



Ofício nº 48/2020 - COLÉGIO ELEITORAL

Curitiba, 06 de julho de 2020.

Do: Presidente do Colégio Eleitoral

Para: sr. Antonio Gonçalves de Oliveira - Coordenação Campanha Candidato Schiefler

Assunto: **Resposta ao Ofício nº 36/2020 - PPGPGP-CT**

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 23064.019197/2020-63.

Prezado Senhor,

Este Colégio Eleitoral tomou conhecimento, neste domingo às 09:30 horas, do Ofício nº 36/2020 - PPGPGP-CT, datado de 05/07/2020, e encaminhado ao Colégio Eleitoral às 02:19 h (madrugada).

O Colégio Eleitoral passa a seguir a responder às solicitações.

Questão I

*Que seja disponibilizada de imediato, na página institucional desse CE, com ampla divulgação pelos canais de comunicação institucional, **a lista de votantes por urna, OBVIAMENTE SEM A IDENTIFICAÇÃO DO VOTO** na vez que além de ser ilegal e imoral tal conduta, tem-se como pressuposto que tal ator seria impossível, haja vista a segura do sistema, **não obstante as inúmeras vulnerabilidades evidenciadas no Ofício nº 30/2020 - PPGPGP-CT** enviado a esse CE no âmbito do Processo SEI nº 23064.019197/2020-63. Entenda-se por votantes as pessoas que participaram do pleito depositando o voto na urna, portanto, quem votou em um dos candidatos, ou mesmo optou por branco ou nulo.*

Resposta do Colégio Eleitoral:

Partindo da hipótese de que a solicitação não se trata de um pedido de apuração e nem da identificação do voto de cada eleitor, mesmo que por apelido, da mesma maneira que ocorreu na votação simulada, o Colégio Eleitoral fará a divulgação do número total de votantes por urna, especificando quantos votos cada candidato

obteve em cada urna, bem como o número de votos brancos e nulos, na forma do art. 32 do regulamento aprovado pela Deliberação COUNI nº 13/2020.

Os dados do sistema foram congelados no dia 30/06/2020 e estão sob a tutela da Polícia Federal, podendo ser auditado após a apuração e divulgação do resultado.

Questão II

Que, em respeito a comunidade ao Conselho Universitário, não se de continuidade a apuração, consoante todas as dúvidas que pairam sobre a segurança, integridade e conformidade do sistema, frente a todos os acontecimentos sabidos e narrados.

Resposta do Colégio Eleitoral:

A continuidade das atividades deste Colégio Eleitoral está amparada nos documentos (publicados na página do Colégio Eleitoral):

1 - Deliberação COUNI nº 14/2020 - *Ad Referendum*;

2 - Ofício COUNI nº 20/2020 da Presidência do COUNI.

A base normativa para a solicitação desse Colégio Eleitoral de reconsideração e consequente retorno do processo a este Colégio foi explicitada no ofício nº 45/2020 do Colégio Eleitoral, cuja resposta poderia ter sido negativa ou positiva. Informamos ao requerente que todo o processo está sendo acompanhado e auditado pelo perito criminal da Polícia Federal e pelo auditor do Tribunal Regional Eleitoral (TRE-PR).

Questão III

Que se reconheça a invalidade da Deliberação COUNI 14-ad-referendum, uma vez que a vice-reitora encontra-se em suspeição para decidir ad referendum em matéria de seu interesse, uma vez que sabidamente ela é candidata a vice-reitora na chapa do candidato Pilatti, portanto parte interessada no processo, colidindo-se aí frontalmente com os princípios da impessoalidade e moralidade, sem falar na infringência legal a dispositivos infraconstitucionais.

Resposta do Colégio Eleitoral:

Não foi delegada competência ao Colégio Eleitoral para julgar a suspeição da reitora em exercício com base na Deliberação COUNI nº 14/2020 - *Ad Referendum*.

Questão IV

Não sendo este o entendimento desse CE, que se observe/providencie e responda, no PRAZODE 24 HORAS DA PROTOCOLIZAÇÃO DESTE OFÍCIO NO DIA DA VISTA A URGÊNCIA E RELEVÂNCIA E A DATA/HORÁRIO PREVISTOS PARA INÍCIO APURAÇÃO, no mínimo:

Resposta do Colégio Eleitoral:

Este Colégio Eleitoral tomou conhecimento, neste domingo às 09:30 horas, do Ofício nº 36/2020 - PPGPGP-CT, datado de 05/07/2020, e encaminhado ao Colégio Eleitoral às 02:19 h (madrugada).

