DESCRIÇÃO SOLUÇÃO

SISTEMA BEEVOTER

1. SUMÁRIO

2. VISÃO GERAL

2.1. A segurança é o coração de qualquer eleição.

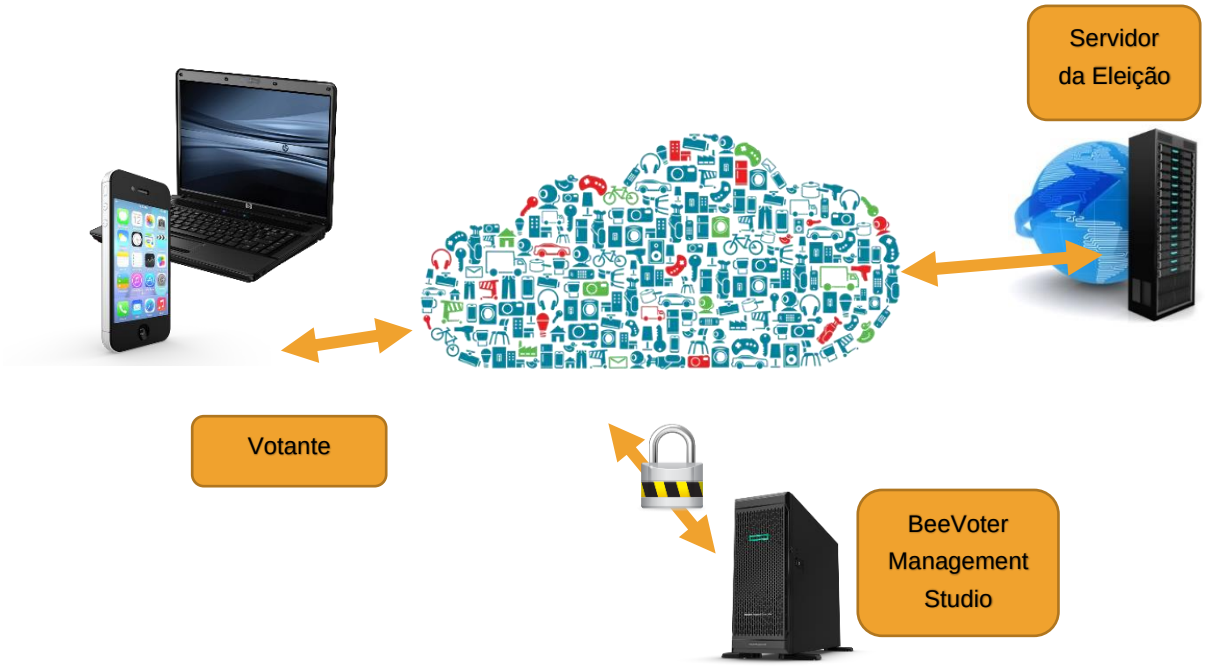
Eleições justas e democráticas dependem de medidas de segurança rígidas e robustas que fornecem sigilo aos eleitores autenticados, mantêm a integridade das cédulas e permitem a auditoria transparente de todos os processos eleitorais, como cabines de votação privadas e envelopes de voto e registros físicos de papel que não existem nas eleições online.

Protocolos de segurança alternativos foram desenvolvidos para garantir o sigilo, integridade e capacidade de auditoria ao usar a tecnologia de votação online.

Este documento objetiva a apresentação dos detalhes do sistema para votação eletrônico que permitem proteger o sigilo, a integridade e a capacidade de auditoria de uma eleição de votação online.

