WPv2

A proposta do GRITA! sobre o VOTO DIGITAL CERTIFICADO repercutiu nos três poderes da República, e alguns dos conceitos já valem para 2022. Apresentamos agora, a Versão 2 de nosso White Paper, onde propomos melhorias ainda mais relevantes, para futuras atualizações do processo eleitoral brasileiro

VOTO DIGITAL CERTIFICADO

Ferramenta para evolução do processo de votação no Brasil

Brasil, 23 de setembro de 2021

GRITA! TT VOTO DIGITAL

PROPOSTA DE MELHORIAS NO

SISTEMA DE GESTÃO DE SEGURANÇA DO PROCESSO DE VOTAÇÃO USANDO AS URNAS ELETRÔNICAS

SUMÁRIO

Observamos uma discussão permanente, com picos recorrentes a cada dois anos, no que diz respeito à segurança e a confiabilidade do processo eleitoral brasileiro, que terá um importante marco em outubro de 2022, com a realização de eleições gerais.

Em 2021, o debate em torno da Proposta de Emenda Constitucional (PEC) 135/2019, fez com que a temperatura do debate atingisse a níveis jamais vistos, com frequência fugindo da essência: **afinal, o voto de cada eleitor será fiel e corretamente registrado pelas máquinas de votação? E, ao final do processo, esse voto, junto com todos os outros, estarão perfeitamente totalizados, permitindo uma proclamação dos eleitos de forma a refletir perfeitamente a expressão dos eleitores?**

O GRITA! vem estudando o assunto desde antes das eleições municipais de 2020, quando contou com o inestimável apoio do Tribunal Regional Eleitoral do Paraná (TRE-PR), visando oferecer uma contribuição cidadã à nação brasileira.

Para isso, o GRITA! criou seu primeiro 'think-tank', composto por engenheiros com bastante experiência em sistemas de votação, segurança de dados, sistemas críticos de alta complexidade e exigências. Esse 'think-tank' desenvolveu uma proposta de melhoria das urnas eletrônicas, com viabilidade técnica e econômica para implantação já nas eleições gerais de 2022.

O primeiro White Paper foi publicado em 21/02/2021 e pode ser acessado aqui.

Em paralelo, o GRITA! apresentou a proposta a outros Tribunais Regionais Eleitorais e ao Tribunal Superior Eleitoral (TSE) em duas oportunidades, em fevereiro e em junho de 2021, assim como a parlamentares que compuseram a Comissão Especial da PEC 135/2021 e ao Poder Executivo, através do Ministério da Ciência, Tecnologia e Inovações.

Também interagimos com diversas entidades governamentais e da sociedade civil tais como fabricantes de equipamento, empresas de software, especialistas em processos de votação e segurança digital, quando chegou-se à conclusão de que, apesar da robustez já existente nos equipamentos e sistemas de gestão, ainda há espaço para melhorias nos processos, em especial no que diz respeito à assinatura digital conforme previsto na legislação eleitoral (Lei nº 9.504/1997):

> *"Art. 59 .....*
>
> *§ 4º A urna eletrônica disporá de recursos que, mediante **assinatura digital**, permitam o registro digital **de cada voto** e a identificação da urna em que foi registrado, resguardado o anonimato do eleitor.*

1. PREMISSAS

- O sistema eletrônico de votação atual ainda é robusto, embora com projeto base de 1995;
- Para termos a percepção de segurança e confiabilidade do processo, é recomendável a implementação prática do Princípio da Segregação de Funções conforme recomendado pela norma internacional ISO/IEC 27001;
- Como qualquer sistema baseado em tecnologia digital, que evolui continuamente, suas funcionalidades e procedimentos devem ser permanentemente melhorados, de forma a aumentar cada vez mais a robustez do sistema de votação eletrônico;
- A contagem pública dos votos melhora a confiança de eleitores e candidatos.

2. PADRÕES NACIONAIS. E INTERNACIONAIS DE SEGURANÇA DE DADOS

2.1. GESTÃO – AUDITORIA DA INTEGRIDADE DO SISTEMA DE GESTÃO DE SEGURANCA DA INFORMAÇÃO

2.1.1. A Norma ISO/IEC 27001[1]

ISO/IEC 27001 é um padrão (norma) internacional sobre como gerenciar a segurança da informação. A norma foi originalmente publicada em conjunto pela International Organization for Standardization (ISO) e pela International Electrotechnical Commission (IEC) em 2005 e depois revisada em 2013. Mais recentemente, foi adotada como norma europeia (EN) pelo CEN/CENELEC em 2017.

Deve-se salientar que a norma ABNT NBR ISO/IEC 27001:2013 é idêntica ao padrão internacional ISO/IEC 27001:2013[2]

O padrão (norma) ISO/IEC 27001 á reconhecido e aceito mundialmente como um conjunto de melhores práticas que devem ser implementadas por organizações onde a segurança das informações seja essencial.

O objetivo da norma é ajudar as organizações a tornar mais seguros os ativos de informação que possuem. As organizações que atendem aos requisitos do padrão podem e devem ser certificadas por um organismo (entidade) independente credenciado a nível nacional, após a conclusão bem-sucedida de uma auditoria.

