IntegraSolução®

FÁBRICA DE SOFTWARE

POLÍTICA DE SEGURANÇA E SIGILO DO VOTO

IntegraSolução®
FÁBRICA DE SOFTWARE

POLITICA DE SEGURANÇA DA INFORMAÇÃO E SIGILO DO VOTO

DESCRITIVO DE SEGURANÇA

Versão 1.0

01 de Janeiro de 2023

INTRODUÇÃO

Um processo de eleição online herda da legislação nacional brasileira determinadas características. Destas, as principais, que devem conter em um sistema informatizado de gestão e execução de uma eleição online são o sigilo do voto (confidencialidade), a garantia de que a escolha do eleitor foi computada e armazenada exatamente como o eleitor escolheu (integridade), a garantia de que o eleitor só pode exercer seu poder de voto uma vez por processo eleitoral (unicidade de voto) e a garantia de que o eleitor, dentro do período pré-determinado pelo processo eleitoral, poderá exercer seu poder de voto (disponibilidade). Além destes requisitos, um sistema informatizado de gestão e execução de uma eleição online deve ser passível de validação (auditável), garantir a segurança das informações que trafegam entre o eleitor e os servidores onde o sistema encontra-se hospedado (segurança de comunicação, camadas de criptografia de comunicação) e garantir a inviolabilidade dos dados após serem armazenados (integridade).

Um processo eleitoral atende a 3 (três) principais grupos: os eleitores, os candidatos e a comissão eleitoral. Demais grupos, como auditores, são grupos opcionais, de apoio ao processo.

Este documento apresenta os elementos constantes na tecnologia da ferramenta de eleições ELEJA ONLINE que possuem como objetivo a implementação dos itens acima expostos. Entendendo também que segurança é algo etéreo, apresenta-se neste documento módulos auxiliares que podem ser utilizados com o intuito de aumentar a sensação de segurança por parte dos grupos envolvidos em um processo eleitoral.

TECNOLOGIAS UTILIZADAS

A solução ELEJA ONLINE utiliza tecnologias baseadas em FOSS (Free Open Source Software), a saber:

- Banco de Dados relacional Postgresql
- Banco de Dados NOSQL mongodb
- Linguagem de programação Python
- Aplicativo de servidor HTTP Nginx
- Protocolo de segurança SSL
- Sistema Operacional Linux e FreeBSD

DA ESTRUTURA DE TECNOLOGIA

A ferramenta principal, com os códigos responsáveis pelas API, que fornecem as interfaces web e processam as informações é desenvolvida na linguagem Python e executada como um serviço com um ou mais processos “escutando” a solicitação de comunicação.

Todos os dados, com exceção de dados de sessão, são armazenados e consultados em banco de dados relacional com o software de banco de dados PostgresSQL.

A comunicação entre a aplicação em Python e os usuários se dá através da aplicação web Nginx, que atua como “proxy” e promove balanceamento de carga. Esta comunicação ocorre através de conexão segura (SSL).

A comunicação com o banco de dados relacional ocorre exclusivamente entre a aplicação em Python e o banco de dados, através de conexão segura (SSL).

O sistema operacional responsável pelas aplicações Nginx e PostgresSQL pode ser Linux ou FreeBSD. O sistema operacional responsável pela aplicação API, em python, é o FreeBSD.

O sistema operacional FreeBSD possui recursos de segurança que podem ser utilizados para garantir a não modificação de arquivos, utilizando atributos do sistema de arquivos e níveis de kernel.

Atributos: o sistema operacional FreeBSD possui atributos especiais para arquivos. Dois deles são relevantes aos tópicos deste documento e utilizados na solução Eleja Online. O atributo “imutável” (immutable) e o atributo “apenas adição” (append-only).

- Imutável: com este atributo o arquivo não pode ser alterado, movido ou excluído nem mesmo pelo usuário root. Este atributo é definido em todos os arquivos da aplicação da API.
- Apenas adição: com este atributo um arquivo só pode receber novas informações ao final do mesmo, mas não pode ser modificado nem excluído. Este atributo é definido em arquivos de log.

Níveis de kernel: o usuário root ou proprietário do arquivo pode a qualquer momento alterar os atributos especiais de um arquivo enquanto o nível de kernel do SO encontra- se menor ou igual a 2. Após elevar o nível de kernel a 3, nem mesmo o usuário root poderá alterar os atributos previamente ativados. Por sua vez, o nível de kernel nunca pode ser diminuído, exceto reiniciando o sistema operacional por completo.

Com a utilização destes recursos, é possível comprovar que um código fonte auditado após a adição do atributo de imutável e o aumento do nível de kernel não foi alterado, desde que o tempo ativo do sistema operacional não seja menor do que o tempo ativo no momento da auditoria do código.

De igual forma, as informações dos arquivos de log sempre serão verossímeis, uma vez que o arquivo só permite adicionar informações ao final do mesmo, e a retirada do atributo de “apenas adição” não pode ser feito sem o reinício do sistema operacional.

MÓDULOS

O sistema possui 2 módulos: o módulo de eleição, responsável por permitir que o eleitor conecte no sistema, se identifique, efetue seu voto e visualize seu comprovante de votação, e o módulo de gestão da eleição (back office), responsável por permitir que os organizadores da eleição gerenciam eleições, eleitores, candidatos, chapas, demais formatos de votos, além da emissão de relatórios, inicialização e fechamento de eleições, emissão de zerésimas e apuração de resultados e relatórios de auditorias.

