# COMISSÃO ELEITORAL NACIONAL/CEN

## RESOLUÇÃO CEN Nº 01/2019

Recebido em 02/06/19 às 11h35
Rosa Escudero de Almeida
Relatora-Geral

**Assunto:** Voto Eletrônico nas eleições para os Conselhos Executivo e Fiscal da ANFIP - Biênio 2019/2021.

A Comissão Eleitoral Nacional/CEN, no uso de suas atribuições estatutárias e regimentais, e

**Considerando** o que dispõe o art. 80, § 6º do Regulamento Eleitoral, aprovado em reunião conjunta dos Conselhos de Representantes, Fiscal e Executivo realizada em 29 de maio de 2019;

**Considerando** o que dispõe o art. 32, § 4º do Estatuto aprovado na XXVI Convenção Nacional, realizada no período compreendido entre 20 a 23 de maio de 2017: *"As eleições previstas neste Estatuto serão sempre realizadas pelo voto nominal, direto, secreto, universal, consignado em cédula única oficial, distintas para os Conselhos Executivo e Fiscal, manifestado nas urnas, por correspondência* ***ou por meio eletrônico****, na forma que for estabelecida no Regulamento Eleitoral".*;

**Considerando** que o sistema de votação eletrônico atualmente disponível na Anfip, é vulnerável por não utilizar função de ciframento criptográfico para proteger os votos depositados, conforme Parecer Técnico emitido em 16/05/2019 pelo Professor do Departamento de Ciência da Computação da UFMG, Jeroen Van de Graaf, contratado por decisão do Conselho Executivo da ANFIP (cópia anexa);

**Considerando** os prazos estabelecidos no Regulamento Eleitoral, aprovado na reunião conjunta dos três Conselhos realizada no dia 29 de maio de 2019, quais sejam:



SEDE : SBN - Qd. 01 - Bl. H Ed. ANFIP - BRASÍLIA DF - 70040-907
CNPJ: 03.636.693/0001-00
Tel.: (0xx61) 3251-8100
Fax.: (0xx61) 3326-8113 ramal 2281

Art. 80 - § 1º do RE – Encaminhar a senha para voto eletrônico, por correios, até 25 dias antes da eleição, o que será até dia 23/06/2019;

Art. 80 – Inciso III – alínea "b" do RE - Início da votação eletrônica será 10 dias antes da eleição, o que será 08/07/2019.

**Considerando** o curto prazo para realização do processo eleitoral, que permita a adequação à eleição da Anfip de novo sistema eletrônico de votação e a implementação dos testes necessários que garantam a convicção da segurança do voto eletrônico;

**R E S O L V E:**

**Art. 1º Não adotar o voto eletrônico** na eleição para os Conselhos Executivo e Fiscal da ANFIP a ser realizada no dia 18 de julho de 2019, ficando à disposição do eleitor as modalidades de voto em urna e por correspondência

Brasília, 02 de junho de 2019.

**Rozinete Bissoli Guerini**
**Coordenadora da CEN**

**Ercília Bernardo Leitão**
**Secretária da CEN**

**Maria dos Remédios Bandeira**
**Membro da Comissão**

**Cássio José de Oliveira**
**Membro da Comissão**

**Nilza Garutti**
**Membro da Comissão**

**Lucimar Ramos Lima Ramalho**
**Suplente**

**Margarida Lopes de Araújo**
**Suplente**

**Tânia Maria Faria Garcia**
**Suplente**

**Paulo César Andrade Almeida**
**Suplente**



SEDE : SBN - Qd. 01 - Bl. H Ed. ANFIP - BRASÍLIA DF - 70040-907
CNPJ: 03.636.693/0001-00
Tel.: (0xx61) 3251-8100
Fax.: (0xx61) 3326-8113 ramal 2281
Internet: www.anfip.org.br

# Parecer técnico

## Introdução

A Associação de Auditores Fiscais da Receita Federal do Brasil -- ANFIP solicitou uma avaliação técnica do seu sistema de eleições pela internet. No dia 9 de maio de 2019 o parecerista visitou a sede da ANFIP e entrevistou o gerente de TI, Venilton Lopes Roberto, que mostrou o sistema de eleições desenvolvido. Esse parecer está em grande parte baseado no que foi discutido e mostrado nesta entrevista.

# Descrição do sistema de eleições da ANFIP

## Componentes de software

O sistema de eleições consiste dos seguintes componentes (camadas) de software:

- sistema operacional: Linux Debian;
- banco de dados: MySQL
- servidor web: Apache
- linguagem da programação das páginas web: PHP

Trata-se de uma configuração bastante padrão e muito confiável.

Todos estes componentes de software estão instalados numa máquina virtual que fica hospedada no *data center* da Amazon (EUA), o que também é comum. Esta máquina virtual hospeda apenas a aplicação de eleições. Isso é positivo porque garante uma segurança maior (não há usuários usando a mesma máquina virtual durante as eleições).

