UNIVERSIDADE FEDERAL DE OURO PRETO

Relatório de Auditoria Interna

Auditoria do sistema de votação eletrônica da Universidade Federal de Ouro Preto intitulado sistema e-Votação UFOP

Janniele Aparecida Soares Araujo, Helen de Cassia Sousa da Costa Lima, Fernando Bernardes de Oliveira, Theo Silva Lins.

Relatório técnico de auditoria do sistema e-Votação UFOP submetido à Comissão de Consulta Paritária para Reitor da UFOP/2020.

16 de Outubro de 2020

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

CET Comissão Especial Técnica

CPP Comissão de Pesquisa Paritária

DECSI Departamento de Computação e Sistemas

ICEA Instituto de Ciências Exatas e Aplicadas

IFSC Instituto Federal de Santa Catarina

LDAP *Lightweight Directory Access Protocol*

NTI Núcleo de Tecnologia da Informação

UCL *Université Catholiquede Louvain*

UFOP Universidade Federal de Ouro Preto

UFSCar Universidade Federal de São Carlos

UFSC Universidade Federal de Santa Catarina

VPN *Virtual Private Network*

XSS *Cross-Site Scripting*

.

Capítulo 1

Introdução

A Equipe de Auditoria do sistema de votação eletrônica da Universidade Federal de Ouro Preto (UFOP), intitulado sistema e-Votação UFOP, atendendo ao pedido oficial da Comissão de Pesquisa Paritária (CPP) para Reitoria da UFOP/2020 no que tange a colaboração dos docentes do Departamento de Computação e Sistemas (DECSI) para auditar o sistema, juntamente com o apoio da Comissão Especial Técnica (CET), vem, por meio deste, encaminhar o Relatório de Auditoria Interna para apreciação e conhecimento do resultado da Auditoria. A finalidade deste relatório é cientificar a CPP acerca dos resultados observados na auditoria para possibilitar a lisura e transparência do processo de votação eletrônica.

A auditoria em questão, segundo Imoniana (2016), trata-se de uma Auditoria de Sistemas de Produção, em que preocupa-se com os procedimentos e resultados dos sistemas já implantados, sua segurança, integridade e tolerância à falhas. O sistema e-Votação UFOP utiliza o Helios, o qual é um sistema de código aberto baseado na web, que proporciona rastreabilidade, auditoria fim-a-fim e privacidade. O Helios está acessível publicamente[1] e qualquer instituição pode criar, realizar uma eleição e auditar todo o processo (Adida, 2008). A seguir são apresentadas as estruturas das comissões e chapas que envolvem o processo de pesquisa paritária. A Figura 1.1 apresenta a composição das comissões de pesquisa paritária e especial técnica instituídas pelo regulamento de Pesquisa Paritária para Reitoria.

A Figura 1.2 apresenta a composição das chapas candidatas que se inscreveram no edital de convocação de pesquisa paritária Nº 001/2020 UFOP.