Questão V

Que a apuração só seja iniciada se a comissão técnica disponibilizar descritivo técnico da falha, como foi detectada e quais são todos os passos adotados para solução da falha que possibilitaram a abertura da urna. Além disso, um relato de quais urnas foram abertas durante o teste, sendo exibido o estado de cada urna na cópia onde foram realizados os testes (para garantir que não houve apuração prévia total, ou mesmo parcial da eleição na comissão técnica).

Resposta do Colégio Eleitoral:

A solicitação será atendida em momento oportuno.

Questão VI

Que a apuração seja realizada, necessariamente em uma cópia da cópia que se encontra sob guarda da PF, permitindo que a cópia original armazenada pela PF permaneça intacta permitindo gerar várias novas cópias da máquina para tempestivo teste dos fiscais técnicos de cada candidato e/ou por peritos judiciais e assistentes técnicos externos.

Resposta do Colégio Eleitoral:

Existem duas cópias idênticas, com o mesmo HASH-MD5, lacradas e assinadas pelos auditores do TRE-PR e da Polícia Federal e qualquer uma das duas poderá ser utilizada. Sendo uma sobre a tutela do auditor da Polícia Federal e outra no cofre do núcleo de concursos.

Questão VII

Que se permita que mais cópias sejam realizadas do arquivo snapshot da máquina virtual sob guarda da PF antes de qualquer intervenção, para permitir repetição dos passos de correção da apuração e do descritivo mencionado no item 1 novamente por parte dos fiscais técnicos ou por um perito externo, que com a imagem e repetição dos procedimentos consigam em cotejamento os mesmos resultados.

Resposta do Colégio Eleitoral:

De acordo com a legislação esses dados somente podem ser disponibilizados mediante ordem judicial.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, **mediante ordem judicial**, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

Questão VIII

Que se preserve 1 cópia intacta da máquina, seja no disco da PF ou em outro - conferido pelo mesmo hash.

Resposta do Colégio Eleitoral:

O Colégio Eleitoral informa que a apuração será feita na cópia sob a tutela da Polícia Federal ou na cópia que é idêntica e foi feita na presença dos auditores da Polícia Federal e do TRE e está lacrada e assinada por todos os presentes e guardada no cofre do Núcleo de Concursos. Sendo que uma será utilizada e a outra poderá ser preservada.

Questão IX

Que se faça a transmissão completa de todas as ações a serem realizadas no servidor antes da apuração, de modo que fiquem gravados e visíveis a comunidade os passos de solução do problema.

Resposta do Colégio Eleitoral:

Esta etapa apresenta dados sigilosos (do tipo senha, configurações da máquina, endereços de e-mail etc., os quais estão sob responsabilidade da UTFPR), não podendo ser transmitida. Esta etapa será fiscalizada pelos auditores do TRE-PR e da Polícia Federal, além dos fiscais de apuração e técnicos presentes na apuração.

Questão X

Que se proceda e publicize o resultado de auditoria interna no processo de solução para que se comprove que não houve disponibilização antecipada do resultado a nenhum dos candidatos ou suas equipes.

Resposta do Colégio Eleitoral:

O Colégio Eleitoral emitirá e publicará, em momento oportuno, o relatório circunstanciado, onde também constará pareceres dos auditores do TRE-PR e da

Questão XI

A disponibilização do sistema de votação novamente on-line, com todas as ferramentas de auditoria própria do sistema liberadas para acesso.

Resposta do Colégio Eleitoral:

A disponibilização a todos os eleitores ocorrerá a partir do momento da finalização da apuração.

Questão XII

Que se proceda, para o devido controle social, a realização de campanha massiva, diariamente em broadcast, mídias sociais e portal institucional para que os eleitores que votaram façam a conferência do voto depositado através do hash gerado no momento da colocação do voto na urna.

Resposta do Colégio Eleitoral:

A disponibilização a todos os eleitores ocorrerá a partir do momento da finalização da apuração.

Questão XIII

Que seja providenciado e disponibilizado a requerentes o arquivo de log do sistema de votação, do django, do servidor (apache, nginx ou outro a qual tenha se adotado) e do banco de dados, durante todo o período entre 12 horas antes da votação, durante e depois do término da apuração, disponível para retirada em arquivo digital pelos candidatos ou seu fiscal técnico.

Resposta do Colégio Eleitoral:

De acordo com a legislação esses dados somente podem ser disponibilizados mediante ordem judicial.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

*§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, **mediante ordem judicial**, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.*

Questão XIV

Que seja realizado procedimento de congelamento de cópia fiel após apuração do resultado, retirando imagem do sistema e guardando em cópia "snapshot" com documentação do hash para eventuais auditorias e perícias do e sobre o processo no futuro.

Resposta do Colégio Eleitoral:

Poderá ser realizado após o término da apuração.

Questão XV

Quantas chaves foram geradas em todos o processo eleitoral, desde a configuração das urnas até o congelamento do sistema?