## Como o eleitor se autentica perante o sistema

Ao entrar na página da eleição, a aplicação mostra a tela de autenticação. No primeiro campo o eleitor digita seu CPF, e no segundo digita sua senha. Esta senha é idêntica àquela usada para entrar na *Área Restrita* do site principal, www.anfip.org.br.

## Como o eleitor vota

Após a autenticação, a aplicação mostra uma tela com botões correspondendo à(s) chapa(s) que podem ser escolhidas, como também botões para votar BRANCO ou NULO.

Quando o eleitor clica em uma dessas opções, o navegador mostra uma nova tela resumindo o voto intencionado, e mostrando a opção CORRIGE ou CONFIRMA.

Em seguida há a tela com botões correspondendo aos candidatos ao Conselho Fiscal, como também botões para votar BRANCO ou NULO.

Quando o eleitor clica em uma dessas opções, o navegador mostra uma nova tela resumindo o voto intencionado, e mostrando a opção CORRIGE ou CONFIRMA.

## O comprovante

Quando o eleitor clica em CONFIRMA, o navegador envia os votos ao servidor, que os armazena no banco de dados. Depois o sistema gere um comprovante eletrônico usando os seguintes valores:

- CPF: o CPF do eleitor;
- SIAPE: o SIAPE do eleitor;
- Chapa: o voto do eleitor para chapa;
- DataHora: a data e hora da votação;
- NrEleição: o número identificador da eleição (o banco de dados é preparado para guardar os dados de várias eleições ao memso tempo).

Departamento de Ciência da Computação
Av. Antonio Carlos, 6627 – Pampulha
Belo Horizonte, MG – 31270-010

Tel: +55 31 3409-5860
Fax: +55 31 3409-5858
www.dcc.ufmg.br

Os valores destas cinco variáveis juntos constituirão o valor de entrada para uma função de *hash* criptográfica, a SHA256.

Comprovante = SHA256(CPF, SIAPE, Chapa, DataHora, NrEleição)

O valor *hash* resultante, o comprovante, é gravado no banco de dados, e também é mostrado ao eleitor na tela, que tem a opção de imprimi-lo. Desta forma a transação é "selada", já que é impossível encontrar outros valores de entrada que darão o mesmo resultado.

## O sigilo do voto violado

Por causa da forma que o comprovante foi implementado, um adversário com acesso ao banco de dados pode, a qualquer momento depois da eleição, reconstruir o voto de cada eleitor. Ele age de seguinte maneira: ele busca no banco de dados os valores CPF, SIAPE, DataHora, e NrEleição. Depois ele chuta (adivinha) o valor da Chapa (são poucos possibilidade), ele calcule o valor SHA256(CPF, SIAPE, ChapaChute, DataHora, NrEleição), e compara o resultado ao valor hash já armazenado, o comprovante. Se for igual, ele sabe que o eleitor votou nesta chapa. Ou seja, o adversário executa o seguinte teste de igualdade:

Comprovante = SHA256(CPF, SIAPE, NrEleição, ChapaChute, DataHora)

Se a condição do teste é verdadeira, então o adversário sabe que ChapaChute é o valor correto. Este ataque é muito eficiente, então é possível executá-lo para todos os eleitores.

## Como o voto é armazenado no sistema

O modelo de dados para uma eleição é relativamente simples: sempre existem três relações:

- uma relação para todos os **eleitores**;
- uma para todas as **alternativas** (chapas, candidatos);
- uma relação para os **votos** depositados.

No entanto, existem várias maneiras de armazenar os votos depositados. No caso da ANFIP, a cada alternativa corresponde um contador no banco de dados que mantém o valor total de votos já depositados nesta alternativa.

Ao depositar um novo voto no banco de dados acontece o seguinte:

1. O contador que corresponde à alternativa selecionada (ou seja, o voto) é incrementado;
2. O sistema gere um comprovante (descrito anteriormente) que fica guardado na relação "eleitor";
3. O sistema registra que o eleitor já votou.

Não ficou claro o que acontece quando ocorre uma falha inesperada durante o processo de votar. A rigor se requer *atomicidade* do processo: ou o voto foi depositado com sucesso, ou a transação falhou completamente e o sistema volta ao estado anterior. Se o sistema atende a este requisito não foi estabelecido.

### Votar duas vezes

Um teste mostrou que o sistema impede um eleitor que tenta votar duas vezes.

### A apuração

O sistema não usa criptografia e guarda o número dos votos num contador no banco de dados, já totalizado. Portanto, a apuração consiste em meramente imprimir os valores contidos nestes contadores.

## Observações

### 1: A falta de criptografia

Um ponto fraco do sistema é que os totais dos votos ficam armazenados no banco de dados em texto clara, sem nenhuma proteção criptográfica. Então qualquer pessoa com acesso

ao banco de dados pode simplesmente modificar os valores dos registros que contém os totais dos votos para as chapas, assim modificando o resultado da eleição, sem que isso possa ser detectado.

