Norma do SIGEleição da Unifesspa

UNIFESSPA
Universidade Federal do Sul e Sudeste do Pará

Histórico de revisão

Data	Versão	Descrição	Autor
26/03/2019	1.0	Documento de Referência 1, Versão inicial	Ralfh Alan Gomes Machado, Maria Eliane Sobrinho
15/05/2019	1.1	Revisão	Ralfh Alan Gomes Machado, Vitor de Souza Castro
04/09/2019	1.2	Revisão	Edney A. N., Ralfh Alan Gomes Machado, Vitor de Souza Castro
04/12/2019	1.2	Aprovação pelo CGD	Edney A. N., Ralfh Alan Gomes Machado, Vitor de Souza Castro
30/11/2020	1.3	Alteração do artigo 14	Ralfh Alan Gomes Machado, Roberto Figueredo Rodrigues, Vitor de Souza Castro

Apresentação

Esta norma dispõe sobre características, uso e procedimentos do SIGEleição da Unifesspa para discentes, docentes e técnicos administrativos.

SIGEleição

Art. 1º - O SIGEleição pode ser definido como um sistema eleitoral em que se pode registrar votos de qualquer localidade, sem a necessidade de montar uma estrutura física específica e particular.

Art. 2º - O sistema realiza a contagem automática dos votos, o resultado é divulgado de maneira instantânea após o fim da eleição. A votação on-line vem maximizar a conveniência e acesso dos eleitores, permitindo o pleito eleitoral em qualquer lugar que tenha acesso à Internet.

Conceitos e definições

Art. 3º - O sistema trabalha com os seguintes conceitos:
I – Eleição: representa uma eleição, por exemplo, “Eleição para administração do instituto”.
II – Cargo: representa os possíveis cargos de uma eleição, por exemplo, os cargos de (i) Reitor, (ii) Diretor de instituto, (iii) Membro de conselho.
III – Candidatura: Cada cargo pode ter vários candidatos para o eleitor escolher, por exemplo, para o cargo de “Diretor de instituto” pode ter os candidatos: (01) José, (02) João e (03) Maria.
IV – Voto: representa 1 Voto na candidatura, como por exemplo, um voto em (01) José para o cargo de (iii) Diretor de instituto da eleição “Eleição p/ instituto”.

Soluções de Segurança do SIGEleição

Art. 4º - Os mecanismos de segurança do SIGEleição foram implementados, de forma a atender aos requisitos de segurança da seguinte maneira:
I - **Sigilo do Voto**: sistema de votação eletrônico deve garantir que os votos registrados sejam sigilosos. Ou seja, ninguém, em tempo algum, nem mesmo o administrador da base de dados, pode obter a informação: “Em quem o eleitor votou? ”
II - **Não Permitir Alteração de um Voto Válido**: toda eleição criada no SIGEleição deve possuir uma comissão eleitoral, cujo presidente tem como principal função, caso a eleição possua auditoria interna, gerar e guardar sigilosamente uma chave de segurança para a eleição. A chave de segurança é uma sequência de 64 caracteres gerados aleatoriamente. O ponto primordial da segurança do SIGEleição é que essa chave de segurança não é persistida em nenhum lugar pelo sistema. Ela fica apenas na memória do servidor que executa SIGEleição, dificultando assim a obtenção dessa chave.