3. A SOLUÇÃO BEEVOTER

O sistema de votação é completamente auditável.



a) O voto poderá ser realizado de forma remota a partir de computadores pessoais ou dispositivo móvel, através de páginas responsivas;

b) O votante só poderá realizar seu voto a partir de sua senha secreta[1];

c) As senhas serão enviadas ao eleitor diretamente do computador da administração do processo eleitoral, sendo que o servidor da Eleição nunca terá conhecimento destas;

d) Suportar o sistema de votação durante o período da eleição;

---

[1] *Opcionalmente poderá ser utilizado autenticação segura através de certificados digitais ICP-Brasil ou biometria facial.*

e) A apuração será realizada em duas fases:

- Remoção do vínculo entre o eleitor e o voto encriptado (mixagem dos votos), realizado no Servidor da Eleição e verificação da integridade dos dados no banco de dados;
- Decriptografia dos votos e contagem do resultado, realizado na máquina de Administração do processo eleitoral[2].

3.1. O SISTEMA ABRANGE SOLUÇÕES QUE ATENDE OS SEGUINTES ATORES:

a) VOTANTE:

Canal dedicado ao votante onde será divulgado todo o material referente a assembleia/eleição, no qual poderá registrar seu voto, contendo:

- Cédula de votação personalizada;
- Recibo de voto personalizado;
- Mecanismo de integridade que garante que o voto seja apurado tal qual a vontade do eleitor.

b) COMISSÃO ELEITORAL:

Suporte a comissão eleitoral de forma a permitir a manutenção dos dados, de forma completamente personalizada, bem como a personalização do sistema eleitoral de forma a transmitir corretamente as informações da eleição.

c) AUDITORIA:

Provimento de todas as informações que permitam aos auditores garantir a integridade e o sigilo dos votos realizados, como:

- Todas as configurações do sistema;
- Relação dos votantes e credenciais habilitadas para votar;

- *2 Um ambiente isolado no qual um computador não precisa necessariamente estar conectado a redes, principalmente à Internet pública. Esta é uma medida de segurança para manter as cédulas online protegidas contra manipulação, uma vez que são baixadas e durante o procedimento de contagem.*

- Relação dos votos realizados (encriptados) com os respectivos elementos de segurança;
- Entre outras informações que eventualmente possa ser solicitado pela auditoria.

4. DETALHAMENTO TÉCNICO

4.1. PREMISSAS

Nossa solução foi construída e concebida com a seguinte premissa: *Não basta fazer a coisa certa. Também é necessário PARECER estar fazendo certo.*

Desta forma, foram introduzidos elementos de segurança que permitam comprovar que mesmo os funcionários e administradores de banco de dados da nossa empresa, que tem a prerrogativa de acesso irrestrito ao banco de dados do sistema, não possam alterar o conteúdo do banco de dados sem que isso produza rastros que permitam invalidar o processo.

A maioria dos sistemas tem como único elemento de proteção, as *logs*[3] produzidas pelos bancos de dados, no entanto estas *logs* são arquivos textos que podem facilmente serem manipuladas.

O que buscamos em nossa solução foi o uso abundante de soluções de criptografia de forma a garantir a confiança no resultado obtido a partir das informações do banco de dados, sem que seja necessário sequer esta log do banco de dados.

4.2. AMBIENTE

Nossa solução está subdivida em:

a) Um sistema que tenha como premissa a apresentação das informações acerca do processo, da autenticação do eleitor, da COLETA segura do voto do eleitor e do armazenamento destes votos, do qual chamaremos de CAIXA PRETA;
b) Uma camada responsável por produzir toda a configuração que alimentará a CAIXA PRETA e por consumir o resultado dos votos registrados na CAIXA PRETA, do qual chamaremos de **BeeVoter Management Studio**.

[3] *log de dados é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional.*

Todas as trocas de informações entre o **BeeVoter Management Studio** e a CAIXA PRETA são feitos através de arquivos XML assinados digitalmente, e que apenas arquivos assinados corretamente serão aceitos tanto para a carga de informações no sistema eleitoral quanto para a apresentação dos resultados do processo eleitoral, o que impede que intervenções maliciosas possam alterar o andamento e o resultado da votação.

Esta separação da CAIXA PRETA e do **BeeVoter Management Studio** permite segregar algumas ações que só possam ser desempenhadas pela comissão eleitoral, auditores ou outros, onde esta função do **BeeVoter Management Studio** poderá ser instalada em um computador completamente desconectado da internet e armazenado em um espaço fiscalizável, protegido por meio de chaves criptográficas.