O comprovante produzido pelo sistema não cumpre este papel, de proteger o sistema. Primeiro, trata-se uma função de *hash* criptográfico, que não usa uma chave secreta; ela "sela" apenas os dados. Isso é diferente de uma função de ciframento criptográfico, que usa uma chave secreta. O único papel do comprovante é o de registrar que a votação aconteceu, já que seu valor e armazenado no banco de dados também. E infelizmente, como foi argumentado antes, o comprovante pode levar à violação do sigilo do voto.

Em geral, podemos distinguir os seguintes tipos de sistemas de votação on-line:

1. Sem criptografia: o caso da ANFIP.
2. Com criptografia simétrica: os votos são cifrados usando uma chave criptográfica e ficam armazenados de forma cifrada no banco de dados, até o momento da apuração. Neste momento introduz-se a chave ao sistema, e os votos são decifrados e apurados. O grande problema desta solução é que as chaves para cifrar e decifrar são idênticas, então é necessário "esconder" a chave usada para cifrar no código fonte. Isso cria uma vulnerabilidade: um atacante poderia descobrir esta chave.
3. Com criptografia assimétrica: os votos são cifrados usando uma chave pública e ficam armazenados de forma cifrada no banco de dados, até o momento da apuração. Neste momento introduz-se a chave privada ao sistema, e os votos são decifrados e apurados. A vantagem desta solução é que as chaves para cifrar e decifrar são diferentes, então nenhuma vulnerabilidade é introduzida.
4. Com criptografia homomórfica: os votos são cifrados usando um algoritmo muito específico, que permite adicionar os votos mesmo enquanto ainda cifrados. Consequentemente não é mais necessário decifrar os votos individuais; basta decifrar o total cifrado. Então, o eleitor pode ver seu voto, de forma cifrada, no conjunto de votos a serem apurados, o que aumenta a credibilidade do processo.

A implementação correta destas primitivas é muito além das competências da grande maioria dos professionais de desenvolvimento de software no Brasil (e no mundo).

### 2: A falta de cerimônias

Um grande problema nos sistemas de votação tradicionais baseados em software é o seguinte: *Como o eleitor tem certeza o programa na sua frente é autêntico, que não foi modificado?* Tradicionalmente se resolve isso através de medidas adicionais como cerimônias. Nelas a equipe de TI, na presença de testemunhas da comissão eleitoral, mostra as qualidades do sistema. Exemplos típicos de cerimônias são:

- Cerimônia para inspecionar os códigos fontes;
- Cerimônia para selar os códigos fontes usando uma função de *hash* como SHA256, compilá-los, e gravar os resultados em CD-ROM;
- Cerimônia para fazer a instalação no ambiente de produção.

Me chamou atenção a ausência total deste tipo de cerimônias. Pelo que me foi comunicado, nada disso foi sequer contemplado, deixando a ANFIP muito vulnerável a uma chapa perdedor questionando o processo eleitoral.

**Outras boas práticas para a separação de deveres**

- Pode se combinar que, durante a eleição, a senha do administrador da máquina que fica sob guarda do Presidente da comissão eleitoral num envelope lacrado, assim deixando evidente que ninguém teve acesso ao servidor.
- Separação do ambiente de desenvolvimento do ambiente de produção.

## Conclusões e recomendações

As conclusões são os seguintes:

1) O sistema de eleições atual da ANFIP é muito elementar, pouco sofisticado.
2) O software não usa uma função de ciframento criptográfico para proteger os votos depositados, e é, portanto, muito vulnerável.

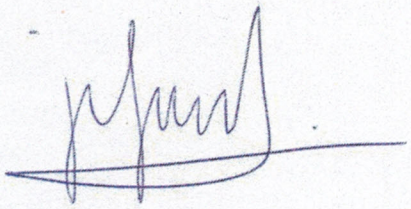
3) A tentativa de aumentar a segurança criando um comprovante, na verdade abriu uma possibilidade de atacar o sigilo do voto.
4) Existe pouca conscientização no setor de TI quanto a segurança e transparência do processo eleitoral.

Observando

1) A necessidade de melhor a segurança do sistema acrescentando funcionalidades criptográficas;
2) as dificuldades inerentes ao uso apropriado da criptografia e à implementação correta;
3) a falta de competência em segurança e criptografia do setor de TI diante desafios deste tipo;
4) o prazo curto até as eleições em julho;

eu recomendo que a ANFIP pare o desenvolvimento do seu sistema de votação e contrate uma empresa para conduzir suas eleições pela internet.

Belo Horizonte, 16 de maio de 2019.



Jeroen van de Graaf
Professor do Departamento de Ciência da Computação
ICEx -- UFMG