

Registro impresso do voto, autenticado e com garantia de anonimato

Rodrigo Carneiro Munhoz Coimbra
José Roberto Menezes Monteiro
Gladiston da Silva Costa

¹Tribunal Superior Eleitoral (TSE)
Brasília, DF

{rodrigo.coimbra,jose.monteiro,gladiston.costa}@tse.jus.br

Abstract. *The electoral reform approved in the year 2015 brought again the need to produce a material paper record of the vote in Brazilian voting machines. The mere printing of voters' choices, without the addition of any security mechanism, while meeting the requirements of current legislation, opens the door to a series of fraud attempts at recount. This paper presents a printed voting format that allows for an easy conference of voter choices, including mechanisms for automating the counting and checking the authenticity of the vote, while preserving its anonymity. It is not proposed here to debate the effectiveness of the printing of votes by the voting machine, but rather to present a technological solution to a problem that needs to be addressed by the Brazilian Electoral Court.*

Resumo. *A reforma eleitoral aprovada no ano de 2015 trouxe novamente a necessidade de produção de um registro material em papel do voto realizado nas urnas eletrônicas brasileiras. A simples impressão das escolhas do eleitor, sem a adição de qualquer mecanismo de segurança, embora atenda aos requisitos da legislação vigente, abre espaço para uma série de tentativas de fraude no momento da recontagem. Este trabalho apresenta um formato para voto impresso, que permita uma conferência fácil de suas escolhas pelo eleitor, incluindo mecanismos para automação da contagem e verificação da autenticidade do voto, ao mesmo tempo em que seu anonimato é preservado. Não se propõe aqui fazer um debate sobre a efetividade da impressão de votos pela urna eletrônica, mas sim apresentar uma solução tecnológica para um problema que precisa ser tratado pela Justiça Eleitoral brasileira.*

1. Introdução

A Lei nº 13.165/2015 [Presidência da República 2015] institui o registro impresso do voto para conferência pelo eleitor. A lei determina:

Art. 59-A. No processo de votação eletrônica, a urna imprimirá o registro de cada voto, que será depositado, de forma automática e sem contato manual do eleitor, em local previamente lacrado.

Parágrafo único. O processo de votação não será concluído até que o eleitor confirme a correspondência entre o teor de seu voto e o registro impresso e exibido pela urna eletrônica.

O novo normativo determina, portanto, que a urna deverá imprimir as escolhas do eleitor e ele não terá qualquer contato manual com o papel, que será depositado em receptáculo fisicamente seguro (lacrado). A lei demanda também que o voto só será computado pela urna após a validação do registro impresso pelo eleitor. Nesse sentido, qualquer formato adotado para o voto impresso deve priorizar a facilidade de verificação pelo eleitor.

Não há na lei qualquer sugestão de mecanismos de segurança associados ao registro impresso, tampouco há a determinação de como deve ser realizada a conferência dos votos em caso de contestação do resultado eletrônico. Esse vácuo normativo demanda que seja dada uma atenção especial a elementos da única etapa do processo que demandará intervenção manual. A recontagem de votos precisa de uma garantia de autenticidade do voto impresso, de modo a evitar fraudes associadas à troca de registros em papel ou à inserção de registros fraudulentos. A contagem também deve ser facilitada e passível de automação e validação.

A seguir é apresentada uma dinâmica de impressão do voto, associada a um formato do registro impresso, que promova uma conferência simples e ágil dos votos pelo eleitor. Em seguida é introduzido um mecanismo de assinatura digital do voto impresso, que acrescenta um elemento autenticador, ao mesmo tempo que preserva o anonimato do voto. Essa assinatura digital está associada a um mecanismo que permitirá o desenvolvimento de aplicativos independentes de apuração segura dos votos impressos. Essas propostas devem ser de fácil implementação pelo Tribunal Superior Eleitoral — TSE, que é o responsável pelo desenvolvimento do software da urna eletrônica.

2. Dinâmica de impressão do voto

O sistema brasileiro de votação consiste na apresentação individual e sequencial dos cargos que estão em disputa na eleição, de modo que o eleitor digita o número do seu candidato para o respectivo cargo e, após a confirmação do seu voto, segue para o próximo cargo até que se encerrem as escolhas possíveis.