[1] `https://github.com/benadida/helios-server`

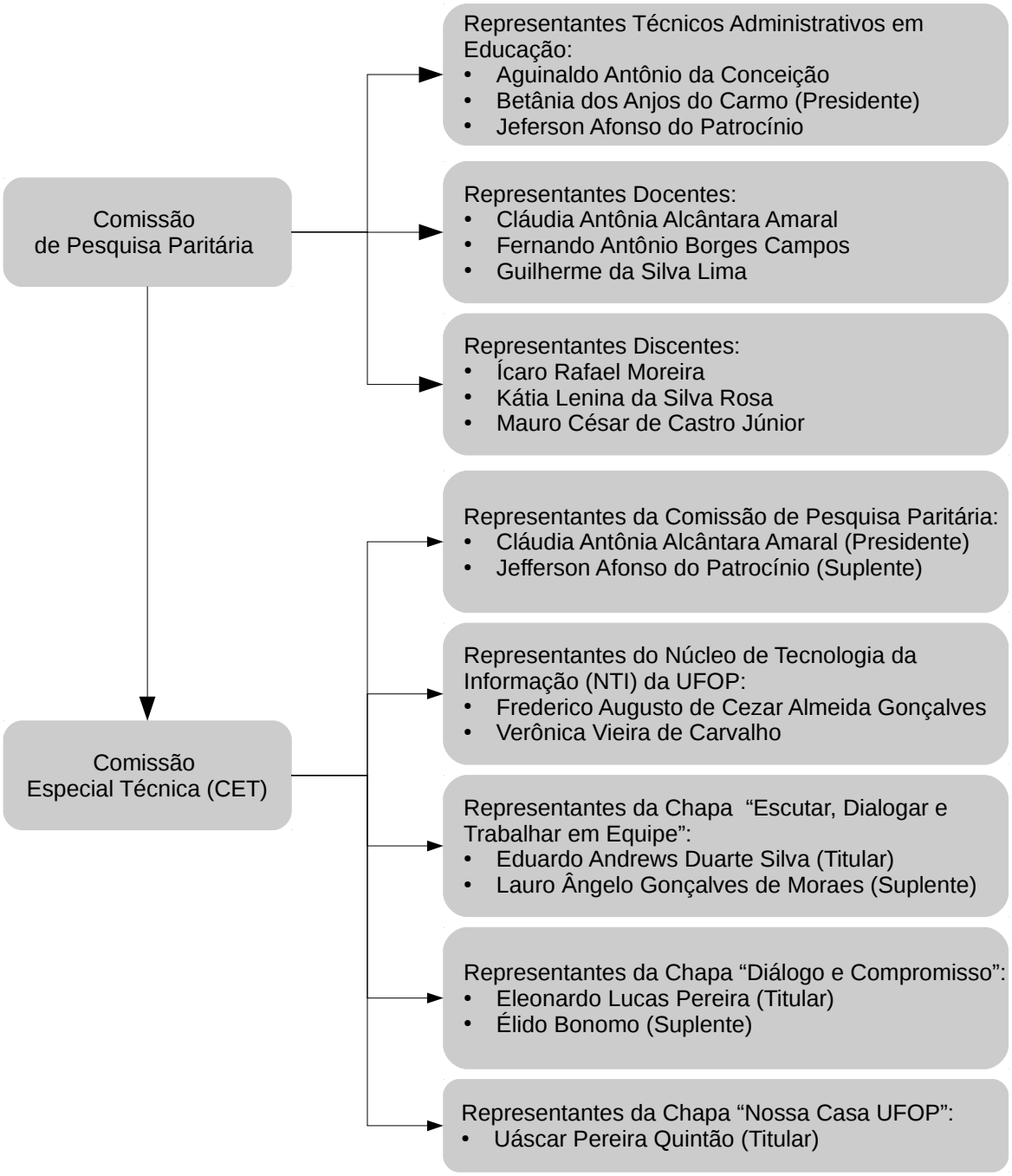

Figura 1.1: Composição das comissões de pesquisa paritária e especial técnica

A equipe de auditoria, composta por quatro membros, foi instituída pela provisão da assembleia departamental do DECSI, departamento pertencente ao Instituto de Ciências Exatas e Aplicadas (ICEA) da UFOP, sendo esta, uma comissão interna independente das comissões da pesquisa paritária. A equipe foi formada inicialmente após o contato

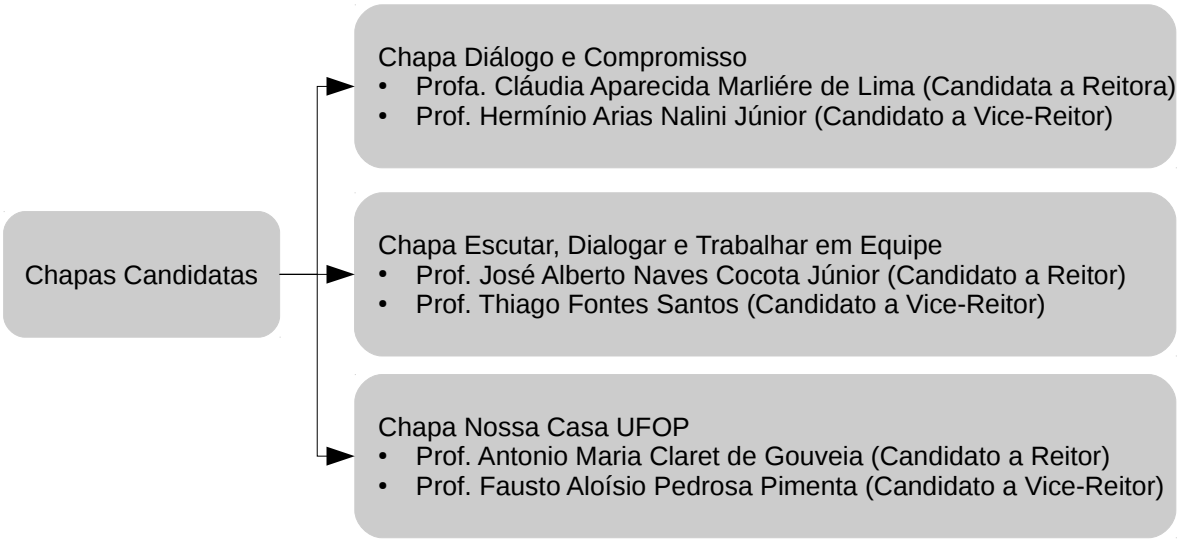

Figura 1.2: Composição das chapas candidatas à reitoria da UFOP

do Núcleo de Tecnologia da Informação (NTI) e da CPP com os departamentos das áreas de computação e de sistemas da UFOP, afim de se conseguir a colaboração voluntária de docentes para auditar o sistema e-Votação UFOP. A equipe foi formalizada pelo ofício da CPP N.06/2020. A Figura 1.3 apresenta a composição da auditoria interna, com os docentes da área que se voluntariaram.