A seguir, apresentamos os elementos de segurança utilizados em cada um dos módulos.

MÓDULO VOTO

DA COMUNICAÇÃO

O eleitor, para votar, acessa, utilizando um navegador de internet, o endereço (URL) previamente fornecido pelo contratante da eleição.

Se o eleitor não informar o protocolo HTTPS antes do endereço, o servidor automaticamente redireciona para o endereço com o protocolo HTTPS.

O certificado digital ativo no servidor web garante a comunicação segura entre o servidor que fornece as páginas web que permitem o voto e o navegador de internet do eleitor (criptografia de ponta a ponta).

As informações de sessão são armazenadas no servidor (Server Side Session), com a referência a esta sessão na forma de cookie utilizando token.

O botão Voltar do navegador, como medida extra de segurança, comporta-se como uma atualização da página atual.

DA SEGURANÇA DAS INFORMAÇÕES AUTENTICAÇÃO

A autenticação ocorre em dois momentos. Na primeira página o eleitor informa o login. Se o sistema reconhece o login como válido, na tela seguinte solicita a senha. A cada erro de senha o sistema retorna à tela de login. Neste momento um contador associado ao login é incrementado. Após 5 tentativas erradas, o sistema bloqueia o login por 1 minuto. A recorrência da sequência de 5 erros bloqueia o login por 5 minutos, e uma última recorrência bloqueia o login permanentemente, só podendo ser desbloqueado via interface de gestão da eleição. Este bloqueio é baseado na associação do login com o IP de origem, para evitar que seja possível, tendo acesso à lista de logins (CPF, por exemplo), que haja um ataque em massa na tentativa de bloquear vários logins.

As informações iniciais de usuário e senha, mesmo no ambiente de conexão segura, não trafegam no formato “texto aberto” entre a página web e o servidor API. A página web recebe uma chave pública da API, criptografa a informação (login ou senha) e o envia criptografado para o servidor API. O mesmo descriptografa a informação com a chave privada e então processa a informação recebida.

No banco de dados, a senha encontra-se criptografada utilizando criptografia simétrica com o módulo de seguranção Fernet, da liguagem Python, que é uma implementação de AES. A chave encontra-se no módulo de segurança do código-fonte.

LOG

Todas as ações, desde a primeira conexão, login, senha, voto, qualquer tipo de erro ao gravar alguma informação, tentativas excessivas de login, impressão do comprovante, enfim, todas as ações resultantes da interação do eleitor são gravadas em uma tabela de log, facilitando a análise e auditoria do sistema.

VOTAÇÃO

Para cada votante, as opções de voto são geradas no servidor, associadas a tokens aleatórios (que mudam a cada atualização da página), e enviados à página web para compor as opções de voto do eleitor. Cada opção de voto já é criptografada com a chave privada do certificado digital instalado no sistema. Após escolher o voto, a página web criptografa a escolha com a chave pública e envia para o servidor API. O servidor API descriptografa a informação com a chave privada e então armazena a opção de voto.

Caso os testes internos permitam a aceitação do voto, o servidor API armazena a escolha na tabela de voto. Também gera um hash único com informações do eleitor como medida de proteção adicional à unicidade do voto, armazenando também esta informação no registro do voto do eleitor.

Como opcional, um arquivo PDF pode ser gerado para cada voto. O conteúdo deste arquivo PDF é a mesma informação criptografada gravada no banco de dados, e corresponde a 1 (voto). O conteúdo desta informação criptografada pode ser aberto utilizando a chave privada. Este arquivo PDF também é assinado digitalmente com o certificado digital, para fins de avaliação da veracidade da informação no mesmo armazenada. Também é possível promover o envio assíncrono de cada arquivo PDF gerado para outro endereço, garantindo a não manipulação posterior dos arquivos.

BACKOFFICE

O sistema de gestão das eleições por parte dos organizadores ou comissão eleitoral utiliza os mesmos princípios de comunicação segura para criptografia de ponta a ponta e segurança dos dados utilizados no módulo de voto.

Tal como o sistema de voto ,todas as ações no backoffice são gravadas em uma tabela de log, facilitando a análise e auditoria do sistema.

O principal atributo de segurança no módulo backoffice é o sistema de permissões, que garante que cada usuário autenticado no sistema só poderá acessar as funcionalidades e informações definidos pelos administradores, garantindo a confidencialidade dos dados por níveis hierárquicos e estratégicos da empresa.

DOS MÉTODOS DE CRIPTOGRAFIA

O sistema utiliza AES para criptografia simétrica, chaves pública e privada para o envio de dados criptografados entre o formulário web e o REST/API, chave privada para assinatura de dados e documentos e chave HASH para cálculo de dados seguros.

DO ARMAZENAMENTO DAS CHAVES

O sistema mantém em arquivos separados as chaves públicas e privada utilizadas pelo sistema. Estes arquivos são de leitura apenas do usuário master do sistema operacional.

DO ARMAZENAMENTO DE DADOS

Os dados são armazenados em banco de dados relacional. Todos os dados sensíveis que precisam ser acessados, como o voto, são criptografados, e todos os dados sensíveis passíveis de ser analisados por cálculo criptográfico são armazenados em formado de HASH.

DA COMUNICAÇÃO

Todo o tráfego de informações ocorre em conexões seguras encapsuladas em SSL, a saber: navegador do eleitor e servidor web; servidor web e servidor RESP/API e servidor REST/API e banco de dados relacional.