Auditoria do sistema de votação eletrônica da Universidade Federal de Lavras

Prof. Dr. Joaquim Quinteiro Uchôa - DAC-UFLA
Prof. Dr. Mauricio Cunha Escarpinatti - FACOM-UFU
Prof. Dr. Paulo Afonso Parreira Júnior - DCC-UFLA
Prof. Dr. Rodrigo Sanches Miani - FACOM-UFU

3 de maio de 2024

Conteúdo

Capítulo 1

Introdução

O avanço de tecnologias no campo da segurança da informação, como mecanismos de controle de acesso, serviços de monitoramento e segurança de tráfego de dados, algoritmos de criptografia, entre outros, tornou possível e viável a criação de uma série de novas tecnologias e aplicações, de fácil acesso, que evolvam Tecnologia de Informação e Comunicação, as chamadas TICs. Dentre os inúmeros serviços que se beneficiaram pelos avanços citados, pode-se mencionar e, por que não destacar, as soluções voltadas para a realização de eleições eletrônicas (e-Voting). Os Sistemas de Votação Eletrônica permitiram flexibilizar os processos de votação, aumentar a velocidade de apuração, reduzir custos e aprimorar a precisão dos resultados em comparação com o método tradicional de votação com cédulas impressas [1]. Do ponto de vista da segurança, os principais sistemas de votação eletrônica utilizam um processo totalmente auditável e podem eliminar a margem de erro humano. Essas são características que, teoricamente, garantem a confiabilidade de um sistema de votação eletrônica [2].

Ao aliar essas soluções aos recursos da rede mundial de computadores, surgiram os Sistemas *Online* de Votação Eletrônica, que são serviços disponíveis para acesso a partir da Internet, que permitem aos seus usuários produzirem consultas e eleições e disponibilizarem estas para que seus eleitores possam, de forma remota e eletrônica, manifestarem suas opiniões através de votos de forma anônima e segura. Dentre essa importante classe de sistemas, o Helios Voting[1] merece destaque, dado o seu alcance e usabilidade em nível mundial. Ele foi desenvolvido por um pesquisador do MIT chamado Ben Adida [3] e possui mecanismos seguros de recebimento e apuração eletrônicas dos votos. Nele, são exigidos login e senha individuais para o acesso à cabine de votação e todos os votos são cifrados antes de serem enviados pela rede. Além disso, cada eleitor pode auditar o próprio voto e o código-fonte do sistema está disponível de forma pública no repositório do autor[2]. Um importante mecanismo de segurança do Helios Voting é conhecido como verificabilidade fim-a-fim ($e2eV$). O objetivo de tal propriedade é reduzir drasticamente a desconfiança do eleitor no sistema, de modo que cada eleitor passa a ter garantias de que seu voto foi corretamente registrado, permitindo que qualquer pessoa possa verificar se os votos foram incluídos corretamente na contagem final [4].

Nos últimos anos, diversas instituições, públicas e privadas, impulsionadas principalmente pela necessidade de isolamento causada pandemia da doença COVID-19, provocada pelo vírus SARS-CoV 2, passaram a adotar o Helios Voting em diferentes

[1] https://vote.heliosvoting.org

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

tipos de eleição. Nos ambientes universitários, foram inúmeras as instituições de ensino superior que adotaram o Helios em suas eleições e consultas eleitorais, sendo elas desde as mais simples - conselhos de unidades - até as mais complexas como as consultas para reitor [5, 6, 7, 8].

Dentro deste contexto, o Conselho Universitário da Universidade Federal de Lavras (CUNI-UFLA) optou por realizar sua Consulta Pública como subsídio no processo de organização da lista tríplice para escolha de Reitor(a) Gestão – 2024-2028 de forma remota e eletrônica utilizando o sistema Helios Voting. Para tanto, a Diretoria de Gestão de Tecnologia da Informação da UFLA (DGTI-UFLA) baixou a versão mais atual, disponível à época, do sistema Helios Voting que, como mencionado anteriormente está disponível de forma pública no repositório do autor, customizou essa versão de modo a acomodar os textos para a língua portuguesa, preparou o ambiente e instalou o sistema em seus servidores e o disponibilizou para que a referida consulta pudesse ser realizada.

Realizado o processo e divulgado o resultado da consulta pública, o Colégio Eleitoral da Universidade Federal de Lavras (UFLA) indicou a necessidade de uma auditoria da votação eletrônica para a consulta pública que subsidiou o processo de organização da lista tríplice para escolha de Reitor(a) Gestão – 2024-2028 nesta instituição. Esse pedido, inicialmente, foi realizado à Diretoria de Gestão de Tecnologia da Informação que apontou, corretamente, que não seria de bom grado que ela auditasse a si mesma, já que foi esta diretoria quem operou os equipamentos e sistemas utilizados no processo dessa consulta pública.

Dessa maneira, em resposta às solicitações do Colégio Eleitoral, a reitoria buscou montar uma equipe de auditoria composta por membros externos e internos, com o objetivo de auditar a votação eletrônica para esta consulta pública, ocorrida no dia 22 de novembro de 2023, das 8h às 21h. A equipe de auditoria foi constituída em fevereiro do corrente ano, composta por dois professores da Universidade Federal de Uberlândia (UFU), Maurício Cunha Escarpinati e Rodrigo Sanches Miani, e dois professores da Universidade Federal de Lavras (UFLA), Joaquim Quinteiro Uchôa e Paulo Afonso Parreira Júnior. Parte do trabalho, aquela que não dependia de formalidades, iniciou-se nessa época, com aprofundamento sobre os processos de votação eletrônica e o sistema utilizado para isso na UFLA, justamente o Helios Voting.

O termo de cooperação, que permitiu a atuação dos auditores da UFU, foi finalmente assinado no dia 1 de abril de 2024, quando os trabalhos oficiais foram iniciados. Inicialmente, encaminhamos memorando à DGTI, para solicitarmos acesso aos servidores e seus dados, bem como realizarmos uma reunião para podermos entender melhor a infraestrutura utilizada para a votação. A reunião foi realizado no dia 12 de abril de 2024, com a presença dos quatro auditores e diversos profissionais da DGTI, principalmente os coordenadores de setor e a diretoria. A reunião foi aberta aos demais funcionários da DGTI, mas esses optaram por não participar, por estarem em greve. Sem estar envolvido na gestão da DGTI e seus setores, houve apenas a participação do técnico Giovanni Viol Assis, convidado pela administração da DGTI, por estar diretamente envolvido com questões de segurança computacional ligada ao sistema Helios Voting.

Durante esta reunião, a equipe de auditoria conseguiu acesso ao sistema de votação, bem como a *backups* dos sistemas utilizados na votação, bem como uma relação de usuários com exposição de dados de acesso, conforme relatório enviado em janeiro de 2024 pelo Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pes-

quisa (CAIS-RNP). A equipe de auditoria solicitou esse relatório por conta de dúvidas surgidas a partir de contatos da DGTI com os setores da UFLA sobre esse tema. Em posse dos acessos e dos arquivos necessários, a equipe iniciou os trabalhos efetivos de auditoria, conforme apresentado neste relatório.