Resposta do Colégio Eleitoral:

Uma chave pública para cada apurador (uma humana e outra do sistema) e, da combinação dessas duas, gera-se uma terceira chave pública para cada urna, totalizando 3 chaves públicas para cada urna.

Questão XVI

Como os votantes poderão verificar seus votos, já que o sistema não está mais disponível?

Resposta do Colégio Eleitoral:

A disponibilização a todos os eleitores ocorrerá a partir do momento da finalização da apuração.

Questão XVII

Quando se afirma que houve uma "duplicidade de chaves", quais são essas chaves?

Resposta do Colégio Eleitoral:

Para gerar a chave pública de cada urna, devido a um erro do sistema, foi combinada somente a chave pública do apurador humano com ela mesma. O correto deveria ser a combinação da chave pública do apurador humano com a chave pública do administrador do sistema.

Questão XVIII

Porque as chaves divulgadas abrem somente metade das urnas, se na configuração das urnas, todas as chaves deveriam ser geradas para as mesmas urnas?

Resposta do Colégio Eleitoral:

O erro ocorreu apenas com as urnas 1 a 19 pois apenas nessas urnas a ausência do ordenamento (comando SQL "order by") na consulta que retorna os apuradores trouxe um resultado incorreto.

Conforme PostgreSQL (disponível em <http://pgdocptbr.sourceforge.net/pg80/queries-order.html>):

"Se nenhuma ordenação for especificada, as linhas retornam em uma ordem aleatória. Neste caso, a ordem real depende dos tipos de plano de varredura e de junção e da ordem no disco, mas não se deve confiar nisto. Uma ordem de saída específica somente pode ser garantida se a etapa de ordenação for especificada explicitamente".

Questão XIX

O LOG do Helios Voting será disponibilizado para os fiscais dos candidatos?

Resposta do Colégio Eleitoral:

De acordo com a legislação esses dados somente podem ser disponibilizados mediante ordem judicial.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

*§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, **mediante ordem judicial**, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.*

Questão XX

Conforme relatado no "Relatório Técnico Sucinto da Comissão Técnica do Colégio Eleitoral", emitido dia 03/07/20, aproximadamente às 23:20, os votos que foram analisados não estavam congelados. Portanto, qual a possibilidade de que estes votos possam ser modificados, já que os mesmos ainda não tinham sido congelados pelo Helios Voting?

Resposta do Colégio Eleitoral:

O congelamento das urnas (e não dos votos) ocorreu no dia 26/06/2020, durante a configuração das urnas para o processo de consulta. Dessa forma, não seria possível ocorrer modificação nos votos uma vez que eles não existiam.

Toda a análise e busca pela solução do problema ocorreu em uma cópia de teste utilizada para investigação do problema, onde foram incluídos quatro eleitores de teste (com e-mails da comissão técnica) e foi feita a apuração com esses 4 votos. Ressalta-se que há duas cópias intactas, lacradas e assinadas por todos os presentes (auditor da Polícia Federal, auditor do TRE, fiscais de apuração dos candidatos, membros do Colégio Eleitoral e da Comissão Técnica) na apuração do dia 30/06/2020, sendo que uma está sob a tutela da Polícia Federal e a outra guardada no cofre do Núcleo de Concursos..

Questão XXI

Apesar de haver o congelamento do sistema, os votos recuperados após o descongelamento são seguros, já que não estavam congelados pelo Helios Voting?

Resposta do Colégio Eleitoral:

Não existem votos congelados. O congelamento é da urna. Após às 18:00 horas do dia 30/06/2020 não foi possível o registro de novos votos. Os votos são confiáveis e cada eleitor poderá conferir.

Questão XXII

Pela análise do código fonte, porque a chave de metade das urnas foi gerada de uma forma (combinação de um par de chaves públicas identificas do operador humano) e as chaves da outra metade das urnas foi gerada da combinação das chaves públicas do operador humano e do administrador?

Resposta do Colégio Eleitoral:

O erro ocorreu apenas com as urnas 1 a 19 pois apenas nessas urnas a ausência do ordenamento (comando SQL "order by") na consulta que retorna os apuradores trouxe um resultado incorreto.

Conforme PostgreSQL (disponível em <http://pgdocptbr.sourceforge.net/pg80/queries-order.html>):

"Se nenhuma ordenação for especificada, as linhas retornam em uma ordem aleatória. Neste caso, a ordem real depende dos tipos de plano de varredura e de junção e da ordem no disco, mas não se deve confiar nisto. Uma ordem de saída específica somente pode ser garantida se a etapa de ordenação for especificada explicitamente".

