Tribunal Superior Eleitoral

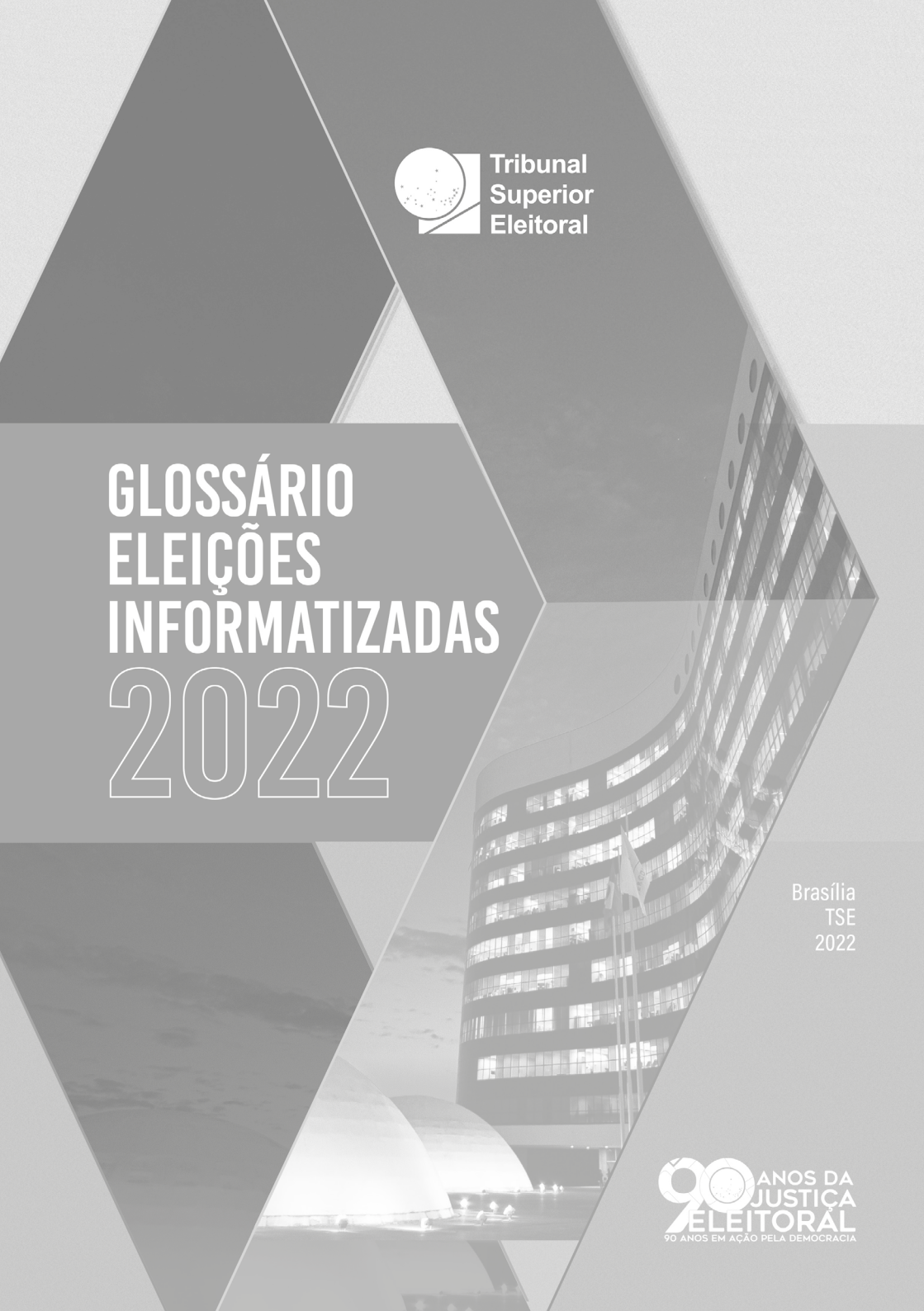
GLOSSÁRIO ELEIÇÕES INFORMATIZADAS 2022

Brasília
TSE
2022

90 ANOS DA JUSTIÇA ELEITORAL
90 ANOS EM AÇÃO PELA DEMOCRACIA

Tribunal Superior Eleitoral

GLOSSÁRIO ELEIÇÕES INFORMATIZADAS 2022



Brasília
TSE
2022

90 ANOS DA JUSTIÇA ELEITORAL
90 ANOS EM AÇÃO PELA DEMOCRACIA

Secretaria de Gestão da Informação e do Conhecimento
SAFS, Quadra 7, Lotes 1/2, 1º andar
Brasília/DF – 70070-600
Telefone: (61) 3030-9225

Secretária-Geral da Presidência
Christine Oliveira Peter da Silva

Diretor-Geral da Secretaria do Tribunal
Rui Moreira de Oliveira

Secretário de Gestão da Informação e do Conhecimento
Cleber Schumann

Coordenador de Editoração e Publicações
Washington Luiz de Oliveira

TRIBUNAL SUPERIOR ELEITORAL

Presidente
Ministro Edson Fachin

Vice-Presidente
Ministro Alexandre de Moraes

Ministros
Ministro Ricardo Lewandowski
Ministro Mauro Campbell Marques
Ministro Benedito Gonçalves
Ministro Sérgio Banhos
Ministro Carlos Bastide Horbach

Procurador-Geral Eleitoral
Augusto Aras

SUMÁRIO


TSE

ASSINATURA DIGITAL

A assinatura digital é uma tecnologia utilizada para autenticar de forma segura e íntegra os documentos eletrônicos. Ela utiliza as chaves criptográficas, ou seja, um protocolo que impede terceiros, ou pessoas não autorizadas, de reproduzirem a assinatura de uma outra pessoa ou sistema. Como somente o signatário (pessoa ou sistema) tem acesso a uma chave privada, somente ele poderia ter gerado tal assinatura. De posse de outra chave correspondente, é possível que qualquer pessoa possa verificar se uma assinatura é íntegra e autêntica. Essa parte compartilhada é chamada de "chave pública". Assim, considerando que outras pessoas têm acesso à chave pública, mas não tem acesso à chave privada, é impossível que alguém consiga gerar uma assinatura digital autêntica. A chave pública está normalmente inserida em um certificado digital.

O mecanismo pode ser aplicado a contratos, procurações, laudos médicos, atestados e diversos documentos, transações on-line, além de autenticar programas digitais, conferindo a eles, em vários casos, validade jurídica. É um procedimento simples e parte do mesmo conceito da assinatura ou rubrica que é feita em documentos físicos.

Na urna eletrônica, a assinatura digital é utilizada para a proteção de todos os dados de entrada (eleitores, candidatos, configuração da eleição, entre outros) e de saída da urna, como Boletim de Urna e Registro Digital de Voto (RDV), por exemplo. Também é empregada para a proteção dos softwares da urna. Dessa forma, garante-se que

os dados e o software se mantenham íntegros e autênticos, ou seja, não foram alterados indevidamente.

O hardware da urna, por exemplo, possui chaves criptográficas protegidas em um circuito eletrônico que permite tanto que a urna funcione apenas com sistemas oficiais da Justiça Eleitoral quanto conferem uma assinatura única para cada uma das mais de meio milhão de urnas do país. Assim, um Boletim de Urna assinado por uma urna, somente pode ter sido assinada por aquela determinada urna, conferindo além da autenticidade, a origem dos dados gerados.