Nas Eleições 2002, quando houve a primeira experiência brasileira de impressão de votos conferidos pelo eleitor, essa sistemática foi preservada. Contudo, após a confirmação do voto no último cargo, era produzido o registro impresso dos votos e solicitado ao eleitor que o confirmasse. Nesse momento não havia nada na tela da urna eletrônica que auxiliasse o eleitor a verificar o registro impresso, nada com que ele pudesse confrontar o registro em papel. Esse cenário fatalmente confundiu muitos eleitores, que devem ter rejeitado indevidamente o registro impresso do voto ou sequer o validaram.

Para facilitar a conferência do voto impresso pelo eleitor faz-se necessária a adição de uma nova tela ao Software de Votação — a tela resumo (Figura 1). Após a confirmação do voto no último cargo, é apresentada uma

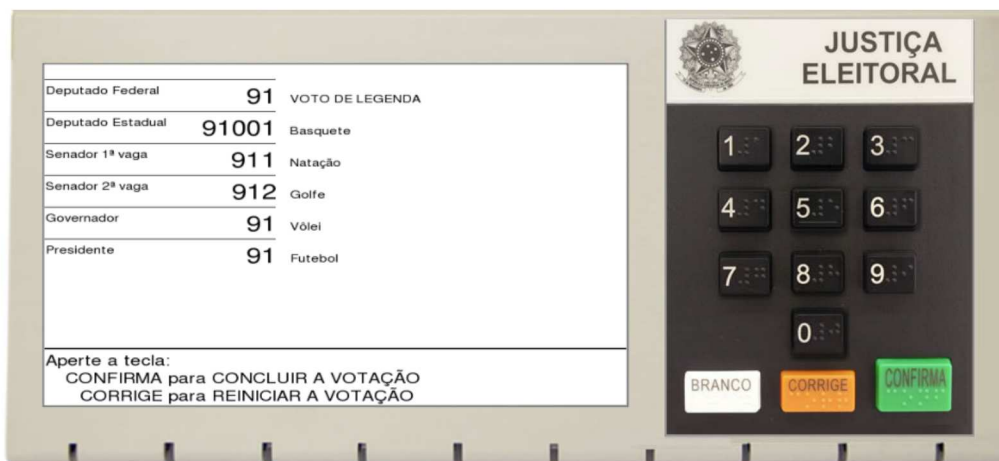


Figura 1. Exemplo de tela resumo para a conferência do voto impresso. As linhas de separação, quando alinhadas ao registro impresso auxiliam na conferência do voto.

tela com o resumo da votação do eleitor, ou seja, são listados na tela os votos em todos os cargos, de forma resumida, ao mesmo tempo em que o registro impresso é apresentado na impressora. Dessa forma, o eleitor pode confrontar o registro impresso com o registro eletrônico, sem a necessidade de recorrer à sua memória.

Nesse ponto, tanto o registro impresso do voto quanto a tela resumo devem apresentar exatamente os mesmos números digitados pelo eleitor. Caso um eleitor anule o seu voto pela digitação de um número de candidato inexistente, esse número deve ser apresentado e não somente a sua interpretação (ou seja, a marcação de voto nulo).

A apresentação da tela resumo, associada com o alinhamento da área de visualização da impressora com a tela da urna, está em conformidade com as recomendações mais modernas de usabilidade de sistemas de votação com registro impresso do voto [EAC 2015].

A partir da tela resumo, deve ser possível ao eleitor confirmar o seu voto ou cancelá-lo. Ao confirmar o seu voto, o registro impresso deve ser depositado automaticamente em receptáculo lacrado, conforme determina a Lei nº 13.165/2015. Caso contrário, o registro impresso também será depositado no mesmo recipiente lacrado, mas com marcação de "cancelado" e a votação reiniciada. Essa nova dinâmica é sintetizada pela Figura 2.