Figura 1.3: Composição da Equipe de Auditoria Interna

Capítulo 2

Método de trabalho

O método de trabalho, aqui apresentado, para a auditoria do sistema e-Votação UFOP, está dividido em três fases que contemplam o planejamento, a execução e a entrega dos relatórios. As fases apresentadas na Figura 2.1 são detalhadas atribuindo, a cada uma, os procedimentos esperados no projeto de auditoria desde o levantamento do escopo até a entrega dos relatórios.

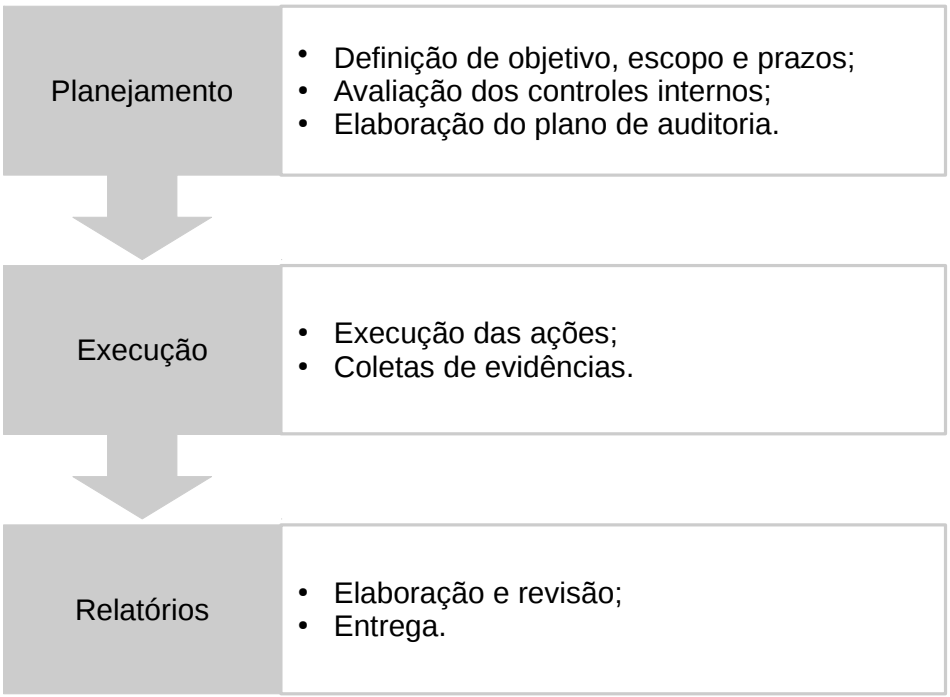

Figura 2.1: Fases da auditoria do sistema e-Votação UFOP

Ainda, haverá o acompanhamento das ações tomadas em resposta aos apontamentos

da auditoria. Nesta auditoria o acompanhamento se dará na fase de Monitoramento. A Figura 2.2 apresenta o fluxo do monitoramento, que compreende desde a verificação das ações tomadas pela CET e pela CPP, até a elaboração dos relatórios finais.

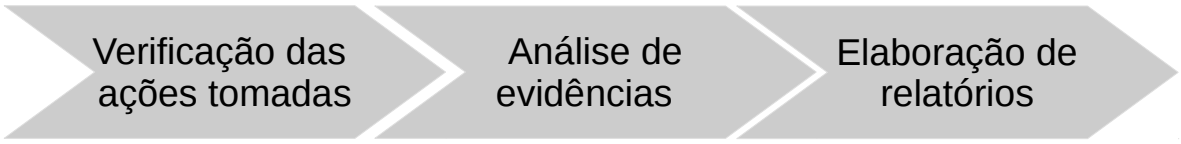

Figura 2.2: Fases de monitoramento da auditoria do sistema e-Votação UFOP

A metodologia aqui aplicada baseia-se na proposta de Imoniana (2016). Em que temos as seguintes atividades a serem desenvolvidas:

1. Identificar claramente o escopo, determinar a abrangência da auditoria e prazos.
2. Iniciar o processo de levantamento das informações relevantes sobre o sistema.
3. Identificação e inventário dos pontos de controle; priorização, seleção e avaliação dos pontos de controle do sistema auditado.
4. Conclusão da auditoria.

Capítulo 3

Planejamento

O planejamento e controle do projeto de auditoria visa identificar as ações e recursos necessários, definindo a abrangência das ações. Este capítulo descreve os objetivos, o escopo (abrangência) dos procedimentos a serem avaliados e as abordagens que devem ser adotadas pela equipe de auditoria até o dia 06 de novembro de 2020.

3.1 Objetivo e escopo

O objetivo da auditoria é promover a revisão, avaliação, adequação e recomendações para o aprimoramento dos controles do sistema e-Votação UFOP. Além de avaliar o processo eleitoral da votação eletrônica, em se tratando do acesso e utilização do sistema no ambiente que o envolve.

O escopo do trabalho de auditoria obedecerá o seguinte: (a) entendimento global do processo de votação eletrônica; (b) revisão da literatura acerca do sistema Helios; (c) análise do ambiente de instalação e de mudança do sistema; (d) análise do ambiente do sistema e-Votação UFOP após o período eleitoral.

