TRIBUNAL SUPERIOR ELEITORAL

Ofício GAB-SPR nº 537/2022

Brasília, 10 de fevereiro de 2022.

A Sua Excelência o Senhor
General de Divisão HEBER GARCIA PORTELLA
Centro de Defesa Cibernética do Comando de Defesa Cibernética do Exército Brasileiro
Integrante da Comissão de Transparência das Eleições

Referência: Ofícios nºs 001, 002, 003 e 004/2021. NUP: 65298.001410/2021-68
Assunto: Processo Eleitoral Brasileiro

Senhor General de Divisão,

Encaminho as respostas referentes aos questionamentos apresentados pelo Ministério da Defesa, decorrente da necessidade identificada por aquele órgão de ampliar o conhecimento sobre o processo eleitoral brasileiro, a fim de permitir que seu representante na Comissão de Transparência das Eleições (CTE) possa opinar com mais assertividade sobre o assunto.

Os temas suscitados nas perguntas são de grande relevância e fazem parte das nossas reflexões, aquisições e programações futuras. Desnecessário enfatizar que as informações que envolvem a *cibersegurança* dos sistemas do Tribunal precisam ser tratadas com o máximo de reserva, para não se criarem vulnerabilidades ou se facilitarem ataques. Infelizmente, há maus precedentes nessa matéria. De fato, como é público, há uma investigação policial em curso, em razão de vazamento de informação constante de processo sigiloso, atribuído ao Excelentíssimo Senhor Presidente da República (Inquérito nº 4.878/DF, Rel. Min. Alexandre de Moraes). O fato delituoso em apuração consistiu na divulgação, em redes sociais, de documentos produzidos em investigação sigilosa envolvendo ataque hacker contra o Tribunal Superior Eleitoral (TSE). Informações sensíveis, que facilitam a atuação criminosa, foram divulgadas em rede mundial.

Dessa forma, não constam deste documento detalhes que possam viabilizar ataques aos sistemas da Justiça Eleitoral, de modo que esclarecimentos complementares podem ser prestados em reuniões agendadas entre os técnicos da área de Defesa Cibernética do Ministério da Defesa e a equipe da Secretaria de Tecnologia da Informação do TSE.

Seguem as respostas elaboradas com apoio da equipe técnica deste Tribunal Superior, as quais se referem a quatro documentos submetidos pelo Ministério da Defesa, a saber:

- Ofício nº 001 (SEI 1873478) – contendo 27 petições de listagens, normativos, relatórios e documentos;
- Ofício nº 002 (SEI 1873497) – contendo 5 questionamentos não numerados;
- Ofício nº 003 (SEI 1886913) – contendo questões numeradas de 1 a 5. Ressalte-se que o Ofício nº 3 reproduz o teor do Ofício nº 2, de modo que as respostas não serão replicadas; e
- Ofício nº 004 (SEI 1886914) – contendo questões numeradas de 6 a 48.

Atenciosamente,

LUÍS ROBERTO BARROSO
PRESIDENTE

Documento assinado eletronicamente em **10/02/2022, às 15:02**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

90 ANOS DA JUSTIÇA ELEITORAL

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1926563&crc=E3D93C1C, informando, caso não preenchido, o código verificador **1926563** e o código CRC **E3D93C1C**.

RESPOSTAS AO OFÍCIO nº 001

1. Organograma, incluindo os responsáveis pelas estruturas de Tecnologia da Informação do TSE.

Resposta: O documento em tela é público e pode ser obtido a partir do link:

https://www.tse.jus.br/o-tse/sobre-o-tse/contatos-organograma (ANEXO 01).

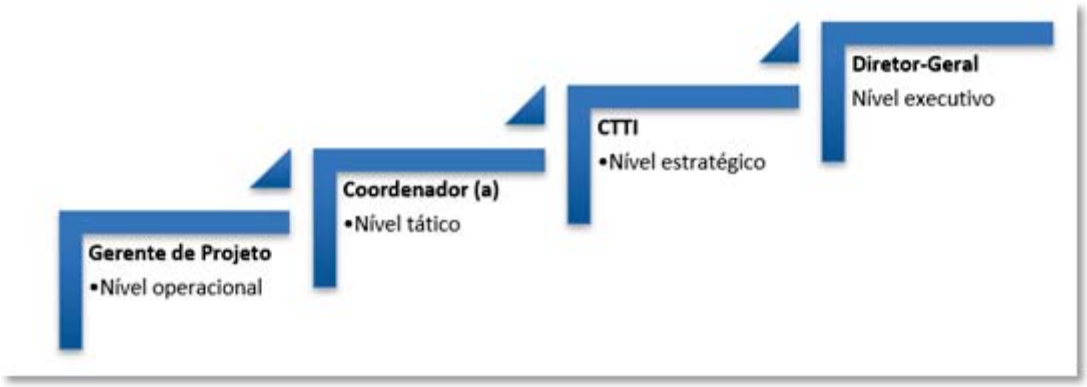
2. Norma de Gestão de Riscos relacionada à Gestão de Segurança da Informação do TSE.