4.3. SEGURANÇA E AUDITABILIDADE

A solução foi concebida de forma a ser totalmente auditável.

Imaginemos que um sistema eleitoral SEMPRE será uma **CAIXA PRETA**.

Não é possível auditar, em tempo real, o que é feito a partir do registro dos votos pelos eleitores.

Desta forma, nossa proposta foi remover o máximo de inteligência desta **CAIXA PRETA**, tornando-a apenas um mecanismo de armazenagem de votos e introduzir elementos de segurança que permita verificar se os dados armazenados estão realmente íntegros, não sendo possível, nem mesmo para o administrador do sistema ou do banco de dados do sistema, alterar o conteúdo de um voto sem que tal ação não possa ser verificada.

O principal elemento de segurança que fora introduzido foi o uso das chaves assimétricas, que permitirá a garantia da autenticidade, integridade das informações do sistema eleitoral e ainda o sigilo dos votos.

> *Um processo de criptografia que usa a mesma chave para criptografar e decriptografar mensagens é conhecido como criptografia simétrica, enquanto um processo que usa uma chave para criptografar mensagens e uma chave diferente para decriptografá-las é conhecido como criptografia assimétrica.*
>
> *Uma chave assimétrica é uma forma de criptografia que permite a cifragem de uma informação com uma chave e a decifragem com outra chave (par da primeira).*

Na prática, chamamos uma destas chaves de chave privada, que deve ser mantida em segredo com seu proprietário e a outra de chave pública, que poderá ser divulgada e será utilizada para comunicar-se com o proprietário da chave.

São duas as formas de utilizar esta chave:

- *Criptografa-se com a chave pública, onde apenas o proprietário poderá decriptografar o conteúdo, o que permitirá a troca de informações sigilosas com o proprietário da chave;*
- *Criptografa-se com a chave privada, onde apenas o proprietário poderá criptografar o conteúdo, no entanto qualquer um com acesso a chave pública poderá decriptografar, o que permitirá a criação de elementos criptográficos que garantem a autoria de alguma ação efetuada pelo proprietário (assinatura digital).*

E como fazemos isso?

Vamos pensar em alguns tipos de atores distintos: comissão eleitoral/auditoria, apoiadores do processo eleitoral, eleitores e o próprio sistema eleitoral (**CAIXA PRETA**).

Na eventualidade de não ser possível auditar com detalhes esta **CAIXA PRETA**, partimos da premissa que o sistema NUNCA terá as chaves privadas da comissão eleitoral ou dos eleitores, e que todas as ações destes outros atores possam ser confirmadas a partir da verificação de assinaturas efetuadas por suas respectivas chaves privadas.

Como forma de garantir que alguma ação tenha sido feita pelo próprio sistema eleitoral (**CAIXA PRETA**), ele também contém sua chave assimétrica, onde a chave privada ficará na memória do programa para uso enquanto o programa estiver rodando e, quando o programa for encerrado, esta chave some.

Um tema que merece destaque em um sistema eleitoral é a necessidade do sigilo do voto, uma premissa que faz parte do fundamento de qualquer sistema democrático de forma a inibir a prática de vendas de votos ou de votos coercivos. Ocorre que a garantia deste sigilo comumente traz um problema que é a impossibilidade de garantir que o voto do eleitor não sofreu nenhuma modificação pelo sistema eleitoral. Conseguimos solucionar isto da seguinte forma:

a) No momento em que se configura o processo eleitoral, gera-se uma chave assimétrica para o processo eleitoral, protegendo a chave privada por meio de PIN ou segredo compartilhado[4] pela comissão eleitoral;

b) No momento que a credencial do eleitor é gerada, também é gerada a chave assimétrica deste eleitor;

c) Para garantir que não será possível obter acesso a chave privada do eleitor, esta é encriptada com a senha que será entregue ao eleitor e que o sistema eleitoral não terá conhecimento.