Questão XXIII

De acordo com o §2º do Artigo 21 do CAPÍTULO VI, "A chave de segurança será armazenada em uma unidade flash USB (pen drive), e seus backups, gerada pelo

Apurador por ocasião da configuração das urnas na presença dos candidatos ou de seus fiscais indicados (Art. 35), ficarão em um envelope selado pelo presidente do Colégio Eleitoral e pelos candidatos ou seus fiscais até o momento do início da apuração, quando este envelope será aberto na presença destes”, fica claro que deveria ser gerada somente “uma única chave”. **Porque foi gerada uma chave para o ADMINISTRADOR**, e esta chave foi usada na geração das chaves das urnas, conforme informado pela Comissão Técnica? Mais uma ilegalidade Formal!

Resposta do Colégio Eleitoral:

Ao realizar o cadastro de uma urna é gerada automaticamente a chave pública do apurador do sistema (administrador).

A chave de segurança armazenada no *pen drive* é a chave privada do apurador humano que foi gerada no momento do cadastro da primeira urna, no dia 26/06/2020.

Portanto, não existindo ilegalidade.

Questão XXIV

A Comissão Técnica irá publicar e quando, o código HASH MD5 correspondente a cada arquivo compondo a versão customizada do Sistema Helios Voting, no dia do congelamento?

Resposta do Colégio Eleitoral:

Não houve modificação no código fonte. A conferência dos códigos HASH MD5 (<https://evoto.utfpr.edu.br/md5sum>) estará novamente disponível após restaurarmos o servidor, com o *snapshot* que foi gerado na noite de 30/jun/2020.

Questão XXV

Se o erro, conforme amplamente publicizado está no fato de que a chave criptográfica foi utilizada indevidamente em duplicidade, por que, onde, quando e como é possível se a chave é única?

Resposta do Colégio Eleitoral:

A função de cálculo da chave pública da urna é uma combinação das chaves dos operadores. O sistema combinou a chave pública do operador humano com ela mesma, devido a um erro no código que não ordenava a consulta que buscava os apuradores.

O erro ocorreu apenas com as urnas 1 a 19 pois apenas nessas urnas a ausência do ordenamento (comando SQL “order by”) na consulta que retorna os apuradores trouxe um resultado incorreto.

Conforme PostgreSQL (disponível em <http://pgdoctbr.sourceforge.net/pg80/queries-order.html>):

“Se nenhuma ordenação for especificada, as linhas retornam em uma ordem aleatória. Neste caso, a ordem real depende dos tipos de plano de varredura e de junção e da ordem no disco, mas não se deve confiar nisto. Uma ordem de saída específica somente pode ser garantida se a etapa de ordenação for especificada explicitamente”.

Portanto, não existindo ilegalidade.

Questão XXVI

Tratando-se de um procedimento computacional, como pôde ocorrer o erro de utilização da chave criptográfica em duplicidade para a metade das urnas e para a outra metade não?

Resposta do Colégio Eleitoral:

O erro ocorreu apenas com as urnas 1 a 19 pois apenas nessas urnas a ausência do ordenamento (comando SQL “order by”) na consulta que retorna os apuradores trouxe um resultado incorreto.

Conforme PostgreSQL (disponível em <http://pgdocptbr.sourceforge.net/pg80/queries-order.html>):

“Se nenhuma ordenação for especificada, as linhas retornam em uma ordem aleatória. Neste caso, a ordem real depende dos tipos de plano de varredura e de junção e da ordem no disco, mas não se deve confiar nisto. Uma ordem de saída específica somente pode ser garantida se a etapa de ordenação for especificada explicitamente”.

Questão XXVII

Para a recuperação das urnas 1 a 19, quais técnicas e/ou procedimentos foram utilizados para tal?

Resposta do Colégio Eleitoral:

Essas urnas não foram recuperadas. O problema ocorreu na apuração, sendo os seguintes procedimentos que permitem a apuração:

- 1 - Reiniciar as *flags* (campo do banco de dados) para permitir a apuração das urnas com problema já apuradas.
- 2 - Substituir a chave pública do operador do sistema pela chave pública do operador humano.

Questão XXVIII

Houve o emprego de técnicas de criptoanálise com o objetivo de quebrar as chaves criptográficas?

Resposta do Colégio Eleitoral:

Não. Foi realizada somente a investigação de como o erro ocorreu. Esclarecemos que todo o procedimento foi acompanhado pelo auditor da Polícia Federal.

Portanto, não existindo ilegalidade.

Questão XXIX

Em sendo positiva a resposta anterior, não caracterizaria tal procedimento um "hackeamento" jogando por terra a confiabilidade do software Helios Voting?

Resposta do Colégio Eleitoral:

Vide item anterior.

Questão XXX

Houve modificação do código-fonte do software durante este processo?

Resposta do Colégio Eleitoral:

Não.