Os procedimentos adotados para avaliar os controles internos são:

- identificar e reportar pontos falhos no processo da votação eletrônica;
- revisar a literatura acerca dos controles de segurança e de auditoria do sistema Helios e melhores práticas de uso;

- identificar e atualizar a compreensão dos controles de sistemas aplicativos e os controles gerais de atualização servidor;
- extrair dados do sistema para análises substantivas após o período eleitoral.

3.2 Plano da auditoria

O plano de auditoria apresentado na Tabela 3.1, funciona como uma agenda de auditoria, onde são detalhados os processos, o local, o período e o tempo gasto.

Tabela 3.1: Plano da auditoria do sistema e-Votação UFOP

Ação	Descrição	Local	Duração	Início - Fim
1	Reuniões de apresentação dos membros voluntários da auditoria, conhecimento do sistema e dos processos estabelecidos pela CPP.	Google Meet	3h	01/09/2020 - 14/09/2020
2	Levantamento bibliográfico do sistema Helios.	Home Office	6h	14/09/2020 - 30/09/2020
3	Formalização da equipe de auditoria.	E-mail	1h	23/09/2020
4	Envio de ofício de requisição para acesso remoto aos servidores de aplicação e banco de dados do sistema.	Home Office	30m	23/09/2020
5	Criação de eleição teste para auditoria.	Servidor	2h	15/10/2020
6	Acesso ao ambiente de instalação do sistema.	Servidor	10h	24/09/2020 - 15/10/2020
7	Avaliação dos pontos de controle e criação colaborativa do relatório de auditoria.	Google Meet, Google Drive, OverLeaf	5h	23/09/2020 - 16/10/2020
8	Conclusão, envio e apresentação do relatório inicial de auditoria.	Google Meet, E-mail	2h	16/10/2020 - 19/10/2020
9	Monitoramento das ações tomadas pelas comissões frente às recomendações e do processo de eleição, envio do relatório final de auditoria.	Servidor, Google Meet, E-mail	4h	16/10/2020 - 06/11/2020

Capítulo 4

Execução dos trabalhos

As próximas seções apresentam informações detalhadas sobre a execução do trabalho da equipe de auditoria interna.

4.1 Análises de evidências do sistema de votação eletrônica Helios

Em 2008, Adida (2008) apresentou o Helios, o primeiro sistema de votação de auditoria aberta ao público (fim-a-fim) baseado na web, que permite a qualquer um criar e executar uma eleição. O sistema permite, da mesma maneira, a qualquer pessoa, que esteja disposta e interessada, auditar todo o processo eleitoral.

O primeiro uso, em um caso real, foi em 2009, em que a *Université Catholiquede Louvain* (UCL) elegeu seu presidente usando uma versão personalizada do sistema Helios. Dos 25.000 eleitores em potencial, 5.000 se cadastraram e quase 4.000 votaram em cada turno da eleição. A utilização deste sistema em um caso real acabou agregando valor para uma versão aprimorada. A nova versão do Helios usada nesta eleição, bem como as especificações da implantação na UCL e as lições aprendidas foram todas documentadas e com sugestões sobre como conduzir futuras eleições de auditoria aberta em Adida et al. (2009).

Uma contribuição muito importante após a aplicação na eleição real foi a adição da descriptografia distribuída. Vários apuradores (curadores) são necessários para a descriptografia, garantindo que apenas a contagem homomórfica de todos os votos seja

descriptografada, nunca uma cédula individual, assim, cada apurador gera uma chave pública El-Gamal típica usando os mesmos parâmetros (p, q, g) e combinando as chaves públicas usando multiplicação simples (Adida et al., 2009).

Em 2018, o Conselho de Administração da Universidade Federal de São Carlos (UFSCar), 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". O relatório disponível em Santos et al. (2018) apresenta algumas questões acerca da segurança, com base nos seguintes princípios:

1. 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.

2. A identificação dos usuários é feita por login e senha utilizados nos próprios sistemas da UFSCar - sistema de matrícula e digitação de notas.

3. 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.

4. O código fonte do sistema é totalmente aberto, e pode ser verificado por qualquer pessoa com conhecimento em programação.

5. 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.

6. 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.

7. Uma Comissão Eleitoral, designada formalmente no Sistema, poderá acompanhar, avaliar, e nortear todo o processo: lista de eleitores, fechamento de urnas, apuração, etc.

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

Outras universidades brasileiras já estão utilizando o sistema Helios para eleições, mais informações podem ser obtidas em de Chaves e de Mello (2014). O Sistema de Votação On-Line e-Democracia[1] disponibilizado pela Universidade Federal de Santa Catarina (UFSC) utiliza o sistema Helios. Na UFSC foi utilizada uma modificação feita pelo Instituto Federal de Santa Catarina (IFSC) da versão original[2] do projeto. As modificações foram necessárias para permitir integrar com a base de usuários, traduzir a interface para a língua portuguesa e alguns ajustes para melhorar a usabilidade. É importante destacar que no momento atual da escrita deste relatório, a UFSC só está atendendo as eleições internas em um serviço beta. A solicitação de agendamento é feita pelo Presidente da Comissão Eleitoral via abertura de chamado[3].