Muitas organizações possuem vários controles de segurança da informação. No entanto, sem um sistema de gestão de segurança da informação (SGSI), esses controles tendem a ser um tanto desorganizados e desconexos, tendo sido implementados como soluções pontuais para cobrir situações específicas ou simplesmente por uma questão de necessidade operacional.

[1] No Brasil, Norma ABNT NBR ISO/IEC 27001:2013

[2] https://www.abntcatalogo.com.br/norma.aspx?ID=306580

A norma ISO/IEC 27001 especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gerenciamento de segurança da informação (SGSI) no contexto de uma organização.

A norma também inclui requisitos para a avaliação e tratamento dos riscos de segurança da informação. Esses requisitos são genéricos e devem ser aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza da organização. A exclusão de qualquer um dos requisitos especificados nas Cláusulas 4 a 10 da norma não é aceitável quando a organização reivindica conformidade (através de certificação independente) com esta norma.

A norma ISO/IEC 27001 requer que a gerência da organização:

• Examine sistematicamente os riscos de segurança da informação da organização, levando em consideração as ameaças, vulnerabilidades e impactos.

• Projete e implemente um conjunto coerente e abrangente de controles de segurança da informação e/ou outras formas de tratamento de risco (como prevenção ou transferência de risco) para lidar com os riscos considerados inaceitáveis.

• Adote um processo de gestão abrangente para garantir que os controles de segurança da informação continuem atendendo às necessidades de segurança da informação da organização de forma contínua ao longo do tempo.

A certificação ISO/IEC 27001, como outras certificações de sistema de gestão ISO, geralmente envolve um processo de auditoria externa de três estágios como definido pelas normas ISO/IEC 17021[3] e ISO/IEC 27006[4]:

• **Estágio 1** é uma revisão preliminar e informal do SGSI, por exemplo, para verificar a existência e integridade da documentação principal, como a política de segurança da informação da organização, Declaração de Aplicabilidade e Plano de Tratamento de Risco. Esta etapa serve para familiarizar os auditores com a organização e vice-versa.

• **Estágio 2** é uma auditoria de conformidade mais detalhada e formal, testando independentemente o SGSI em relação aos requisitos especificados na norma ISO/IEC 27001. Os auditores buscarão evidências para confirmar se o sistema de gestão foi adequadamente projetado e implementado e está de fato em operação (por exemplo, confirmando que um comitê de segurança ou órgão de administração semelhante se reúne regularmente para supervisionar o SGSI). A aprovação desse estágio resulta no SGSI sendo certificado em conformidade com a ISO/IEC 27001.

• **Estágio contínuo** envolve revisões de acompanhamento ou auditorias para confirmar que a organização permanece em conformidade com a norma ao longo do

[3] ISO/IEC 17021-1:2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements
[4] ISO/IEC 27006:2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

tempo. A manutenção da certificação requer auditorias de reavaliação periódicas para confirmar que o SGSI continua a operar conforme especificado. Isso deve acontecer pelo menos uma vez por ano.

2.1.2. Estrutura da norma ISO/IEC 27001

A ISO/IEC 27001 contém dez cláusulas e um anexo, que cobrem:

1. Escopo do padrão
2. Referências normativas
3. Termos e definições
4. Contexto da organização
5. Liderança (a gerência deve demonstrar liderança e compromisso com relação ao sistema de gestão de segurança da informação)
6. Planejamento de um sistema de gestão de segurança da informação; avaliação de risco; tratamento de risco
7. Apoio a um sistema de gestão de segurança da informação
8. Operações (tornando operacional um sistema de gestão de segurança da informação)
9. Avaliação de desempenho (revisão do desempenho do sistema)
10. Melhoria (ação corretiva)

Anexo A (normativo): objetivos e controles de referência

A cláusula 6 é bastante importante, especialmente no que se relaciona à avaliação de risco e tratamento dos riscos. Salientamos abaixo duas seções dessa cláusula que são muito importantes em termos de avaliação e tratamento de riscos que se aplicam diretamente a uma organização:

<u>Seção 6.1.2 Avaliação de risco de segurança da informação</u>

A organização deve definir e aplicar um processo de avaliação de risco de segurança da informação que:

a) estabelece e mantém critérios de risco de segurança da informação que incluem: 1) os critérios de aceitação de risco; e 2) critérios para realizar avaliações de risco de segurança da informação;
b) garante que as avaliações repetidas de riscos à segurança da informação produzam resultados consistentes, válidos e comparáveis;
c) identifica os riscos de segurança da informação: 1) aplicar o processo de avaliação de riscos de segurança da informação para identificar os riscos associados à perda de confidencialidade, integridade e disponibilidade de informações no escopo do sistema de gestão de segurança da informação; e 2) identificar os proprietários (owners) do risco;
d) analisa os riscos de segurança da informação: 1) avaliar as consequências potenciais que resultariam da materialização dos riscos identificados em 6.1.2 c) 1); 2) avaliar a

probabilidade realista de ocorrência dos riscos identificados em 6.1.2 c) 1); e 3) determinar os níveis de risco;
e) avalia os riscos de segurança da informação: 1) comparar os resultados da análise de risco com os critérios de risco estabelecidos em 6.1.2 a); e 2) priorizar os riscos analisados para o tratamento dos riscos.