Questão XXXI

Em sendo positiva a resposta anterior, não caracterizaria tal procedimento um "hackeamento" jogando por terra a confiabilidade do software Helios Voting?

Resposta do Colégio Eleitoral:

Vide item anterior.

Questão XXXII

Que seja publicizado diagrama de fluxo de dados para uma melhor transparência ao processo, para que todas as partes e comunidade/controle social, tenham ciência de como o sistema funciona, identificando também os indivíduos ou entidades com acessos privilegiados. Para exemplificar, a título de fragilidade, um usuário com acesso aos servidores, poderia extrair manualmente as senhas dos eleitores por meio do arquivo/scriptextract-passwords-for-email.py disponível no código fonte do Helios Voting, podendo também (Frise-se não se tem aqui a mínima intenção de fazer-se acusações prévias, e sim, somente contribuir para uma maior integridade do sistema) manipular registros (logs) e e-mails enviados.

Resposta do Colégio Eleitoral:

O sistema possui o código aberto e o diagrama pode ser solicitado ao seu desenvolvedor. Sobre as fragilidades questionadas, já foram respondidas em momento anterior.

Portanto, não existindo ilegalidade.

Atenciosamente,

Jair Ferreira de Almeida
Presidente do Colégio Eleitoral



Documento assinado eletronicamente por **JAIR FERREIRA DE ALMEIDA, PRESIDENTE DO COLÉGIO ELEITORAL**, em 06/07/2020, às 09:16, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.utfpr.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1510517** e o código CRC **BC9926A5**.



Ministério da Educação
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
UTFPR - CAMPUS CURITIBA
DIRETORIA GERAL - CÂMPUS CURITIBA
DIRETORIA DE PESQUISA E POS-GRADUAÇÃO-CT
PROG. POS-GRAD. PLAN. GOV. PÚBLICA - CT
Avenida Sete de Setembro, 3165 - CEP 80230-901 - Curitiba - PR -
Brasil
Telefone: (41) 3310-4545 - www.utfpr.edu.br



Ofício nº 36/2020 - PPGPGP-CT

Curitiba, 05 de julho de 2020.

A(o) Sr(a).

Presidente do Colégio eleitoral

Assunto: **Geral: Análise e Encaminhamento de Documentos - Apuração da Votação Helios Voting, problemas técnicos, Impossibilidade declarada, devolução à presidência do COUNI para soluções, interrupção/suspensão, dúvidas comunidade, respeito regulação, ad referendum indevido.**

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 23064.019197/2020-63.

Assunto: Geral:

Senhor presidente do Colégio Eleitoral

Cumprimentando-o cordialmente, na condição de **Conselheiro Universitário eleito**, "cidadão" eleitor e no exercício do Controle Social, bem como de membro da Coordenação de campanha do candidato Schiefler na Consulta para escolha de reitor da UTFPR para o quadriênio 2020-2024, CONSIDERANDO:

1. Que coube a esse Colégio Eleitoral (CE) organizar, conduzir, realizar e supervisionar o processo de consulta, junto à comunidade acadêmica da UTFPR, destinada a indicar nomes de docentes para a formação da lista tríplice de candidatos a Reitor da Instituição, para submissão ao Presidente da República por meio do Ministro de Estado da Educação.
2. Que a **Deliberação COUNI nº 13, de 25/05/2020** é norma com prazo de validade determinado expressamente em si mesma, qual seja, 03/07/2022 as 12h00, tornando-se juridicamente extinta desde então.
3. Extinta a norma a mesma perde imediatamente a eficácia, uma vez que não mais tem o poder legiferante de agir sobre objeto definido
4. Que não foi possível, por problemas técnicos desconhecidos até então, a apuração dos votos conforme previsto no regulamento, desde as 18:00 do dia 30/06/2020, de forma ininterrupta com publicação para a comunidade até as 18:00 do dia 01/07/2020, consoante ata disponibilizada na página desse CE.