III - **Auditar os Resultados de uma Eleição**: ao término da eleição, para homologar os resultados, o presidente deve informar novamente essa chave de segurança ao sistema, que então é utilizada para verificar se todos os votos foram registrados. Somente se todos os votos forem válidos e a quantidade de votos registrado for válida, o resultado da eleição é homologado e publicado. Caso ocorra algum problema durante a eleição e o sistema seja reiniciado, a informação da chave de segurança é perdida. Cabe ao presidente da comissão eleitoral entrar no sistema e fornecer novamente a chave de segurança. Pois, nenhum voto pode ser registrado no SIGEleição enquanto a chave de segurança não estiver carregada na memória do servidor.
IV - **Auditoria Externa os Resultados de uma Eleição:** o sistema também possui uma maneira de realizar uma auditoria externa. Ou seja, caso se desconfie que a eleição foi fraudada é possível auditar os resultados em um meio de armazenamento externo ao sistema. Para isso, o sistema permite que se informe um endereço de e-mail para onde ele enviará o registro de cada voto realizado.
V - **Auditar o Código fonte do Sistema**: o sistema possui a auditoria do código fonte do sistema. Essa auditoria possibilita caso seja solicitada uma auditoria do código fonte do sistema, verificar se o código fonte entre é o mesmo que executou no momento da eleição.
VI - **Assegurar voto único por eleitor**: além um uma regra de negócio no código do sistema que verifica a tentativa de realizar um voto duplicado, existem mecanismos nas tabelas do banco de dados do sistema impedindo que um mesmo eleitor vote duas ou mais vezes para a mesma eleição.
VII - **Assegurar que só votaram as pessoas registradas:** o SIGEleição assegura a autenticidade do eleitor, ou seja, dificulta que uma outra pessoa, que não seja o próprio eleitor, possa registrar seu voto se passando por um eleitor válido. Para isso, foram implementados alguns esquemas de autenticação, além do login e senha tradicionais, dos usuários do SIGEleição.
VIII - **Modo de Autenticação com Login e Senha**: modo padrão de autenticação da maioria dos sistemas e é um mecanismo obrigatório do SIGEleição. Todo eleitor para entrar no sistema deve informar pelo menos um login e uma senha que são pessoais e intransferíveis. A segurança desse método de autenticação está na segurança da senha do eleitor. O SIGEleição conta com um sistema de bloqueio de logins inválidos. Na primeira tentativa inválida, o eleitor fica impedido de tentar novamente essa operação por um período de 1 minuto. Na segunda tentativa, 2 minutos; na terceira, 4 minutos e assim progressivamente. Esse bloqueio dificulta a tentativa de quebra da senha por força bruta.
IX - **Modo de Autenticação com Pergunta de Segurança:** o SIGEleição solicita que o eleitor responda uma pergunta de segurança, selecionada aleatoriamente do banco de dados. Esse modo de autenticação é opcional e complementar. Essas perguntas de segurança têm por objetivo dificultar que usuários não humanos tentem acessar o sistema. Um exemplo de uma pergunta de segurança utilizada neste módulo de autenticação: “Quantas letras têm a palavra ‘casa’? ”.
X - **Modo de Autenticação com Captcha:** estratégia opcional e complementar ao modo de autenticação por login e senha é exibir um campo de captcha junto ao campo de login e senha para impedir que usuários não humanos tentem acessar o

sistema. Esse modo de autenticação é alternativo às perguntas de segurança.
XI - **Modo de Autenticação em Duas Etapas:** módulo de autenticação opcional e complementar e pode ser utilizado em combinação com qualquer um dos métodos anteriores. O objetivo é dificultar ainda mais a quebra da senha do eleitor. Quando ativado, após autenticação com login e senha, e algum dos outros métodos de autenticação que também estejam ativados, o sistema gerará aleatoriamente uma segunda senha para o eleitor. Essa segunda senha é então enviada para o e-mail do eleitor registrado no sistema. Para ele conseguir se logar no sistema terá que acessar o seu e-mail, verificar a senha gerada e informá-la ao sistema em uma segunda tela de autenticação.
XII - **Disponibilidade:** essa característica implica que o sistema de votação esteja disponível durante todo o período de votação; e ser acessível para usuário com necessidades especiais. Isso garante que quem queira votar possa utilizar o sistema. Para isso se utilizou a estratégia de sincronização que impede que o mesmo trecho do código seja executado por processos diferentes ao mesmo tempo em as instâncias do sistema.
XIII - **Acessibilidade do Sistema:** as páginas do sistema foram testadas para garantir que deficientes visuais consigam votar na eleição, mediante o uso de um software próprio que leem as informações na tela do sistema.