Seção 6.1.3 Tratamento de risco de segurança da informação

A organização deve definir e aplicar um processo de tratamento de risco de segurança da informação para: a) selecionar opções de tratamento de risco de segurança da informação apropriadas, levando em consideração os resultados da avaliação de risco;
b) determinar todos os controles que são necessários para implementar as opções de tratamento de risco de segurança da informação escolhidas;
c) comparar os controles determinados em 6.1.3 b) acima com aqueles no Anexo A e verificar se nenhum controle necessário foi omitido;
d) produzir uma Declaração de Aplicabilidade que contenha os controles necessários [ver 6.1.3 b) e c)] e a justificativa para as inclusões, implementadas ou não, e a justificativa para as exclusões dos controles do Anexo A;
e) formular um plano de tratamento de riscos de segurança da informação;
f) obter a aprovação dos proprietários (*owners*) do risco do plano de tratamento de risco de segurança da informação e aceitação dos riscos residuais de segurança da informação.

Alguns controles extraídos do Anexo A aplicáveis diretamente a uma organização:

A.6.1 Organização Interna, com o objetivo de estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização, especialmente

- A.6.1.2 Controle de segregação de funções: "*deveres e áreas de responsabilidade conflitantes devem ser segregados para reduzir as oportunidades de modificação não autorizada ou não intencional ou uso indevido dos ativos da organização*"

Alguns outros controles extraídos do Anexo A aplicáveis ao SGSI:
Existem 114 controles descritos no Anexo A da norma ISO/IEC 27001. Alguns controles fundamentais para o sistema de gestão de segurança da informação (SGSI) são:

A.9.4 Controle de acesso do sistema e dos aplicativos, com o objetivo de prevenir o acesso não autorizado a sistemas e aplicativos, especialmente

- A.9.4.2 Controle de procedimentos de logon seguro: "*quando exigido pela política de controle de acesso, o acesso aos sistemas e aplicativos deve ser controlado por um procedimento de logon seguro*".
- A.9.4.3 Controle do sistema de gerenciamento de senha: "*os sistemas de gerenciamento de senhas devem ser interativos e garantir senhas de qualidade*".

- A.9.4.4 Controle do uso de programas utilitários privilegiados: "*o uso de programas utilitários que podem ser capazes de substituir os controles do sistema e dos aplicativos deve ser restrito e rigidamente controlado*".
- A.9.4.5 Controle de acesso ao código-fonte do programa: "*o acesso ao código-fonte do programa deve ser restrito*".

A.12.1 Procedimentos operacionais e responsabilidades, especialmente

- A.12.1.4 Separação de desenvolvimento, teste e ambientes operacionais: os ambientes de desenvolvimento, teste e operacional devem ser separados para reduzir os riscos de acesso não autorizado ou alterações no ambiente operacional.

A.12.4 Registro e monitoramento

- A.12.4.1 Controle de registro de eventos: os registros de eventos que registram as atividades do usuário, exceções, falhas e eventos de segurança da informação devem ser produzidos, mantidos e revisados regularmente.
- A.12.4.2 Controle de proteção de informações de registro: as instalações de registro e as informações de registro devem ser protegidas contra adulteração e acesso não autorizado.

A.13.1 Gerenciamento de segurança de rede, com o objetivo de garantir a proteção da informação nas redes e nos seus meios de suporte ao processamento de informação.

- A.13.1.2 Controle de segurança de serviços de rede: os mecanismos de segurança, níveis de serviço (SLA - Service Level Agreements) e requisitos de gestão de todos os serviços de rede devem ser identificados e incluídos nos contratos de serviços de rede, sejam esses serviços prestados internamente ou externamente.
- A.13.1.3 Segregação no controle de redes: grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes.

A.14.2 Segurança nos processos de desenvolvimento e suporte, com o objetivo de garantir que a segurança da informação seja projetada e implementada no contexto do ciclo de vida de desenvolvimento dos sistemas de informação.

- A.14.2.1 Controle de política de desenvolvimento seguro: as regras para o desenvolvimento de software e sistemas devem ser estabelecidas e aplicadas aos desenvolvimentos dentro da organização (por exemplo: incluir uma certificação prévia independente pelo INMETRO dos equipamentos utilizados no sistema eleitoral).

A.16.1 Gestão de incidentes e melhorias de segurança da informação, com o objetivo de garantir uma abordagem consistente e eficaz para o gerenciamento de incidentes de segurança da informação, incluindo a comunicação sobre eventos de segurança e pontos fracos.

- A.16.1.5 Resposta aos incidentes de segurança da informação: os incidentes de segurança da informação devem ser respondidos de acordo com procedimentos documentados.

A.18.1 Conformidade com os requisitos legais e contratuais, com o objetivo de evitar violações de obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.