A UFSC também apresenta informações sobre as atividades permitidas e não permitidas na sua versão do sistema Helios, aumentando assim a credibilidade do sistema (de Santa Catarina, 2020).

O Sistema de Votação On-Line e-Democracia permite:

- que o eleitor verifique se seu voto foi depositado corretamente;
- que todos as cédulas depositadas na urna sejam exibidas publicamente em sua forma criptografada;
- que qualquer um possa verificar que as cédulas depositadas na urna foram corretamente apuradas.

E não permite:

- que a escolha de um eleitor (seu voto) seja revelada, mesmo que este eleitor queira revelar (p.e. apresentando um recibo de votação);
- que o voto de um eleitor seja adulterado ou excluído.

[1] `https://e-democracia.ufsc.br`
[2] `https://vote.heliosvoting.org`
[3] `https://otrs.setic.ufsc.br/otrs/customer.pl?Action=NewTicketWizard;ServiceID=159`

4.1.1 Etapas de auditoria oferecidas pelo Helios

O sistema Helios possui algumas etapas de auditoria oferecidas pelo seu sistema de preparação de cédulas, que é composto por três fases: selecionar as respostas, revisar e encriptar a cédula; gerar um número de rastreamento que torna possível contestar o sistema e; por fim, enviar para contagem na urna (Pereira, 2016). A seguir são descritas as etapas de auditoria oferecidas pelo sistema Helios:

1. **Verificar se o voto foi encriptado conforme a intenção de voto**: logo após o rastreador da cédula ser disponibilizado, o próprio votante tem a opção de contestar a cédula antes de autenticar no sistema e fazer sua submissão de voto. Assim, é permitido auditar o sistema de preparação da célula em qualquer momento da eleição, já que o sistema não sabe se é uma encriptação que vai ser submetida na urna ou auditada.

2. **Verificar se o voto foi depositado na urna conforme encriptação gerada**: permite ao próprio votante saber se sua cédula foi registrada no servidor Helios de maneira apropriada usando o rastreador gerado para seu voto e a lista de todos os votantes e seus respectivos rastreadores, que serão usados na contagem de votos. Essa lista é disponibilizada para qualquer pessoa (sem autenticação) na página da eleição.

3. **Verificar se a contagem dos votos corresponde a todos os votos da lista de votantes**: permite qualquer um (única verificação universal) verificar que todos os votos válidos registrados foram incluídos na contagem. A partir da lista de votantes disponibilizada, qualquer um pode coletar a lista de pessoas que submeteram uma cédula e seus rastreadores correspondentes. Após verificação e confirmação da lista de rastreadores e seus respectivos usuários associados, a lista de rastreadores pode ser comparada com a lista de todas as cédulas válidas na abertura da urna, que também é disponibilizada pelo servidor Helios.

4.1.2 Considerações sobre a segurança do Helios

Foram identificados no trabalho de Pereira (2016) alguns pontos de controles internos importantes, que garantem a sua segurança. Esses pontos de controle são:

1. **Autenticação do usuário**: acontece no final do processo de votação, o que

proporciona ao votante receber a ajuda de outra pessoa sem medo de ter suas credenciais roubadas; além disso, evita que servidores corrompidos ofereçam uma versão diferente do sistema de preparação de cédula como função das credenciais do votante.

2. **Resistência à coerção de eleitor**: os eleitores podem enviar quantas cédulas quiserem para a urna de eleição, porém, apenas a última será computada. Esse recurso, além de suas enormes vantagens para lidar com eleitores que usam uma conexão de Internet não confiável ou eleitores desconfortáveis com uma interface de navegador, permite que eleitores que se sentam pressionados a votar de forma indesejada em um determinado momento possam submeter outra cédula posteriormente, quando estiverem em um contexto seguro.

3. **Associação de codinomes aos eleitores cadastrados**: a cada eleitor é possível designar um codinome que será informado apenas a ele no convite para a eleição. Essa medida garante a anonimidade da lista de votantes quando há esta necessidade e evita também que candidatos numa eleição possam identificar, durante o processo de votação, eleitores que não depositaram ainda seu voto e disparar assim, uma "boca de urna" direcionada. Em contrapartida, o uso de codinomes abre espaço para um administrador malicioso associar um grupo de eleitores a um mesmo codinome. Caso ele saiba que determinado grupo de pessoas votará em um candidato específico, isso pode reduzir drasticamente o número de votos para esse candidato. A única forma de descobrir a fraude é se dois votantes tornarem seus rastreadores disponíveis online ou se um eleitor perceber que seu voto está listado no servidor Helios antes mesmo dele ter votado.