Resposta: O Tribunal Superior Eleitoral (TSE) possui uma Política de Gestão de Riscos (ANEXO 02), disponível a partir do link: https://www.tse.jus.br/legislacao/compilada/prt/2017/portaria-no-784-de-20-de-outubro-de-2017.

Essa Política foi instituída formalmente pela Portaria TSE nº 784, de 20 de outubro de 2017. O processo de gestão de riscos no TSE é tratado de forma sistematizada e adota as boas práticas preconizadas nas estruturas das normas COSO II ERM e ABNT ISO 31.000:2009.

Com o objetivo de apoiar a alta administração e demais gestores do Tribunal na gestão de riscos, foi elaborado o Manual de Gestão de Riscos do TSE, em 2018. Esse manual foi revisado em 2021 e, atualmente, está em fase de aprovação pelo Comitê de Gestão de Riscos.

No âmbito da Secretaria de Tecnologia da Informação (STI), de forma alinhada à Portaria TSE nº 784/2017 e ao Manual de Gestão de Riscos do TSE, foi elaborado o Manual de Gestão de Riscos de Projetos de TI e o Guia Operacional de Gestão de Riscos na STI, que tratam, respectivamente, da gestão do risco no ciclo de vida dos projetos de TI e do registro estruturado do risco na ferramenta EPM (Enterprise Project Management), contemplando as etapas de identificação, análise, tratamento e monitoramento do risco. Dentro do processo de gestão de riscos de projetos de TI, é possível escalonar um risco às esferas hierárquicas superiores e às comissões ou comitês deliberativos, para conhecimento e determinação de ações de respostas específicas que extrapolam o escopo de atuação dos níveis mais baixos. Esse escalonamento está dividido em quatro níveis, a saber: Operacional, Tático, Estratégico e Executivo, conforme descrito na imagem a seguir.