- A.18.1.3 Controle de proteção de registros: os registros devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos legislativos, regulamentares, contratuais e comerciais.

3. RECOMENDAÇÕES

No caso do sistema eleitoral brasileiro, pode-se concluir, tendo em vista as cláusulas mencionadas acima que o **TSE, como organização responsável por sua implementação e gestão não poderia receber um certificado de conformidade** (*compliance*) com ISO/IEC 27001 em relação aos quesitos:

1) auditoria da organização
2) auditoria do sistema de gestão da segurança de informação

Deixamos como sugestão que o TSE inicie o mais rápido possível um processo de auditoria externa independente, tendo como objetivo obter um certificado de conformidade (*compliance)* à norma ISO/IEC 27001.

Uma auditoria externa do TSE como organização e do seu sistema de gestão de segurança da informação (SGSI) feita por uma entidade independente e credenciada a nível nacional ou internacional aumentaria a confiança dos cidadãos no processo eleitoral brasileiro além de incentivar melhorias significativas em seu SGSI.

3.1. COMO RESOLVER A CONTAGEM PÚBLICA DOS VOTOS

A solução concebida por engenheiros formados no ITA através da Associação GRITA! resolve a questão da não conformidade da Administração Eleitoral com a norma internacional ISO/IEC 27001 aplicável a organizações e sistemas de gestão da segurança de informação e atende aos requisitos apresentados por quem defende o voto auditável: transparência, verificação do voto pelo eleitor, contagem pública na seção eleitoral com a fiscalização dos partidos, e recontagem, após a votação, no caso de auditorias independentes.

A solução é criar, para cada voto, um documento eletrônico com validade jurídica certificado pela ICP-Brasil, utilizando um certificado digital armazenado em um token criptográfico conectado na urna eletrônica. Em seguida, o voto é gravado em uma nova memória de resultados, com tecnologia de última geração para proteger o voto contra

apagamento ou alteração. O sigilo do voto do eleitor fica garantido, com a gravação do documento na memória, de modo aleatório, sem dados do eleitor e sem informação temporal.

O documento eletrônico criado para cada voto deve substituir o atual arquivo RDV (Registro Digital dos Votos), que reúne todos os votos em um único arquivo na urna eletrônica. O atual RDV não dá ao voto a certificação legal da ICP-Brasil e não protege os votos contra alterações ou apagamento, em caso de quebra de segurança, porque o arquivo fica aberto durante todo o tempo de votação, enquanto recebe novos votos.

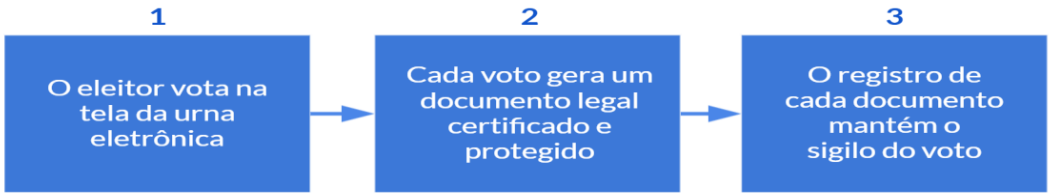
Para a verificação e a confirmação pelo eleitor, o novo documento eletrônico do voto será exibido ao eleitor, na tela da urna eletrônica. Auditorias independentes farão a recontagem dos documentos eletrônicos dos votos, após a eleição, em cada TRE.

A totalização dos votos deve ser descentralizada e realizada em cada Tribunal Regional Eleitoral, com as respectivas auditorias independentes, para confirmar a integridade do sistema e a assertividade dos resultados.

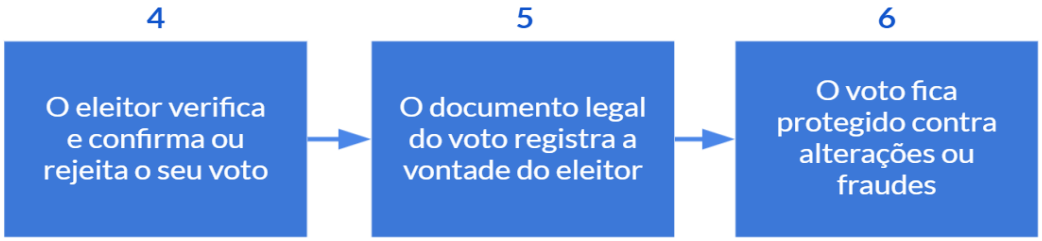
A autenticidade legal do documento eletrônico do voto será sempre garantida pela certificação digital da ICP-Brasil, de acordo com a legislação vigente.