BARREIRAS DE SEGURANÇA

Assim como uma casa tem cadeados e trancas para ajudar na segurança e proteger o patrimônio, no meio digital também existem camadas de proteção para que outros "bens" – que são dados de informações pessoais ou financeiras - não sejam divulgados ou adquiridos sem autorização. Esses mecanismos,desenvolvidos em software e em hardware, são denominados de barreira de segurança digital.

As barreiras de segurança bloqueiam ameaças ao sistema, pois identificam e detectam as tentativas de invasão e interrompem o acesso.

Barreiras na urna eletrônica

A urna eletrônica conta com diversos mecanismos de segurança, por meio dos quais o próprio eleitor, os partidos políticos, as instituições públicas e as entidades da sociedade civil podem verificar a confiabilidade e o pleno funcionamento do sistema eletrônico de votação.

Ao todo, existem 30 camadas de segurança que protegem os sistemas da urna de qualquer tentativa de invasão, formando um mecanismo complexo. Para alterar uma informação, um hacker teria de passar por diversas dessas barreiras, o que é inviável na prática, uma vez que o tempo e esforço necessários seriam muito maiores do que qualquer benefício eventualmente obtido, além do pouco tempo disponível que teria para conseguir algum êxito.

Entre as tecnologias implementadas pelo Tribunal Superior Eleitoral (TSE) para garantir a segurança do software e do hardware da urna estão a criptografia, a assinatura digital e o resumo digital, técnicas amplamente utilizadas e reconhecidas no mundo digital.

BIOMETRIA

Por definição, a biometria é a análise de características físicas ou comportamentais das pessoas com a finalidade de identificá-las de forma única – a impressão digital é um exemplo que todos conhecem. A biometria é usada na identificação criminal, controle de acesso e várias outras ocasiões que possam tornar a identificação exclusiva daquele indivíduo. Os sistemas chamados biométricos podem utilizar características de diversas partes do corpo humano, por exemplo: os olhos, a palma da mão, as impressões digitais do dedo, a retina ou íris dos olhos.

Para tornar o processo eleitoral ainda mais seguro, a Justiça Eleitoral utiliza, desde 2008, a verificação biométrica dos eleitores por meio das impressões digitais. Após verificar os documentos do eleitor ou da eleitora, a urna só é liberada para votação quando o leitor biométrico ratifica sua identidade conforme os respectivos dados biométricos

codificados na urna. Além da verificação biométrica, há a chamada identificação biométrica, onde é verificado se uma mesma pessoa possui mais de um título eleitoral, apenas pelo cruzamento de suas informações biométricas constantes do banco de dados unificado da Justiça Eleitoral em todo o país.

A Justiça Eleitoral espera que todos os eleitores estejam aptos a votar com identificação biométrica até as eleições de 2026.

BLOCKCHAIN

Blockchain é uma tecnologia de dados que tem como objetivo garantir a segurança de informações digitais, e permite o rastreamento ao enviar e receber informações pela internet, mas sem a possibilidade de alterar ou excluir elementos. É como se fosse um grande livro ata, onde uma única pessoa não tem o poder de alterá-lo, pois o controle desse livro está distribuído entre várias pessoas.

O blockchain deriva do termo traduzido "cadeia de blocos" ou "corrente bloqueada". O sistema digital tem dados inseridos em blocos, que faz parte da cadeia de informações e é protegido por um código criptografado e armazena uma informação. Com a validação, os dados se juntam aos demais blocos, ganha um registro definitivo e não pode ser alterado.

Esses blocos estão espalhados pela internet e cada um deles tem um código complexo composto por letras e números. E para dificultar ainda mais decifrar essas informações, cada um desses blocos tem também o código do anterior (como um vagão de trem, por exemplo), o que permite que se conectem e também garante que não houve

violação. Essa conexão entre os inúmeros blocos de informações forma uma corrente de dados complexa e segura.

Esse protocolo tecnológico já está sendo avaliado pelo Tribunal Superior Eleitoral (TSE), e foi observado durante os testes do Projeto Eleições do Futuro, realizado durante as eleições de 2020, como alternativa de ampliação da rede de segurança do processo eletrônico de votação.

BOLETIM DE URNA (BU)

O Boletim de Urna (BU) é um relatório em papel emitido pela urna eletrônica ao final da votação. Esse documento permite que fiscais de partidos e sociedade em geral possam conferir imediatamente após o encerramento da eleição o quantitativo de votos existentes em todas as urnas, ou seja, a apuração de uma seção eleitoral.

É com esse comprovante, emitido e publicado no final do pleito em cada seção eleitoral, que se pode conferir os resultados, inclusive comparando com o que é divulgado pela Justiça Eleitoral na internet.

O BU traz as seguintes informações relativas aos dados registrados na urna eletrônica: total de votos por partido; total de votos por candidato; total de votos nominais; total de votos de legenda, quando for cargo proporcional; total de votos nulos e em branco; total de votos apurados; eleitorado apto para votar na seção; identificação da seção e da zona eleitoral; hora do encerramento da eleição; código interno da urna eletrônica; e a sequência de caracteres para a validação do boletim. O documento também pode ser acessado no Portal do TSE. E por meio de um aplicativo de celular, o eleitor pode obter uma cópia digital do BU fazendo a leitura do QR Code impresso

no boletim, o que garante o acesso e a conferência dos resultados publicados na internet.

CADEIA DE SEGURANÇA DE HARDWARE

A cadeia de segurança de hardware faz parte da engenharia que envolve o design de um equipamento com controle de acesso para garantir que todos os suprimentos que compõe produtos tecnológicos seja segura. No caso da urna eletrônica, a cadeia de segurança garante que sejam executados apenas os softwares desenvolvidos e assinados digitalmente pelo Tribunal Superior Eleitoral (TSE). O conceito da cadeia de segurança em hardware foi implementado pela primeira vez em 2009 e apresentado em artigo científico em 2010 e é implementada pelo hardware de segurança da urna.

A proteção do sistema é feita em camadas formadas por diversas barreiras que, em conjunto, não permitem que a urna seja violada. Qualquer tentativa de ataque causa um efeito dominó, que bloqueia o sistema e trava o equipamento, assim como qualquer tentativa de executar software não autorizado na urna eletrônica resulta no bloqueio do funcionamento. De igual modo, tentativas de executar o software oficial em um hardware não certificado resultam no cancelamento da execução do aplicativo.

A Justiça Eleitoral utiliza o que há de mais moderno em termos de segurança da informação para garantir a integridade, a confiabilidade, a transparência e a autenticidade do processo eleitoral. Essa cadeia de segurança tem inúmeras etapas todas supervisionadas pela Justiça Eleitoral, que vai desde a fabricação, passando pela manutenção, inclusão e lacração de sistemas e que coloca o equipa-

mento como exclusivo para o exercício da democracia, pois a urna eletrônica só é utilizada para votações e funciona somente na hora e na data dos pleitos eleitorais.

CERIMÔNIA DE ASSINATURA DIGITAL E LACRAÇÃO

A cerimônia de Assinatura Digital e Lacração dos Sistemas Eleitorais é um evento que legitima os programas que serão utilizados nas urnas eletrônicas e equipamentos correlatos nas eleições. A cerimônia de lacração é prevista no art. 66, §2º da Lei nº 9.504 e detalhada em resolução. Essa cerimônia funciona como garantia de que todos os sistemas que serão utilizados na eleição têm uma versão única e estão seguros.