Capítulo 2

Método de trabalho

Uma auditoria consiste na comparação do estado dos ativos de uma organização (processos de negócio, sistemas de informação, ambientes, entre outros) contra um critério de auditoria. Como resultado desta comparação, espera-se comprovar a **conformidade** ou **não conformidade** do ativo a esse critério [9].

Tomando como base os trabalhos de Silva Júnior *et al.* [10] e Araujo *et al.* [11], o método utilizado para a auditoria do sistema Helios Voting na UFLA foi dividido em três fases, a saber, "Planejamento", "Execução" e a "Entrega do relatório".

2.1 Planejamento

Na fase **Planejamento**, foram definidos três objetivos genéricos que um possível atacante poderia ter [10]: (i) impedir a realização da eleição (Seção 3.2); (ii) quebrar o sigilo da eleição (Seção 3.3); e (iii) interferir no resultado da eleição (Seção 3.4). Uma vez que cada um desses objetivos pode provocar consequências danosas ao processo eleitoral, não seria preciso que o atacante obtivesse êxito em todos eles. Tais objetivos foram utilizados como critérios de auditoria, a fim de se comprovar a conformidade ou não do sistema Helios Voting na UFLA.

2.2 Execução

Uma auditoria não pode ser baseada em opiniões ou avaliações pessoais dos indivíduos envolvidos nela, portanto, as conformidades e não conformidades devem ser aplicadas com base em evidências [9]. Assim sendo, na fase **Execução**, foram realizadas ações para a coleta de evidências que pudessem comprovar ou não a violação de um ou mais dos critérios de auditoria. Dentre estas ações, estão: (i) realização de uma reunião presencial entre a equipe de auditoria e a DGTI, para conhecimento do sistema e dos processos estabelecidos pelo setor em questão; (ii) levantamento bibliográfico sobre o sistema Helios Voting; (iii) envio de ofício de requisição para acesso remoto aos servidores de aplicação, banco de dados e e-mail; (iv) acesso ao ambiente de produção onde estava hospedado o sistema Helios Voting; entre outros.

2.3 Relatório

Por fim, a fase **Entrega do relatório** consistiu na elaboração, revisão e entrega da versão final do relatório de auditoria, que inclui um conjunto de recomendações para aprimoramento do sistema de votação eletrônica na UFLA, utilizando o Helios Voting.

Capítulo 3

Execução dos trabalhos

3.1 Identificação dos principais objetos da auditoria

Como já mencionado no capítulo 2, o trabalho desta auditoria focou suas atenções na investigação dos registros dos sistemas envolvidos na execução do sistema Helios Voting durante o período da Consulta Eleitoral e na busca por quaisquer evidências que pudessem apontar incoerências no seu funcionamento.

Uma vez iniciado o projeto da auditoria, os membros da equipe de auditores se reuniram virtualmente e definiram as estratégias e os principais pontos a serem avaliados durante os trabalhos. A primeira atividade a ser realizada foi a leitura e análise de toda a documentação disponibilizada, onde se destaca o relatório final da Comissão Organizadora da Consulta Pública. Após esta etapa, a equipe definiu que a próxima ação a ser realizada seria uma reunião presencial com a equipe da DGTI-UFLA, para colher informações sobre os procedimentos adotados na instalação do sistema Helios Voting, seu processo de customização e os passos adotados por aquela equipe ao longo da Consulta Eleitoral, objeto desta auditoria.

No dia 12 de Abril de 2024, a equipe de auditores se reuniu, nas dependências da DGTI-UFLA, com a equipe de servidores daquele setor que trabalharam na instalação, customização, configuração e disponibilização do sistema Helios Voting utilizado na referida Consulta Eleitoral. Participaram da reunião, além dos quatro membros da equipe de auditores, as seguintes pessoas: Erasmo Evangelista de Oliveira (Diretor DGTI); Fernando Elias de Oliveira (Coordenador de Operação e Segurança da Informação); Thiago Beloti Furtado (Coordenador de Sistemas de Informação); Giovanni Viol Assis; e Thiago do Prados Ramos (Coordenador de Infraestrutura Computacional). Vale lembrar que a reunião aconteceu em um período no qual os servidores da UFLA estavam em greve e, ainda assim, se disponibilizaram a atender os auditores.

Durante a reunião foi informado a existência de um disco rígido onde fora realizado, em 28 de dezembro de 2023, uma clonagem (*backup*) de todos os servidores envolvidos na operacionalização do sistema Helios Voting durante a realização da Consulta Eleitoral. Esta mídia, que estava de posse, em envelope lacrado, da administração superior da UFLA, foi prontamente disponibilizada para a equipe de auditores. Também foi solicitado à direção da DGTI, o acesso aos servidores de votação clonados e que estavam em produção. Este acesso foi prontamente disponibilizado, o que permitiu aos auditores acessá-los e baixar os arquivos de log, o código-fonte do sistema Helios Voting utilizado, os dados do Banco de Dados e todas as demais informações pertinentes ao trabalho de

auditoria.

Os auditores também enviaram um e-mail a todos os membros da Comissão Organizadora da Consulta Pública, questionando sobre informações adicionais que, porventura, não constassem no relatório apresentado pela mesma e que pudessem apontar possíveis irregularidades e/ou inconsistências do sistema Helios Voting. Em resposta, um dos membros da comissão respondeu não ter havido, durante o período da Consulta Eleitoral, qualquer evento que merecesse destaque e que não tivesse sido relatado no relatório final dessa Comissão.

De posse dos dados constantes no referido disco rígido, que continha a clonagem dos servidores e também dos dados coletados nos servidores em produção[1], foi possível verificar a consistência dos dados fornecidos e validar que os dados disponibilizados pelo processo de clonagem correspondiam aos servidores que operacionalizaram o uso do sistema Helios Voting durante a Consulta Eleitoral. Foi verificado, por exemplo, que os arquivos de banco de dados utilizado pelo Helios Voting no *backup* eram compatíveis com o do servidor em produção, pois apresentavam da mesma maneira os registros relativos à votação eletrônica da consulta pública. Obviamente, foi possível verificar a existência de registros posteriores, relativos a votações mais recentes. Aqui vale destacar que os quatro auditores, ao receberem a mídia com o clone dos servidores, o acesso ao sistema Helios Voting e aos servidores em produção, assinaram um termo de confidencialidade dos dados ali disponíveis, de modo a garantir os termos da LGPD (Lei Geral de Proteção de Dados).

Atestada a confiabilidade dos dados fornecidos e coletados, a equipe de auditores passou a analisar os registros do sistema e o resultado deste trabalho é apresentado nas seções seguintes deste capítulo.