4. **Segurança do lado do cliente**: a aplicação disponibiliza o código de identificação da eleição, que pode ser publicado no edital de convocação da eleição, na parte inferior de cada tela do sistema para verificação pelo eleitor. Esse código de identificação não é disponibilizado pelo servidor apenas para visualização, mas é, na verdade, recalculado pelo sistema de preparação de cédula como uma função de todos os parâmetros de eleição, por exemplo, URL de eleição, chaves de criptografia de cédula, perguntas, regras de resposta e etc. Este recurso fornece uma medida de segurança para o eleitor e também pode ajudar a detectar um servidor Helios malicioso ou um convite para eleição que usa um sistema de preparação de cédula independente.

5. **Segurança da aplicação**: o Helios guarda apenas informações públicas como

descrições da eleição, chaves públicas, votos encriptados e dados para auditoria; as chaves secretas dos apuradores não passam pelo servidor, nenhum texto simples de voto é armazenado no servidor, o que garante a privacidade, mesmo que o servidor seja monitorado por auditores durante todo o processo de eleição.

Adicionalmente, pode-se encontrar uma revisão do código do Helios no trabalho de Heiderich et al. (2012). Os autores identificaram vários ataques em potencial, como *Cross-Site Scripting* (XSS) e outras maneiras de extrair dados confidenciais, e propuseram correções que já foram integradas ao sistema. Por fim, no site de documentação do sistema Helios[4] são descritos outros ataques e defesas, que estão disponíveis na literatura, contra várias versões do sistema.

4.2 Analises de vulnerabilidades da infraestrutura

A auditoria da infraestrutura será realizada remotamente, os auditores não terão nenhum contato com a infraestrutura física alocada no NTI da UFOP, que é responsável pela hospedagem do sistema e-Votação UFOP. A segurança física de acesso aos prédios é atribuída aos setores responsáveis da UFOP. A infraestrutura física deve atender os requisitos mínimos para o funcionamento do sistema. Entre os principais requisitos podemos citar o uso de memória, capacidade de armazenamento, largura de banda, uso de *nobreaks* e processamento. Para definir estes requisitos é necessário a realização de testes, levando em conta o número de votantes.

A infraestrutura do sistema e-Votação UFOP possui uma plataforma de gerenciamento onde é possível fazer o controle de toda infraestrutura. Para o funcionamento do sistema e-Votação UFOP estão sendo utilizados três *containers*, um responsável pelo banco de dados, um responsável pela interface e funcionalidades da aplicação, além de um terceiro *container* utilizado apenas para as informações de ajuda do sistema.

Através da plataforma de infraestrutura não é possível fraudar ou modificar o sistema de votação, pois a plataforma não possui funcionalidades relacionadas ao sistema e-Votação UFOP. Os acessos aos sistemas operacionais dos *containers* podem ser feitos pela plataforma, mas as informações relacionadas as votações são salvas e protegidas pelo banco de dados.

[4]https://documentation.heliosvoting.org/attacks-and-defenses

4.2.1 Acessos externo ao sistema e-Votação UFOP

Foi realizada uma busca por portas e serviços no servidor que hospeda o sistema e-Votação UFOP, com objetivo de detectar serviços não necessários e que podem gerar vulnerabilidades. Nenhum serviço/porta extra foi detectada, estando disponíveis somente as portas 80 e 443 dos protocolos http e https do serviço apache que disponibiliza o acesso aos eleitores e a interface do sistema e-Votação UFOP através de navegadores de internet.

4.2.2 Acessos interno a infraestrutura do sistema e-Votação UFOP

O acesso a infraestrutura da votação só pode ser feita através de *Virtual Private Network* (VPN), o que torna o ambiente mais seguro. Este acesso via VPN à infraestrutura está liberado apenas para dois usuários, sendo um usuário da comissão técnica e um usuário da equipe de auditoria. Para este último usuário, optou-se por nomear apenas uma pessoa da equipe de auditoria para possuir as credenciais de acesso, restringindo ao mínimo a quantidade de pessoas que podem acessar a infraestrutura.

4.2.3 Análises dos softwares e serviços presentes no sistema e-Votação UFOP

Foi verificado as versões e possíveis atualizações dos softwares instalados no servidor para o funcionamento do sistema e-Votação UFOP. Entre os principais serviços responsáveis pelo funcionamento do sistema, podemos citar o banco de dados PostgreSQL, o servidor HTTPD Apache e a linguagem Python com o *framework* Django. Todos os serviços no momento encontram-se com uma versão estável e sem falhas conhecidas (Limited, 2020; Storm, 2020).

