O uso de um sistema de votação on-line para escolha do conselho universitário

Shirlei Aparecida de Chaves[1] **, Emerson Ribeiro de Mello**[1]

[1]Instituto Federal de Santa Catarina – SC –Brasil

{shirlei.chaves, mello}@ifsc.edu.br

Resumo. *A necessidade de uma participação ampla e democrática em pleitos realizados pela instituição de ensino multicampi exigia que problemas como o deslocamento de pessoas da comissão eleitoral e urnas para os municípios onde houvesse um campus ou polo de Educação à Distância, bem como a realização da apuração, não fossem impeditivos para a efetividade do processo. Este trabalho apresenta os requisitos que culminaram na escolha do sistema Helios, a personalização realizada para adequá-lo às necessidades da instituição, os resultados de seu uso na eleição do conselho universitário e os trabalhos futuros para que o mesmo possa ser ofertado como um serviço de tecnologia da informação à comunidade.*

Abstract. *The need for a broader and democratic participation in elections conducted by a multi-campi education institution demanded that issues like travel of election commission members and taking voting booth to several campuses, as well as tallying the results, did not become an obstacle to the process effectiveness. This paper presents the requirements to chose the Helios Voting System, the customisations performed in this system, the results from using it in an important election process. Our future work aim to deliver it as a technology information service to the community.*

1. Introdução

No Brasil, instituições federais de ensino são compostas basicamente pelos segmentos discente, docente e técnico-administrativo. O reitor é o cargo mais alto dentro da instituição, nomeado pelo Presidente da República para um mandato de 4 anos, após processo de consulta à comunidade interna. Como esta consulta é conduzida, depende do estatuto de cada instituição.

Ao reitor compete representar externamente a instituição, bem como administrar e superintender as atividades da mesma. Contudo, as instituições também definem em seus estatutos órgãos colegiados, como o Conselho Universitário (para as Universidades) ou Conselho Superior (para os Institutos). Este colegiado é um órgão máximo da instituição e possui caráter normativo, consultivo e deliberativo. Sua composição varia de instituição para instituição, porém é comum a todas que haja pelo menos um membro de cada segmento da comunidade interna (discentes, docentes, técnicos-administrativos), geralmente escolhidos por seus pares.

Recentemente essas instituições de ensino passaram por uma expansão e novos campi foram criados. Se até a década de 70 as instituições federais eram criadas com

um único campus por instituição, hoje algumas instituições surgem com vários campi, ou seja, vários endereços físicos espalhados pelo estado, ou mesmo, espalhados por alguns estados da federação.

Em uma instituição multicampi, o processo eleitoral tradicional para a escolha do reitor ou outro pleito de grande proporção, com cédulas em papel depositadas em urnas lacradas, torna-se mais complexo e custoso se comparado com instituições com único endereço. A distribuição das urnas, o deslocamento de pessoas da comissão eleitoral para cada um dos campi, o retorno das urnas e a apuração em si, são os principais pontos dificultadores para a realização do pleito.

Em 2011, o Instituto Federal de Santa Catarina - IFSC, deflagrou o processo eleitoral para escolha de seu reitor. Por possuir pólos de Educação a Distância (EaD) em outros estados e devido a eleição em questão ter tido candidato único, o pleito teve que ser realizado com cédulas em papel e urnas tradicionais, pois o Tribunal Regional Eleitoral (TRE), impõe as seguintes regras para uso da urna eletrônica brasileira: (1) solicitar ao TRE com uma antecedência mínima de 90 dias; (2) as urnas devem ser usadas exclusivamente dentro do estado; e (3) a disputa deve ter no mínimo dois candidatos. Apesar de neste caso o uso da urna eletrônica brasileira trazer alguns benefícios, principalmente para a apuração, ainda assim haveria a problemática de deslocamento de fiscais, servidores do quadro permanente da instituição, para todos os pólos no dia da eleição.

No IFSC, o mandato dos membros do Conselho Superior é de 2 anos e estes são escolhidos por seus pares através de um processo eleitoral. No início de 2012 em razão da dificuldade dos discentes organizarem o seu processo eleitoral, conforme prevê o estatuto, o Conselho Superior resolveu que a escolha se daria por meio de sorteio dos discentes inscritos. Contudo, a instituição comprometeu-se atuar para que nas próximas eleições os representantes discentes fossem escolhidos através de um processo eleitoral. Sendo assim, para 2014 a instituição precisaria conduzir um processo eleitoral que permitisse a toda sua comunidade interna eleger seus pares, o que inclui os alunos dos pólos de Educação a Distância.