3.2 A1 - Impedir a realização da eleição

3.2.1 Análise do servidor Web

A análise de eventuais problemas no servidor Web, que hospeda o sistema Helios Voting, envolveu o estudo do arquivo "error.log", gerado de forma automática pela aplicação em questão (Apache). De acordo com o site oficial da ferramenta, o referido arquivo é o mais importante gerado pelo Apache. É para ele que a aplicação enviará informações de diagnóstico e registrará quaisquer erros encontrados no processamento de solicitações. É o primeiro lugar a procurar quando ocorre um problema ao iniciar o servidor ou à operação do servidor, pois geralmente contém detalhes sobre o que deu errado e como corrigir o problema. Os erros em tais logs estão divididos conforme apresentado na Tabela 3.1:

O objetivo aqui é entender se a aplicação passou por problemas sérios que poderiam, de alguma forma, prejudicar o andamento da consulta eleitoral. Portanto, o foco da análise é nas mensagens de alerta dos seguintes níveis: *error*, *crit*, *alert* e *emerg*. Os arquivos de log dos dias 21 e 22 de novembro de 2023 formaram a base de tal análise.

Ao longo do dia 21 (dia anterior à Consulta Eleitoral), 120 eventos foram registrados

[1]Por "servidor em produção", entende-se um servidor que está em execução naquele momento, estando em seu completo funcionamento. Geralmente essa definição é utilizada em contraposição a um servidor de testes ou a um *backup* do sistema.

Tabela 3.1: Níveis de alerta do servidor Web - Apache

Nível	**Descrição**
emerg	Sistema é inutilizável
alert	Ação deve ser tomada imediatamente
crit	Condições críticas
error	Condições de erro
warn	Avisos
notice	Condições normais, mas significativas
info	Mensagens informativas
debug	Mensagens de depuração

no arquivo "error.log". A Figura x, ilustra a distribuição desses 120 eventos nos quatro níveis de interesse. É possível notar que nenhum problema grave (*emerg*, *alert* e *crit*) foi identificado em tal dia. Sobre as 116 mensagens de erro, elas estão concentradas nos seguintes tipos:

- ***authz core:error*** - alertas relacionados ao módulo de autenticação do Apache
- ***ssl:error*** - alertas relacionados ao módulo SSL/TLS do Apache
- ***wsgi:error*** - alertas relacionados ao módulo WSGI do Apache

Somente um alerta do tipo "error", relacionado ao módulo de autenticação, foi encontrado. Um cliente com endereço IP gerenciado pelo Google tentou acessar um determinado recurso do Helios Voting e foi impedido por não ter fornecido as credenciais de acesso. Considerando que o sistema Helios Voting está aberto para a Internet, essa é uma mensagem de alerta esperada. Veja o exemplo da mensagem: *AH01630: client denied by server configuration: /opt/helios/wsgi.py [client 35.216.166.21:42396].*

O módulo relacionado a SSL/TLS também produziu somente um alerta do nível "error". Um cliente com endereço IP gerenciado pela Amazon teve a sessão TLS rejeitada pelo servidor. O servidor do sistema Helios Voting pode ter simplesmente rejeitado uma solicitação por conta de uma escolha inadequada dos parâmetros TLS. Outra possibilidade pode estar associada com a execução de testes de vulnerabilidade oferecidos por plataformas como *Qualys SSL Labs*[2]. Em ambos os casos, consideramos um comportamento comum para um servidor exposto à Internet. A mensagem completa que foi emitida é: *AH02042: rejecting client initiated renegotiation [client 18.212.156.106:46992].*

Por fim, 114 mensagens de alerta foram geradas pelo módulo WSGI. O *mod_wsgi* é um módulo Apache usado para hospedar qualquer aplicativo Web escrito na linguagem Python, que suporte a especificação Python WSGI (*Web Server Gateway Interface*). Portanto, é um módulo comum do Apache, usado para encaminhamento de requisições escritas na linguagem Python, que é o caso do Helios Voting. É importante notar que o módulo *mod_wsgi*, concentra todos os tipos de mensagens de alerta dentro de

[2]https://www.ssllabs.com

[wsgi:error], ou seja, é possível ter alertas do tipo *info* e *warn* dentro do tipo *[wsgi:error]*. Esses dois exemplos ilustram essa situação:

- *[Tue Nov 21 15:47:03.007831 2023] [wsgi:error] [pid 443345:tid 139970439493184] [remot[redacted]0] 2023-11-21 15:47:03,005 INFO URL https://vote.ufla.br/helios/t/votacao-reitoria-docentes/apurador1@ufla.br/AUHmrqmf7NiB*
- *[Tue Nov 21 06:34:48.042267 2023]; [wsgi:error]; [pid 443345:tid 139970531812928]; [remote 66.249.73.198:47376]; 2023-11-21 06:34:48,041 WARNING Not Found: /robots.txt*

Nenhum alerta crítico ou de interesse para a auditoria foi encontrado no arquivo do dia 21 de novembro de 2023.

No decorrer do dia 22 de novembro de 2023, dia da Consulta Eleitoral, o número de alertas gerados pelo Apache e presentes no arquivo "error.log" cresceu consideravelmente, o que já era esperado. Novamente, nenhum alerta crítico (*emerg*, *alert* e *crit*) foi encontrado no arquivo. Dos 6834 alertas gerados, 6830 alertas estão associados ao módulo WSGI do Apache. A grande maioria dos alertas está relacionado a mensagens de aviso típicas da aplicação Helios Voting. Contudo, alguns alertas (41), estão relacionados a erros (*Internal Server Error*) em três URLs do Helios Voting:

- `vote.ufla.br/helios/elections/40a3af40-889f-11ee-b609-c3201c6b5e99/view` - Urna dos Discentes
- `vote.ufla.br/helios/elections/111db7c6-889e-11ee-b609-c3201c6b5e99/view` - Urna dos Docentes
- `vote.ufla.br/helios/elections/c6cdf418-889a-11ee-b609-c3201c6b5e99/view` - - Urna dos Técnicos administrativos

Como cada um dos erros possui o endereço IP de origem, decidimos investigar cada um dos alertas para tentar entender o ocorrido. Cada um dos endereços IP presentes nos 41 alertas foi cruzado com a lista de endereços IP que acessaram o sistema Helios Voting no dia da eleição gerada pelo DGTI-UFLA e também com o arquivo "access.log" do Apache, que registra todos os acessos ao sistema Helios Voting.

A análise mostra que dos 27 endereços IPs associados aos 41 alertas, 17 deles depositaram corretamente seus votos. Ou seja, o erro registrado pelo sistema não impediu que o usuário associado a tal endereço IP depositasse o seu voto. Contudo, 10 endereços IP presentes em tais alertas não registraram o seu voto no sistema. As razões para isso podem ser as mais diversas possíveis. Ao investigar o arquivo "access.log" é possível elaborar os seguintes pontos:

- Em alguns casos, é possível notar que o usuário associado a um dos endereços IP em questão acessou o sistema, fez as escolhas mas não depositou o voto. Isso é um comportamento que pode ocorrer, visto que o Helios Voting exige, depois da seleção das escolhas, que o usuário confirme o depósito do voto;

- Em outros casos, o usuário associado a um dos endereços IP em questão teve a sessão encerrada por conta de inatividade (*timeout*) e não acessou o sistema novamente usando tal endereço IP.