O evento, que ocorre no Tribunal Superior Eleitoral (TSE), é o momento em que os arquivos dos sistemas são assinados, por meio de certificação digital, e também fisicamente, pelo presidente do TSE. Outras autoridades e entidades também podem participar dessa cerimônia e assinar os sistemas, tais como: Ministério Público; Polícia Federal; partidos políticos, federações e coligações; Ordem dos Advogados do Brasil (OAB); Congresso Nacional; Supremo Tribunal Federal (STF); Controladoria-Geral da União (CGU); Sociedade Brasileira de Computação; Conselho Federal de Engenharia e Agronomia (Confea); Conselho Nacional de Justiça (CNJ); Conselho Nacional do Ministério Público (CNMP); Tribunal de Contas da União (TCU); Forças Armadas; entidades privadas brasileiras sem fins lucrativos, com notória atuação em fiscalização e transparência da gestão pública, credenciadas junto ao TSE; e departamentos de Tecnologia da Informação de universidades credenciadas junto à Corte Eleitoral.

Nessa cerimônia, os códigos-fonte (conjunto de instruções e comandos definidos pelos programadores de sistemas) são convertidos em programas entendidos pelos computadores e urnas eletrônicas em um procedimento chamado de "compilação".

As assinaturas digitais geram uma blindagem em todos esses códigos-fonte e programas e ainda garantem a autoria e a integridade das informações. Cada uma das assinaturas feitas gera um resumo digital, que corresponde a um código único, tal como um identificador que pode ser recalculado por qualquer pessoa. Assim, qualquer alteração no arquivo lacrado geraria um resumo digital completamente diferente e a alteração seria facilmente detectada, mesmo se for apenas uma única letra.

Essa técnica é utilizada também por peritos da Polícia Federal para avaliar alteração de arquivos. Como os resumos digitais dos programas são publicados na Internet, não haveria como qualquer pessoa, incluindo servidores da Justiça Eleitoral alterarem qualquer arquivo lacrado nessa cerimônia sem que a alteração seja detectada. Essa técnica garante a integridade da versão única dos sistemas de preparação, sistemas da urna eletrônica, e os de totalização dos votos. A partir das Eleições 2022, os logs das urnas também estarão disponíveis na Internet para qualquer cidadão.

CÓDIGO-FONTE DA URNA

Código-fonte é um conjunto de linhas de programação de um software, que fornece as instruções para que ele funcione. O profissional de TI, um programador, "escreve" o programa em uma certa linguagem específica de programação. Depois ele precisa converter as linhas de

programação em linguagem de máquina, a única que o computador é capaz de entender. Essa linguagem de máquina também é chamada de código executável. Quando você compra um programa, portanto, você compra a linguagem de máquina, e não o código-fonte.

Alguns tipos de programa, no entanto, possuem código-fonte aberto. É o caso do Linux e dos sistemas operacionais chamados de "código aberto". Quando você obtém o Linux, além da linguagem de máquina, você também leva o código-fonte. Com o código-fonte de um programa em mãos, um programador de sistema pode alterar a forma como esse software funciona, adicionar recursos, remover outros —enfim, adaptar o software às suas necessidades. Mas modificar os códigos-fonte deixa rastros e que podem ser detectados facilmente.

O código-fonte das urnas e de totalização é disponibilizado aos partidos políticos, OAB (Ordem dos Advogados do Brasil), Ministério Público, Congresso Nacional, Supremo Tribunal Federal, Controladoria-Geral da União, Polícia Federal, Sociedade Brasileira de Computação, Conselho Federal de Engenharia e Agronomia, Conselho Nacional de Justiça, Conselho Nacional do Ministério Público, Tribunal de Contas da União, Forças Armadas, Confederação Nacional da Indústria e sistemas integrantes, entidades de fiscalização sem fins lucrativos e departamentos de TI credenciados junto ao TSE. Embora os eleitores, em geral, não tenham conhecimento para auditar códigos-fonte, a representatividade de dezesseis classes de instituições traz a figura do chamado terceiro confiável, pois não haveria como um fraudador, ou os próprios técnicos do TSE realizarem qualquer fraude sem que haja detecção por parte dessas instituições.

CRIPTOGRAFIA

Criptografia é uma forma de codificar determinada mensagem de maneira que só aqueles que conhecem o código podem decifrar. Em segurança da informação, é a conversão de dados de um formato legível para um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem decifrados. É a forma mais simples e mais importante de garantir que as informações de um sistema digital não sejam roubadas e lidas por alguém que deseja usá-las para fins maliciosos.

Na Justiça Eleitoral, a criptografia digital é um mecanismo de segurança para a proteção de dados sensíveis, tais como os votos gravados no RDV e a biometria dos eleitores. Como os dados tornam-se embaralhados, eles ficam inacessíveis a pessoas não autorizadas. O Tribunal Superior Eleitoral (TSE) usa uma combinação de algoritmos proprietários e de domínio público para cifração simétrica e assimétrica.

FLASH CARD

A urna eletrônica, como qualquer computador, necessita de dispositivos para armazenamento de dados (mídias). Desde a urna modelo 98, utiliza-se, para esse fim, o flash card, um cartão de memória que apresenta características de leitura e gravação, como se fosse um HD.

Além dos flashs cards, são utilizadas outras mídias para gravação dos resultados da votação, bem como para a ativação de aplicativos específicos da urna. Até as eleições de 2010 utilizavam-se para esse

fim disquetes de 3½". Desde aquelas eleições, teve início a substituição dos disquetes por uma mídia criada especificamente para a Justiça Eleitoral, denominada Memória de Resultado, que é um pen drive que possui um formato físico exclusivo da Justiça Eleitoral para facilitar seu uso e evitar problemas de conexão.

Geração de Mídias

Em cerimônia pública, geralmente realizada nos cartórios eleitorais, ocorre a geração das mídias que vão preparar as urnas de cada seção daquela zona eleitoral. Gerar as mídias significa dizer que o ecossistema da urna – alimentado com os dados eleitorais específicos daquele pleito, a exemplo dos nomes dos candidatos aptos e dos eleitores – será gravado nos flashs cards de carga para a preparação das urnas. Também são preparados os flashs cards de votação e as "mídias de resultado" que alimentarão as urnas.

Para efeitos de controle, são registrados na ata da cerimônia a quantidade de mídias de carga e de votação geradas, bem como os nomes dos técnicos responsáveis pela operação.

GEDAI

Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE), é um dos aplicativos que compõe o Ecossistema da urna eletrônica, responsável por automatizar as atividades e processos para a geração das mídias necessárias para que o equipamento funcione efetivamente.

O sistema Gedai-UE é responsável por gerar as mídias de carga e de votação para a urna, além de receber e enviar as informações de

correspondência entre número interno da urna e número da seção eleitoral preparada para os TREs. É um programa para execução no sistema Windows que foi desenvolvido pela Seção de Voto Informatizado do TSE. Assim como os demais sistemas de votação, apuração e totalização, o Gedai-UE também é lacrado na Cerimônia de Assinatura Digital e Lacração dos Sistemas.