Este trabalho apresenta os motivos pela instituição ter optado pelo sistema de votação *on-line* Helios [Adida 2008] para realizar a eleição dos representantes discentes, docentes e técnico-administrativos do Conselho Superior, bem como a personalização realizada para adequar com as necessidades da instituição, questões sobre a mudança de paradigma e os resultados obtidos.

O artigo está organizado da seguinte forma. Na Seção 2 é apresentado um relato das experiências de outras instituições de ensino na condução de seus processos eleitorais. A Seção 3 apresenta as premissas de uma eleição e diferentes tecnologias para a realização do pleito. A Seção 4 apresenta a arquitetura e as funcionalidades do sistema Helios. Na Seção 5 é apresentado o relato sobre como foi realizada a primeira eleição para escolha dos membros Conselho Superior fazendo uso de um sistema de votação *on-line*. Por fim, na Seção 6 são apresentadas as conclusões e os trabalhos futuros.

2. Experiências na literatura

Em 2011 a Sociedade Brasileira de Computação (SBC) decidiu por fazer uso do software livre para votação *on-line Helios Voting* [Adida 2008], para a escolha da Diretoria e do

Conselho da SBC para o biênio de 2011/2013. Na ocasião, estavam aptos a votar 1.757 sócios, sendo estes pertencentes a categoria sócio fundador ou efetivos, quites com a anuidade de 2011 até a data de trinta de março de 2011. Destes somente 783 de fato registraram seus votos, uma vez que o voto não era obrigatório [Pôrto et al. 2011].

A SBC também usou o Helios para escolha de seu estatuto em 2012 e novamente para escolha de sua diretoria e conselho para o biênio 2013/2015. Apesar do Helios ser oferecido na modalidade *Software as a Service* (SaaS), a SBC optou por fazer uma instalação local da solução. De acordo com observações feitas pelos autores do presente trabalho, não foram feitas personalizações no código de referência do Helios para adequá-lo a qualquer necessidade da SBC. Segundo [Cunha et al. 2013], a atual diretoria administrativa da SBC vislumbra comercializar o Helios como um serviço para outras entidades.

O sistema *Helios Voting* também foi usado pela Defensoria Pública da União para escolha do atual defensor público-geral federal. A interface com o usuário foi adaptada pela equipe do Laboratório de Tecnologias da Tomada de Decisão (Latitude) da Universidade de Brasília (UnB), permitindo que os 521 defensores públicos de todo o Brasil pudessem registrar suas escolhas por meio de qualquer dispositivo conectado à Internet [UNB 2013].

A Universidade Federal do Rio Grande do Norte (UFRN) fez uso do SIGEleição, um sistema desenvolvido internamente, em diversas eleições, entre estas a escolha de chefes de departamentos, do diretório central de estudantes e inclusive para consulta sindical de ajustes salariais. Segundo [UFRN 2012, PortalJH 2012], a facilidade e a possibilidade de ampliação da participação da comunidade foram os principais motivos para usar um sistema *on-line*.

Foi realizada uma pesquisa no mecanismo de busca do Google, para se verificar como as Universidades e os Institutos Federais realizaram a eleição do Conselho Universitário ou Conselho Superior nos últimos dois anos. Considerando-se os critérios citados, para facilitar a pesquisa, foram montadas duas *strings* de busca: `(("Instituto Federal") AND ("eleição"OR "eleições") AND "Conselho Superior"AND ("2013"OR "2014"))` para os Institutos Federais; e `(("Universidade Federal") AND ("eleição"OR "eleições") AND "Conselho Universitário"AND ("2013"OR "2014"))` para as Universidades Federais. Foi considerada até a terceira página de resultados.

Dos resultados da busca efetuada para os Institutos Federais, constatou-se, através dos editais de convocação, que os Institutos IFSP, IFF, IFAL, IFB, IFPE, IFPA, IFES, IFBaiano, IFAM, IF Sertão-PE, IFTM, IFGoiano e IFMS realizaram eleições com cédulas de papel. O IFTO e o IFBA fireram uso da Urna Eletrônica Brasileira, cedida pelo TRE.

No caso das Universidades, daquelas que foi possível extrair tal informação, constatou-se que sete delas (UFES, Unipampa, UFPel, UFFS, Unila, UFRR e UFV) realizaram a eleição através de cédulas de papel. Segundo [UFPA 2012], Universidade Federal do Pará (UFPA) fez uso do sistema SIGEleição. E a Universidade Federal do Rio Grande do Sul (UFGRS) fez uso de um sistema próprio de votação *on-line*.