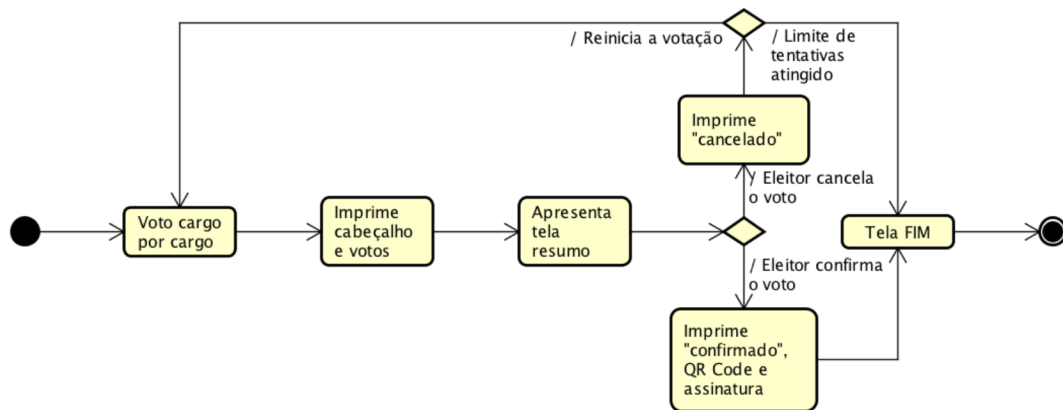


Figura 2. Novos estados do ciclo de votação. Ao cancelar um registro impresso a votação é reiniciada, mas até um determinado limite — nesse caso nenhum registro eletrônico é realizado. Ao confirmar o voto o registro eletrônico é realizado e a votação concluída.

Uma característica desse novo processo de votação é que passa a existir um registro material fidedigno da sequência de escolhas de um eleitor. Esse cenário consiste numa fragilização do anonimato do voto. Isso porque um atacante que está coagindo o eleitor a votar num determinado candidato pode exigir que ele vote numa sequência determinada de votos ou anule seus votos em cargos específicos com números previamente combinados. Numa eventual recontagem dos votos, haveria então um registro impresso que poderia ser verificado pelo atacante como sendo aquele combinado com o eleitor.

Para mitigar essa fragilização do anonimato do voto, seria necessário imprimir um registro individual para cada cargo votado pelo eleitor. Essa solução, porém, prejudica a usabilidade do sistema de votação, uma vez que aumenta significativamente o número de interações entre o eleitor e o equipamento. Outro problema é o aumento do volume de papel demandado para essa solução, uma vez que o formato apresentado a seguir precisaria ser mantido. Além dos custos envolvidos em sua própria aquisição, usar mais papel resulta em diversos custos indiretos associados ao aumento do tamanho da impressora, necessário para comportar uma bobina de papel maior.

Para que a implantação do voto impresso seja bem sucedida, é necessário que o eleitor vote com facilidade e que os custos da solução sejam equilibrados.

3. Formato do registro impresso do voto

O registro impresso do voto, naturalmente, deve conter as escolhas do eleitor para cada cargo em disputa. Adicionalmente, devem ser incluídas informações que permitam rastrear a origem desse documento, com dados sobre a urna eletrônica, a impressora utilizada, onde a urna foi utilizada (ou seja, em qual seção eleitoral ela foi instalada) e dados sobre a eleição.

O voto impresso também precisa conter uma marca bem legível sobre a confirmação da sua validade pelo eleitor. Em seguida, pode-se incluir um QR Code contendo todos os dados que já foram impressos, além de outros que podem ser usados para a assinatura digital, e a própria assinatura. Essa mesma assinatura pode ser impressa após o QR Code. Como será visto adiante, essa assinatura será grande demais, além de ser impressa num momento que se seguirá uma ejeção rápida do papel, o que inviabilizará qualquer tentativa de memorização pelo eleitor.

4. Assinatura do voto impresso

Sob o ponto de vista de segurança, o maior problema é quanto à fraude do voto impresso. O registro impresso deve ter as escolhas do eleitor, um QR Code e um campo de autenticação. Por ser sujeito a um processo de recontagem manual, alguma pessoa pode fraudar o processo fazendo uma inclusão, exclusão, troca ou alteração de algum voto impresso.

Para resolver as disputas, além da autenticação e do QR Code, pode-se usar outros meios adicionais, como o registro digital do voto — RDV gerado pela urna eletrônica e o caderno de votação para a conferência dos eleitores que foram votar na seção.

Especificamente, o procedimento de exclusão vai gerar disputas que só podem ser resolvidas com os meios adicionais (RDV e caderno de votação). Um juiz pode resolver usar o RDV, se o número de assinantes do caderno de votação confere com o de votos do RDV, e é superior ao de votos impressos, então o RDV pode ser usado para obter votos excluídos.

Um procedimento de alteração poderá ser resolvido através do QR Code e do campo de autenticação. Mas também pode-se usar os meios adicionais.