4.3 Análises do processo eleitoral no sistema e-Votação UFOP

O sistema e-Votação UFOP disponível no endereço `https://evotacao.ufop.br/` utiliza o sistema Helios. Esse sistema é disponibilizado no GitHub, uma plataforma para hos-

pedagem de códigos-fontes e desenvolvimento de programas com controle de versão. Isso significa que qualquer modificação, seja a inclusão, a alteração ou a exclusão de qualquer arquivo ou pasta de um projeto pode ser verificada, indicando qualquer item que tenha sido modificado. Os projetos são hospedados em *repositórios*, os quais permitem todos os controles de versões. O repositório original do sistema Helios está disponível em: `https://github.com/benadida/helios-server`. Para que as traduções e atualizações necessários pudessem ser realizadas, o Instituto Federal de Santa Catarina (IFSC) criou um *fork*[5] do projeto original. O *fork* representa uma cópia do repositório original para o repositório do IFSC, preservando a relação entre esse projetos[6]. Uma versão com atualizações de usabilidade e tradução da versão original do projeto Helios foi realizada pelo IFSC e disponibilizada no seguinte endereço: `https://github.com/ifsc/server`.

Considerando a versão já traduzida e adaptada visualmente, um *fork* do projeto do IFSC foi realizado pelo NTI da UFOP e disponibilizado no seguinte endereço `https://github.com/nti-ufop/helios-server`. A partir da verificação das atualizações no repositório disponibilizado pelo NTI, foi possível observar que os arquivos alterados se referem à adequação da identidade visual da UFOP, como a alteração do nome e sigla, cores, imagens e afins. Algumas modificações de traduções e texto também foram identificadas. A correção acerca da utilização do *login* no sistema com o CPF com e sem pontos também foi realizada. Entretanto, nenhuma modificação no núcleo principal da aplicação, do processo de votação e afins, foi realizada e/ou identificada. Assim, o sistema Helios está preservado conforme aquela versão disponibilizada pelo IFSC. A última atualização identificada no repositório do NTI, considerando quando este relatório foi redigido, foi realizada no dia 30 de setembro de 2020.

É importante observar que é possível a qualquer pessoa com conhecimentos de computação verificar as modificações efetuadas nos repositórios, tanto do projeto original quanto das versões disponibilizadas pela IFSC e pelo NTI.

4.3.1 Simulações das eleições testes

Para validar as análises de evidências efetuadas sobre o sistema Helios e sobre a infraestrutura do ambiente de instalação do sistema e-Votação UFOP, foram estabelecidos alguns pontos de controles a serem analisados durante a simulação das eleições testes:

[5]Para mais informações sobre *fork*, veja em: `https://guides.github.com/activities/forking/`

[6]Todos os *forks* realizados do projeto original podem ser encontradas em: `https://github.com/benadida/helios-server/network/members`

1. Testes na inclusão de votantes com CPF duplicado, CPF não registrado no portal MinhaUFOP e e-mail inválido.
2. Validação de apuradores (curadores).
3. Validação do parâmetro que permite ou não o uso de codinomes.
4. Validação do parâmetro que permite ou não a auditoria do voto.
5. Validação da auditoria dos sistemas de preparação de cédulas e de contagem dos votos.

Durante as reuniões da auditoria para a simulação de eleições testes foi possível validar o correto funcionamento dos pontos de controles selecionados e priorizados. As principais constatações foram:

1. Ao incluir a lista de eleitores por arquivo do tipo ".csv" com requisição de autenticação, eleitores com CPF duplicados foram descartados, prevalecendo somente um. Observou-se também que eleitores com CPF não registrado no portal MinhaUFOP foram cadastrados na urna, porém não foi possível votar, uma vez que o sistema necessita da autenticação *Lightweight Directory Access Protocol* (LDAP). Por fim, para eleitores com e-mail inválido, o sistema retornou um aviso para o administrador da eleição corrigir o arquivo.
2. A apuração da urna só é possível após a inserção das chaves secretas de todos os apuradores cadastrados na criação da eleição.
3. Ao não marcar a opção de associar codinomes aos eleitores, as informações dos votantes aparecem explicitamente na lista de votantes da eleição, juntamente com seu respectivo rastreador de cédula.
4. Várias tentativas de auditar a cédula de votação ao invés de submetê-la na urna foram feitas, e constatou-se o funcionamento correto do sistema de encriptação de votos. O sistema é capaz de apresentar ao votante a opção por ele escolhida e inserir essa cédula em uma urna específica para cédulas auditadas, ou seja, esse voto não é computado na eleição até que o votante opte por submeter seu voto na urna oficial.
5. Ao acessar o centro de auditoria disponível na página Web da eleição, é possível a qualquer eleitor auditar todas as partes da eleição, permitindo ainda, após o encerramento, baixar todas as cédulas depositadas.

Capítulo 5

Recomendações

A seguir são apresentadas as recomendações desta auditoria. É indicado que caso a CPP entenda ser correto, apresente e requisite ao CET que atenda às recomendações. É importante enfatizar que, devido aos prazos, algumas recomendações já estão sendo planejadas pelo CET.

5.1 Recomendações para o processo de criação da urna eletrônica

1. Recomenda-se que as listas de eleitores sejam adicionadas apenas uma única vez, para evitar oportunidades de fraude por parte dos administradores da eleição; esta recomendação está em conformidade com o Calendário para Consulta Paritária Reitoria UFOP, que prevê a data de 16 de outubro como prazo para divulgação das listas definitivas de eleitores.