3. Sistemas de votação eletrônica

Em 2012 a escolha dos membros docentes e técnico-administrativo do Conselho Superior (CONSUP) do IFSC foi realizada por meio de cédulas de papel e urnas de lona, porém os membros discentes foram escolhidos por meio de sorteio dos candidatos inscritos, como apresentado na Seção 1.

Para 2014 a instituição precisaria oferecer uma solução que permitisse aos discentes escolherem seus representantes no CONSUP através de uma eleição direta. Diante da dificuldade de realizar o certame da maneira convencional, com cédulas de papel e urnas de lona, foram realizados estudos para identificar um sistema de votação eletrônica que atendesse os seguintes requisitos:

- R.1 Só poderão votar os eleitores que forem considerados aptos pela comissão eleitoral;
- R.2 Cada eleitor só terá direito a um único voto por segmento que este estiver apto a votar (docente, discente e técnico-administrativo);
- R.3 A escolha do eleitor deve ser mantida em sigilo. Ninguém poderá saber em quem o eleitor votou, mesmo se este quiser revelar (p.e. apresentando um recibo de votação);
- R.4 A solução e o resultado da eleição devem ser auditáveis. A integridade dos votos deve ser garantida, ninguém poderá alterar, incluir ou remover votos;
- R.5 A solução deve ser economicamente viável, tanto para sua aquisição ou implantação, quanto para realização do pleito;
- R.6 A solução deve ser de fácil uso por eleitores e pela comissão eleitoral;
- R.7 Não permitir a realização de apurações parciais antes do término da eleição, visando assim garantir as mesmas chances para todos os candidatos e evitando a possibilidade de revelar escolhas de eleitores individuais.

Segundo [POST 2001], existem três tipos principais de sistemas de votação eletrônica:

Máquina de votar de gravação eletrônica direta do voto
: Eleitor faz uso de teclado ou monitor sensível ao toque para fazer suas escolhas e estas são registradas diretamente na máquina;

Contagem de cédulas realizada por máquina
: Eleitores marcam suas escolhas em cédulas de papel e as mesmas são digitalizadas para fazer a leitura ótica;

Sistemas on-line
: Eleitores poderão ir a um local físico para votar ou poderão fazer uso de qualquer computador conectado à Internet. As escolhas dos eleitores são transmitidas diretamente pela Internet para um sistema central da eleição.

A urna eletrônica brasileira é um tipo de máquina de votar de gravação eletrônica direta do voto (*Direct Record Electronic* – DRE). Seu uso na referida eleição teria como benefícios a facilidade de uso, agilidade na apuração e o fato que a maioria dos eleitores já estarem habituados com a mesma. Ou seja, muitos confiam na integridade deste equipamento, apesar de estudos apontarem fragilidades na solução [Kohno et al. 2004, Dill et al. 2003]. De qualquer forma, esta opção foi desconsiderada,

uma vez que o Tribunal Regional Eleitoral de Santa Catarina, em resposta ao ofício enviado pelo IFSC, indicou que as urnas só poderiam ser usadas dentro do estado, o que não permitiria levá-las para os pólos EaD fora do estado.

A contagem de cédulas realizada por máquina, como é visto no sistema de votação Scantegrity [Chaum et al. 2008], apesar de impor uma maior confiança ao eleitor, uma vez que atende o "princípio da independência do software em sistemas de votação" [Rivest 2008], não apresentou ser economicamente viável (requisito R.5) para a eleição em questão, pois seria necessário adquirir ou alugar equipamentos digitalizadores específicos e estes teriam que ser enviados para todos os campus e pólos EaD.

A possibilidade dos eleitores fazerem suas escolhas por meio de qualquer computador conectado à Internet, tornam os sistemas de votação *on-line* atrativos para a realização de eleições não-políticas [Qadah and Taha 2007]. Em buscas por soluções que atendessem o requisito R.5, chegou-se às seguintes opções:

Sistema Aberto de Eleições Eletrônicas (SAELE)
: Desenvolvido pela Universidade Federal do Rio Grande do Sul, trata-se de um software livre disponível no portal de software público brasileiro;

SIGEleição
: Desenvolvido pela Universidade Federal do Rio Grande do Norte, o SIGEleição[1] faz parte do Sistema Integrado de Gestão, também desenvolvido pela UFRN. Apesar de não estar sob uma licença de software livre, todo o código fonte é fornecido para instituições que firmarem acordo de cooperação com a UFRN;

Helios versão 3
: Segundo seu autor [Adida 2008], trata-se do primeiro sistema de votação *on-line* baseado na *web* e com auditoria aberta ao público (*End-to-End voter verifiable* – E2E), permitindo que:
  - Alice verifique que seu voto foi capturado;
  - Todos os votos capturados sejam exibidos publicamente em sua forma criptografada;
  - Qualquer um possa verificar que os votos capturados foram corretamente apurados.