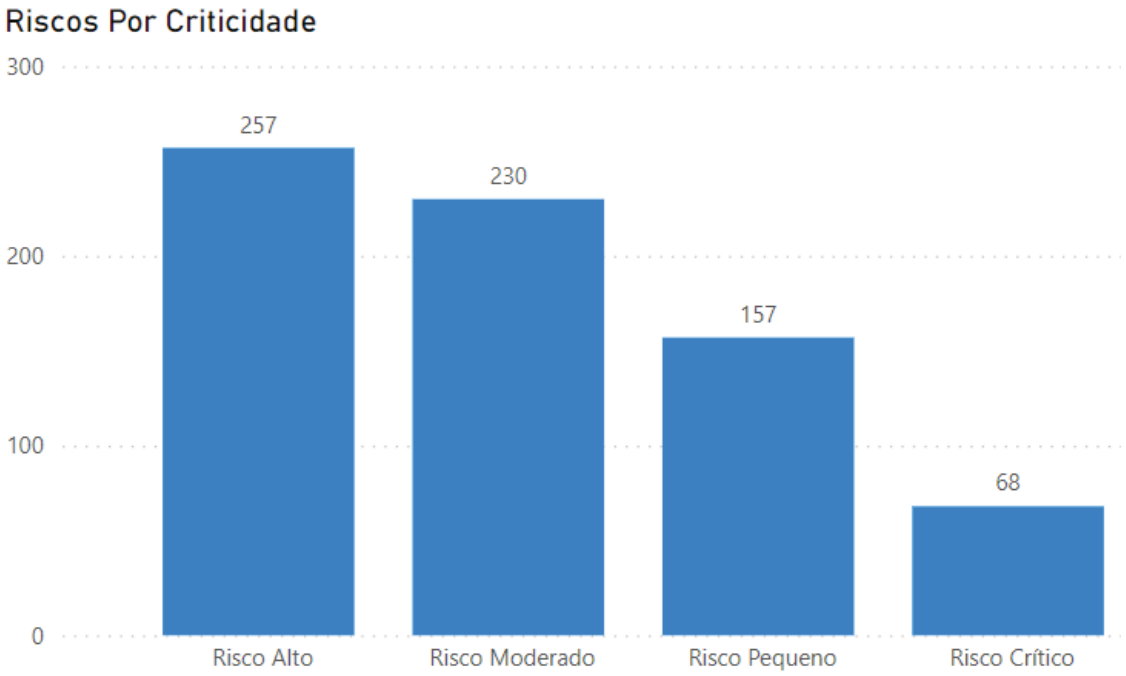


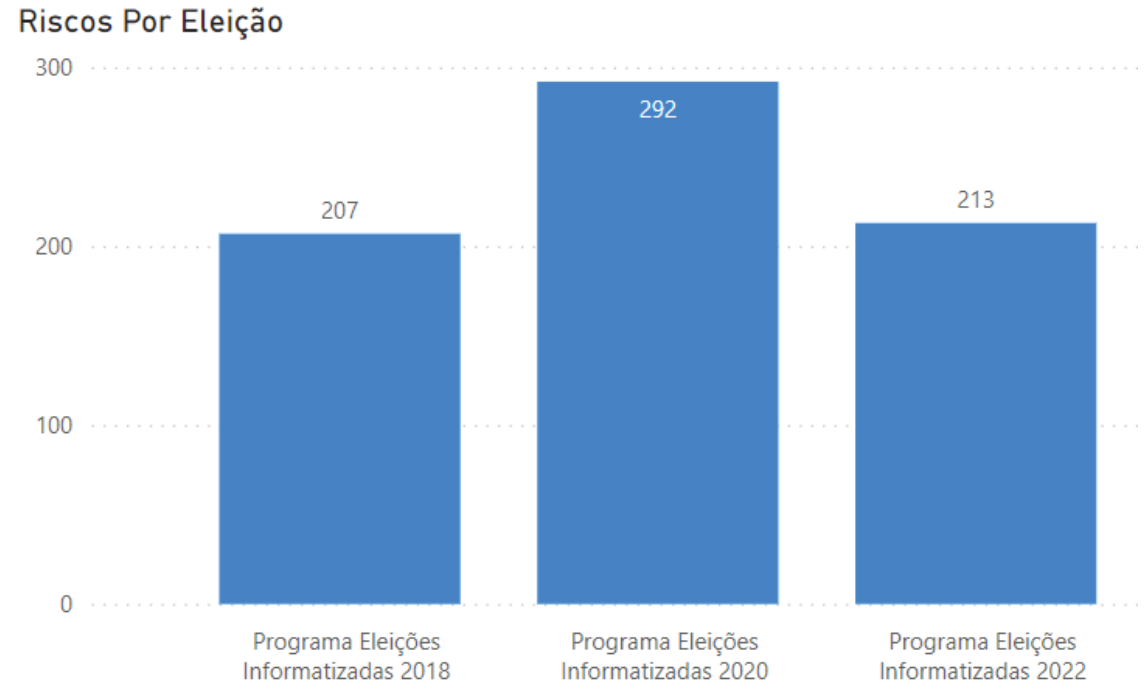
O Diretor-Geral pode, se assim entender, escalonar o risco para o nível de CDTI – Comissão Diretiva de TI ou ainda para o Ministro Presidente do TSE.

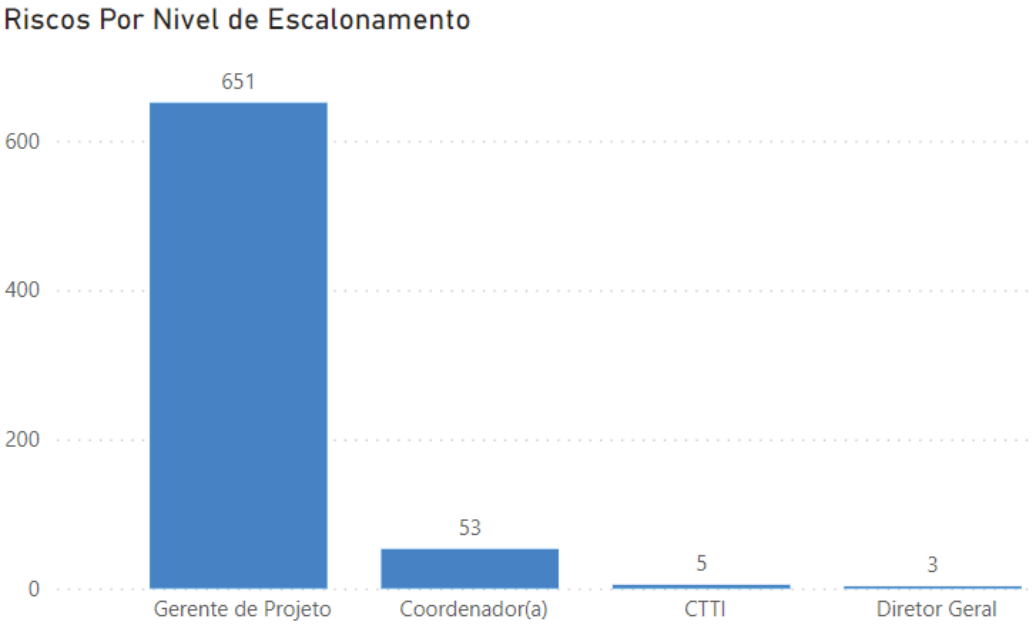
3. Relatório de Riscos do TSE dos últimos 4 anos.