Além disso, como os endereços IP são reusados pelos provedores de Internet, é possível que os usuários associados a tais endereços IP tenham acessado o sistema em um outro momento, a partir de outro endereço IP e depositado o seu voto. De toda a forma, de um universo de mais de 5725 votantes, é um número extremamente baixo, que não implica em qualquer suspeição perante a indisponibilidade do sistema.

3.2.2 Análise da infraestrutura de rede

O DGTI-UFLA disponibilizou diversos relatórios sobre a disponibilidade do ambiente computacional necessário para o funcionamento do sistema Helios Voting durante o dia 22 de novembro de 2023. Tais dados são sumarizados nas Figuras 3.1, 3.2 e 3.3.

Figura 3.1: Disponibilidade do servidor web - Apache - 1

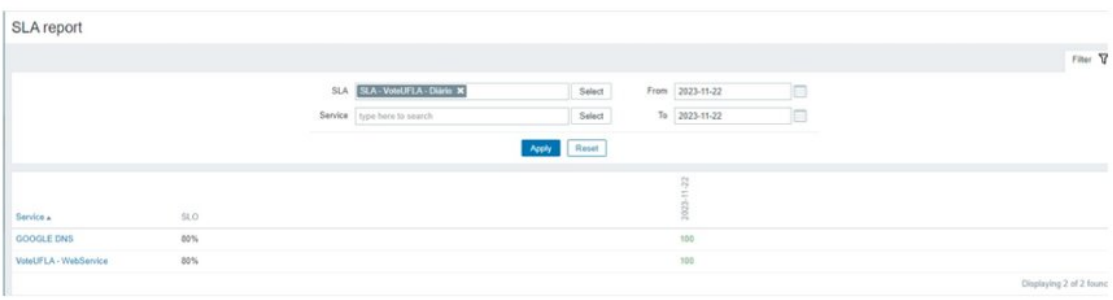

Figura 3.2: Disponibilidade do servidor web - Apache - 2

As Figuras 3.1 e 3.2 ilustram a disponibilidade do servidor Web - Apache - que hospedou o sistema Helios Voting. É possível notar que não houve problemas de interrupção no serviço durante a eleição. Além disso, detalhes sobre o consumo de banda durante a consulta eleitoral são vistos na Figura 3.3. O número de bytes recebidos/transferidos só diminui perto do fim da eleição, dentro do comportamento esperado. Em nenhum momento, a taxa de bytes recebidos/transferidos apresentou valores condizentes com eventuais ataques de disrupção ao serviço Web. Portanto, a análise apresentada nesta seção indica que o sistema se comportou dentro do esperado.

Figura 3.3: Consumo de banda do servidor web - Apache

3.3 A2 - Quebrar o sigilo da eleição

3.3.1 Análise do acesso às chaves privadas

Foram definidos três apuradores no processo eleitoral, além do próprio sistema Helios Voting. Cada apurador possuía a sua própria chave privada. O acesso a somente uma das chaves privadas não permite a decifragem e, portanto, quebra do sigilo da eleição. Ou seja, um atacante teria que ter as três chaves privadas de cada um dos usuários e também ter acesso à chave privada do próprio Helios Voting. De acordo com consultas feitas à Comissão Eleitoral, nenhuma intercorrência aconteceu nesse sentido. Isso foi confirmado em reunião com a DGTI-UFLA. Outro ponto relevante é que o processo de apuração de votos e, consequentemente, decifragem do mesmo, aconteceu logo após o encerramento da pleito, às 21h01, em sessão pública e gravada no YouTube[3]. Portanto, não foram encontrados indícios de acesso indevido às chaves privadas da eleição.

3.3.2 Análise do processo de decifragem dos votos

A análise do processo de decifram dos votos consistiu em examinar o conteúdo do banco de dados do sistema Helios Voting. A ideia aqui é verificar (i) se os apuradores foram realmente adicionados no sistema, (ii) se a eleição foi congelada, (iii) se o processo de decifragem realmente envolveu somente os três apuradores e (iv) se o processo de decifragem ocorreu exatamente no período esperado.

A Tabela 3.2 mostra os dados coletados da tabela *helios_electionlog* do bando de dados do Helios Voting. É importante destacar que tais dados foram coletados diretamente do ambiente responsável pela execução da eleição no dia 22 de novembro de 2023.

Os três apuradores foram adicionados um dia antes da eleição e a eleição foi congelada no mesmo dia, alguns minutos depois. O processo de decifragem ocorreu somente após a finalização da eleição, após às 21h. Portanto, não foi encontrada nenhuma evidência sobre problemas associados a decifragem dos votos.

[3]https://www.youtube.com/watch?v=8whNBOEgexo

Tabela 3.2:

Status	**Dia e hora**
Trustee apurador1 added	21/11/2023 15:56
Trustee apurador2 added	21/11/2023 15:57
Trustee apurador3 added	21/11/2023 15:57
frozen	21/11/2023 16:03
decryptions combined	22/11/2023 21:07
decryptions combined	22/11/2023 21:09
decryptions combined	22/11/2023 21:11

3.4 A3 - Interferir no resultado da eleição

3.4.1 Análise dos votos depositados durante o período estipulado para a eleição

O objetivo desta análise é verificar se os votos foram depositados somente dentro do horário estipulado da consulta eleitoral: 08h00 - 21h00. Para isso, duas abordagens foram investigadas: (i) verificar se nenhuma tentativa foi feita diretamente pela aplicação do Helios Voting; e (ii) verificar se nenhuma tentativa foi feita diretamente pelo banco de dados do Helios Voting.

A primeira abordagem envolve analisar o arquivo "access.log" do servidor Web Apache, que hospedou o Helios Voting. A busca nos arquivos de log se resumiu a encontrar o primeiro e último voto depositado, a partir da chamada do método *cast_confirm* por meio de uma requisição HTTP POST. Os resultados encontrados indicam que nenhum voto foi depositado em horários fora do estipulado, a partir da aplicação Helios Voting. Primeiro voto depositado:

189.93.234.28 - - [22/Nov/2023:08:00:49 -0300] "POST /helios/elections/40a3af40-889f-11ee-b609-c3201c6b5e99/cast_confirm HTTP/1.1"302 1096 "https://vote.ufla.br/helios/elections/40a3af40-889f-11ee-b609-c3201c6b5e99/cast_confirmMozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Mobile Safari/537.36"

Último voto depositado:

[redacted]*- - [22/Nov/2023:21:00:04 -0300] "POST /helios/elections/40a3af40-889f-11ee-b609-c3201c6b5e99/cast_confirm HTTP/1.1"302 5669 "https://vote.ufla.br/helios/elections/40a3af40-889f-11ee-b609-c3201c6b5e99/cast_confirmMozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36"*

A segunda abordagem envolve a investigação dos votos depositados, a partir do próprio banco de dados do Helios Voting. Para tanto, os auditores trabalharam com um *dump* do banco de dados do sistema Helios Voting, extraído da própria máquina que hospedou tal aplicação. Os trabalhos se concentraram na análise da tabela *helios_castvote* do banco de dados, que é preenchida assim que os usuários confirmam o seu voto na aplicação. A análise dos dados mostra que o primeiro voto inserido para

quaisquer das três urnas da consulta eleitoral para reitor aconteceu no dia 22 de novembro de 2023 às 08:00:49. Já o último voto foi registrado no banco de dados às 20:59:56. Primeiro voto depositado no banco de dados:

s94g9LM1Qk8+iq2mspv3owVSy36ZBTIwPU4l9INANRA às 08:00:49

Último voto depositado no banco de dados:

7zJsEQ1z8o9IuST8SUzu9wsBU/u7Mpz4qyDFgZ6cGJ8 às 20:59:56

Portanto, nenhuma anormalidade foi encontrada sobre inserções/alterações de votos em períodos fora do estipulado para a consulta eleitoral.