Uma troca consiste em uma exclusão e uma inclusão. Assim, para ser efetiva, é preciso fraudar uma inclusão, e isso será mostrado a seguir. Uma inclusão será evitada através do campo de autenticação. Para inserir um voto fraudado, é preciso criar um campo de autenticação correto.

O campo de autenticação será basicamente uma assinatura feita sobre as escolhas do eleitor, que ficará registrada no voto impresso e poderá ser lida, de forma automática, com o auxílio do QR Code.

Esse último procedimento de fraude será discutido a seguir, sob o aspecto de geração das assinaturas e sua autenticação.

(a)
(b)

TRE-AC Fase: SIMULADO
Pleito: 15100 - (07/10/2018)
Mun: 01392 Zona: 0001 Seção: 0008
UE: 01600559 MI: 12365400

Deputado Federal 91
LEGENDA

Deputado Estadual 92001

Senador 1ª vaga 999
NULO

Senador 2ª vaga 931

Governador BRANCO

Presidente 95


CONFIRMADO


ASSINATURA: 1DF7621B84CC2C8BDF119D901BF
A989A921FFF3CCEE892AD8C48B1B28167D235B
7F8C5F75966EF97891D1E19AA5A0AEB86558EF
31A2741F52CF8CE9A1D1E520A

TRE-AC Fase: SIMULADO
Pleito: 15100 - (07/10/2018)
Mun: 01392 Zona: 0001 Seção: 0008
UE: 01600559 MI: 12365400

Deputado Federal BRANCO

Deputado Estadual BRANCO

Senador 1ª vaga BRANCO

Senador 2ª vaga BRANCO

Governador BRANCO

Presidente BRANCO


CANCELADO

Figura 3. Exemplos de votos impressos. (a) confirmado pelo eleitor. É incluída uma marca gráfica indicando a confirmação do voto, seguida do QR Code e da assinatura digital. (b) cancelado pelo eleitor. Nesse caso o QR Code não precisa ser impresso e é incluída uma marca gráfica bem clara de que o voto foi cancelado. As linhas de separação, quando alinhadas à tela resumo, auxiliam na conferência do voto.

4.1. Dados a serem assinados e especificação da assinatura

O conjunto de dados contido no registro impresso do voto que devem ser assinados são:

1. identificadores da urna eletrônica ($IdUE = Nue \parallel ImpV \parallel RecV \parallel Corr$):
 - (a) número interno da urna eletrônica (Nue)
 - (b) identificação da impressora de votos ($ImpV$)
 - (c) identificação do receptáculo de votos ($RecV$)
 - (d) código de carga da urna ($Corr$)
2. identificadores da eleição ($IdEl = IdProc \parallel IdPl \parallel DtE$):
 - (a) processo eleitoral ($IdProc$)
 - (b) pleito ($IdPl$)
 - (c) data do pleito (DtE)
3. identificadores da seção eleitoral ($IdSe = UF \parallel Mun \parallel Zona \parallel Sec$):
 - (a) sigla da UF (UF)
 - (b) município (Mun)
 - (c) zona ($Zona$)
 - (d) seção (Sec)
4. identificador de cada cargo seguido do voto do eleitor
 ($Votos = (IdP, VotoP) \parallel (IdG, VotoG) \parallel (IdS_1, VotoS_1, IdS_2, VotoS_2) \parallel (IdD_F, VotoD_F) \parallel (IdD_E, VotoD_E) \parallel (IdC_n, VotoC_n) \parallel \dots$):
 - (a) Presidente ($IdP, VotoP$)
 - (b) Governador ($IdG, VotoG$)
 - (c) Senadores ($IdS_1, VotoS_1, IdS_2, VotoS_2$)
 - (d) Deputado Federal ($IdD_F, VotoD_F$)
 - (e) Deputado Estadual/Distrital ($IdD_E, VotoD_E$)
 - (f) Cargo N ($IdC_n, VotoC_n$)

Esses campos encontram paralelo naqueles já utilizados pelo TSE no QR Code do boletim de urna [TSE 2016b]. Com isso, não deve haver dificuldade para que a equipe do TSE implemente a proposta apresentada.

Nenhum dado aleatório será incluído na assinatura. A geração de uma assinatura sem aleatórios sobre esses dados implica em dizer que ao se repetir o mesmo voto, na mesma seção e mesma urna, será produzida a mesma assinatura. Essa propriedade é importante, pois decisão do Supremo Tribunal Federal — STF impede que seja associado um número único ao registro impresso do voto [STF 2014].

