

Assunto **Resposta ao Ofício nº 52/2020 - COLÉGIO ELEITORAL - Processo nº 23064.016637/2020-21**  
De Silvino Schlickmann Junior <schlickmann.ssj@pf.gov.br>  
Para consultacomunidade@utfpr.edu.br <consultacomunidade@utfpr.edu.br>  
Data 22-07-2020 16:59



- 
- Informacao\_083\_2020\_SETEC\_SR\_PF\_PR.pdf (~149 KB)
- 

Referência: Processo nº 23064.016637/2020-21

Ofício nº 52/2020 - COLÉGIO ELEITORAL

Prezado Senhor,

Em resposta ao ofício da referência, encaminho em anexo a Informação 083/2020/SETEC/SR/PF/PR.

Atenciosamente,

Silvino Schlickmann Junior  
Perito Criminal Federal



Ministério da Justiça e Segurança Pública  
Polícia Federal  
Superintendência Regional de Polícia Federal no Paraná  
Setor Técnico-Científico

Informação Nº 083/2020/SETEC/SR/PF/PR

Curitiba, 22 de julho de 2020.

Ao  
Chefe do Setor Técnico-Científico

**Assunto: Relatório.**

1. Em resposta ao Ofício nº 79/2020 - GABIR-UTFPR, datado de 29/05/2020, no qual a Universidade Tecnológica Federal do Paraná solicitou apoio no acompanhamento ao processo de consulta para reitor da UTFPR – 2020 que se pretendia realizar através da plataforma de votação Helios Voting, o Sr. Chefe do Setor Técnico-Científico desta Superintendência de Polícia Federal, determinou que eu prestasse apoio aquela instituição educacional.
2. Em atendimento à determinação, mantive contato com o Professor Jair Ferreira de Almeida do Departamento de Processos Seletivos, que transmitiu, em linhas gerais, o planejamento para o processo de votação. Além disso, me colocou em contato com o Professor Joilson Alves Júnior, presidente da comissão técnica do processo de votação.
3. Esclareço que o sistema Helios Voting é um projeto desenvolvido por Ben Adida, em código fonte aberto, e que detém ótima reputação internacional. Seu repositório principal pode ser acessado através do endereço: <https://github.com/benadida/helios-server>. Como medida de precaução, e visando possibilitar à comunidade a oportunidade de verificação quanto ao funcionamento do sistema, e a fidelidade de seu código em relação à distribuição original do sistema Helios, a comissão eleitoral disponibilizou, em página criada para agrupar assuntos relativos a consulta para reitor, cópias dos arquivos que foram utilizados na instalação local do sistema Helios, bem como seus códigos hash. O arquivo compactado contendo o código fonte



Inf. 083/20-SETEC/PR

utilizado pode ser encontrado no endereço <http://portal.utfpr.edu.br/comissoes/consulta/consulta-para-reitor-2020/arquivos/helios-server-tar.gz>, e seus respectivos códigos hash no endereço: <http://portal.utfpr.edu.br/comissoes/consulta/consulta-para-reitor-2020/arquivos/md5sum.txt>.

4. Em decorrência das discussões mantidas com os Profs. Jair e Joilson, compareci à sede da UTFPR em 26/06/2020 para acompanhar o processo de configuração da eleição, mediante a criação e configuração de 39 urnas (eleições) em cópia local do sistema Helios Voting. Também presente, se encontrava Claudemir Pereira de Carvalho, do Tribunal Regional Eleitoral, igualmente cedido por aquela instituição para prestar apoio ao processo eletivo.

5. Durante a configuração das urnas, documentada através de ata (Anexo 01), foi observado elevado grau de proficiência por parte dos profissionais a cargo da configuração dos servidores e instalação do sistema Helios, bem como daqueles responsáveis pela manipulação do sistema, equipe esta composta, além do professor Joilson, pelos servidores Thiago Alexandre Herek, José Goncalves De Oliveira Júnior e Eduardo Renan Manika. Foram criadas ao todo 39 urnas(eleições) distintas, todas configuradas para ocorrer dia 30/06/2020, entre 06:00 e 18:00, e contar com um apurador automático, pelo próprio sistema Helios, e um apurador humano, função que foi atribuída ao professor Ubiradir Mendes Pinto.

6. Com esse formato de eleição, a contagem dos votos fica condicionada a participação do administrador do sistema juntamente à anuência do apurador humano, que deve fornecer sua chave criptográfica no momento da apuração dos votos. Cabe esclarecer que o modelo de apuração escolhido proporciona grandes vantagens de segurança ao sistema, visto que impede eventual tentativa de contagem de votos sem que haja participação do apurador humano.

7. Compareci novamente àquela instituição dia 30 de junho para acompanhar o processo de apuração dos votos, que teve início logo após as dezoito horas, conforme documentado em ata (Anexo 02). A apuração das urnas foi iniciada mediante a inserção da chave privada do apurador, que havia sido armazenada em pendrive que foi guardado em envelope lacrado, depositado em cofre. Por volta das 18:26 foi identificado que o sistema era incapaz de totalizar os votos da primeira urna. O processo foi repetido até a urna 5, sendo que para nenhuma delas foi possível realizar a contagem dos votos. Foi tentando apurar as urnas em sequência inversa, a partir da urna 39, o que resultou em sucesso, que continuou até a apuração da urna

20. As apurações das urnas 19 e 18 apresentaram erro, nos mesmos moldes das urnas 1 a 5, ocasião em que a comissão deliberou por suspender o processo de apuração para que se pudesse analisar o código fonte, analisar a base de dados, e avaliar a possibilidade de eventual ataque.