3.4.2 Análise do perfil de votação durante o período estipulado para a eleição

Para fins de contextualização, é importante salientar que a DGTI desenvolveu um *script* (trecho de código executável) que registrava algumas informações do usuário quando ele se autenticava no sistema Helios Voting. Estas informações são: o *IP* de acesso, a *data/hora* do acesso, o *login* e o *nome do usuário*. Este *script* também foi objeto de análise pela equipe de auditoria e o parecer se encontra na Seção 3.4.6 deste relatório.

A partir dos registros feitos por este *script*, foi possível verificar se havia alguma anomalia (observação que se desviava do que é padrão ou esperado) nos dados de acessos dos usuários. Isso foi realizado por meio de três tipos de análise, saber: (i) análise da quantidade de acessos de usuários por intervalo de tempo; (ii) análise da quantidade de IPs compartilhados por mais de um usuário; e (iii) análise da quantidade de usuários que fizeram acessos no sistema a partir de múltiplos IPs.

Análise da quantidade de acessos de usuários por intervalo de tempo

Para este tipo de análise, os registros gerados pelo *script* da DGTI foram importados em uma planilha eletrônica e um gráfico (Figura 3.4) foi gerado, a fim de evidenciar o padrão de acesso ao sistema Helios Voting. Este gráfico pode ser interpretado da seguinte forma: no eixo Y, têm-se os horários de acesso ao sistema, enquanto que no eixo X, têm-se a quantidade acumulada de acessos ao sistema Helios Voting.

A curva crescente apresentada no gráfico da Figura 3.4 indica que os acessos ao sistema ocorreram de forma bem distribuída ao longo do período de votação. Um acesso em massa ao sistema - muitos usuários acessando o sistema ao mesmo tempo - ficaria evidenciado por um platô neste gráfico. Cabe aqui ressaltar que o acesso ao Helios Voting não implica, necessariamente, que houve um depósito do voto; o eleitor pode ter acessado unicamente para verificar as opções.

O resultado obtido com a análise dos logs de acesso ao Helios Voting foram comparados com o envio de e-mail pelo usuário helios junto ao servidor de e-mail, que se encontrava em outro servidor. Um gráfico bastante similar foi obtido ao levantarmos o envio de e-mail realizado por esta conta (Figura 3.5). Neste gráfico, é possível verificar que a curvatura é bastante similar. O número menor de e-mails enviados refere-se ao fato que o Helios Voting envia e-mail apenas para confirmar a votação, não o acesso.

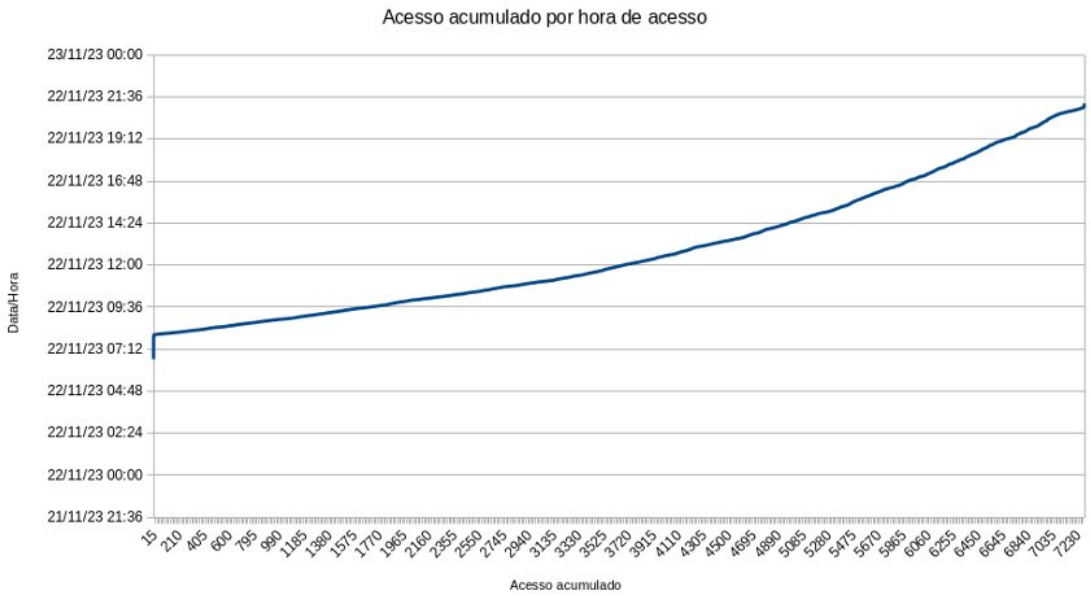

Figura 3.4: Quantidades de acesso ao servidor (valor acumulado)

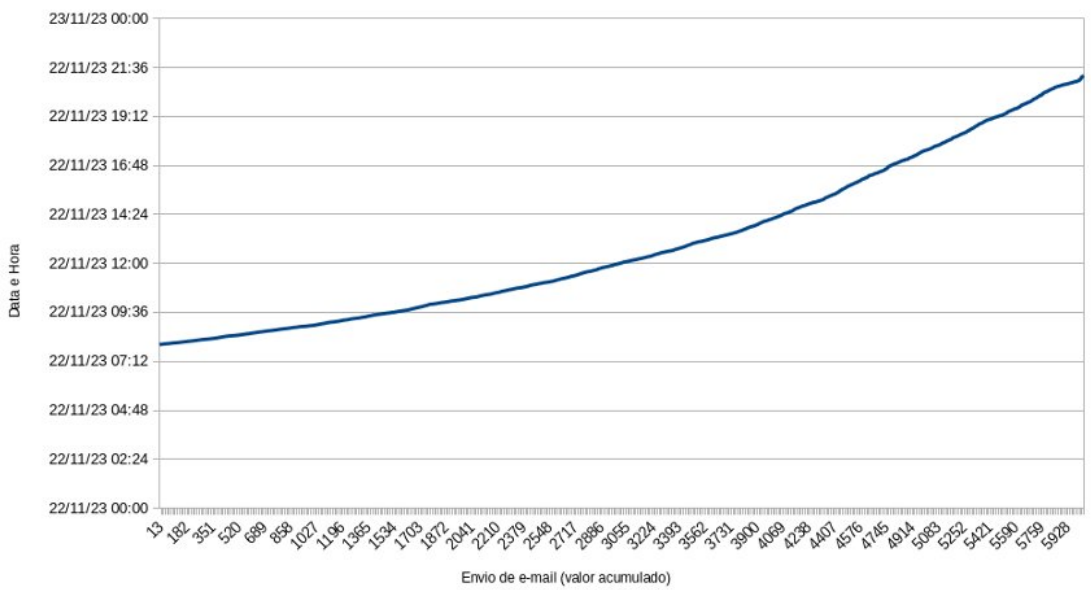

Figura 3.5: Quantidades de envio de e-mail pelo usuário do Helios (valor acumulado)

Nesse sentido, destaca-se que os dados obtidos no servidor de e-mail mostraram-se compatíveis com os registros de acesso ao Helio. Mais ainda, ambos mostraram-se dentro da normalidade para a equipe de auditoria. Por exemplo, seria bastante suspeito se tívessemos verificado uma grande quantidade de e-mails de votos depositados sendo enviados no mesmo momento (bots ou invasores votando) – platô – ou um grande período de tempo sem envio de emails (poderiam ter bloqueado o serviço de email) - representado por uma subida acentuada (quase vertical) no gráfico.