Após análise dos códigos do SAELE e SIGEleição, conclui-se que ambos não fornecem garantias necessárias para atender os requisitos R.3 e R.7, e atendem parcialmente o requisito R.4. Os votos são registrados em claro no banco de dados e o resultado de uma eleição estaria passível de adulteração, sem gerar provas necessárias para uma auditoria.

Por outro lado, o Helios faz uso de mecanismos criptográficos para prover uma solução simples, baseada na *web* e que permite a qualquer um verificar a integridade de uma eleição, mesmo se a instalação do Helios estiver completamente comprometida [Adida 2008, Joaquim et al. 2013].

Com o Helios é possível carregar a lista de eleitores de uma eleição através de um arquivo CSV[2] no formato (login, e-mail, nome completo), contemplando o requisito R.1. O requisito R.2 também é satisfeito, pois é possível criar e conduzir ao mesmo tempo quantas eleições se desejar.

[1] https://www.sigeleicao.ufrn.br/sigeleicao

[2] *Comma-separated values*

A cédula de uma eleição pode ser acessada e preenchida por qualquer um que tiver o endereço da eleição. O eleitor pode fazer suas escolhas e o sistema cifra a cédula diretamente no navegador *web*, fazendo uso de rotinas em *javascript*. A autenticação do eleitor só é exigida no momento que este for depositar a cédula na urna. O Helios ou mesmo um atacante, não teria como descobrir as escolhas que o eleitor fez[3]. Neste ponto, pode-se deduzir que durante a transmissão da cédula pela rede, o requisito R.3 estaria sendo atendido, pois haveria proteção contra interceptação do tráfego entre o computador usado pelo eleitor e o Helios, tendo em vista que a cédula estaria cifrada e sabendo ainda que o Helios estaria sendo executado sobre o SSL/TLS.

Segundo [Jonker et al. 2013], a versão 3 do Helios apresentou algumas melhorias para lidar com ataques contra a privacidade das versões anteriores. A atual versão do Helios faz uso de criptografia homomórfica [Rivest et al. 1978], o que permite apurar todos os votos cifrados (conhecer o resultado da eleição), sem que nenhuma parte possa revelar as escolhas em cada voto individual. Sendo assim, depois da cédula depositada, ninguém poderia descobrir as escolhas do eleitor, mesmo que tenha acesso a base de dados do Helios. Isto atende o requisito R.3. Cabe frisar que o Helios foi projetado para eleições com baixo risco de coação dos eleitores, sendo este o cenário da eleição em questão, a qual é uma eleição não política conforme descrito em [Qadah and Taha 2007].

Segundo [Adida 2008, Joaquim et al. 2013], com o Helios o eleitor pode verificar que seu voto foi corretamente registrado; todos os votos (em sua forma cifrada) podem ser vistos por qualquer um; e qualquer um poderá verificar se todos os votos registrados foram corretamente apurados. E por ainda ser software livre e por fornecer documentação técnica[4] necessária para validação, pode-se afirmar que a solução atende o requisito R.4.

O Helios faz uso de criptografia de limiar [Shamir 1979] no processo de apuração. Assim, vários pessoas podem ser cadastradas como apuradores e todas precisam atuar em conjunto para realizar a apuração. Isto impõe um dificultador para a quebra do sigilo do voto dos eleitores, o que contempla o requisito R.7.

Os trabalhos [Karayumak et al. 2011, Weber and Hengartner 2009] avaliaram a usabilidade do Helios, sendo este ponto o menos favorável para a solução. As críticas estão voltadas para a interface que apresenta termos técnicos ligados a criptografia e o uso de rotinas em *javascript*, que dependendo do computador e do navegador *web* do eleitor, podem dificultar o processo para depositar a cédula na urna.