Assim, pode-se gerar a seguinte assinatura para um voto impresso usando um algoritmo assimétrico para assinatura $E_{pri}()$ com um par de chaves ($priVI, pubVI$):

$$hash_{VI} = SHA512(IdUE \parallel IdEl \parallel IdSe \parallel Votos) \quad (1)$$

$$Sig_{VI} = E_{priVI}(hash_{VI}) \quad (2)$$

A verificação da assinatura Sig_{VI} pode ser feita por qualquer pessoa que possua a chave $pubVI$, o voto e conheça o algoritmo de verificação $E_{pub}^{-1}()$.

Uma característica desse procedimento de assinatura é que ele não distingue criptograficamente um mesmo voto quando dado por pessoas diferentes. Mais uma vez, essa característica é necessária para atendimento a decisão STF. Dessa forma, é garantido o anonimato do voto: um registro impresso com votos que são únicos já é um registro único e associá-lo a uma assinatura única não altera a sua distinguibilidade; um registro impresso com os mesmos votos de outro, ao conter a mesma assinatura desse outro, não adiciona nenhum elemento que o torne distinguível de outro registro, o que preserva o seu anonimato.

Por outro lado, a indistinguibilidade de votos iguais dá espaço para ataques de inclusão de votos válidos replicados. Esse cenário pode ser minimizado com o reforço de proteção física sobre o receptáculo dos votos impressos e maior controle no processo de contagem dos votos. Outra possibilidade é criar uma associação direta entre RDV e registro impresso, fazendo com que os votos no RDV sejam agrupados da mesma forma que no registro impresso, incluindo a sua assinatura. Dessa forma, disputas ocasionadas por inclusões inválidas por replicação poderiam ser resolvidas considerando como válidos os votos contidos no RDV. Contudo, alterações no formato do RDV não serão tratadas neste trabalho.

Para se usar um padrão de assinatura que possa ser conferido por qualquer pessoa, de forma transparente, propõe-se o uso da assinatura EdDSA [Bernstein et al. 2012], baseada na *Curve25519*, que já tem sido utilizada pelo TSE [TSE 2016b, TSE 2016a].

A assinatura EdDSA não é da forma (r, s) , na qual r é um "aleatório" e s a assinatura. Com EdDSA é satisfeito o requisito de que na mesma seção e mesma urna, se produza a mesma assinatura para os mesmos dados, pois o valor r é gerado de forma determinística por meio de um hash. O valor r é gerado com base na chave privada e nos dados a serem assinados [Bernstein et al. 2012].

Assim, para gerar a assinatura do Voto Impresso (VI) usa-se o algoritmo $EdDSA_{pri}()$ com o par de chaves $(priVI, pubVI)$, e com o aleatório r gerado pelo próprio algoritmo. Então a urna executará as seguintes operações:

$$\begin{aligned} hash_{VI} &= SHA512(IdUE || IdEl || IdSe || Votos) \\ s &= EdDSA_{priVI}(hash_{VI}) \\ Sign_{VI} &= (r, s) \end{aligned} \quad (3)$$

A verificação da assinatura $Sign_{VI}$ pode ser feita por qualquer pessoa que possua a chave $pubVI$, os dados de D e conheça o algoritmo de verificação $EdDSA_{pub}^{-1}()$. O tamanho da assinatura é de 512 bits, que podem ser representados por 128 dígitos hexadecimais. Esse comprimento de assinatura pode ser impresso ao final do registro em papel do voto, pois é impraticável a sua memorização pelo eleitor.

O método é bem rápido e seguro, pelo uso do SHA512 e do EdDSA, e já foi usado anteriormente pelo TSE nos QR Codes dos boletins de urna [TSE 2016b, TSE 2016a].

5. Automação segura da apuração

Embora a Lei nº 13.165/2015 não tenha estipulado o que fazer com os registros impressos após a conclusão da votação, certamente era vontade do legislador que, em alguma escala, os votos impressos fossem contados e sua apuração confrontada com o resultado eletrônico, de modo a auditar as urnas eletrônicas. Sabidamente, processos manuais de contagem são propensos a erro. Por isso, a disponibilização de um mecanismo que propicie a automação da apuração dos votos impressos agregará segurança ao processo de auditoria das eleições.