Resposta: Todos os riscos identificados no âmbito de projetos de TI do TSE encontram-se registrados na ferramenta de Gestão de Projetos (EPM), desde sua identificação até o seu efetivo tratamento, com histórico de escalonamento e medidas de contingência.

Segue quadro resumo do quantitativo de riscos registrados nas eleições de 2018, 2020 e 2022 (até o presente momento):







4. Política de Segurança da Informação (PSI) do TSE.

Resposta: A política de segurança da informação do TSE foi instituída pela Res.-TSE nº 23.644 (ANEXO 03), que pode ser obtida por meio do link:

https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021

5. Todos os normativos que suportam a política de segurança da informação (PSI) do TSE.

Resposta: Entendemos que os normativos requeridos são aqueles relacionados nas perguntas seguintes, à exceção da composição da Comissão de Segurança da Informação, Portaria TSE nº 157/2020 (ANEXOS 04 e 05), que pode ser obtida por meio do link:

https://www.tse.jus.br/legislacao/compilada/prt/2020/portaria-no-157-de-4-de-marco-de-2020

6. Política de Antivírus do TSE.

Resposta: O TSE possui solução de antivírus contratada para toda a Justiça Eleitoral (contemplando o próprio TSE e todos os Tribunais Regionais Eleitorais), abrangendo todo o seu parque de servidores de rede, para os quais também há a funcionalidade de XDR (*Extended Endpoint Detection and Response*) e estações de trabalho, para as quais há a funcionalidade de EDR (*Endpoint Detection and Response*).

A efetiva configuração da solução pode ser consultada, com apoio da Coordenadoria de Infraestrutura, nas dependências do TSE.

Do ponto de vista normativo, a Política de Segurança da Informação da Justiça Eleitoral estabelece como um de seus objetivos "*definir as ações necessárias para evitar ou mitigar os efeitos de atos acidentais ou intencionais, internos ou externos, de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição*", que dá o suporte para a adoção de soluções como o antivírus.

Por sua vez, a Portaria TSE nº 455/2021 (ANEXO 06), que institui a norma de configuração segura de ambientes, complementa a questão do antivírus no tocante às configurações de segurança que devem ser aplicadas sobre os diversos ativos de TI para alcançar o nível de segurança adequado.

7. Política de Auditoria e Registro de Logs do TSE.

Resposta: Portaria TSE nº 459/2021 (ANEXO 07), que pode ser obtida por meio do link:

https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-459-de-13-de-julho-de-2021

8. Política de Backup do TSE.

Resposta: A política de backup do TSE foi instituída pela Portaria TSE nº 457/2021 (ANEXO 08), que pode ser obtida por meio do link:

https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-457-de-13-de-julho-de-2021

9. Política de Continuidade de Negócio do TSE.

Resposta: O Tribunal Superior Eleitoral aprimora rotineiramente seus procedimentos de forma a garantir a continuidade de negócio, identificando e priorizando os mais críticos, dentre eles, a realização das eleições brasileiras.

A cada ciclo eleitoral os sistemas são atualizados, aprimorados e, antes de serem submetidos à assinatura digital e lacração, passam por baterias de testes locais, testes em campo, testes de desempenho e simulados nacionais que garantem o pleno e bom funcionamento desses. Além disso, antes de serem utilizados pelos eleitores, são ainda submetidos ao Teste Público de Segurança, que visa aprimorar os aspectos de segurança da informação.

Assim como os sistemas, também os dados sensíveis ao processo eleitoral, tais como: o cadastro de eleitores, a filiação partidária, e o registro de candidaturas, entre outros tantos, estão submetidos à Política de Segurança da Informação, ou seja, protegidos contra ataques internos e externos, submetidos à política de backup, preservados para garantir que as eleições transcorram dentro do esperado pela sociedade brasileira.