De todos os requisitos apresentados nesta seção (R.1 a R.7), pode-se afirmar que o Helios não atende plenamente o R.6 e precisaria de melhorias em sua interface com o usuário, seja este um eleitor ou o administrador de uma eleição. Desta forma, optou-se pelo Helios como o sistema de votação *on-line* a ser usado na eleição para escolha dos membros do Conselho Superior no IFSC. A Seção 4 apresenta o trabalho desenvolvido para melhorar a usabilidade do sistema, além de outras personalizações.

[3]Assumindo que não exista qualquer *software* malicioso hospedado e em execução no computador do eleitor.

[4]http://documentation.heliosvoting.org/verification-specs/helios-v3-verification-specs

4. Personalização e melhorias no sistema de votação Helios

O código fonte do Helios está disponível no Github e pode-se observar que seu desenvolvimento continua ativo[5]. Para o desenvolvimento de qualquer melhoria no Helios deve-se levar em consideração este fato, pois caso contrário as melhorias realizadas poderiam inviabilizar a atualização para futuras versões do projeto original do Helios.

Diante do exposto foi criada uma ramificação[6] (*fork*) do projeto original. Como o Git permite que se informe qual é o projeto base desta ramificação, então é possível fazer um realinhamento com o código do projeto base sempre que for desejado, por exemplo, quando são lançadas novas versões do Helios. Durante o desenvolvimento deste trabalho foi necessário realizar dois realinhamentos, os quais resultaram em alguns poucos conflitos de código, mas que puderam ser corrigidos facilmente.

A interface *web* do Helios, vista por eleitores e administradores de eleições, foi desenvolvida na linguagem Python, fazendo uso do *framework* Django, e combinada com rotinas em Javascript, estas usadas para garantir que processos de criptografia sejam realizadas diretamente no navegador do usuário e não no servidor onde o Helios está hospedado. A arquitetura do Helios é composta por quatro grande componentes [Adida 2008]:

Administrador da Eleição – Página *web* usada por usuários para criarem e gerenciarem suas eleições, informando as questões que farão parte da eleição, a lista de eleitores, a lista de apuradores, envio de e-mail para eleitores e apuradores, etc;

Cabine de Votação – Página *web* pra que os eleitores possam fazer suas escolhas, se autenticarem e por fim, depositarem sua cédula na urna, ou seja, submeter suas escolhas para o servidor onde o Helios está hospedado;

Servidor de depósito de cédulas – Responsável por receber e computar as cédulas recebidas. Trata-se de um processo executado no servidor onde o Helios está hospedado;

Centro de auditoria – Página *web* que permite a qualquer usuário auditar todas as partes da eleição. Se uma eleição já estiver encerrada, o centro permite ao usuário baixar todas as cédulas daquela eleição e realizar localmente a apuração.

As subseções a seguir apresentam os motivos e as melhorias que foram desenvolvidas nestes componentes.

4.1. Tradução de interface e usabilidade

O *framework* Django fornece suporte à internacionalização[7], contudo os componentes *web* do Helios não foram codificados para usufruir desta funcionalidade e, por consequência, não oferecem qualquer facilidade que permita traduzir as mensagens das interfaces com o usuário. Outros componentes se quer possuem suporte à internacionalização, como é o caso da Cabine de Votação, cujos os respectivos arquivos HTML são servidos estaticamente pelo servidor *web* e não passam pelo processador de modelos do Django.

Embora seja possível fazer a marcação de todas as *strings* que aparecem na interface do usuário (eleitor ou administrador), para depois relacioná-las com arquivos

[5]https://github.com/benadida/helios-server/graphs/contributors

[6]https://github.com/shirlei/helios-server

[7]Adaptação das mensagens de um sistema para diferentes línguas.

de tradução do Django, ainda assim não atenderia todas as partes do sistema, p.e. Cabine de Votação. Sendo assim, optou-se neste primeiro momento por uma solução mista. Onde era possível utilizar as facilidades do Django para tradução, o mecanismo de internacionalização do mesmo foi utilizado (maior parte do sistema). Onde não era possível (Cabine de Votação), a tradução foi feita diretamente nos documentos HTML e nas rotinas Javascript dos mesmos.

Conforme apresentado na Seção 3, a usabilidade é o ponto menos favorável do Helios. Para contornar essa questão, uma das medidas tomadas foi a de, durante a tradução, adaptar o texto para ficar mais amigável ao usuário, pois o texto original tinha como principal objetivo apresentar uma explicação sobre como os requisitos de segurança estão sendo garantidos pelo sistema.