Análise da quantidade de IPs compartilhados por mais de um usuário

.

Para esta análise, a equipe de auditoria desenvolveu um *script* capaz de ler os registros de acessos ao sistema Helios Voting e gerar como saída um arquivo, conforme exemplificado na Tabela 3.3. A primeira coluna desta tabela apresenta o endereço IP utilizado para acessar o sistema Helios Voting, a segunda apresenta a quantidade de logins que utilizaram este IP e a terceira descreve quais login foram estes.

Tabela 3.3: Dados de acesso ao sistema Helios Voting, agrupados por IP

IP	**Quantidade de logins**	**Logins que utilizaram o IP**
ip1	2	login1, login2
ip2	1	login3

É importante salientar que todos os arquivos e *scripts* utilizados durante a auditoria estão disponíveis para acesso, caso necessário, e que dados fictícios foram adotados neste relatório, a fim de não expor conteúdo sensível dos usuários do sistema.

A partir deste agrupamento de dados, foi possível observar que a maior parte dos endereços IP (aproximadamente 85%) foram utilizados exclusivamente por um único usuário. No entanto, existem alguns casos de endereços IP compartilhados por mais de um usuário, com destaque para os seguintes: IP 187.60.128.134, compartilhado por 15 logins; IP [redacted] compartilhado por 20 logins; e IP [redacted] compartilhado por 677 logins.

Após uma análise destes endereços IP, verificou-se que o IP 187.60.128.134 é do provedor de Internet *Stratus Telecomunicações*, possivelmente utilizado por alguma república. O IP [redacted] compartilhado por 677 logins, é o IP utilizado pela rede sem fio UFLA+. Ou seja, é um um IP utilizado por qualquer usuário da principal rede sem fio da UFLA. O IP [redacted] (*m232-lemaffuturo*), compartilhado por 20 logins, também pertence à UFLA. Apesar de o nome se referir ao LEMAF (Laboratório de Estudos e Projetos em Manejo Florestal), segundo o responsável pela Coordenadoria de Infraestrutura Computacional da UFLA, este é um IP que faz o NAT (*Network address translation*) para os laboratórios da ABI (Área Básica de Ingresso das Engenharias).

Aqui cabe pontuar que, muitas vezes, a atribuição de nomes de servidores e equipamentos não acompanha o uso atual desses equipamentos. Muitas vezes, roteadores e servidores de um dado espaço físico são movimentados, sem que se faça a devida adequação da configuração no serviço de nomes. Essa não é uma boa prática, mas é compreensível em se tratando de equipes de TI com deficiência de pessoal, o que infelizmente sabemos ser o caso das maiorias das instituições superiores de ensino, que tem perdido seus quadros para a iniciativa privada. Entretanto, cabe destacar que, como o equipamento é um roteador que faz NAT, é extremamente natural a quantidade de acessos vindo deste IP. Assim, indiferente se o IP [redacted] refira-se a um laboratório para as ABIs ou para o LEMAF, 20 acessos são uma quantidade perfeitamente dentro do que é normal para um equipamento deste tipo.

No que diz respeito ao IP 187.60.128.134, como já apontado anteriormente, a equipe suspeita que trata-se de uma república ou algo similar. Essa suspeita, entretanto, não pode ser verificada com facilidade, principalmente por conta da LGPD. Ou seja, mesmo

que a equipe consultasse a provedora de acesso para obter essa informação, a mesma estaria cometendo um crime ao fornecer esses dados sem amparo legal.

Por fim, foi possível verificar que todos os outros compartilhamentos possuíam bem menos que 15 usuários por ponto de acesso. Dado o contexto da comunidade acadêmica, com endereços IP compartilhados em repúblicas ou locais similares, já era esperado casos em que vários usuários (em geral menos que 10) acessassem o sistema de um mesmo endereço IP. Dessa maneira, para a equipe de auditoria, o acesso ao sistema esteve dentro do esperado, não apresentando indícios que levantassem maiores suspeitas.

Análise da quantidade de usuários que fizeram acessos no sistema a partir de diferentes IPs

Analogamente, para esta análise, a equipe de auditoria desenvolveu um *script* capaz de ler os registros de acessos ao sistema Helios Voting e gerar como saída um arquivo, conforme disposto no exemplo da Tabela 3.4. A primeira coluna desta tabela apresenta o login utilizado para acessar o Helios Voting, a segunda apresenta a quantidade de acessos que este login fez no sistema e a terceira indica se estes acessos foram feitos de apenas um endereço IP ou se vieram de múltiplos IPs.

Tabela 3.4: Dados de acesso ao sistema Helios Voting, agrupados por Login

Login	**Quantidade de acessos**	**Usou múltiplos IPs?**
login1	2	True
login2	1	False

A partir deste agrupamento de dados, foi possível observar que a maioria dos usuários fez acesso ao sistema apenas uma vez e, portanto, de um único IP. A capacidade de o usuário realizar acessos várias vezes ao sistema é uma característica do próprio sistema Helios Voting. O fato de um mesmo usuário ter acessado o sistema a partir de endereços IP diferentes por ser explicado por diversas maneiras, tais como: (i) o usuário realizou um acesso na UFLA e outro mais tarde, em casa, onde o IP era diferente; (ii) o usuário fez mais de um acesso ao sistema conectado à rede móvel do seu dispositivo e pode ter havido mudança de torre entre um acesso e outro; entre outros.

Entre os casos pontuais, destaca-se que um usuário acessou o sistema 9 vezes, três usuários acessaram o sistema 7 vezes, doze usuários acessaram 6 vezes e onze usuários acessaram o sistema 5 vezes. Assim, tem-se que menos que 30 usuários acessaram o sistema cinco vezes ou mais. É importante destacar, novamente, que o acesso ao sistema Helios Voting não implica no depósito do voto, apenas no login do usuário. Essa quantidade de acessos já era esperado por parte de usuários indecisos ou ansiosos em verificar se sua opção encontrava-se mantida. A baixa quantidade de usuários nessa situação indicou normalidade do processo de votação, no que diz respeito a esse quesito.