É com a ação desse programa que são gerados cartões de memória que contêm os dados de candidatos e os eleitores (mídias de votação) e os cartões que contém a instalação dos sistemas da urna (mídias de carga). O funcionamento desse aplicativo é de uso exclusivo para a preparação da urna eletrônica brasileira, conjuntamente com os diversos sistemas que compõe o equipamento eletrônico de votação.

HASHES – RESUMOS DIGITAIS

Os resumos digitais (hashes) têm relação direta com a segurança do processo eleitoral e são gerados a cada eleição, na cerimônia de lacração dos sistemas, realizada no Tribunal Superior Eleitoral (TSE). A chamada "conferência de hash" possibilita aos partidos políticos e ao Ministério Público verificar se os sistemas encontrados em qualquer urna do país correspondem à versão única e oficial dos sistemas lacrados no TSE.

Esses resumos digitais são gerados na cerimônia de lacração dos sistemas eleitorais realizada no TSE, na presença de todos os representantes das entidades fiscalizadoras. Os sistemas (fontes e executáveis) e os resumos digitais gerados na cerimônia pública são assinados digitalmente pelo presidente do TSE e pelas demais autoridades previstas. Depois disso, são gravados em mídia não regravável e assinados fisicamente por todos, para então serem

lacrados e armazenados na sala-cofre do Tribunal. É proteção física e digital para garantir ainda mais legitimidade e segurança para o sistema eletrônico de votação.

HACKER

Hackers são pessoas com muito conhecimento de informática e computação. Geralmente trabalham desenvolvendo e modificando softwares e hardwares de computadores, não necessariamente para cometer algum crime. Mas há também aqueles que utilizam o conhecimento para invadir sistemas de forma ilícita.

Eles também desenvolvem novas funcionalidades no que diz respeito a sistemas de informática. Geralmente são indivíduos capazes de encontrar alguma brecha na segurança de um website, por exemplo.

O Tribunal Superior Eleitoral (TSE) utiliza os mais modernos artefatos em termos de Segurança da Informação para assegurar a integridade, a confiabilidade e a autenticidade das eleições brasileiras. A urna eletrônica é fruto da dedicação de profissionais altamente capacitados, não apenas da Justiça Eleitoral, mas também de outros órgãos do governo brasileiro.

Participação no Teste Público de Segurança

Um ano antes de cada eleição o TSE convida "hackers" para ampliar a segurança e afastar questionamentos sobre o sistema eletrônico de votação. O setor de tecnologia do Tribunal promove o Teste Público de Segurança (TPS), onde especialistas que queiram colocar a segurança das urnas eleitorais à prova podem bolar um projeto e tentar invadir o sistema, supervisionado por técnicos da Justiça Eleitoral.

HARDWARE

Hardware é todo componente físico, interno ou externo do seu computador, ou celular, por exemplo. A parte física destes equipamentos é quem sustenta e determina o que um dispositivo é capaz e como você pode usá-lo. Os equipamentos eletrônicos dependem sempre de um software para funcionar (e vice-versa), o hardware é um elemento igualmente importante.

O termo é usado para se referir aos componentes externos como o gabinete de um computador ou a capa e tela de um celular, e também para componentes de dispositivos em geral, como processador, placa-mãe, memória RAM, unidades de armazenamento (HDs, SSDs e memória Flash), controles remotos, etc.

Qualquer desses equipamentos (hardware) não funciona sem um programa (software). Da mesma forma que não é possível usar um software sem o hardware adequado, para o qual ele foi desenvolvido. Nos equipamentos da Justiça Eleitoral que estão presentes no sistema eleitoral: a urna eletrônica, suas teclas, tela, o coletor biométrico são exemplos de hardwares.

KIT JE-CONNECT

JE-Connect é um conjunto de sistemas inseridos em mídias, que possibilita a transmissão de dados obtidos na urna eletrônica a partir de computadores de terceiros (computadores já disponíveis no local de votação). Com o mecanismo, os resultados das urnas podem ser enviados dos próprios locais de votação a partir de qualquer compu-

tador por meio de rede Virtual Private Network (VPN) – Rede Virtual Privada. Sendo assim, a ferramenta traz agilidade na apuração e divulgação dos resultados, bem como possibilita a redução de custos com logística.

Por meio de uma rede virtual VPN, na internet, que se conecta à rede privada da Justiça Eleitoral, os dados são transmitidos para o TSE. As informações que saem da urna são criptografadas até chegar ao TSE. Também recebem outra camada de criptografia, que torna inviável qualquer invasão ou acesso não autorizado ou ainda adulteração dos resultados de uma seção eleitoral.

O kit de transmissão JE-Connect só envia dados para a rede da Justiça Eleitoral e para as portas específicas. Se o programa transportador não encontrar a assinatura digital que é gerada na urna eletrônica, não irá ler a mídia, o que inviabiliza acesso a qualquer informação.

O sistema foi desenvolvido por técnicos em tecnologia da informação do TRE-Tocantins em 2008 e aprimorado em 2010, junto a outros Tribunais Eleitorais. A partir de 2012, o JE Connect tornou-se tornou padrão da Justiça Eleitoral, conforme Portaria do TSE 334/12.

LACRES DE SEGURANÇA

Os lacres de segurança das urnas eletrônicas são dispositivos feitos em material autoadesivo com uma numeração sequencial de sete dígitos que, após a aplicação, deixam evidências de sua retirada, ou seja, quando alguém tenta tirá-los eles denunciam imediatamente a tentativa de violação ou falsificação.

Depois que as urnas estão preparadas, eles são colados em todas as portas de acesso físico da urna e das mídias, resultando em uma garantia visual às entidades fiscalizadoras de que não houve acesso às interfaces ou à parte interna da urna desde sua preparação.

Desde as eleições de 1996, a Justiça Eleitoral tem contrato com a Casa da Moeda do Brasil, empresa pública com centenas de anos de expertise, que produz não só estes itens, mas outros, como os envelopes de segurança utilizados nas eleições. A partir das Eleições 2010 os lacres passaram a utilizar um material especial que permite evidenciar se for retirado, mas não deixa resíduo na superfície das urnas.

É importante ressaltar que a segurança das urnas não depende dos lacres, pois sua arquitetura de segurança de hardware e software não permite a continuidade do funcionamento da urna se os programas ou os dados forem adulterados. Assim, os lacres conferem proteção adicional, permitindo a auditoria forense por parte de peritos, pois complementam as evidências colhidas e permitem a ligação ao evento de preparação das urnas.

A parceria com a instituição federal está garantida para as Eleições 2022 e estima-se que serão impressos 1,4 milhão de lacres para o pleito, sendo 700 mil para o primeiro turno e 700 mil para eventual segundo turno. Este número é calculado pela quantidade de adesivos em cada urna, que são definidos a cada eleição pelo Tribunal Superior Eleitoral (TSE). Por meio de resolução, a Corte define quantos e quais serão os lacres, formatos, materiais e a forma como serão utilizados.

LOG DE URNA

Em linguagem de computação, log de dados é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional. Os logs são os registros de atividade, como o histórico, de qualquer sistema. É onde se pode localizar possíveis alterações e acessos, como um histórico de atividades desenvolvidas naquele programa.

Esse conjunto de dados se apresenta sob a forma de uma ficha de texto clássico, recolhendo cronologicamente todos os eventos que afetaram um sistema informático (software, aplicação, servidor, etc) e todas as ações que resultaram desses eventos.