A interface de gerenciamento de eleições foi reorganizada, de modo a facilitar a visualização de ações a serem tomadas. Também iniciou-se processo de utilização do Bootstrap[8] como *framework* de desenvolvimento da interface. Este fornece diversas facilidades para tratamento de estilos de elementos comuns como formulários e botões, além de *plugins* Javascript para menus e ainda, é preparado para operar com *layouts* responsivos, ou seja, que adequam a apresentação da página *web* de acordo com o tamanho da tela do dispositivo do usuário.

4.2. Módulo super administrador

Na forma como o Helios é oferecido em seu sítio *web*, qualquer pessoa pode usar o sistema para criar e gerenciar suas próprias eleições, para isto basta que possua uma conta de usuário em um dos serviços: Google, Facebook ou Yahoo. No caso tratado por este artigo, foi realizada uma instalação local do sistema e tinha-se como necessidade garantir que somente usuários autorizados previamente pudessem criar e gerenciar suas eleições.

O *framework* Django trabalha com o conceito de aplicativos Django (*django apps*), ou seja, componentes de software com regras bem definidas e auto contidos. A instalação padrão do Django possui diversos aplicativos, entre estes o *admin app*. Este aplicativo fornece uma interface automática de administração a qual permite ler metadados dos modelos de projeto, bem como inserir conteúdo nestes modelos. Por padrão este módulo está desabilitado no Helios.

Com a habilitação deste módulo e com algumas modificações, foi possível criar uma área chamada de "super administração". Voltado para a equipe de administração do serviço Helios, este módulo oferece funcionalidades para inserir, alterar e remover usuários da lista de autorizados a gerenciar eleições no sistema.

Como informado na Seção 3, o Helios é um sistema de eleição *on-line* totalmente verificável, porém a auditoria se resume nas informações da própria eleição e não abrange questões, como por exemplo, sobre como e quando o sistema foi acessado pelo administrador de uma eleição.

No portal do super administrador foi criada uma área de auditoria para registrar as ações tomadas pelo administrador de uma eleição. O código padrão do Helios permite ao administrador de uma eleição, enquanto esta estiver aberta, adicionar ou remover eleitores da lista de eleitores aptos a votar. Com o centro de auditoria desenvolvido neste trabalho,

[8] http://getbootstrap.com

toda ação administrativa de remoção de eleitor é registrada, e cada registro contém dados sobre qual eleitor foi removido, data e hora da ação e qual administrador fez tal ação.

Nas modificações realizadas incluiu-se também características relativas ao registro dos votos depositados pelos eleitores. No caso, o Helios registrava, além do voto, a data e a hora do mesmo. Adicionalmente passou-se a registrar também o endereço IP do computador usado pelo eleitor. Estas informações foram disponibilizadas na interface do super administrador.

Cabe frisar que tais registros não ferem a privacidade dos eleitores, pois não é possível através destes determinar em quem o eleitor votou. O objetivo desta funcionalidade é para gerar uma ferramenta de investigação que possa ser usada diante de uma possível disputa. Por exemplo, verificar se um mesmo computador foi usado para registrar vários votos em um curto espaço de tempo, podendo assim caracterizar coação de um conjunto de eleitores.

4.3. Autenticação de usuários no serviço de diretórios LDAP

Primeiramente, é importante destacar que o Helios não permite o voto anônimo, ou seja, todo eleitor deve passar por um processo de autenticação para provar sua identidade. Ao criar uma eleição é possível indicar se a mesma é uma eleição fechada, isto é, só poderão votar os eleitores que foram carregados através de um arquivo CSV, ou se é uma eleição aberta, isto é, poderá votar qualquer pessoa que consiga se autenticar através dos mecanismos que o Helios provê suporte.

Como optou-se por fazer uma instalação local do Helios e os administradores de eleições deveriam ser obrigatoriamente servidores públicos da instituição, a opção de autenticar através de serviços como Google, Facebook e Yahoo foi considerada inadequada. O mesmo para as eleições públicas, pois é desejado que somente pessoas que possuam credenciais da instituição possam votar.

A instituição possui um serviço de diretórios LDAP [Wahl et al. 1997] o qual é usado por todos os sistemas de informação. Sendo assim, o Helios precisaria também autenticar seus usuários através do LDAP.

O Helios provê um módulo de autenticação que inicialmente só permite autenticação através de nome de usuário e senha, armazenados em uma base local, e através do OAuth [Hammer-Lahav 2010], usado para Google, Facebook e Yahoo. Este módulo foi então estendido para permitir a autenticação de usuários, eleitores ou administradores, presentes em uma base LDAP.