3.4.3 Análise dos votantes

Para esta análise é importante entender dois conceitos do sistema Helios Voting customizado pela equipe da DGTI-UFLA:

- **Modulo de Auditoria:** conforme explicado no início da Seção 3.4.2, durante o processo de customização do sistema Helios Voting pela equipe da DGTI, foi adicionado um *script* no código-fonte do Helios que permitiu registrar, em arquivo de log chamado *log_acessos_helios_dd-mm-aa.txt*, o momento que o usuário acessava o sistema, sua identificação e o IP de onde esse acesso era feito. A existência desse registro não garante que aquele eleitor tenha, de fato, depositado uma cédula na urna eletrônica, uma vez que, após acessar o Helios Voting, o usuário pode simplesmente abandonar o sistema sem confirmar seu voto.

- **Registro de votos depositados do Helios:** o sistema Helios Voting disponibiliza, tanto durante a votação, como após a apuração dos votos, a relação de todos os eleitores cadastrados e aptos a votar, bem como um campo com um código *hash* que indica que aquele eleitor depositou uma cédula na urna eletrônica e que o permite rastrear sua cédula para garantir que, de fato, ela foi depositada. Veja que este processo não permite ao eleitor verificar em quem ele de fato votou e sim, apenas, garantir que a cédula foi depositada. Esta é uma função nativa do Helios disponibilizada pelos seus criadores e que não pode ser modificada;

Novamente, o *script* de auditoria implementado pela DGTI, que registra todo o eleitor que se loga ao Helios Voting, não garante que este eleitor tenha de fato depositado uma cédula na urna, pois, como já mencionado anteriormente, este pode abandonar o sistema antes de confirmar o depósito da mesma. No entanto, se cruzarmos esta informação com log do Helios Voting e for encontrado um eleitor com o código *hash* e que não tenha sido registrado pelo sistema de auditoria implementado, isso indicaria que este voto teria sido inserido na base de dados do Helios Voting de forma maliciosa, ou seja, o voto não teria sido depositado pelo sistema.

Esse recurso permitiu à equipe de auditores cruzar as informações dos dois sistemas de registro e conferir se, de fato, todos os eleitores com cédulas depositadas tiveram, ao menos, um registro realizado pelo sistema de auditoria. Essa conferência foi realizada através da construção de duas tabelas, uma com os registro do Helios Voting e outra com o registro do dito módulo de auditoria. Ao final do processo, pode-se constatar que todos os eleitores com cédulas depositadas possuíam ao menos um registro no arquivo de log do sistema de auditoria implementado pela DGTI.

3.4.4 Análise de usuários potencialmente comprometidos

Para esta análise, a equipe de auditoria desenvolveu um *script* capaz de ler os registros de acessos ao sistema Helios Voting e compará-los com os logins de usuários que apareceram nos alertas do Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pesquisa (CAIS-RNP), como potencialmente comprometidos. Além disso, este *script* gera um arquivo com dados agrupados, conforme exemplo apresentado na Tabela 3.5. A primeira coluna desta tabela apresenta o login utilizado para acessar o sistema Helios Voting, a segunda apresenta se este login estava na listagem de alertas do CAIS-RNP e a terceira indica a partir de quais endereços IP estes acessos foram feitos.

A partir da análise deste arquivo, foi possível observar que 35 (trinta e cinco) logins que acessaram o sistema Helios Voting estavam na lista do CAIS-RNP, sendo que apenas

Tabela 3.5: Credenciais potencialmente comprometidas, de acordo com o CAIS-RNP

Login	**Login comprometido?**	**Endereços de IP utilizados**
login1	True	ip1, ip2
login2	False	ip3

2 deles acessaram o sistema utilizando um mesmo endereço de IP. Diante disto, concluise que não há indícios de que os dados de login potencialmente comprometidos foram utilizados por agentes mau-intencionados (humanos ou software) para adicionar votos ao sistema Helios Voting.

3.4.5 Análise do acesso remoto aos sistemas responsáveis pela eleição

Durante a reunião com a DGTI, esta nos informou que não houve qualquer acesso da equipe ao servidor de votação durante o processo de eleição. Para e equipe de auditoria, confirmar essa afirmativa era extremamente importante, uma vez que garantiria que não houve tentativas de modificação do sistema ou de seus resultados durante o processo de votação eletrônica. Para tanto verificamos tanto o servidor em produção como o *backup* fornecido. Foi possível verificar que o servidor foi acessado apenas nos dias 21 e 23 de novembro de 2023. No dia 21, o sistema foi acessado pelos usuários *erasmo* e *fernando.oliveira*, sendo o último acesso às 17h58, pelo usuário *erasmo*. Esse mesmo usuário acessou o sistema novamente às 11h13 no dia 23. Não foi identificado qualquer outro acesso entre as 17h58 do dia 22 e as 11h13 do dia 23.

Essa verificação foi realizada por análise de diversos arquivos de registro (logs) do sistema, incluindo */var/syslog* e */var/lastlog*. Este último, inclusive, é um arquivo em formato binário, não sendo trivial a sua alteração. Mesmo com sua alteração, outros rastros poderiam ser percebidos em outros arquivos de logs. Dessa maneira, é possível afirmar que não houve realmente acesso ao servidor utilizado para hospedar a votação no dia da consulta pública, como informado pela diretoria da DGTI.

3.4.6 Análise do código-fonte do sistema

O objetivo desta análise é verificar a consistência do código-fonte do sistema usado na eleição. Para isso, alguns arquivos Python (módulos) presentes no código-fonte do sistema usado no dia da eleição foram comparados com o conteúdo do código-fonte presente no repositório original do Helios Voting [4]. Utilizamos uma ferramenta de visualização de diferenças em código-fonte para estudar os seguintes módulos Python, descritos na Tabela 3.6.

É importante notar que tais módulos foram escolhidos devido a potenciais alterações que poderiam ocorrer para uma eventual manipulação da eleição. Por exemplo, alterar os parâmetros criptográficos definidos no código-fonte original para outros mais "fracos" ou inserção de trechos de código maliciosos (*backdoors*). Os resultados presentes na Tabela 3.6, mostram que os principais módulos internos do sistema Helios Voting que foram executados no dia eleição estão consistentes com o esperado, ou seja, apenas

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

Tabela 3.6: Módulos do código-fonte do Helios Voting analisados pela equipe de auditoria

Nome do módulo Python	**Caminho**	**Diferenças**
algs.py	helios/crypto	Nenhuma alteração
electionalgs.py	helios/crypto	Nenhuma alteração
elgamal.py	helios/crypto	Nenhuma alteração
numtheory.py	helios/crypto	Nenhuma alteração
utils.py	helios/crypto	Nenhuma alteração
models.py	helios	- Alterações ligadas a tradução do texto - Alterações ligadas ao fuso horário - Alteração na função que carrega arquivos de texto no sistema
security.py	helios	Nenhuma alteração
tasks.py	helios	- Alterações ligadas a tradução do texto
utils.py	helios	Nenhuma alteração
views.py	helios	- Alterações ligadas a tradução do texto - Alterações ligadas ao fuso horário
homomorphic.py	helios/workflows	Nenhuma alteração

pequenas alterações relacionadas a tradução do sistema, fuso horário e tratamento de arquivos de texto foram encontradas. Além disso, nenhuma modificação foi feita em tais arquivos nos dias anteriores ou ainda no mesmo dia da eleição.