d) Estas ações descritas acima são realizadas FORA do sistema eleitoral, na ferramenta **BeeVoter Management Studio**, o que produzirá arquivos de configurações assinados que serão carregados no sistema eleitoral e farão parte dos artefatos entregues a auditoria para que possam ser verificados a qualquer momento;

e) Quando o sistema eleitoral é iniciado, ele também cria sua chave assimétrica, deixando sua chave privada apenas na memória do sistema e divulgando sua chave pública no banco de dados;

f) No momento em que o eleitor se autentica, ele recebe do sistema eleitoral a chave pública do processo eleitoral, bem como sua chave privada encriptada por sua senha, que apenas o eleitor tem conhecimento;

g) O eleitor então encripta sua escolha de voto com a chave pública do processo eleitoral, e utiliza sua chave privada (que só pode ser revelada com sua senha secreta) para assinar o voto encriptado, enviando para o sistema eleitoral o voto encriptado (com a chave pública do processo eleitoral) e a assinatura (voto encriptado, encriptado novamente com a chave privada do eleitor);

---

[4] A técnica de segredo compartilhado permite selecionar um número mínimo de pessoas dentre um grupo que serão exigidas para revelar a chave.

h) Ainda no processo de envio do voto, o computador do eleitor gera um número aleatório, que será de conhecimento apenas do eleitor, efetua um resumo criptográfico deste número aleatório (*função hash*), e envia ao servidor como se fosse uma requisição de recibo;

i) O servidor, ao receber o voto do eleitor, armazena o voto encriptado, e utiliza a assinatura do voto apenas para a verificação da integridade entre o percurso da máquina do votante até o servidor, substituindo-a por uma assinatura realizada pela chave privada do servidor, e devolve ao eleitor uma assinatura da requisição de recibo do eleitor com sua chave privada (chave do servidor), garantindo assim que recebeu e armazenou o voto do eleitor corretamente.

O processo descrito acima garante que:

- O voto do eleitor está em sigilo, uma vez que seu conteúdo está encriptado com uma chave que apenas a comissão eleitoral tem acesso;
- O voto do eleitor está íntegro, uma vez que está assinado com uma chave que reside apenas na memória do servidor, e que poderá ser verificado contra a chave pública deste;
- O eleitor tem um artefato criptográfico que permitirá, sem a necessidade da violação do sigilo, garantir que seu voto fora computado na apuração.

Todas as ações efetuadas no sistema eleitoral são armazenas em uma log, que registra os endereços IPs das ações realizadas, e todas as mensagens trocadas com os usuários (informações de requisição e resposta).[5]

Estas logs estão protegidas por um mecanismo de *proteção*[6], que não permite a introdução, remoção ou alteração de uma das logs sem isto não provoque a quebra da sequência das demais e, são assinadas pela chave privada do servidor, que só é de conhecimento do sistema eleitoral por estar presente apenas na memória do sistema.

---

[5] *Exceto o voto encriptado, de forma a inibir a quebra do sigilo do voto.*

[6] *A proteção utilizada implica em assinar o conteúdo de cada log mais a assinatura da log imediatamente anterior. Isso garante que seja impossível a modificação não só de seu conteúdo, mas também da sequência das logs, uma vez que todas as logs estão encadeadas.*

Ao final do processo eleitoral, inicia-se o processo de apuração, que consiste:

A comissão eleitoral solicita o download dos votos armazenados no sistema eleitoral, onde o sistema eleitoral efetua a verificação de todas as assinaturas dos votos, impedindo que algum voto que tenha sido modificado no banco de dados possa ser usado para computar o resultado da eleição, e, na eventualidade do voto ser realmente secreto, o sistema eleitoral busca separar qualquer referência entre os votos e seus autores, embaralhando a ordem dos votos que serão submetidos à comissão eleitoral;

- O sistema eleitoral efetua também a verificação do encadeamento de todas as logs, de forma a garantir que nenhuma log fora suprimida, alterada ou inserida antes de ser entregue a comissão eleitoral;