5. Que, não obstante tentativa de invocação de “força maior”, nenhuma força descomunal da natureza sobreveio ao ato de apuração, portanto, descabido seria tal invocação, há clara ilegalidade formal pelo descumprimento da exigência expressa no artigo 31 do referido regulamento, uma vez que houve ininterrupção formalizada, inclusive, pela própria ata assinada por todos os presentes. Máxime que fato foi invocado e alertado pelo fiscal de apuração do candidato Schiefler.
6. Que no dia 01/07/2020 vencidas as 18:00, também não foi possível a esse CE, consoante regulamento das eleições, cumprir o prazo regulamentar e publicizar para a comunidade o resultado da apuração. Evidencia-se aí mais uma ilegalidade formal.
7. A Nota de esclarecimento desse CE, de 01/07/2020 se comprometeu perante à comunidade em esclarecer mediante nota, até as 18:00 do dia 02/07/2020 todo o ocorrido.
8. A Nota de Esclarecimento de 02/07/2020, desse CE **expressamente assume que, encerrou a suspensão temporária da apuração deixando de apresentar o resultado da consulta**, deixando claro para a comunidade que o **RESULTADO FINAL DA VOTAÇÃO SÓ SERÁ POSSÍVEL SE FOR REFEITO O SISTEMA DE COTAÇÃO EM 19 (DEZENOVE) URNAS**. Alega a referida nota, finalmente que: **“(…) CHEGANDO NO LIMITE DE NÃO TER OUTRA OPÇÃO A NÃO SER A DE REMETER O PROCESSO DE VOTA À REITORA EM EXERCÍCIO PARA AS PROVIDÊNCIAS QUE O CASO REQUER.”**
9. O pronunciamento da Reitora em exercício ratificando no dia 03/07/2020: <https://www.youtube.com/watch?v=0iyAQYq3RWg> a impossibilidade oficial registrada no item imediatamente supra, verbalizando à comunidade que enviaria o caso para a PROJU para obter um parecer orientativo, e que na sequência o COUNI deliberaria sobre o caso.
10. A surpreendente Nota de Esclarecimento desse CE de 04/07/2020 “dessuspendendo” o que já estava solucionado, uma vez que havia se **“(…) CHEGANDO NO LIMITE DE NÃO TER OUTRA OPÇÃO A NÃO SER A DE REMETER O PROCESSO DE VOTA À REITORA EM EXERCÍCIO PARA AS PROVIDÊNCIAS QUE O CASO REQUER.”**
11. O pronunciamento da Reitora em exercício em 05/07/2020: <https://www.youtube.com/watch?v=XiPVV06iCJA>, dando conta que não mais mandaria nada para o COUNI e, sem mencionar o parecer orientativo que solicitou a PROJU informa a comunidade que descobriram e resolveram o erro que havia “enterrado” as urnas não apuradas por problemas técnicos insolúveis, conforme mencionado em itens anteriores; e que assinaria, como assinou ad referendum, a Deliberação COUNI nº 14, Ad Referendum, de 04/07/2020 alternado datas do cronograma eleitoral. Assevera ainda que o erro estava em que a chave criptografica foi utilizada indevidamente em duplicidade.
12. Houve então uma ressurreição de um regulamento extinto, e em desrespeito ao COUNI não foi colocado em discussão um novo regulamento, simplesmente ressuscitando o anterior e fazendo um puxadinho incorporou novas datas para proceder-se a apuração das urnas insolúveis que deram cabo ao termo do regulamento anterior **Deliberação COUNI nº 13, de 25/05/2020**.
13. **Não é admissível subestimar a capacidade intelectual da comunidade UTFPR**, a qual é formada por pessoa com recrudescimento político suficiente para entender todos os contornos que permeiam as atabalhoadas decisões tomadas pela gestão superior institucional.
14. Que o processo eleitoral para escolha do Reitor da UTFPR para o quadriênio 2020-2024, nos termos da legislação aplicável, é processo administrativo levado a cabo no âmbito da Administração Pública, de grande relevância para a comunidade universitária e municipais/regionais em contiguidades aos 13 Campi da UTFPR, consoante ao compromisso/objetivo de desenvolvimento regional positivada na sua lei de criação;
15. Que a Administração Pública, sem desmerecimento de outros, obedecerá aos princípios da legalidade, finalidade, motivação, razoabilidade, proporcionalidade, moralidade, segurança jurídica, supremacia do interesse público, publicidade e transparência dos atos.
15. Que Nos processos administrativos serão observados, entre outros, os critérios de:
 1. atuação conforme a lei e o Direito;
 2. atuação segundo padrões éticos de probidade, decore e boa-fé;
 3. divulgação oficial dos atos administrativos, ressalvadas as hipóteses de sigilo previstas na Constituição;
 4. observância das formalidades essenciais à garantia dos direitos dos administrados,

nesse caso os eleitores e candidatos;

5. adoção de formas simples, suficientes para propiciar adequado grau de certeza, segurança e respeito aos direitos dos administrados eleitores e candidatos;
6. a transparência deve ser a regra no Estado Democrático de Direito, sendo o sigilo a exceção.

16. A manifestação da comunidade em busca de respostas a diversos questionamento havidos de pessoas atuantes na área de computação.
17. Que a Comissão Técnica em sua composição plena foi não participou em nenhum momento desde a configuração da cotação ate à análise "solução" do insolúvel problema em relação às urnas problemáticas (1 a 19).
18. A longa "discussão" no grupo de WatsApp do COUNI acerca do fato.