4. Nove passos para o voto auditável certificado pela ICP-Brasil

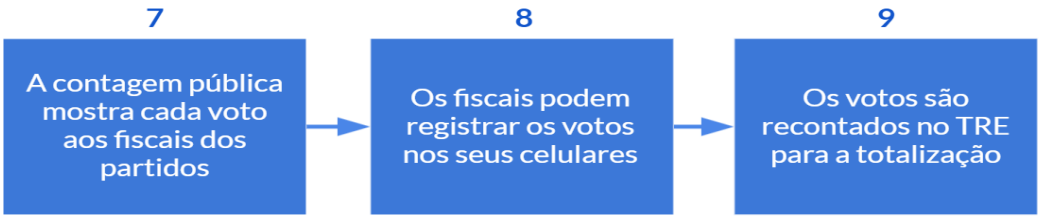
Cada voto é gravado individual e indelevelmente em um documento eletrônico com a validade jurídica da ICP-Brasil:



Cada documento eletrônico do voto exibido na tela da urna para a confirmação pelo eleitor:



A exibição da contagem pública dos votos poderá ser realizada na seção eleitoral ou na zona (comarca) eleitoral com a exibição de cada documento eletrônico do voto na tela da urna, que pode, opcionalmente também ser exibida, de modo simultâneo, em uma tela grande[5].



[5] Esse processo poderá atender a demanda existente de demonstrar aos eleitores, fiscais de partidos, candidatos e demais interessados, que os registros de voto estão adequadamente feitos de forma confiável.

4.1. Auditorias regulares e independentes realizadas após a eleição

- Os votos são recontados, em modelo estatístico definido previamente, para confirmar a assertividade do sistema
- Um sistema de monitoramento de integridade de arquivos e programas, realizada de modo independente por organizações externas credenciadas para tal, de modo independente do TSE, deve ser implantado no sistema de votação por urna eletrônica como parte integrante do processo eleitoral. Deve ser incluído no teste de conformidade da norma ISO/IEC 27001
- Auditoria da integridade física e lógica das urnas eletrônicas, realizada de forma independente após a eleição.

O GRITA! oferece a solução em conformidade com a norma internacional ISO/IEC 27001.

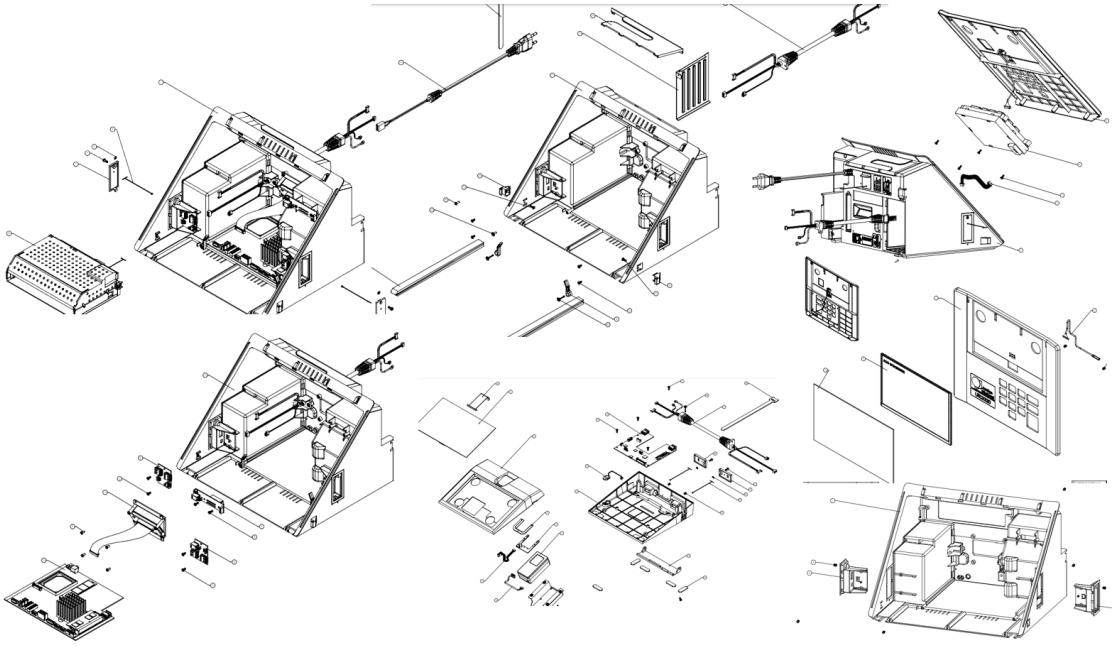
4.2. Requisitos do voto Auditável

- Cada voto é gravado digitalmente em um documento com total aderência legal, com a certificação da ICP-Brasil
- O eleitor verifica e confirma o seu voto na tela da urna eletrônica
- O voto é armazenado em uma memória permanente, que não permite apagamento ou alteração, que deve substituir a atual Memória de Resultados, hoje feita em um 'pendrive' comum.
- A contagem pública na seção eleitoral poderá ser realizada automaticamente, com cada voto exibido em uma grande tela, para permitir a fiscalização, pelos partidos, e o registro de cada voto nos celulares dos fiscais.
- Recontagem pública em cada TRE, com auditorias externas independentes