5. Condução e resultados da eleição com sistema de votação *on-line*

A mudança de paradigma é algo que pode gerar resistência por parte dos envolvidos. Visando minimizar uma possível resistência ou mesmo questionamento sobre a lisura do processo, fora apresentado para o Comitê Gestor de Tecnologia da Informação e para a Comissão Eleitoral, o funcionamento do sistema, suas características e também uma analogia com a votação por meio de cédulas de papel, sobre as fases de uma eleição, que são: identificação dos eleitores, votação e apuração.

O Conselho Superior possui representantes dos segmentos discente, docente e técnico administrativos em educação, sendo estes eleitos por seus pares. Optou-se por

criar uma eleição para cada segmento, carregando para cada um arquivo CSV com a lista de eleitores aptos a votar. Estas listas foram geradas a partir de extração dos sistemas de informação da instituição e tornadas públicas no sítio *web* (*hot site*) da eleição, de forma que os interessados pudessem entrar em contato com a comissão e sugerir correções.

O trabalho de criação das eleições foi conduzido pela equipe de TI em conjunto com os membros da comissão eleitoral. O Helios permite determinar um número mínimo e máximo de respostas para cada questão. Ao invés de se considerar a opção de resposta mínima igual a zero, para englobar brancos e nulos, a comissão optou por explicitamente criar uma opção de resposta BRANCO e uma opção NULO. Desta forma, as questões foram configuradas para que o eleitor escolhesse no mínimo uma e no máximo uma resposta.

Para todas as eleições foi feito uso de pseudônimos para os eleitores e foram adicionados três apuradores, estes escolhidos entre os membros da comissão eleitoral. O par de chaves criptográficas de cada apurador foi gerado naquela ocasião, sendo que a chave privada de cada apurador foi salva em um pendrive diferente e entregue ao apurador em questão.

Ciente que seria necessário ter a chave dos três apuradores para abrir a urna e apurar os votos, uma cópia da chave privada de cada apurador também foi salva em um pendrive backup, o qual foi colocado dentro de um envelope que depois foi lacrado e assinado pelos membros da comissão. Este procedimento foi adotado como medida de segurança, caso um dos apuradores viesse a perder seu pendrive.

Nas eleições anteriores, com urna de lona, era dedicado um único dia para realizar a votação. Por esta solução depender da infraestrutura de TI onde está hospedado o Helios, optou-se por estender para 4 dias o período para votação. Assim, mesmo que houvesse uma indisponibilidade temporária do Helios ou mesmo perda de conectividade de algum campus, haveria tempo hábil para que todos eleitores pudessem depositar seus votos.

No dia e hora de abertura do período de votação, a comissão eleitoral, através do Helios, fez o envio do usuário e senha para o e-mail de cada eleitor cadastrado. Isto resultou no envio de mais de 14.347 e-mails e foram necessárias quase quatro horas para que todos os e-mails fossem entregues. Verificou-se que o motivo desta demora estava relacionado com o mecanismo de fila de tarefas distribuída[9], pois existia somente um processo responsável por todo o envio de e-mail. A solução foi iniciar cinco processos (*workers*) de forma concorrente, porém isto só foi útil para o envio de e-mails de lembrete de votação para aqueles eleitores que ainda não haviam depositado seus votos.

O processo de apuração ocorreu sem problemas, sendo feita em uma sessão pública. Na eleição para TAEs, 63% dos eleitores compareceram às urnas (568), 59% dos docentes (572) e apenas 5% dos discentes (689). Números bem próximos com os da última eleição em 2011 realizada com cédulas de papel, 65% de TAEs (451) e 64% de docentes (513). Discentes não participaram da eleição de 2011.

6. Conclusões

A principal facilidade de um sistema de votação *on-line* é a possibilidade do eleitor votar por meio de qualquer dispositivo conectado à Internet. Porém, em eleições com grande

[9]https://celery.readthedocs.org/en/latest/

probabilidade de coação de eleitores, tal solução pode ser questionada pelos interessados, principalmente sobre a garantia da pessoalidade do voto, ou seja, nenhum eleitor poderia se passar por outro.

Para este caso, poderia-se fazer uso de mecanismos de forma que o acesso ao servidor do Helios só fosse feito através de computadores previamente registrados, por meio de firewall, VPNs, etc. Desta forma, cada campus teria um computador atuando exclusivamente como urna em uma sala com controle de acesso restrito. Ou seja, para ingressar na sala o eleitor teria que assinar uma lista de presença e somente um eleitor por vez. Este computador garantiria que o eleitor só pudesse depositar o voto uma única vez.