Conforme mencionado na Seção 3.4.2, a DGTI desenvolveu um *script* que registrava algumas informações dos usuários (IP de acesso, data/hora do acesso, login e nome), no momento em que ele se autenticava no sistema Helios Voting. Este *script* foi implementado como um trecho dentro de um arquivo original do sistema Helios Voting, denominado *helios_auth/views.py*.

Apesar de ser possível apontar vulnerabilidades no código do *script* em questão (ver Seção 4), entende-se que elas não afetam a segurança da eleição. O *script* apenas consultava os dados acima dos usuários e os gravava em um arquivo de texto.

Capítulo 4

Considerações finais e recomendações

4.1 Conclusões

Com base nas informações levantadas, analisadas e apresentadas ao longo do Capítulo 3, **esta equipe de auditores se sente segura em afirmar não ter encontrado qualquer evidência que aponte irregularidades no uso do Sistema Helios Voting** - customizado, instalado, configurado e disponibilizado pela equipe da DGTI - durante a realização da Consulta Pública realizada em 22 de novembro de 2023, que subsidiou a organização da lista tríplice para escolha do Reitor(a) da UFLA para a Gestão 2024-2028.

4.2 Recomendações

Após o trabalho de coleta de dados a respeito dos processos que envolveram a referida Consulta Pública, esta comissão se sente na liberdade de apontar alguns pontos que possam tornar o uso do sistema Helios Voting, em futuras consultas públicas e eleições, ainda mais transparente para a comunidade universitária da UFLA, são eles:

1. Documentação de todas as práticas feitas pela DGTI, inclusive aquelas relacionadas a políticas de rede e segurança implementadas nos sistemas;

2. Criar uma máquina nova, específica para eleições mais importantes, como a para direção de faculdades ou a própria reitoria de reitor. Isso evitaria a contaminação dos arquivos de logs e de banco de dados de uma eleição mais importante com registros de eleições menos significativas;

3. Avaliar a possibilidade de permitir que o acesso ao sistema de votação Helios Voting seja feito somente a partir da rede interna da UFLA. Aqueles que não estejam presencialmente na Universidade poderiam acessar o sistema a partir de uma rede privada virtual (*VPN - Virtual Private Network*);

4. Padronizar o cadastro dos eleitores no sistema Helios Voting, de modo que sua identificação possa ser realizada de forma única, inequívoca e eficaz;

5. Remover senha *hard coded* do *script* utilizado para registrar informações dos usuários que se autenticaram no sistema Helios Voting e implementá-la em algum mecanismo mais seguro para controle de *secrets* - recomenda-se ainda checar se esta senha não foi "commitada" no sistema de controle de versões;

6. Fortalecer e capacitar a equipe de servidores da DGTI, de modo que estes possam trabalhar de forma mais tranquila, confiante e segura, proporcionando assim uma melhor qualidade nos serviços prestados no âmbito das TICs para a UFLA, e não somente. A *expertise* da equipe da DGTI no tema poderia ser aproveitada, por exemplo, para oferta do serviço de votação eletrônica para outras instituições.

Por fim, ainda que o Sistema Helios tenha se mostrado seguro e confiável, esta equipe considera que, especialmente em eleições para reitoria, a comissão eleitoral avalie seriamente a possibilidade de terceirizar o processo de votação eletrônica. Aqui não se questiona a capacidade técnica da DGTI, preocupa-nos a possibilidade de contaminação política do processo eleitoral, aumentando o risco de assédio moral a seus funcionários. Caso a comissão eleitoral não considere necessária a terceirização, recomenda-se que o processo eleitoral seja acompanhado por profissionais externos e independentes, com vistas a garantir que o mesmo seja isento de interferência.

Terminados os trabalhos, esta equipe de auditoria coloca-se à disposições para maiores esclarecimentos. Informamos, adicionalmente, que iremos manter os arquivos de *backup* e arquivos sensíveis por um prazo de 40 dias, caso sejam necessários para responder algum questionamento do Colégio Eleitoral. Após esta data, iremos apagar os arquivos sensíveis e devolveremos a mídia de *backup* à DGTI.

Bibliografia

[1] Mona FM Mursi, Ghazy MR Assassa, Ahmed Abdelhafez, and Kareem M Abo Samra. On the development of electronic voting: a survey. *International Journal of Computer Applications*, 61(16), 2013.

[2] Jéssica Pegorini, Natália Yada, Alinne Souza, Rodrigo Pagno, and Newton Will. Desafios e soluções em sistemas de votação eletrônica: Um mapeamento sistemático. In *Anais do IV Workshop de Tecnologia Eleitoral*, pages 13–24. SBC, 2019.

[3] Ben Adida. Helios: Web-based open-audit voting. In *USENIX security symposium*, volume 17, pages 335–348, 2008.

[4] Fábio Cristiano Souza Oliveira. Criptografia homomórfica aplicada ao voto eletrônico. Master's thesis, Universidade Federal de Pernambuco, 2014.

[5] Claiton Leoneti Lencina, Matheus Cruz, Renata Vieira Rodrigues Severo, and Rodrigo Costa de Moura. Guia para eleições eletrônicas na ufpel: Helios voting ufpel, 2021.

[6] Flávia Caroline Augusto Salmázio. A votação eletrônica ea representação discente nos conselhos superiores da universidade federal de são carlos. Master's thesis, Universidade Federal de São Carlos, 2020.

[7] Shirlei Aparecida de Chaves and Emerson Ribeiro de Mello. O uso de um sistema de votaç ao on-line para escolha do conselho universitário. 2014.

[8] Denis Clayton Alves Ramos and Rodolfo Nadai. Informatização das eleições e consultas da unicamp. *Sínteses: Revista Eletrônica do SimTec*, (6):28–28, 2016.

[9] André Campos. *Sistema De Seguranca Da Informacao - Controlando Os Riscos*. Visual Books, 2014.

[10] Cleovaldo José De Lima E Silva Junior, Igor Medeiros Vanderlei, Jean Carlos Teixeira De Araujo, and Rodrigo Rocha. Evaluation of open-source e-voting systems using helios voting in public university elections. In *Proceedings of the Brazilian Symposium on Multimedia and the Web*, WebMedia '22, page 11–18, New York, NY, USA, 2022. Association for Computing Machinery.

[11] Janniele Aparecida Soares Araujo, Helen de Cassia Sousa da Costa Lima, Fernando Bernardes de Oliviera, and Theo Silva Lins. Relatório de auditoria interna: Auditoria do sistema de votação eletrônica da universidade federal de ouro preto

intitulado sistema e-votação ufop. https://pesquisaparitaria.assufop.com.br/wp-content/uploads/2020/10/Relatorio_Auditoria_Interna_Helios_UFOP-1-1.pdf, 2020.