A inclusão de um QR Code ao final do registro impresso do voto, contendo todos os campos que são assinados digitalmente, além da própria assinatura, permitirá o desenvolvimento de aplicativos que rapidamente digitalizem o voto impresso e verifiquem a sua assinatura. Aproveitando a experiência adquirida pelo TSE com o QR Code no boletim de urna, para o voto impresso pode ser adotado o mesmo formato já empregado no boletim, assim como a infraestrutura para publicação de chaves.

A seguir são apresentados os campos que devem estar codificados no QR Code (Tabela 5), assim como um exemplo de QR Code para o voto impresso (Figura 4).

Tabela 1. Tabela de campos do QR Code do voto impresso.

PROC:nnnnn	Número do processo eleitoral.
DTPL:aaaammdd	Data do pleito.
PLEI:nnnnn	Número do pleito.
TURN:n	Número do turno (1 – primeiro turno; 2 – segundo turno).
FASE:x	Fase dos dados (O – oficial; S – simulado; T – treinamento).
UNFE:xx	Sigla da UF.
MUNI:nnnnn	Número do município.
ZONA:nnnn	Número da zona eleitoral.
SECA:nnnn	Número da seção eleitoral.
IDUE:nnnn...	Número de série da urna.
IMIE:nnnn...	Número de série da impressora de votos.
IRVI:nnnn...	Número de série do receptáculo de votos.
IDCA:nnnn...	Código de identificação da carga (24 dígitos).
cc:vvvvv	Código do cargo (cc) seguido do voto (vvvvv).
HASH:xxxxxx...	$hash_{VI}$ codificado em hexadecimal.
ASSI:xxxxxx...	$Sign_{VI}$ codificada em hexadecimal.



Figura 4. Exemplo de QR Code para o voto impresso.

6. Conclusões

O voto impresso é uma necessidade para as Eleições 2018 imposta por lei. A sua introdução traz desafios de usabilidade e segurança ao processo eleitoral brasileiro. A adição de uma tela resumo para conferência dos registros eletrônico e impresso certamente promoverá uma experiência mais adequada para o eleitor, se comparado às Eleições 2002 quando esse mecanismo não existia. A inclusão de uma assinatura digital baseada em EdDSA agrega um forte mecanismo de autenticação, ao mesmo tempo que preserva o anonimato do voto. Finalmente, a adição de um QR Code ao registro impresso viabilizará a construção de aplicativos que automatizem a apuração dos votos numa eventual auditoria das eleições. As principais propostas apresentadas devem ser implementadas sem grande dificuldade pelo TSE, uma vez que se baseiam em tecnologias já experimentadas no boletim de urna.

Futuramente, após a implantação da proposta apresentada, é necessário avaliar eventuais melhorias de usabilidade e de segurança que podem ser agregadas ao registro impresso do voto.

Referências

- Bernstein, D. J., Duif, N., Lange, T., Schwabe, P., and Yang, B.-Y. (2012). High-speed high-security signatures. *Journal of Cryptographic Engineering*, pages 1–13.
- EAC (2015). Voluntary voting system guidelines. <https://www.eac.gov/assets/1/28/VVSG.1.1.VOL.1.FINAL1.pdf>. United States Election Assistance Commission.

Presidência da República (2015). Lei nº 13.165 de 2015. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113165.htm. Altera as Leis nº 9.504, de 30 de setembro de 1997, nº 9.096, de 19 de setembro de 1995, e nº 4.737, de 15 de julho de 1965 - Código Eleitoral, para reduzir os custos das campanhas eleitorais, simplificar a administração dos Partidos Políticos e incentivar a participação feminina.

STF (2014). ADI 4543 — ação direta de inconstitucionalidade. <http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?numero=4543&classe=ADI&origem=AP&recurso=0&tipoJulgamento=M>. Relatora: Min. Cármen Lúcia.

TSE (2016a). QR Code no boletim de urna: instruções adicionais para a verificação de assinatura digital e exemplos de código. <http://www.justicaeleitoral.jus.br/arquivos/tse-qr-code-no-boletim-de-urna-verificacao-assinatura-digital>.

TSE (2016b). QR Code no boletim de urna: manual para criação de aplicativos de leitura. <http://www.justicaeleitoral.jus.br/arquivos/tse-manual-para-a-criacao-de-aplicativos-de-leitura>.