Da mesma forma que dados e sistemas eleitorais, outro insumo importante para a realização das eleições é a urna eletrônica. Essa por sua vez também é objeto de observação quando da realização dos testes dos sistemas e, especialmente para ela, a Justiça Eleitoral realiza um evento denominado Simulado Nacional de Hardware (SNH), quando uma significativa

quantidade de equipamentos é submetida a processos diversos de testes objetivando antecipar e corrigir qualquer problema que possa vir a se manifestar no dia das eleições. O TSE realiza vários eventos de SNH durante um mesmo ciclo eleitoral. Ainda assim, a Justiça Eleitoral dispõe de uma reserva técnica de equipamentos, denominadas urnas de contingência, que, de acordo com a logística de cada tribunal regional eleitoral, ficam dispostas em locais estratégicos para substituírem qualquer equipamento danificado. Ao longo dos últimos anos, a insignificante quantidade de seções eleitorais que no dia das eleições necessitam passar para o processo manual de votação demonstra a eficácia das medidas de continuidade adotadas, lembrando que o uso de urnas de lona, caso não seja possível prosseguir com a votação eletrônica na seção eleitoral, também é uma medida de continuidade adotada.

Ainda no dia das eleições, finalizada a votação, restam os processos de transmissão dos arquivos de urna, de totalização de votos e de divulgação de resultados, que por sua vez, também estão amparados por medidas que visam garantir a continuidade das eleições, medidas essas aprimoradas com a centralização da totalização no Tribunal Superior Eleitoral que passou a dispor de redundância de elementos que compõem uma infraestrutura tecnológica, sobre a qual é executado um processo de trabalho, item essencial para trazer robustez e confiabilidade à execução do processo. No caso de falha em um componente da infraestrutura, o elemento redundante é acionado como contingência ao componente falhado, mantendo-se ativo e o processo operacional, até que o componente principal possa ser restaurado.

Com a centralização da totalização no TSE, o tribunal passou a dispor de:

Servidores de banco de dados	1 equipamento principal: contingência primária com 8 servidores redundantes totalizando 384 núcleos de processamento; 1 equipamento de contingência secundária, com 4 servidores totalizando 192 núcleos de processamento Contingência adicional mediante cópia de segurança; Plantão de equipe do fabricante nas dependências do TSE para pronto atendimento.

Servidores de aplicação	40 equipamentos de 40 núcleos de processamento; Contingência primária por meio de hiperconvergência e VCloud; Contingência secundária mediante snapshots e backup Contingência adicional mediante cópia de segurança;

	Plantão de equipe do fabricante nas dependências do TSE para pronto atendimento.

Firewall	2 equipamentos mais robustos Redundância ativo-ativo Contingência adicional mediante cópia de segurança; Plantão de equipe do fabricante nas dependências do TSE para pronto atendimento.

Backbone Principal	54 enlaces com os TRE Um enlace principal com protocolo MPLS Um enlace de contingência com protocolo IP Redundância ativo-ativo mediante uso de SD-Wan Plantão das operadoras no ambiente do TSE e nos TRE para pronto atendimento.

No dia das eleições, como medida para garantir a continuidade do processo eleitoral, todos os fornecedores cujos produtos e serviços são estratégicos para garantir o bom andamento dos pleitos, são convidados a compor e manter equipe gerencial e técnica nas instalações do tribunal, intervindo em tempo real no caso de qualquer suporte emergencial necessário.

Além desses, outros tantos exemplos podem ser listados, tais como:

– Existência de uma sala-cofre certificada pela norma ABNT NBR 15.247, que protege o TSE contra vandalismo, ocorrências físicas de incêndio, alagamento, possivelmente queda do prédio etc.;

– Portal do TSE reduzido à prestação de serviços essenciais e inerentes às eleições;

– Acordo de Cooperação Técnica firmado com as Forças Armadas para atuação de apoio à Justiça Eleitoral;

– Participação em gabinetes de crise de segurança instituídos por órgãos públicos envolvidos no processo eleitoral;

– Contratação de uma rede de distribuição de conteúdo visando desafogar o site do TSE, dispondo de forma automática das parciais do resultado das eleições para todos os órgãos de imprensa;

– Montagem de um Centro de Divulgação Eleitoral com a participação dos órgãos de imprensa, propiciando um rápido trânsito das informações no dia das eleições.