Feito isso, o sistema eleitoral retorna à comissão eleitoral as seguintes informações:

- Os votos em posição completamente "embaralhada", caso sejam secretos, que serão utilizados para realizar a apuração[7];
- As assinaturas dos recibos dos eleitores possibilitando a qualquer momento futuro a verificação da integridade dos votos processados;
- A relação com todos os registros de eventos de ações realizadas no sistema eleitoral;
- A relação dos votantes e não votantes.
- Por estarem em arquivos, todas estas informações farão parte dos artefatos entregues a auditoria, o que permitirá a qualquer momento futuro garantir a integridade das informações processadas no sistema eleitoral.
- O sistema da comissão eleitoral obtém então o acesso à chave privada [8]do processo eleitoral (protegido através de senha ou segredo compartilhado) e decriptografa cada um dos votos, possibilitando a contagem do resultado da eleição, em que a ferramenta de **BeeVoter Management Studio** possibilitará a "renderização" desta contagem a partir de templates pré-definidos.

---

[7] *Na eventualidade do voto não ser secreto, o voto será entregue associado ao votante, sendo possível relacioná-lo ao seu autor.*

[8] *Em função da necessidade de realização de apuração em ambientes remotos, o sistema permite também que seja carregado no banco de dados a chave privada da eleição completamente encriptada, onde será disponibilizada uma interface para que seja introduzido a(s) senha(s) que a protege(m) em uma interface, decriptando-a apenas na memória do servidor, possibilitando assim a decriptação e contagem dos votos no servidor Web.*

O processo descrito acima permite garantir que:

- Na eventualidade do voto ser secreto, não é possível mais relacionar quem votou em quem, pois a ordem dos votos não preserva nenhuma relação cronológica;
- Será possível verificar a qualquer momento futuro, a partir de testes amostrais e dos recibos de votos, se o voto de algum eleitor foi realmente processado sem a quebra do sigilo.

As técnicas apresentadas neste documento permitem garantir que, ao apurar o resultado da eleição, seja possível atestar que todos os votos utilizados para a apuração permanecem íntegros de acordo com a vontade do eleitor, e que nenhum voto fora suprimido da apuração, mesmo sem existir a possibilidade de relacionar um voto com o seu votante.

Ocorre que o sistema eleitoral, do qual chamamos de **CAIXA PRETA** até este momento, não é exatamente uma **CAIXA PRETA**.

Também faz parte do serviço que oferecemos um processo de apresentação dos códigos-fontes do sistema e do acompanhamento da publicação do sistema eleitoral e dos processos de atualização pela auditoria, no entanto com a técnica que descrevemos acima, o processo de auditoria dos códigos-fontes se torna bem menos complexo, onde basta analisar o trecho do código onde o voto é registrado e onde os votos são "mixados" para entrega para a comissão eleitoral. Todo o restante produz baixo impacto na segurança do voto[9].

Ainda sobre o processo de auditoria, por tratar-se de sistema on-line e o votante realiza seu voto diretamente de seu computador pessoal ou de seu dispositivo móvel, a forma de se auditar esta camada se faz de forma amostral, onde é possível a QUALQUER eleitor, durante a inserção de seu voto, analisar o código-fonte de sua página e as transações de rede trocadas entre o seu navegador e o servidor de forma a

[9] *A apresentação dos códigos-fontes está condicionada a critérios que permitam preservar a propriedade intelectual, sendo impostas algumas restrições de acesso aos participantes.*

avaliar que apenas informações encriptadas são trocadas e que sua senha secreta ou sua escolha nunca será revelada ao servidor.

Ao ser instalado, o sistema eleitoral conta ainda com um mecanismo de *watchdog* que fica constantemente inspecionando qualquer tentativa de modificação dos programas que estão "*rodando*" no ambiente do sistema eleitoral. Isto torna possível garantir que não houve modificações não previstas no sistema eleitoral que permitissem a introdução de algum mecanismo que vise fraude sem que tal ação não possa ser descoberta.