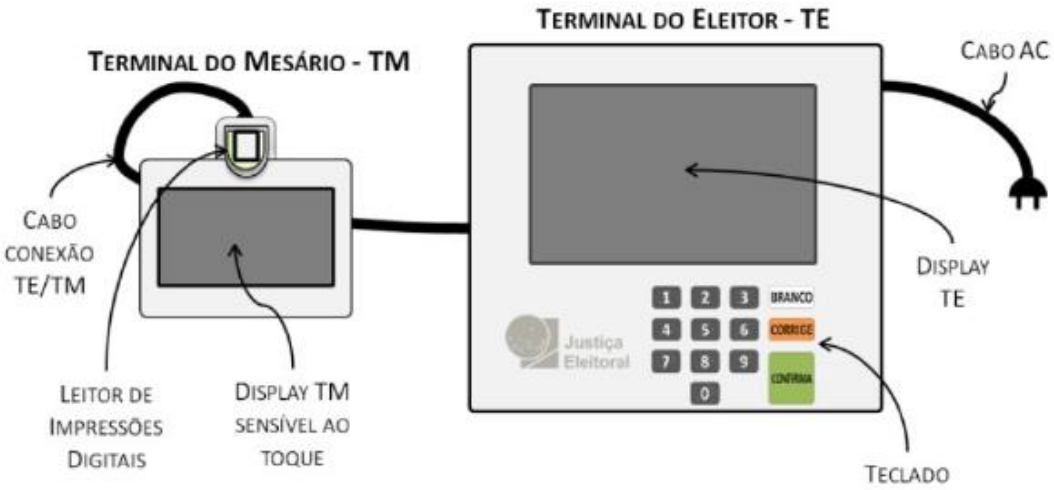
Aproveitamento das urnas eletrônicas atuais é viável em um curto período, a um custo expressivamente menor do que, por exemplo, o registro da imagem do voto através de sua impressão em papel.

5. A URNA ELETRÔNICA ATUAL E SUAS MELHORIAS

A urna eletrônica é um microcomputador de uso específico para eleições, com as seguintes características: resistente, de pequenas dimensões, leve, com autonomia de energia e com recursos de segurança.



Dois terminais compõem a urna eletrônica: o terminal do mesário, onde o eleitor é identificado e autorizado a votar (em alguns modelos de urna, onde é verificada a sua identidade por meio da biometria), e o terminal do eleitor, onde é registrado digitalmente o voto.



Ressalta-se que conforme informações levantadas, o parque de urnas é renovado parcialmente a cada 2 anos. Entretanto, no último ciclo eleitoral (municipal), isso não ocorreu, desta maneira, o parque está em processo de renovação em uma escala bem maior neste ciclo referente a eleição de 2022, conforme segue:

QUANTIDADE DE URNAS ATUAIS E VOLUME A SER MANUFATURADO ADICIONAL ATÉ AGO 2022

Parque atual do TSE:	**1ª Licitação**: Empresa Positivo Tecnologia Paraná	**2ª Licitação**: Em andamento
≈ de **500 mil** urnas	180 mil +25% = **225 mil** urnas	176 mil + 25% = **225 mil** urnas
	Prazo: agosto /2022	**Prazo:** agosto /2022
		Atualmente restrito a disponibilidade de componentes.

Após o encerramento da votação, o resultado de cada urna é gravado na Mídia de Resultado, equipamento conectada atrás da urna, conforme ilustração a seguir:

Desta maneira, os seguintes arquivos são gravados na mídia de Resultado:

a) Boletim de urna;

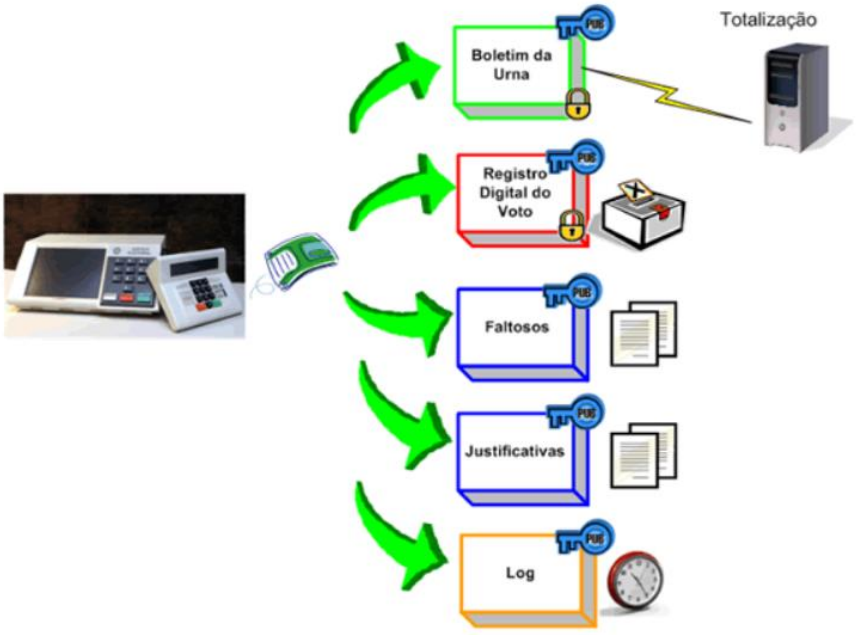
b) Registro digital de cada voto, que deve ser individualmente assinado;

c) Eleitores faltosos;