Como trabalhos futuros pretende-se disponibilizar a solução como um serviço de TIC, exigindo um mínimo ou nenhuma interação da área de TI na configuração de cada eleição. Para isto será necessário desenvolver um mecanismo para gerar automaticamente a lista de eleitores, de acordo com a escolha do administrador da eleição. Outra melhoria importante é a de adicionar na interface de administração a possibilidade de se configurar data e hora inicial e final da eleição, permitindo que a mesma seja aberta e fechada sem a necessidade intervenção manual por parte do administrador.

Todas as alterações e personalizações descritas neste artigo foram disponibilizadas publicamente no GitHub[10] sob a mesma licença de software livre usada pelo Helios. Também foi gerado um arquivo de instruções que detalha todos os passos necessários para uma instalação e configuração funcional do sistema.

Referências

Adida, B. (2008). Helios: Web based open audit voting. In *17th USENIX Security Symposium*.

Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A., and Vora, P. (2008). Scantegrity: End-to-end voter-verifiable optical-scan voting. *Security & Privacy, IEEE*, 6(3):40–46.

Cunha, P. R. F., Granville, L. Z., and de Matos Galante, R. (2013). Plano de gestão para a SBC biênio 2013-2015.

Dill, D., Mercuri, R., Neumann, P., and Wallach, D. (2003). Frequently asked questions about dre voting systems. *Verified Voting*.

Hammer-Lahav, E. (2010). The oauth 1.0 protocol.

Joaquim, R., Ferreira, P., and Ribeiro, C. (2013). Eviv: An end-to-end verifiable internet voting system. *computers & security*, 32:170–191.

Jonker, H., Mauw, S., and Pang, J. (2013). Privacy and verifiability in voting systems: Methods, developments and trends. *Computer Science Review*, 10:1–30.

Karayumak, F., Olembo, M. M., Kauer, M., and Volkamer, M. (2011). Usability analysis of helios-an open source verifiable remote electronic voting system. In *Proceedings of the 2011 USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections. USENIX*.

[10]https://github.com/shirlei/helios-server

Kohno, T., Stubblefield, A., Rubin, A. D., and Wallach, D. S. (2004). Analysis of an electronic voting system. In *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*, pages 27–40. IEEE.

PortalJH (2012). Maioria dos docentes da ufrn aprova proposta do governo federal. http://jornaldehoje.com.br/maioria-dos-docentes-da-ufrn-aprova-proposta-do-governo-federal. Visitado em agosto de 2014.

POST, U. (2001). Online voting. In *POSTNOTE*, number 155. UK Parliamentary Office of Science and Technology.

Pôrto, I. J., Galante, R., and Zorzo, A. (2011). Ata da sessão pública de apuração dos votos para eleição do conselho e da diretoria da sociedade brasileira de computação.

Qadah, G. Z. and Taha, R. (2007). Electronic voting systems: Requirements, design, and implementation. *Computer Standards & Interfaces*, 29(3):376–386.

Rivest, R. L. (2008). On the notion of 'software independence'in voting systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 366(1881):3759–3767.

Rivest, R. L., Adleman, L., and Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11):612–613.

UFPA, I. (2012). Eleição dos servidores técnico-administrativos para os conselhos superiores. http://www.itec.ufpa.br/index.php?option=com_content&view=article&id=552:eleicao-dos-servidores-tecnico-administrativos-para-os-conselhos-superiores&catid=47:noticias&Itemid=192. Visitado em agosto de 2014.

UFRN (2012). Eleita a nova diretoria do dce com o uso do sigeleição. http://sistemasdaufrn.blogspot.com.br/2012/10/eleita-nova-diretoria-do-dce-com-o-uso.html. Visitado em agosto de 2014.

UNB (2013). Unb adapta sistema de voto eletrônico para defensoria pública da união. http://www.unbciencia.unb.br/index.php?option=com_content&view=article&id=605%3Aunb-adapta-sistema-de-voto-eletronico-para-defensoria-publica-da-uniao&catid=43%3Aeletrica&Itemid=9. Visitado em agosto de 2014.

Wahl, M., Howes, T., and Kille, S. (1997). Lightweight directory access protocol (v3).

Weber, J. and Hengartner, U. (2009). Usability study of the open audit voting system helios. www.jannaweber.com/wp-content/uploads/2009/09/858Helios.pdf. Visitado em setembro de 2014.