Soluções de segurança no voto

Art. 5º - Após passar por todos os mecanismos de autenticação do sistema é possível ainda configurar para o sistema solicitar ao eleitor dentro da cabine de votação perguntas pessoais de segurança para confirmação do voto. Neste caso, além dos demais mecanismos de autenticação baseados em senha, um suposto falsário teria que conhecer alguns dados pessoais do eleitor para conseguir registrar um voto por ele.

Art. 6º - Caso o eleitor erre as perguntas, ele ficará bloqueado não podendo mais utilizar o SIGEleição. A não ser por uma cabine de votação registrada explicada na próxima seção. O número de perguntas de segurança e tentativa erradas até que o eleitor seja bloqueado é configurado por eleição e depende do nível se segurança que a comissão eleitoral queira ter na eleição.

Art. 7º - O sistema trabalha com o conceito de grupos de eleitores, um grupo de eleitor é uma consulta no banco de dados que determina quais eleitores podem votar em uma determinada eleição. Cada eleição pode definir as consultas dos seus grupos de eleitores. A partir da consulta no banco de dados pode-se definir com precisões quais eleitores farão parte da eleição. Impedindo que eleitores não autorizados registrem um voto na eleição.

Funcionalidades

Art. 8º - **Registro de Cabine de Votação**: o servidor do SIGEleição realiza o log da votação registrando assim eventos sobre o seu funcionamento, utilização por usuários ou interação com outros sistemas. Um log, após ser gerado, passa a ser incrementado ao longo do tempo com informações que permitem diagnosticar anormalidades em relação ao propósito do sistema e questões de segurança e acessibilidade.

Art. 9º - O SIGEleição identifica as cabines de votação seguras através do endereço IP único.

Art. 10º - O firewall também implementa outras medidas de segurança, como, por exemplo, limitar o número de requisições por segundo vindas de uma mesma máquina.

Art. 11º - O sistema SIGEleição pode ser configurado para só aceitar registro de votos de cabines registradas para uma determinada eleição. Assim a comissão eleitoral pode optar em utilizar o sistema para realizar uma eleição mais restrita, em que o usuário não consiga votar de qualquer computador.

Avaliação do SIGEleição

Art. 12º - O SIGEleição suporta a demanda de mais de 30.000 eleitores aptos a votar. Para isso foram realizados vários testes de stress do sistema com a ferramenta JMeter (ferramenta utilizada para testes de carga em serviços oferecidos por sistemas computacionais) conseguindo-se uma carga de 2.000 eleitores por minuto registrando votos em uma eleição. Esse número foi mais do que suficiente para atender ao universo de 30.000 eleitores esperados.

Tutorial e procedimentos

Art.13º - Em: <https://estatuinte.unifesspa.edu.br/images/2017/tutorial-votacao.pdf>, encontra-se o tutorial para votação no SIGEleição da Unifesspa.

Art. 14º - Os procedimentos para solicitação de eleição por meio do SIG Eleição são:

- Abertura da demanda através do sistema de chamados (https://atendimento.unifesspa.edu.br)
- Regulamento/Regimento da Eleição (contendo informações como grupo de eleitores e eleitores aptos a votar);

- Período da Eleição;
- Período após o resultado para consulta pelos eleitores;
- Nome e Foto das chapas;
- Nome e CPF dos membros da comissão eleitoral;
- Nome e CPF do Presidente.

§ 1º As informações constantes no SIGEleição sobre as chapas concorrentes são limitadas, portanto quaisquer outros dados que sejam necessários acerca disso devem ser dispostos em site complementar (consultar procedimento para solicitações de sites para eventos);
§ 2º Os votos são secretos, ocorrendo de forma individualizada, havendo confirmação de autenticidade de cada eleitor, quando da realização do procedimento;
§ 3º Sob nenhuma hipótese o CTIC tem acesso aos resultados da eleição, o que compete exclusivamente aos membros da Comissão Eleitoral.

Das Prescrições Finais

Art. 15º - Esta norma entra em vigor na data de sua aprovação, revogadas as disposições em contrário.