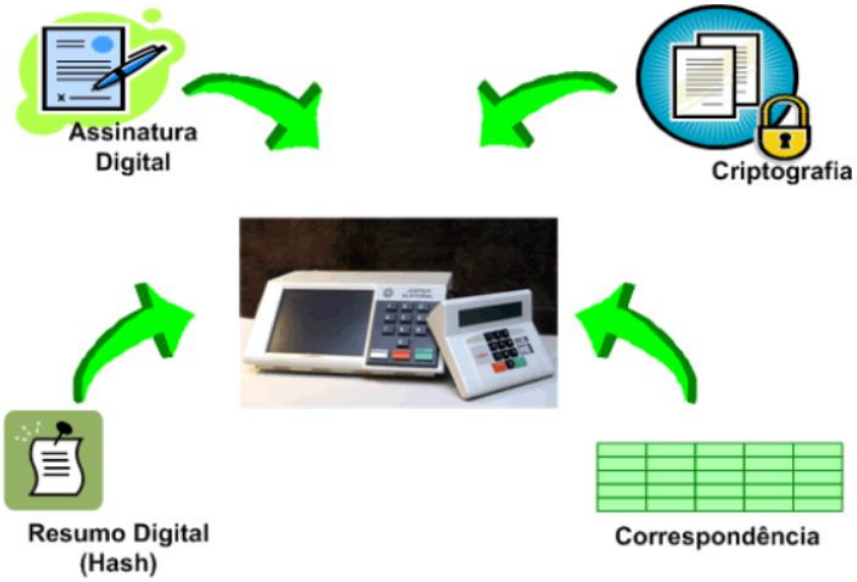
d) Justificativas eleitorais;

e) Registro de eventos (Log).

Todos os arquivos são assinados digitalmente. O Boletim de urna e o registro digital do voto, além de assinados, são criptografados.



6. SEGURANÇA DO PROCESSO:



O processo eletrônico de votação possui mecanismos imprescindíveis para assegurar sua segurança: a assinatura digital e o resumo digital.

A **assinatura digital** é uma técnica criptográfica usada para garantir que um conteúdo, no caso um arquivo digital, possa ser verificado principalmente no que se refere à sua integridade, isto é, busca garantir que o software e os arquivos da urna não foram modificados de forma intencional ou não perdeu suas características originais por falha na gravação ou leitura. Isso significa que se a assinatura digital for válida, o arquivo não foi modificado.

A assinatura digital também é utilizada para assegurar a autenticidade do software e dos arquivos digitais gerados durante o processo e votação, ou seja, confirmar que seu conteúdo tem origem oficial e foi gerado pelo Tribunal Superior Eleitoral. Nesse caso, somente quem assinou digitalmente pode ter gerado aquela assinatura digital.

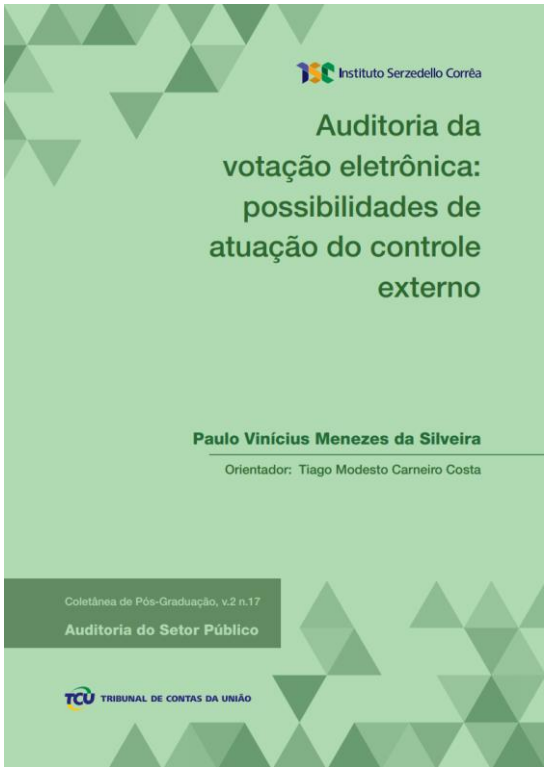
Já o **resumo digital**, também chamado de resumo criptográfico ou *hash*, é uma técnica criptográfica que se assemelha a um dígito verificador. Dado um arquivo digital, pode-se calcular o resumo digital desse arquivo com um algoritmo público. No caso dos sistemas de urna, são calculados os *hash* de todos os arquivos e esses resumos são publicados no portal do TSE.

A **criptografia digital** é um mecanismo de segurança para o funcionamento dos softwares e dos arquivos digitais gerados durante o processo e votação.

Além da criptografia, existe a decriptografia, que é o processo pelo qual são recuperados os dados previamente criptografados, isto é, eles são desembaralhados. É um mecanismo de segurança para o funcionamento do software e dos arquivos digitais gerados durante o processo e votação.