A urna eletrônica registra todos os eventos relevantes de seu funcionamento e das falhas encontradas. Contudo, embora registre a data e hora em que um eleitor iniciou a votação, bem como cada cargo escolhido, não registra o número do título do eleitor. Isso porque, embora o armazenamento dos votos seja feito de modo que ninguém, nem mesmo a Justiça Eleitoral, possa saber em que candidato cada eleitor votou, por precaução, também não é registrado em que horas determinado eleitor votou. De todo modo, o log da urna é um elemento de auditoria importante para os partidos políticos e demais entidades fiscalizadoras.

Na Justiça Eleitoral, os arquivos de logs são arquivados e ficam disponíveis para avaliação. Se houver necessidade, esses arquivos podem ser solicitados para averiguação pelas entidades fiscalizadoras, conforme disposto no art. 46 da Resolução-TSE nº 23.673/2021. A partir das Eleições 2022, os logs das urnas também estarão disponíveis na Internet para qualquer cidadão.

MALWARE

Malware ou software mal-intencionado é a nomenclatura usada para qualquer programa ou arquivo que seja prejudicial ao funcionamento de um equipamento digital como computadores, tablets, telefones celulares, por exemplo.

Esses programas maliciosos são também conhecidos como "vírus de computador". Eles podem executar uma variedade de funções diferentes, como roubar, criptografar ou excluir dados confidenciais, alterar ou sequestrar as principais funções de computação e monitorar a atividade do computador dos usuários sem a permissão deles.

Softwares maliciosos podem ser inseridos na urna eletrônica? A Justiça Eleitoral afirma que isso não é possível. A placa-mãe da urna possui um hardware de segurança, protegido por resina epóxi, que não pode ser desligado ou desabilitado, responsável por atestar a autenticidade dos programas que serão utilizados na urna eletrônica.

Nesse computador são inseridos os certificados digitais – as chaves oficiais do TSE –, que fazem a verificação, camada por camada, de todos os softwares que são carregados na urna. Isso impede, de forma sistemática, que um software não oficial ou minimamente adulterado seja carregado na urna eletrônica. Também impede que o software oficial da urna possa ser utilizado em outro equipamento. Somente o software oficial, assinado na sala-cofre do TSE, funciona na urna eletrônica.

OBSERVADORES ELEITORAIS

Observação Eleitoral é mais um instrumento de auditoria e transparência que vem sendo inserido na realidade eleitoral brasileira. Nesse processo, entidades e organizações independentes da sociedade civil (observação nacional), ou, ainda, organismos regionais e internacionais, governos estrangeiros ou organizações não estatais (observação internacional) acompanham, como observadores, o desenrolar das eleições para avaliar a qualidade dos procedimentos e processos eleitorais.

Após a missão dos observadores, em diferentes instâncias, são publicadas as recomendações. Nas Eleições 2020, o processo eleitoral brasileiro foi fiscalizado por duas missões de observação, uma internacional, da Organização dos Estados Americanos (OEA), e outra nacional, da associação civil Transparência Eleitoral Brasil.

A presença de observadores internacionais tem como objetivo garantir que o processo eleitoral decorra num clima de transparência, isenção e legalidade, visando assegurar a credibilidade dos resultados eleitorais.

PREPARAÇÃO DAS URNAS

A preparação das urnas eletrônicas que serão utilizadas nas eleições se dá após a cerimônia de assinatura digital e lacração dos sistemas. Uma única versão dos sistemas eleitorais, já aprovados, é liberada para todos os Tribunais Regionais Eleitorais (TREs), e a partir dela é possível importar os dados de candidatos, partidos, eleitores e de

configuração, todos assinados digitalmente ou controlados com segurança pela versão única lacrada.

Na urna eletrônica são usadas mídias do tipo Flash Card (CompactFlash®) ou pendrives com formatos exclusivos da Justiça Eleitoral. Todas essas mídias também são protegidas com técnicas criptográficas que garantem sua integridade e autenticidade, como a assinatura digital.

Após indicar a seção que será preparada, o software de carga das urnas eletrônicas formata a mídia interna da urna, insere o sistema operacional e todos os demais arquivos lacrados, além de inserir, ainda, os respectivos candidatos e eleitores da seção. Após, um software, também lacrado, testa todos os dispositivos da urna e somente equipamentos totalmente funcionais podem prosseguir na preparação.

Após essa preparação inicial da urna, informações geradas unicamente naquele momento, com as respectivas assinaturas digitais da urna preparada, são enviadas para o sistema de totalização, que aceitará apenas resultados para a seção provenientes da urna específica correspondente.

PÓS-PREPARAÇÃO DO EQUIPAMENTO

Após a preparação das urnas, os compartimentos delas são lacrados fisicamente com lacres especiais produzidos pela Casa da Moeda, cujas propriedades químicas impedem qualquer tentativa de violação: ao ser retirado, aparece imediatamente a inscrição de que foi violado. Todas as portas de acesso físico à urna são lacradas.

Toda a cerimônia de geração de mídias e de preparação das urnas é pública, convocada por Edital, e é acompanhada ainda por representantes do Ministério Público.

As urnas são armazenadas em local designado pelo TRE para, às vésperas da eleição, serem transportadas para os locais de votação. Qualquer tentativa de uso antes disso será em vão, pois a urna possui sistemas que só permitem que seja utilizada no momento programado para a votação. E lembrando, que o equipamento em momento algum, nem no período de preparação para as eleições nem durante as votações ou na fase posterior, é conectado a qualquer tipo de rede de comunicação externa.

QR CODE

QR Code é a tradução para código de resposta rápida (Quick Response Code). Esse código digital existe há 25 anos, criado em 1994 pela Denso-Wave, uma empresa automotiva do Japão. O QR Code é também uma evolução do código de barras, e consiste em um gráfico 2D que pode ser lido pelas câmeras da maioria dos celulares. O código é utilizado para várias funções que vão de compras a identificação de documentos, por exemplo, além de ser bastante usado ainda para oferecer conteúdo extra sobre um determinado assunto.

Justiça Eleitoral

Na Justiça Eleitoral, o QR Code é encontrado no Boletim de Urna (BU), desde 2016. Ele é mais um mecanismo que promove a fiscalização cidadã do processo eletrônico de votação brasileiro. Como o QR Code permite que informações em texto sejam facilmente lidas pelos

celulares, o QR Code no BU permite que qualquer pessoa possa ler um Boletim de Urna completo e conferir posteriormente com o que foi recebido pelo TSE.

A leitura desse QR Code pode ser feita tanto pelo app BU na mão, disponibilizado pela Justiça Eleitoral, quanto qualquer pessoa ou entidade fiscalizadora pode desenvolver seu próprio aplicativo. Isso porque, a cada eleição, o TSE disponibiliza um manual completo de como os dados são codificados no QR Code. Assim, qualquer pessoa pode comparar, candidato a candidato, se os votos apurados na seção eleitoral correspondem ao que foi processado no TSE. Considerando que às vezes há uma grande quantidade de candidatos e partidos em uma única eleição, pode acontecer de haver até 5 (cinco) QR Codes, para que todas as informações possam ser lidas automaticamente.

RESUMO DIGITAL - HASH

O Resumo digital corresponde a um código único, tal como um identificador que pode ser recalculado por qualquer pessoa. É como uma forma de calcular uma impressão digital de um arquivo, com uma fórmula de cálculo conhecida por todos.