PEDIDOS

Respeitosamente, haja vista a urgência em função da data do pleito, com fundamento nos princípios invocados e fatos descritos, solicitamos em PEDIDOS:

I - Que seja disponibilizada de imediato, na página institucional desse CE, com ampla divulgação pelos cais de comunicação institucional, **a lista de votantes por urna, OBVIAMENTE SEM A IDENTIFICAÇÃO DO VOTO**, uma vez que além de ser ilegal e imoral tal conduta, tem-se como pressuposto que tal ator seria impossível, haja vista a segura do sistema, **não obstante as inúmeras vulnerabilidades evidenciadas no Ofício nº 30/2020 - PPGPGP-CT** enviado a esse CE no âmbito do Processo SEI nº nº 23064.019197/2020-63. Entenda-se por votantes as pessoas que participaram do pleito depositando o voto na urna, portanto, quem votou em um dos candidatos, ou mesmo optou por branco ou nulo.

II - Que, em respeito a comunidade ao Conselho Universitário, nao se de continuidade a apuração, consoante todas as dúvidas que pairam sobre a segurança, integridade e conformidade do sistema, frente a todos os acontecimentos sabidos e narrados.

III - Que se reconheça a invalidade da Deliberação COUNI 14-ad-referendum, uma vez que a vice-reitora encontra-se em suspeição para decidir ad referendum em matéria de seu interesse, uma vez que sabidamente ela é candidata a vice-reitora na chapa do candidato Pilatti, portanto parte interessada no processo, colidindo-se ai frontalmente com os princípios da impessoalidade e moralidade, sem falar na infringência leagl a dispositivos infraconstitucionais.

IV - Não sendo este o entendimento desse CE, **que se observe/providencie e responda**, no PRAZO **DE 24 HORAS DA PROTOCOLIZAÇÃO DESTE OFICIO NO SEI**, HAJA VISTA A URGÊNCIA E RELEVÂNCIA E A DATA/HORÁRIO PREVISTOS PARA INICIO DA APURAÇÃO, no mínimo:

1. **Que a apuração só seja iniciada se a comissão técnica disponibilizar descritivo técnico da falha**, como foi detectada e quais são todos os passos adotados para solução da falha que possibilitaram a abertura da urna. Além disso, um relato de quais urnas foram abertas durante o teste, sendo exibido o estado de cada urna na cópia onde foram realizados os testes (para garantir que não houve apuração prévia total, ou mesmo parcial da eleição na comissão técnica).
2. Que a apuração seja realizada, necessariamente **em uma cópia da cópia** que se encontra sob guarda da PF, permitindo que a cópia original armazenada pela PF permaneça intacta permitindo gerar várias novas cópias da máquina para tempestivo teste dos fiscais técnicos de cada candidato e/ou por peritos judiciais e assistentes tecnicos externos.
3. Que se permita que mais cópias sejam realizadas do arquivo snapshot da máquina virtual sob guarda da PF antes de qualquer intervenção, para permitir repetição dos passos de