10. Política de Gestão de Ativos da Segurança da Informação do TSE.

Resposta: A política de gestão de ativos de segurança da informação foi instituída pela Portaria TSE nº 458/2021 (ANEXO 09), que pode ser obtida por meio do link:

https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-458-de-13-de-julho-de-2021

11. Política de Gestão de Identidade de Acesso (AAA) do TSE.

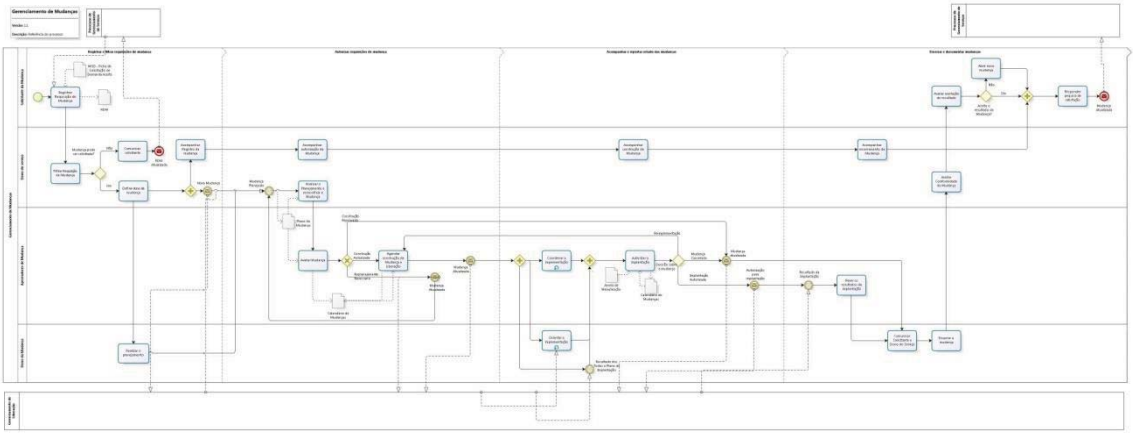
Resposta: A política de gestão de identidade de acesso foi instituída pela Portaria TSE nº 454/2021 (ANEXO 10), que pode ser obtida por meio do link:

https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-454-de-13-de-julho-de-2021

12. Política de Gestão de Mudanças do TSE.

Resposta: O gerenciamento de mudanças no TSE está implementado por meio de processo de trabalho. A ferramenta GSTI – Gestão de Serviços de TI foi customizada para manter os devidos registros e atender aos procedimentos estabelecidos no processo.

Abaixo, a visão do processo de Gestão de Mudanças de TI.



Em anexo, documento com Visão Geral do Processo de Gerenciamento de Mudanças do TSE.

13. Política de Gestão de Vulnerabilidades do TSE.

Resposta: A política de gestão de vulnerabilidades foi instituída pela Portaria TSE nº 460/2021 (ANEXO 11), que pode ser obtida por meio do link:

https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-460-de-13-de-julho-de-2021

14. Política de Privacidade do TSE.

Resposta: A política de privacidade é objeto da Res.-TSE nº 23.650/2021 (ANEXO 12), que pode ser obtida por meio do link:

https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-650-de-9-de-setembro-de-2021

15. Política de Senha do TSE.

Resposta: A política de senha é regulamentada pela Portaria TSE nº 454/2021 (ANEXO 13), que pode ser obtida por meio do link:

https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-454-de-13-de-julho-de-2021

16. Política de Uso Aceitável de TI do TSE.

Resposta: A política de uso aceitável de TI do TSE foi instituída pela Portaria TSE nº 456/2021 (ANEXO 14), que pode ser obtida por meio do link:

https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-456-de-13-de-julho-de-2021

17. Relatório de Análise de Impacto de Negócio relacionado à Gestão de Segurança da Informação do TSE.

Resposta: Estão em execução as Análises de Impacto de Negócio (AIN) sobre os sistemas/processos Cadastro Eleitoral, Biometrias e PJe, com previsão de finalização no final do mês de fevereiro de 2022.

18. Mapeamento dos Processos Críticos dos Sistemas que suportam o Processo Eleitoral.

Resposta: Os processos eleitorais críticos suportados pelos sistemas informatizados estão normatizados e descritos nas resoluções de atos gerais do processo eleitoral e fiscalização e auditoria do sistema eletrônico de votação (respectivamente, Resoluções TSE nºs 23.611/2019 e 23.603/2019, referentes às eleições de 2020, ANEXOS 15 e 16). As referidas resoluções detalham diversos processos, tais como: preparação e carga de urna, votação e justificativa, apuração, totalização, verificação de integridade e autenticidade dos sistemas eleitorais, lacração, dentre outros.

19. Documentação de Requisitos de Software (requisitos funcionais, não funcionais etc) dos Sistemas que suportam o Processo Eleitoral.