O algoritmo, ou fórmula de cálculo, para um resumo digital se chama algoritmo de hash. O hash é, então, uma técnica criptográfica que gera uma identificação única para um arquivo digital. Assim, qualquer alteração no arquivo para o qual um hash foi calculado, geraria um resumo digital completamente diferente e a alteração seria facilmente detectada, mesmo se fosse apenas uma única letra.

Qualquer que seja o tamanho do arquivo, o resumo digital de um determinado algoritmo de hash sempre terá um tamanho único, mas

um número muito grande, representado em um formato de letras, números e caracteres especiais. Mas os resumos digitais possuem uma propriedade importante: não podem ser revertidos. Por analogia, é como se houvesse a tentativa de definir completamente uma pessoa (altura, sexo, cor dos olhos etc.) apenas pela sua impressão digital.

Assim, é possível publicar os resumos digitais de arquivos sem publicar seu conteúdo, mas, a partir do arquivo, é possível calcular o resumo digital novamente, para comprovar que tem o mesmo conteúdo do resumo digital publicado. Isso assegura, como um lacre, que o arquivo não foi modificado.

Utilização

Essa técnica é utilizada também por peritos da Polícia Federal para avaliar alteração de arquivos. Como os resumos digitais dos sistemas eleitorais lacrados são publicados na Internet, não haveria como qualquer pessoa, incluindo servidores da Justiça Eleitoral, ter o poder de alterar qualquer arquivo lacrado na Cerimônia de Assinatura Digital e Lacração dos Sistemas sem que tal alteração fosse detectada. Essa técnica garante a integridade da versão única dos sistemas de preparação, sistemas da urna eletrônica e os de totalização dos votos.

REGISTRO DIGITAL DO VOTO (RDV)

O Registro Digital do Voto (RDV), criado em 2003, permite a recontagem dos votos da urna eletrônica por partidos políticos e coligações a qualquer tempo. O RDV preserva o voto dado pelo eleitor e substitui o voto impresso, além de assegurar o sigilo da votação.

O registro, que pode ser impresso, armazena todos os votos ao final do processo de votação, tal como digitados pelo eleitor. Dessa forma, o RDV possibilita a recuperação dos votos para recontagem eletrônica, além de acrescentar segurança e transparência ao processo eleitoral.

Como funciona

No momento da votação, a urna registra os dados, que são gravados de maneira a preservar o sigilo da votação, utilizando uma técnica que mantém os votos ordenados de acordo com o número digitado pelo eleitor. A medida evita a possibilidade de se vincular o eleitor na fila da seção ao respectivo voto. Assim, o RDV garante o sigilo e, como numa urna de lona tradicional, onde as cédulas de papel ficam embaralhadas, impossibilita a vinculação de cada cédula a um eleitor.

De posse do documento, é possível realizar não somente a recontagem dos votos como também a apuração e a totalização, independentemente dos procedimentos oficiais por parte da Justiça Eleitoral. É um mecanismo de transparência, substituindo de modo eficaz o voto impresso. Pois, uma cédula de papel pode ser subtraída, rasgada ou riscada. Já o RDV não permite que os dados sejam alterados, uma vez que utiliza diversas ferramentas de segurança da informação, como criptografia, assinatura digital e hash (resumo digital) e não há intervenção humana.

SALA-COFRE

Sala-cofre é um espaço dentro da sede do Tribunal Superior Eleitoral (TSE), climatizada, à prova de fogo e terremoto, com 90 computadores onde são armazenados os inúmeros dados do processo eleitoral brasileiro.

São dois espaços construídos no Tribunal em Brasília (DF). No primeiro, ficam armazenados o cadastro nacional de eleitores, o registro e a prestação de contas dos candidatos. É nessa sala-cofre que se centraliza a apuração e totalização dos votos de todo o país. No outro, estão a Autoridade Certificadora das Urnas Eletrônicas e as matrizes dos softwares que fazem funcionar as urnas eletrônicas. Esses programas possuem assinaturas e registros digitais do TSE, da Ordem dos Advogados do Brasil, dos partidos políticos e da Procuradoria Geral Eleitoral.

Sobre o local

O espaço tem sistema de ar-condicionado que mantém a temperatura em 18ºC e verifica constantemente a presença de fumaça. Em caso de incêndio, um gás extintor especial é expelido no ambiente, sem que haja qualquer dano aos computadores.

Para entrar nesse ambiente, cujo acesso é extremamente restrito e monitorado 24h, durante os sete dias da semana, é preciso passar por cinco portas codificadas, sendo que a quarta e a quinta só abrem com duas pessoas que possuem esse acesso. A segurança do local possibilita que a Justiça Eleitoral exerça o trabalho que garante integridade renomada do sistema eletrônico de votação brasileiro.

SISTEMA ELETRÔNICO DE VOTAÇÃO

O sistema eletrônico de votação brasileiro é referência mundial e tem a urna eletrônica como protagonista. O equipamento e seus mecanismos garantem a normalidade dos pleitos, a segurança do voto e a liberdade democrática. Desde que foi adotada no processo

eleitoral, em 1996, a urna eletrônica já contabiliza 12 eleições bem-sucedidas, sem qualquer vestígio ou comprovação de fraude.

Ao contrário, a informatização do processo eleitoral brasileiro eliminou manobras fraudulentas realizadas na época da votação por meio de cédulas de papel. E a explicação é simples: vários procedimentos que eram feitos manualmente passaram a ser feitos automaticamente, como a captura e apuração dos votos. Para tanto, a Justiça Eleitoral utiliza o que há de mais moderno em termos de segurança da informação para garantir essa automatização, primando pela integridade, confiabilidade e autenticidade dos programas e dados do sistema eletrônico de votação.

Além de passar sistematicamente por testes públicos de segurança, as urnas dispõem de uma série de mecanismos de auditoria e de verificação dos resultados, que podem ser utilizados por candidatos, por partidos, por coligações, pelo Ministério Público, pela Ordem dos Advogados do Brasil e pela Polícia Federal, entre outras entidades, bem como pelo próprio eleitor.

Segurança do sistema

A cadeia de segurança da urna eletrônica garante que sejam executados somente os softwares desenvolvidos e assinados digitalmente pelo Tribunal Superior Eleitoral (TSE). A proteção do sistema é feita em camadas formadas por diversas barreiras, que, em conjunto, não permitem que a urna seja violada. Qualquer tentativa de ataque causa um efeito dominó, que bloqueia o sistema e trava o equipamento. A urna eletrônica também conta com modernos dispositivos de criptografia e de assinatura digital.

SOFTWARE

Software é a nomenclatura que se dá para um programa de computador, um aplicativo no celular ou até mesmo o sistema operacional de um dispositivo eletrônico. O termo é usado para descrever programas, apps, scripts, macros e instruções que vai direcionar o que o aparelho eletromecânico deve fazer.

Sem um software, os aparelhos não têm funcionalidade. Um exemplo é que você só vai conseguir fazer funcionar um equipamento eletrônico, digitar um texto no seu computador, enviar mensagens pelo seu celular ou fazer operações financeiras por meio de um software que possibilita executar essas funções.

Todo programa em seu computador, celular, tablet, smart TV ou console de videogame é um software, seja ele um editor de textos, um navegador, um editor de áudio ou vídeo, um jogo, um app de streaming entre outros.

