamp, Princeton e Harvard (veja a Seção 2 deste relatório para mais exemplos de usuários).

Existe outros sistemas de votação on-line? Por que a escolha pelo Helios?

Sim, existem outros, conforme comentado acima. O Helios foi escolhido por proporcionar as melhores características de segurança, por ter código aberto, verificação fim-a-fim, e por estar em constante desenvolvimento. Isso permite que o código fonte evolua contra ataques cibernéticos que possam surgir no futuro.

Alguém da SIn com acesso ao banco de dados poderia adulterar a eleição?

Não, pois qualquer adulteração alteraria os rastreadores de cédula, fato que seria detectado no processo de auditoria.

Como é garantido que todos os eleitores poderão votar, e que somente os eleitores poderão votar, no Helios Voting UFSCar?

Pela lista de votantes, aferida pela Comissão Eleitoral. Além disso, é possível realizar testes (de senha, etc.) previamente ao período de votação.

Como é garantido que o voto de um eleitor não será computado mais que uma vez? Como é garantido que todos os votos serão computados?

Pela lista de votantes - total de votos.

Como é garantida a inviolabilidade da votação, ou seja, de que não haverá invasão do sistema para alteração nos resultados?

Os mesmos mecanismos que impedem a SIn de adulterar a eleição também impedem que um invasor adultere. Qualquer alteração dos votos é detectável, pois causaria mudança dos rastreadores de cédula.

Como é garantido que os resultados serão apurados corretamente?

Tanto o código como as especificações de criptografia são abertas. Como o código é aberto, ele pode ser verificado. Como as especificações são abertas, todos os cálculos podem ser conferidos fora do sistema, por programas escritos de forma independente.

Referências

[1] ADIDA, B. Helios: web-based open-audit voting. In: USENIX security symposium, 17., 2008, San Jose. *Proceedings...* Berkeley: USENIX, c2008. p. 335-348.

[2] ESTEHGHARI, S.; DESMEDT, Y. Exploiting the client vulnerabilities in Internet e-voting systems: hacking Helios 2.0 as an example. In: Electronic Voting Workshop / Workshop on Trustworthy Elections, 10., 2010, Washington. *Proceedings...* Berkeley: USENIX, c2010.

Parte IV – É Juridicamente Possível?

Análise Legal e de Regimentos Internos

Para analisar a viabilidade jurídica do uso do voto online nas eleições da UFSCar, esta Comissão Técnica estudou a legislação, os regimentos internos, e realizou Consulta Específica à PF-UFSCar inquirindo sobre a viabilidade jurídica de utilizar voto online nas eleições da UFSCar, à luz do Decreto 8.539/2015.

O Parecer n. 00082/2018/CONS/PFFUFSCAR/PGF/AGU, em seu artigo 28, conclui:

"Do exposto, do ponto de vista jurídico não nos parece haver impossibilidade de realização de eleição eletrônica ou online para representantes de quaisquer dos conselhos superiores da UFSCar".

O parecer revisita entendimento anterior, prestado no Parecer Nº 366/2017/PF-UFSCar / PGF / AGU, agora à luz do Decreto 8.539/2015, e justifica a conclusão do item 28 acima transcrita através dos itens 25 e 26 do Parecer:

25. Nesse sentido, por certo que os conceitos de cédula e de urna, para além da noção tradicional de, respectivamente, "documento em papel com o nome dos candidatos e no qual o eleitor assinala seu voto" e "caixa onde depositadas as cédulas de votação", admitem a correspondente versão eletrônica ou mesmo virtual. O mesmo se diga de "local previamente designado e divulgado pela Comissão Eleitoral" que pode ser, para além de lugar físico, um sítio na internet. E também, no ato da votação, o comparecimento "munidos de documento de identificação" e a assinatura de lista de votantes são atos que admitem claramente a realização de forma telemática.

26. Destarte, reanalisando o Regimento Interno do ConsUni (Resolução ConsUni nº 795/2014) e o Regimento Interno do CoAd (Resolução CoAd nº 80/2015), parece que os respectivos capítulos sobre o processo eleitoral podem ter suas disposições interpretadas para que, alternativamente à eleição procedida por meio físico ou tradicional, também seja admitida a eleição eletrônica ou online.

Vale também transcrever aqui que o parecer 81/2018/CONS/PFFUFSCAR/PGF/AGU em seu item 23 deixou explícito o entendimento sobre o Art 25 do Regimento Geral da UFSCar, afirmando que o uso da votação eletrônica "não encontra óbice algum na legislação de regência, em especial na disposição constante do art 25 do Regimento Geral, o qual se dá no sentido de garantir a que a eleição seja escoreita independentemente do meio eletrônico ou tradicional utilizado".

Anexamos a este Relatório Técnico a íntegra do Parecer 82/2018/CONS/PFFUFSCAR/PGF/AGU.