Vale reforçar que a preocupação sobre a segurança e transparência do processo eleitoral é também presente nos trabalhos e publicações de especialistas oriundos de órgãos públicos de controle, como o Tribunal de Contas da União.

O documento abaixo referenciado descreve, de maneira técnica e com um excelente didatismo, os pontos mais importantes que merecem revisão no processo de votação em uso no Brasil. Todavia, o autor não ofereceu um referencial de como se fazer uma auditoria externa independente.



7. A PROPOSTA

- Considerando que melhorias em qualquer processo ou produto são sempre possíveis e sempre desejáveis;
- Considerando que no caso do processo eleitoral, aspectos de segurança são primordiais, não só para manutenção da democracia, mas também pensando nos próprios atores envolvidos no processo, que precisam se resguardar contra qualquer possibilidade de adulteração nos resultados do processo eleitoral;
- Considerando também o princípio da **segregação de funções**, parte importante da norma 27001, que basicamente diz que um mesmo órgão não deve ser responsável por todas as etapas de um determinado processo, tais como: planejar, executar, monitorar, certificar, fiscalizar etc.;

Propõe-se que a etapa de certificação digital do hardware e a homologação do software do processo de votação, hoje sob responsabilidade do TSE, seja atribuída à estrutura da **ICP-Brasil**, que é a **Infraestrutura de Chaves Públicas Brasileira**.

A melhor maneira de termos a garantia do processo, dentro das melhores práticas, normas e tecnologias disponíveis atualmente é assegurando que a fabricação das urnas e todo o software desenvolvido sejam certificados/homologados de forma independente antes da realização do processo de votação, e devidamente lacrados. a. A certificação do hardware e a homologação do sistema deve ser feita -antes do evento- por uma autoridade certificadora dentro do ecossistema da ICP Brasil, por exemplo o Inmetro.

O desenvolvimento e manutenção do software e a execução do sistema estaria sob responsabilidade do TSE, como sempre o foi, desde que obedecidos os critérios da ISO/IEC 27001.

A auditoria dos sistemas seria feita por amostragem, via verificação das assinaturas digitais dos conteúdos das urnas em ambiente de auditoria e perícias. Também, recomendamos a análise forense computacional de número reduzido de equipamentos via amostragem, em busca de traços de execução anômalos, a fim de se detectar atividades não previstas que não foram detectadas pela fase de certificação.

As duas auditorias (assinaturas digitais em massa e análise forense computacional) podem ser feitas por equipes que participaram da homologação, mas necessariamente devem incluir equipes independentes que sejam especialistas em análise forense.

Essa estrutura satisfaz, dentro da capacidade das equipes de homologação e auditoria, a garantia de que a urna não minta entre a coleta e a totalização.

É possível ter a assinatura confiável de documentos por certificado via software (e hardware), mas internos. Basta que o certificado seja armazenado no HSM de todas as urnas (atualmente), e que o software de assinatura rode sob verificação e garantia do certificado armazenado no HSM.

Seguindo essas orientações do GRITA!, é possível fazer uma segura e crível demonstração, com amplo apoio da mídia, de transparência e exatidão ao eleitor, este o principal ator desse processo democrático.

8. PRÓXIMOS PASSOS: PREPARANDO O CAMINHO PARA AS ELEIÇÕES DO FUTURO

Em 15/11/2020, o TSE recebeu 26 demonstrações de empresas dos ramos de tecnologia da informação, telecomunicações e entretenimento sobre possíveis aplicações de novas tecnologias para permitir o uso de dispositivos digitais, como o celular, em processos de votação, no contexto do projeto Eleições do Futuro 2020.

Com apresentações nas cidades de São Paulo, Curitiba e Valparaiso de Goiás, todas em locais de votação, as mostras serviram para expor as possíveis rotas da evolução do processo de votação, assim como testar a reação dos eleitores.

Embora não se vislumbre a adoção de nenhuma dessas tecnologias já nas eleições gerais de 2022, o projeto do TSE serviu para despertar o interesse de possíveis fornecedores para o futuro, assim como para tornar mais aberto o debate sobre os melhores caminhos a seguir para, cada vez mais, conseguir mostrar de forma transparente como elegeremos nossos representantes de maneira cada vez mais segura e eficiente.

A proposta do GRITA! permite um importante avanço estrutural, que tem as seguintes vantagens:

a) Utiliza as atuais urnas eletrônicas, com a agregação de procedimentos de certificação e auditoria dentro dos mais modernos requisitos de segurança e de verificação da integridade e da segurança do voto de cada eleitor;
b) Aumenta consideravelmente o nível de confiança do eleitor no processo de votação;
c) Facilita uma suave transição para o futuro Voto Digital
d) Não requer investimentos da Justiça Eleitoral na concepção do modelo, que já existe, e, uma vez proposto pelo GRITA! em fevereiro de 2021, evoluiu desde então, com melhorias criadas dentro da Associação e com sugestões propostas por várias organizações da sociedade.
e) Como deixamos claro desde o início dos trabalhos do Think Tank Voto Digital, ainda em 2020, com amplo apoio de nossos associados, esse projeto pertence, por doação do GRITA!, à Nação Brasileira.