8. De forma a assegurar a lisura do processo, e possibilitar a continuação da apuração caso o problema fosse solucionado, solicitei que fosse criado um snapshot do servidor de votação no momento em que foram cessadas as tentativas de apuração. O processo de snapshot cria a uma cópia fiel do estado que a máquina se encontra, e possibilita retornar àquele estado e dar prosseguimento, sem que haja dúvidas quanto a eventual manipulação de dados. Tal snapshot passou por um processo de hash e foi copiado para dois discos rígidos. Um desses discos ficou em meu poder, enquanto outro ficou depositado no cofre da instituição. O processo de cópia dos snapshots foi concluído pouco após a meia-noite, quando a reunião foi concluída. Além desse snapshot, diversos outros haviam sido criados pela equipe técnica, em momentos importantes do processo, como antes da configuração das urnas e durante o processo de votação. A importância em gerar esses snapshots está no fato de que abre a possibilidade de realização de inúmeros procedimentos técnicos de investigação, incluindo medidas destrutivas, até que eventualmente se encontre um meio de solução. De posse de um meio de solução válido, se restaura um snapshot que tenha sido criado em momento adequado, aplica-se o meio de solução, e o resultado final permanece, sob o ponto de vista técnico, fidedigno.

9. No dia seguinte, bem como em praticamente todos os dias até o dia 06 de julho, mantive contato com a equipe técnica buscando informações sobre o andamento do processo de investigação e prestando suporte quanto às eventuais possibilidades de encontrar a falha e realizar a contabilização dos votos. Além disso, compareci à UTFPR durante a semana para acompanhar os esforços e auxiliar na compreensão do mecanismo de criptografia, visando avaliar se ainda seria possível decifrar os votos e contabilizar o resultado. Mediante a realização de vários testes, a avaliação foi de que, contanto que fossem feitos ajustes no código-fonte ou na base de dados, seria possível realizar a contagem. A equipe técnica da UTFPR persistiu nos esforços e conseguiu identificar o erro que gerou incapacidade de totalização, bem como propôs um método para forçar a contagem dos votos.

10. Em poucas palavras, o erro causador da falha na apuração foi consequência de erro na programação do sistema Helios. Uma das etapas cruciais para a criação da urna, a combinação da chave do sistema com a chave do apurador humano, continha uma falha que poderia gerar

resultados inconsistentes. O código original realiza uma pesquisa na base de dados pelas chaves dos apuradores, porém, devido a forma incompleta como tal pesquisa é realizada, não é possível garantir que o resultado será sempre correto. Como resultado, temos uma falha intermitente, que por vezes funciona corretamente, enquanto em outras, não. Visto que o erro se deu no momento da criação das urnas, a solução que possibilitaria a apuração demandava acesso direto a base de dados, corrigindo os registros que haviam sido criados erroneamente. É importante notar que somente registros da tabela que controla a eleição teriam que ser alterados, sem nenhuma modificação nas tabelas que contém os votos.

11. De posse, então, do meio de solução, a comissão se reuniu novamente dia 06 de julho, conforme registrado em ata (Anexo 3). Na ocasião, foi feita a restauração daquele snapshot gerado dia 30, e as etapas para a aplicação do meio de solução foram minuciosamente explicadas aos membros da comissão e fiscais eleitorais. Aplicadas as correções, com as quais todos os presentes anuíram, pode-se reiniciar a apuração. Dessa vez, não houve nenhuma dificuldade com as urnas 1 a 19, e para as urnas 20 a 39, que já haviam sido abertas dia 30, foi necessário apenas transpor os resultados para planilha de totalização (Anexo 04).

12. Em continuidade aos esforços, dessa vez com o intuito de aperfeiçoar o sistema, e evitar que problemas semelhantes viessem a acontecer em outros processos de votação através da plataforma Helios, a equipe técnica submeteu suas observações ao autor do software, Bem Adida, que agradeceu enfaticamente pela colaboração e se comprometeu a implementar a correção proposta (Anexo 05).

13. Considero importante destacar a competência técnica dos envolvidos, assim como o notável comprometimento com a busca por um processo eleitoral transparente e seguro. A equipe não mediu esforços na configuração e testes do sistema, na escolha do método de apuração (fazendo uso de apurador humano), no monitoramento por eventuais riscos de ataques cibernéticos, e, em especial, na busca de uma solução para o erro ocorrido durante a apuração. O erro que causou a impossibilidade de apuração, assim como a sua identificação e solução, provou requerer além de sólidos conhecimentos, grande esforço pessoal, tendo em vista a exiguidade de tempo. Além disso, ressalto que os cuidados que foram tomados, com relação a preservação dos dados, bem como o meio de solução aplicado, permitem afirmar que o processo ocorreu de forma correta e transparente.

14. Complementarmente, informo que foi agendada visita deste signatário à UTFPR para restituir os materiais que ficaram sob minha guarda, bem como acompanhar o processo de cópia dos dados, que serão resguardados por aquela Universidade.

Respeitosamente,

SILVINO SCHLICKMANN JUNIOR  
PERITO CRIMINAL FEDERAL