Resposta: A documentação dos requisitos funcionais e não funcionais dos sistemas eleitorais é mantida de forma eletrônica em ferramentas de apoio às atividades de desenvolvimento de software e atualizada frequentemente. O acesso a tais documentos é viabilizado durante a fase de inspeção de código-fonte a seguir contextualizada:

O Tribunal Superior Eleitoral, em atenção ao art. 66 da Lei nº 9.504/1997, regulamentado pela Res.-TSE nº 23.673, de 14 de dezembro de 2021 (ANEXO 17), fornece aos

representantes das entidades fiscalizadoras a possibilidade de acompanhar e inspecionar a especificação e o desenvolvimento dos sistemas eleitorais, oportunidade em que têm acesso à documentação e ao código fonte dos sistemas, observando-se as condições descritas na norma.

> Art. 9º É garantido, às entidades fiscalizadoras, a partir de 12 (doze) meses antes do primeiro turno das eleições, o acesso antecipado aos sistemas eleitorais desenvolvidos pelo TSE e o acompanhamento dos trabalhos para sua especificação e desenvolvimento, para fins de fiscalização e auditoria, em ambiente específico e sob a supervisão do Tribunal.

O rol de entidades fiscalizadoras legitimadas a participar da fase de inspeção está descrito nos arts. 6º e 9º da referida Resolução:

> Art. 6º Para efeito dos procedimentos previstos nesta Resolução, salvo disposição específica, são consideradas entidades fiscalizadoras, legitimadas a participar das etapas do processo de fiscalização:
> I - Partidos políticos, federações e coligações;
> II - Ordem dos Advogados do Brasil;
> III - Ministério Público;
> IV - Congresso Nacional;
> V - Supremo Tribunal Federal;
> VI - Controladoria-Geral da União;
> VII - Polícia Federal;
> VIII - Sociedade Brasileira de Computação;
> IX - Conselho Federal de Engenharia e Agronomia;
> X - Conselho Nacional de Justiça;
> XI - Conselho Nacional do Ministério Público;
> XII - Tribunal de Contas da União;
> XIII - Forças Armadas;
> XIV - Confederação Nacional da Indústria, demais integrantes do Sistema Indústria e entidades corporativas pertencentes ao Sistema S;
> XV - Entidades privadas brasileiras, sem fins lucrativos, com notória atuação em fiscalização e transparência da gestão pública, credenciadas junto ao TSE; e
> XVI - Departamentos de tecnologia da informação de universidades credenciadas junto ao TSE.

> Art. 9º (...) § 3° As pessoas participantes do TPS devem manifestar à STI/TSE o interesse em acompanhar a fase de especificação e desenvolvimento dos sistemas eleitorais antes de seu primeiro comparecimento ao Tribunal.

Sendo assim, o conjunto de informações solicitadas pelo Ministério da Defesa está disponível para verificação, nas instalações do TSE, desde a abertura do prazo de acompanhamento da inspeção dos sistemas em 04 de outubro de 2021.

Cabe esclarecer que é possível exportar a documentação em formato portável para que seja acessada em ambiente externo ao TSE, contudo há forte prejuízo na formatação e leiaute dos documentos. Nessa hipótese, é necessária solicitação específica e consequente deferimento por parte desta corte.

20. Documentação do Processo de Desenvolvimento de Software dos Sistemas que suportam o Processo Eleitoral.

Resposta: O TSE adota como norteador de seu modelo de desenvolvimento os princípios e valores ágeis. Em termos de métodos, adota-se, com adaptações típicas do modelo evolutivo, o Scrum, Kanban e técnicas como o XP. Os elementos que compõem esse processo de trabalho estão disponíveis em portal hospedado na intranet do Tribunal, não existindo um documento físico. A apresentação desses elementos pode ser realizada aos interessados bastando agendamento prévio.

21. Documentação do Processo de Auditoria de Software dos Sistemas que suportam o Processo Eleitoral.

Resposta: Os processos eleitorais críticos suportados pelos sistemas informatizados estão normatizados e descritos nas resoluções de atos gerais do processo eleitoral e fiscalização e auditoria do sistema eletrônico de votação (respectivamente, Resoluções TSE nºs 23.611/2019 e 23.603/2019, referentes às eleições de 2020, ANEXOS 15 e 16). As auditorias aplicáveis estão estabelecidas especificamente na Res.-TSE nº 23.673/2021 (ANEXO 17).

22. Lista com todas as versões do ramo principal (master) dos Sistemas que suportam o Processo Eleitoral, destacando as versões utilizadas em eleições.