No caso da urna eletrônica, ela também possui um software. Esse programa usado no equipamento foi integralmente desenvolvido e mantido pela equipe técnica do Tribunal Superior Eleitoral (TSE). Ele é único e de uso específico para execução dos procedimentos de funcionamento da urna.

SOFTWARE ABERTO

Software aberto ou livre é um sistema que possui todo o seu código-fonte aberto para análise e verificação do comportamento programado. O software livre está presente na urna eletrônica, o que

permite a construção de um sistema mais seguro e com um custo menor. Outros órgãos do Estado brasileiro e diversas empresas, inclusive de informática, utilizam softwares de código aberto.

O mais famoso software aberto e também utilizado pela Justiça Eleitoral é o Linux, que, diferentemente de outros sistemas como o Windows e o Mac OS, pode ser livremente modificado e distribuído.

O programa adaptado para a urna eletrônica é de propriedade da Justiça Eleitoral e tem a intenção de: facilitar a auditoria do sistema operacional, ampliando a certificação de que todos os sistemas são confiáveis e seguros; diminuir os custos de aquisição de novas urnas eletrônicas; e ter um único sistema operacional para simplificar e diminuir o custo de desenvolvimento, testes e homologação dos sistemas das urnas eletrônicas.

O software aberto também proporciona à Justiça Eleitoral outras vantagens, como confiabilidade, custo reduzido - pois não há pagamento de propriedade intelectual e de direitos autorais - e manutenção do sistema, que poderá ser feita internamente e com muita rapidez, sem a necessidade de intervenção do fabricante ou fornecedor.

E na vanguarda da modernidade e da segurança digital, o Tribunal Superior Eleitoral (TSE) entrou para o seleto grupo de incorporadores de funcionalidades no sistema operacional Linux. Um mecanismo de segurança criado pela equipe da Corte Eleitoral para equipar a urna eletrônica foi integrado definitivamente ao Kernel (núcleo do sistema operacional) e fará parte da versão 5.13 do Linux. Com isso, o software de segurança criado pelo Tribunal poderá rodar em qualquer computador.

A solução deixa o sistema mais seguro não só para o TSE, mas para o mundo inteiro. Todo o sistema da urna é assinado digitalmente para

garantir que ele só funcione com softwares feitos pelo Tribunal, e a recente modificação feita pela equipe do Tribunal exige que uma dessas assinaturas seja obrigatoriamente atestada pelo próprio sistema operacional, uma característica que não existe por padrão na plataforma Linux.

TECNOLOGIA DA INFORMAÇÃO

Tecnologia da Informação (TI) é um conjunto de todas as atividades e soluções providas por recursos de computação que visam a produção, o armazenamento, a transmissão, o acesso, a segurança e o uso das informações.

Fazem parte do universo da TI a combinação de equipamentos hardware (computadores, smartphones, impressoras etc.) e software (programas de computador, certificados digitais, protocolos de segurança etc).

Importância da TI

A informação sobre qualquer tema ou instituição é um patrimônio. E é a TI e os profissionais dessa área que garantem que os recursos de hardware e de software sejam aplicados e mantidos de modo coerente à cada atividade. É por isso que empresas e outras organizações costumam contar com um departamento de TI (ou uma divisão similar).

No caso do Tribunal Superior Eleitoral (TSE), a Secretaria de Tecnologia da Informação (STI) se tornou uma área extremamente importante. A STI é responsável pela elaboração de estratégias de informática, bem como pelo planejamento e governança em TI, que garantem, no âmbito da Tecnologia da Informação, eleições seguras digitalmente.

TESTE DE INTEGRIDADE DA URNA

Imagine comprar um carro zero quilômetro que, seguramente, tem autonomia para rodar até 20 quilômetros com um litro de gasolina, conforme informado pelo fabricante. Para comprovar a informação, a montadora do carro convida pessoas interessadas em adquirir o veículo para participar de um teste, no qual podem dirigir o carro e confirmar que ele supre as expectativas de consumo de combustível indicado.

É também com exames públicos, os chamados Testes de Integridade da Urna Eletrônica, que se garante a legitimidade, a segurança, promovendo a auditabilidade do processo eletrônico de votação. Os Testes são realizados no dia do pleito em todos os estados do Brasil.

Todos os procedimentos dos Testes são monitorados por entidades fiscalizadoras, representantes dos partidos políticos, do Ministério Público (MP), da Ordem dos Advogados do Brasil (OAB) e por qualquer pessoa interessada. Essa fiscalização é realizada em todas as fases dos trabalhos nos Tribunais Regionais Eleitorais (TREs).

A auditoria por meio do Teste de Integridade é um procedimento utilizado pela Justiça Eleitoral desde 2002, com o objetivo de testar a segurança na captação e na contagem dos votos pela urna eletrônica. Após todas as urnas já estarem preparadas, lacradas e prontas pra eleição, algumas delas são selecionadas na véspera da eleição e levadas até um ambiente controlado. Nesse ambiente, uma votação monitorada equivalente à votação oficial é realizada com o propósito de comprovar que o voto recebido/digitado é exatamente aquele que será contabilizado eletronicamente. Além de público, toda a votação é filmada para garantir que os votos computados correspondem exatamente ao resultado final apurado pela urna.

Para os Testes, é utilizado um sistema de apoio, que tem a finalidade de trazer maior agilidade ao processo de conferência dos resultados produzidos pela urna. Como todos os votos depositados na urna são divulgados e também registrados em papel, os auditores presentes podem fazer a sua própria apuração e compará-la com o boletim produzido pela urna.

TESTE DE CONFIRMAÇÃO

Teste de confirmação é a etapa onde se verifica se alguma inconformidade detectada no sistema durante o Teste Público de Segurança (TPS) teve as respectivas barreiras de segurança readequadas. Os investigadores que atuaram no TPS são convidados para verificar as correções realizadas pela equipe técnica do Tribunal Superior Eleitoral (TSE), relacionadas aos "achados" que poderiam inviabilizar alguma das várias barreiras de segurança da urna.

O grupo de investigadores que identificar eventuais vulnerabilidades volta ao tribunal para repetir o plano de ataque e verificar se foram corrigidas. Participam também técnicos e ministros do TSE, além de representantes do Ministério Público Federal (MPF), Polícia Federal, Ordem dos Advogados do Brasil (OAB) e da Comissão Avaliadora do TPS – esta responsável por avalizar as ações desse encontro.

Todos os detalhes são amplamente divulgados: do código-fonte do sistema até o resultado dos planos de ataque executados pelos investigadores. Desde 2019, o TSE prepara uma estrutura para que todos os cidadãos possam acompanhar o Teste de Confirmação pela internet. Uma câmera fixa capta imagens do ambiente de teste, que são transmitidas ao vivo pelo canal do TSE no YouTube.

TESTE PÚBLICO DE SEGURANÇA (TPS)

O Teste Público de Segurança (TPS) do Sistema Eletrônico de Votação foi criado pela Justiça Eleitoral com o objetivo de fortalecer a confiabilidade, a transparência e a segurança da captação, da apuração, da transmissão e do recebimento dos votos, além de propiciar melhorias no processo eleitoral. O TPS é um evento permanente no calendário eleitoral.