4.4. **CUSTOMIZAÇÃO**

Um sistema eleitoral, ao apresentar a cédula de votação, parece um sistema bastante simples, no entanto para que haja uma divulgação eficaz das informações acerca do processo de votação, é importante munir o eleitor do máximo possível de informações para que este possa tomar sua decisão de forma consciente.

Desta forma, é fundamental que sejam apresentados ao eleitor todas as informações necessárias acerca do processo de votação e nossa solução foi concebida para atuar como se fosse um CMS *(Content Management System - Sistema Gerenciador de Conteúdo)*, permitindo apresentar-se ao eleitor com a identidade visual e adequando-se a necessidade de apresentação do **dono da eleição**.

Outro detalhe bastante importante é que as informações apresentadas ao eleitor durante o processo eleitoral também necessitam serem auditadas, pois é fundamental saber qual informação fora apresentada ao eleitor durante a escolha de seu voto. Uma fraude comum em sistemas eleitorais é a supressão ou mesmo alteração do nome de algum candidato durante a eleição, de forma que o eleitor NÃO possa votar naquele determinado candidato.

Lembre-se que nossa solução foi concebida de forma a ser totalmente auditável.

Isto inclui também as informações que são apresentadas ao eleitor e desta forma, é possível ao administrador configurar não apenas quem serão os concorrentes do processo eleitoral, mas também como serão apresentadas todas as informações do site eleitoral (*HTMLs, CSS e regras de negócios*).

4.5. RECURSOS

Toda a hospedagem da solução em datacenter em nuvem, em provedores de alta disponibilidade e com redundância física, contemplando fornecimento do sistema operacional Windows Server, IIS, banco de dados MS SQL, servidor de DNS, firewall, acesso a rede internet, plano de backups diários, semanais e mensais e administração da infraestrutura de forma a mitigar ataques.

5. NOSSA EMPRESA

A Beehive Technologies tem larga experiência no desenvolvimento de soluções para votação eletrônica com protocolos de segurança baseados em criptografia, atuando desde a concepção da solução tecnológica até a sua efetiva implantação, incluindo etapas tais como modelagem, design, programação, testes, avaliação de desempenho, usabilidade, treinamento de usuários e hospedagem da solução.

A ampla experiência profissional da equipe permite o desenvolvimento de soluções críticas para os mais variados ramos de atividade integrando dados, voz, SMS, telefonia, Workflow, Criptografia de Dados, Sistemas de segurança da informação, Certificação Digital e Internet com elevado desempenho e total segurança.

Fundada em 2016, tem foco no desenvolvimento de soluções para suporte a organização corporativa em várias camadas.

Nossos profissionais atuam no mercado de eleições a distância desde o ano de 2009, com experiência em mais de 100 processos eleitorais no Brasil, com atuação comprovada em diversos clientes, desde conselhos profissionais, associações, sindicados etc.

NOSSA VISÃO

Maior eficiência e qualidade na prestação de serviços por meio da otimização e organização do trabalho, principalmente em grupos.

NOSSA MISSÃO

Ser o maior fornecedor de soluções democráticas a um custo justo e acessível.

NOSSOS VALORES

Entregar com rapidez e qualidade, comprometido com os resultados de nossos clientes, sempre com ética, transparência e respeito.

6. INFORMAÇÕES CADASTRAIS

Razão Social	DGB SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO LTDA
Nome Fantasia	BEEHIVE TECHNOLOGIES
CNPJ	26.652.906/0001-84
Inscrição estadual	07.791.723/001-76
Endereço	SMDB CONJUNTO 12 CL, BLOCO C, SALA 208, SETOR DE MANSÕES DOM BOSCO (LAGO SUL), BRASILIA/DF CEP: 71.680,120

Brasília/DF, 3 de fevereiro de 2022.

Ubiratan Elias
Diretor de Tecnologia
061 98467-7946