2. Recomenda-se que sejam verificados o domínio e/ou validade dos e-mails cadastrados.

3. Recomenda-se usar identificadores explícitos dos votantes, como por exemplo o CPF, para evitar fraude por parte dos administradores da eleição, visto que o uso de codinomes no sistema de votação Helios abre espaço para que um administrador malicioso associe um grupo de usuários a um mesmo codinome.

4. Recomenda-se que apuradores (curadores) escolhidos pela comissão sejam pessoas

que tenham familiaridade com computação, para diminuir a possibilidade da chave ser perdida ou corrompida.

5. Recomenda-se que os apuradores escolhidos assinem um termo de compromisso para com a segurança das chaves recebidas e para a inserção das chaves no sistema e-Votação, com o intuito de mitigar a interrupção da apuração dos votos.

6. Recomenda-se que a copia da chave privada de cada apurador seja salva em um pendrive backup e seja colocado dentro de um envelope lacrado e assinado pelos membros da CPP e das chapas.

7. O Helios tem uma função de auditoria que permite ao votante verificar se a cédula foi encriptada capturando corretamente sua intenção de voto. Logo após o rastreador da cédula ser disponibilizado, há uma opção de contestar a cédula antes do votante autenticar no sistema e fazer sua submissão. Para a eleição principal, recomenda-se que a CPP escolha em conversa com as chapas se esta opção de auditoria ficará disponível ou não. A vantagem é garantir uma maior transparência para o usuário, além de ser de fácil verificação. Uma possível desvantagem poderia ser levar o usuário a se confundir no momento de submeter seu voto, já que ao escolher auditar sua cédula a mesma será descartada da urna oficial e incluída em uma urna de auditoria não contabilizada para voto. Neste caso, o votante teria que preparar uma nova cédula para submissão no sistema.

8. Recomenda-se a criação de vídeos demonstrando o processo de votação e o processo de auditoria do voto caso a opção anterior seja acatada.

9. Recomenda-se que o link da eleição seja disponibilizado no e-mail de convite e não no site institucional, tendo em vista que o código de identificação da eleição pode ser disponibilizado nos meios de comunicação oficiais da Instituição antes mesmo da liberação do link da eleição e que o votante sempre será alertado por e-mail sobre o depósito de sua cédula na urna de votação.

5.2 Recomendações para a Infraestrutura

1. Recomenda-se designar apenas um usuário da equipe técnica para ter as credenciais que dão acesso a plataforma de gerenciamento.

2. Recomenda-se não salvar as credenciais de acessos em e-mails.

3. Recomenda-se não realizar qualquer acesso a infraestrutura do ambiente de instalação do e-Votação UFOP durante a eleição. Caso o acesso seja necessário, justificar e registrar todas as ações realizadas na plataforma de infraestrutura e nos *containers*.

4. Recomenda-se realizar o *backup* do sistema e do banco de dados, para evitar possíveis perdas de informações.

5. Recomenda-se realizar testes de cargas para garantir um bom funcionamento do sistema e-Votação UFOP durante a eleição, evitando perda de desempenho por excesso de acessos oriundos da Internet.

Referências Bibliográficas

Adida, B.: 2008, Helios: Web-based open-audit voting, *Proceedings of the 17th USENIX Security Symposium*, pp. 335–348.

Adida, B., De Marneffe, O., Pereira, O. e Quisquater, J.-J.: 2009, Electing a university president using open-audit voting: Analysis of real-world use of helios, *Proceedings of the 2009 conference on Electronic voting technology/workshop on trustworthy elections - EVT/WOTE*, p. 10.

de Chaves, S. A. e de Mello, E. R.: 2014, O uso de um sistema de votação on-line para escolha do conselho universitário, *Anais do XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais — SBSeg 2014*, pp. 634–645.

de Santa Catarina, U. F.: 2020, e-Democracia Universidade Federal de Santa Catarina - UFSC.
URL: *https://e.ufsc.br/e-democracia-ajuda/*

Heiderich, M., Frosch, T., Niemietz, M. e Schwenk, J.: 2012, The bug that made me president a browser- and web-security case study on helios voting, *E-Voting and Identity*, Springer Berlin Heidelberg, pp. 89–103.

Imoniana, J. O.: 2016, *Auditoria de sistemas de informação*, 3 edn, Atlas.

Limited, O. S. S.: 2020, Exploit database.
URL: *https://www.exploit-db.com/*

Pereira, O.: 2016, Internet voting with helios, *Real-World Electronic Voting: Design, Analysis and Deployment*, CRC Press, pp. 277–308.

Santos, M. T. P., Matias, P., Melo, E. L., Pizzolato, E. B. e Ferrari, R.: 2018, Relatório técnico - v03: Uso do voto online em eleições da UFSCar.
URL: *http://www.cech.ufscar.br/conselho/convocacoes/2018/relatorio_tecnico_voto_online_versa_o_03_31_08_2018.pdf*

Storm, P.: 2020, Packet storm security.
URL: *https://packetstormsecurity.com/*