Realizado preferencialmente no ano anterior às eleições, o teste faz parte da transparência institucional preconizada pela Justiça Eleitoral. Ele reúne especialistas em Tecnologia da Informação e Segurança da Informação das mais diversas organizações, instituições acadêmicas e órgãos públicos para realizar planos de ataque aos sistemas eleitorais envolvidos na geração de mídias, votação, apuração, transmissão e recebimento de arquivos, inclusive à urna eletrônica. Qualquer brasileiro acima de 18 anos pode se candidatar a realizar planos de ataque às urnas eletrônicas e sistemas de apoio.

O TPS envolve várias etapas, desde a apresentação dos planos de ataque, apresentação do sistema aos investigadores e abertura do código, até o período de ataque propriamente dito, finalizando meses depois, quando o TSE convida os envolvidos para testar novamente o sistema e verificar se as falhas foram corrigidas. Quando um investigador ou equipe tem sucesso no respectivo plano de ataque, todos ganham, pois a falha será corrigida e o sistema se tornará cada vez mais seguro.

A primeira edição do Teste Público de Segurança ocorreu em 2009. Ao todo, já foram realizadas seis edições do TPS. Todas as vulnerabilidades encontradas pelos participantes do evento foram corrigidas e as barreiras de segurança do sistema foram aprimoradas.

SUBSISTEMA DE INSTALAÇÃO E SEGURANÇA (SIS)

Trata-se de uma infraestrutura instalada em computadores desktop com Windows para fornecer a instalação segura de sistemas da Justiça Eleitoral e a autenticação de usuários. As principais barreiras implantadas são criptografia e assinatura digital em diversos pontos e variados meios de controle de acesso, além de fazer o controle de versão dos sistemas desktop.

Ele é um dos diversos conjuntos de componentes de segurança que fazem a operacionalidade de parte dos sistemas eleitorais, auxiliando na geração de mídias da urna eletrônica. Assim, o SIS é um dos sistemas que ajudam a garantir a integridade e a segurança de todo o sistema eletrônico de votação brasileiro.

O SIS faz parte dos componentes a serem analisados pelos investigadores que atuam durante o Teste Público de Segurança (TPS) do Sistema Eletrônico de Votação.

O TPS é um evento fixo no calendário eleitoral – previsto na Resolução TSE nº 23.444 –, em que qualquer brasileira ou brasileiro pode apresentar um plano de ataque aos sistemas eleitorais envolvidos na geração de mídias, votação, apuração, transmissão e recebimento de arquivos, incluindo a própria urna eletrônica.

O TPS envolve várias etapas, desde a apresentação dos planos de ataque, apresentação do sistema aos investigadores e abertura do código, até o período de ataque propriamente dito, finalizando meses depois, quando o TSE convida os envolvidos para testar novamente o sistema e verificar se as falhas foram corrigidas.

URNA TRUSTED-DRE

A classificação de urnas em gerações é uma tentativa de enumerar diferentes tipos de urnas em uma sequência que pode levar a uma aludida evolução. Contudo, os equipamentos e sistemas para capturar o voto são muito diferentes no mundo.

A urna eletrônica é um microcomputador de uso específico para eleições, com as seguintes características: resistente, de pequenas dimensões, leve, com autonomia de energia, com diversos recursos de segurança e de fabricação brasileira. Normalmente se classifica a urna brasileira como DRE (Direct Recording Electronic), mas tal classificação não é adequada. Isso porque a urna eletrônica brasileira tem uma arquitetura única no mundo, denominada T-DRE ou Trusted-DRE, com o conceito inicial publicado em artigo científico em 2010. Essa arquitetura vem sendo implementada desde o modelo 2009 e evoluída desde então.

Assim, por ser de tecnologia própria da Justiça Eleitora brasileira, o modelo do equipamento não se enquadra nas classificações de 1ª, 2ª ou 3ª geração. Ela é segura, muito moderna e atende a inúmeros sistemas de verificação e possibilidade de auditoria.

Eleições 2022

Nas Eleições 2022, os eleitores contarão com novas urnas eletrônicas protegidas pela tecnologia de hardware com os mesmos requisitos da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil. São mais de 200 mil urnas do modelo UE 2020 que já sairão da fábrica protegidas por esse novo equipamento certificado.

Continuamente atualizada e modernizada, a cadeia de segurança da urna eletrônica – sistema que garante que as urnas executem somente softwares desenvolvidos e assinados digitalmente pelo Tribunal Superior Eleitoral (TSE) – foi introduzida em 2009, utilizando uma infraestrutura de certificados própria da Justiça Eleitoral. Agora essa estrutura será reforçada por uma certificação que avalia a aderência do perímetro criptográfico da urna eletrônica em relação aos requisitos mínimos definidos pelo Instituto Nacional de Tecnologia da Informação (ITI), que é responsável por manter a Autoridade Certificadora Raiz da ICP-Brasil.

VOTO SECRETO

O voto secreto é a garantia de que apenas o votante saberá qual foi a candidata ou o candidato escolhido naquele processo eleitoral. O sigilo do voto é uma forma de evitar pressão e impedir a coação, garantindo que o voto expresse realmente a vontade da eleitora ou do eleitor.

Por isso, no dia da eleição, ao votar, é proibido o ingresso na cabine de votação portando aparelho celular ou qualquer outro equipamento que possa registrar o voto. Essa proibição foi incluída na Lei das Eleições a partir de 2009 e está em vigor desde então.

O fato de o voto ser sigiloso não impede o uso da liberdade de expressão. No dia da votação, a cidadã ou o cidadão pode manifestar apoio às propostas dos partidos ou dos candidatos silenciosamente, indicando a preferência política. Mas é importante lembrar que o voto é um direito de cada pessoa e deve ser exercido de forma secreta para a escolha dos representantes políticos.

O voto secreto é aquele no qual somente o eleitor sabe em quem votou, garantindo que os candidatos escolhidos sejam de sua vontade e sem qualquer tipo de coerção. Por isso, também não é permitido que o eleitor leve consigo qualquer prova de seu voto, para que não possa ser coagido, intimidado ou mesmo usar tal prova em um acordo para vender seu voto. É um dispositivo constitucional considerado cláusula pétrea, pois não pode ser modificado nem mesmo por Proposta de Emenda à Constituição. O sigilo do voto é a base para a liberdade de escolha e um dos pilares do sistema democrático e, por ser tão importante, nem o próprio eleitor pode abdicar desse direito.

ZERÉSIMA

No dia da eleição, o ponto de partida para começar a votação é a impressão da zerézima. Funciona assim: antes de o primeiro eleitor se dirigir à urna eletrônica para votar em cada uma das seções eleitorais do país, o presidente da mesa já deverá ter ligado o equipamento, na presença dos mesários e fiscais de partidos políticos, para imprimir o relatório da zerésima.

Esse documento contém toda a identificação da urna. Comprova que nela estão registrados todos os candidatos e que não há voto computado para nenhum deles. Ou seja, confirma que a urna tem "zero votos". Após a impressão da zerésima, o presidente da seção eleitoral, os mesários e os fiscais dos partidos ou coligações que estiverem presentes devem assiná-la.

Esta obra foi composta na fonte Myriad Pro, corpo 11,
entrelinhas de 15 pontos, em papel Couché fosco 90g (miolo)
e papel Couché fosco 250g (capa).


90 ANOS DA
JUSTIÇA
ELEITORAL
90 ANOS EM AÇÃO PELA DEMOCRACIA


Tribunal
Superior
Eleitoral