- correção da apuração e do descritivo mencionado no item 1 novamente por parte dos fiscais técnicos ou por um perito externo, que com a imagem e repetição dos procedimentos consigam em cotejamento os mesmos resultados.
4. Que se preserve 1 cópia intacta da máquina, seja no disco da PF ou em outro - conferido pelo mesmo hash.
 5. Que se faça a transmissão completa de todas as ações a serem realizadas no servidor antes da apuração, de modo que fiquem gravados e visíveis a comunidade os passos de solução do problema.
 6. Que se proceda e publicize o resultado de auditoria interna no processo de solução para que se comprove que não houve disponibilização antecipada do resultado a nenhum dos candidatos ou suas equipes.
 7. A disponibilização do sistema de votação novamente on-line, com todas as ferramentas de auditoria própria do sistema liberadas para acesso.
 8. Que se proceda, para o devido controle social, a realização de campanha massiva, diariamente em broadcast, mídias sociais e portal institucional para que os eleitores que votaram façam a conferência do voto depositado através do hash gerado no momento da colocação do voto na urna.
 9. Que seja providenciado e disponibilizado a requerentes o arquivo de log do sistema de votação, do django, do servidor (apache, nginx ou outro a qual tenha se adotado) e do banco de dados, durante todo o período entre 12 horas antes da votação, durante e depois do término da apuração, disponível para retirada em arquivo digital pelos candidatos ou seu fiscal técnico.
 10. Que seja realizado procedimento de congelamento de cópia fiel após apuração do resultado, retirando imagem do sistema e guardando em cópia "snapshot" com documentação do hash para eventuais auditorias e perícias do e sobre o processo no futuro.
 11. Resposta: Quantas chaves foram geradas em todos o processo eleitoral, desde a configuração das urnas até o congelamento do sistema?
 12. Resposta: Como os votantes poderão verificar seus votos, já que o sistema não está mais disponível?
 13. Resposta: Quando se afirma que houve uma "duplicidade de chaves", quais são essas chaves?
 14. Resposta: Porque as chaves divulgadas abrem somente metade das urnas, se na configuração das urnas, todas as chaves deveriam ser geradas para as mesmas urnas?
 15. Resposta: O LOG do Helios Voting será disponibilizado para os fiscais dos candidatos?
 16. Resposta: Conforme relatado no "Relatório Técnico Suscinto da Comissão Técnica do Colégio Eleitoral", emitido dia 03/07/20, aproximadamente às 23:20, os votos que foram analisados não estavam congelados. Portanto, qual a possibilidade de que estes votos possam ser modificados, já que os mesmos ainda não tinham sido congelados pelo Helios Voting?
 17. Resposta: Apesar de haver o congelamento do sistema, os votos recuperados após o descongelamento são seguros, já que não estavam congelados pelo Helios Voting?
 18. Resposta: Pela análise do código fonte, porque a chave de metade das urnas foi gerada de uma forma (combinação de um par de chaves públicas identificas do operador humano) e as chaves da outra metade das urnas foi gerada da combinação das chaves públicas do operador humano e do administrador?
 19. Resposta: De acordo com o §2º do Artigo 21 do CAPITULO VI, "A chave de segurança será armazenada em uma unidade flash USB (pen drive), e seus backups, gerada pelo Apurador por ocasião da configuração das urnas na presença dos candidatos ou de seus fiscais indicados (Art. 35), ficarão em um envelope selado pelo presidente do Colégio Eleitoral e pelos candidatos ou seus fiscais até o momento do início da apuração, quando este envelope será aberto na presença destes", fica claro que deveria ser gerada somente "uma única chave". **Porque foi gerada uma chave para o ADMINISTRADOR**, e esta chave foi usada na geração das chaves das urnas, conforme informado pela Comissão Técnica? Mais uma ilegalidade Formal!

20. Responda: A Comissão Técnica irá publicar e quando, o código HASH MD5 correspondente a cada arquivo compoendo a versão customizada do Sistema Helios Voting, no dia do congelamento?
21. Se o erro, conforme amplamente publicizado esta no fato de que a chave criptografica foi utilizada indevidamente em duplicidade, por que, onde, quando e como é possível se a chave é unica?
22. Tratando-se de um procedimento computacional, como pôde ocorrer o erro de utilização da chave criptográfica em duplicidade para a metade das urnas e para a outra metade não?
23. Para a recuperação das urnas 1 a 19, quais técnicas e/ou procedimentos foram utilizados para tal?
24. Houve o emprego de técnicas de criptoanálise com o objetivo de quebrar as chaves criptográficas?
25. Em sendo positiva a resposta anterior, não caracterizaria tal procedimento um "hackeamento" jogando por terra a confiabilidade do software Helios Voting?
26. Houve modificação do código-fonte do software durante este processo?
27. Em sendo positiva a resposta anterior, não caracterizaria tal procedimento um "hackeamento" jogando por terra a confiabilidade do software Helios Voting?

V - Que seja publicizado diagrama de fluxo de dados para uma melhor transparência ao processo, para que todas as partes e comunidade/control social, tenham ciencia de como o sistema funciona, identificando também os indivíduos ou entidades com acessos privilegiados. Para exemplificar, a título de fragilidade, um usuário com acesso aos servidores, poderia extrair manualmente as senhas dos eleitores por meio do arquivo/scriptextract-passwords-for-email.py disponível no código fonte do *Helios Voting*, podendo também (Frise-se não se tem aqui a mínima intenção de fazer-se acusações prévias, e sim, somente contribuir para uma maior integridade do sistema) manipular registros (logs) e e-mails enviados.

VI -Reprise-se haja vista a relevância e urgência, que as respostas aos pedidos aqui elencados, sejam decididas e publicizadas em **até 24 horas** contados da protocolização deste ofício no SEI com envio para COL_ELEITORAL.

VII- Que em sendo negativo o acatamento a quaisquer dos pedidos elencados nos itens de I a VI e suas subquestões/pedidos supra, nos termos da legislação vigente, SEJA demonstrada e justificada a motivação legal/razoável para tal.

Atenciosamente

Antonio Gonçalves de Oliveira
Membro da Coordenação de Campanha Candidato Schiefler

Conselheiro Universitário – Representante Docente do Câmpus Curitiba



Documento assinado eletronicamente por **ANTONIO GONCALVES DE OLIVEIRA, PROFESSOR DO MAGISTERIO SUPERIOR**, em 05/07/2020, às 02:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.utfpr.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1510336** e o código CRC **95205556**.