Resposta: O conjunto de sistemas que suportam todo o processo eleitoral é compreendido por uma gama de produtos que vão desde sistemas de alistamento eleitoral, registro de candidatura, análise de prestação de contas, filiação de eleitor e outros até votação e totalização. A fim de delimitar o escopo do pedido das questões 22, 23 e 24, serão apresentados os dados referentes aos sistemas utilizados nas urnas eletrônicas, apuração e totalização, nos termos do art. 66, § 1º, da Lei nº 9.504/1997, abaixo transcrito:

> § 1º Todos os programas de computador de propriedade do Tribunal Superior Eleitoral, desenvolvidos por ele ou sob sua encomenda, utilizados nas urnas eletrônicas para os processos de votação, apuração e totalização, poderão ter suas fases de especificação e de desenvolvimento acompanhadas por técnicos indicados pelos partidos políticos, Ordem dos Advogados do Brasil e Ministério Público, até seis meses antes das eleições. (Redação dada pela Lei nº 10.740, de 2003)

Segue lista das versões dos referidos sistemas utilizados nas eleições de 2020:

- Uenux 7.34.1.0
- Criptosevin 1.2.4.1
- Holocron 1.0.7.1
- HotSwapFlash 5.4.5.0
- Gedai-UE 5.26.5.0
- SAVP-Sorteio 4.17.0.2
- SAVP-Votação 4.17.0.1
- Sistot 20.11.10
- RecArquivos 20.10.6
- InfoArquivos 20.10.4
- Transportador 20.10.2

23. Relatório com quantidade de linhas de código (sem contar comentários) e quantidade de arquivos dos Sistemas que suportam o Processo Eleitoral.

Resposta: Ainda sobre os sistemas eleitorais do ecossistema da urna e da totalização disponíveis durante a apresentação de código-fonte de que trata a resolução de fiscalização e auditoria, seguem as informações de quantidade de linhas de código e arquivos por repositório:

Repositório	Quantidade de arquivos	Quantidade de linhas de código sem considerar os comentários
Uenux - API e aplicativos	7.472	839.199
Uenux-kernel - kernel do Linux, módulos e bootloader Syslinux (código original e adaptações)	45.942	17.842.904
libtpm - biblioteca de acesso ao TPM	113	51.738
CriptoSevin - driver monitor do ambiente Windows	38	3.297
Holocron	141	10.710
Gedai-EU	725	73.060
SAVP-Votação	349	28.079
SAVP-Sorteio	267	23.748
libdesktop - biblioteca de uso comum dos aplicativos deskotp	1.842	198.133
libecourna - biblioteca de uso comum entre o Uenux e o desktop	1.184	73.949
HotSwapFlash	157	11.132
info-arquivos-urna	77	2.315
rec-arquivos-urna	139	6.283
sistema-gerenciador-totalizacao	145	4.510
sistema-totalizacao	2.070	777.866
sistot-frontend	29.745	4.015.670
transportador-backend	135	6.581
transportador-desktop	257	25.154
transportador-frontend	168	11.841
comum-raiz	2	126
info-arquivos-negocio	18	534
infra-aplicacao	9	286
infra-arquivo-urna	202	10.286
infra-calcula-hash-t0	4	104
infra-carimbo-tempo	133	4.198
infra-certificado-digital	19	939
infra-chaves-privadas	12	1.009
infra-chaves-publicas	178	11.615
infra-comunicador-desafio	6	295
infra-contexto	16	470
infra-datasource	18	779
infra-eleicao	17	867
infra-exec	9	220
infra-fabrica-arquivo-urna	44	2.863
infra-fabrica-pacotes-integracao	118	9.809
infra-filtro-seguranca	13	1.068
infra-gerador-arquivo-simulado	97	3.658
infra-integracao-contratos-asn1-totalizacao	87	3.281
infra-integracao-mensageria	72	2.563
infra-io	44	1.091

infra-localidade-eleitoral	29	3.425
infra-menu	20	1.165
infra-monitoramento-mensageria	44	1.434
infra-negocio	40	920
infra-negocio-modelo	13	1.886
infra-persistencia	7	143
infra-seguranca	40	2.890
infra-seguranca-cepesc	68	3.550
infra-serializacao-api	6	74
infra-serializacao-asn1	15	2.009
infra-struct-oracle	5	107
infra-struct-oracle-bu	28	1.094
infra-struct-oracle-transportador	7	189
infra-tot-comum	37	2.290
infra-transmissor-http	23	1.316
infra-util	8	265
setot-base	59	4.236
totalizacao-negocio	214	8.457
tot-base	333	15.817
Transportadorjni	8.461	1.158.947
transportador-negocio	11	344

24. Lista com bibliotecas e APIS utilizadas de terceiros dos Sistemas que suportam o Processo Eleitoral.

Resposta: Ainda sobre os sistemas eleitorais do ecossistema da urna e da totalização disponíveis durante a apresentação de código-fonte de que trata a resolução de fiscalização e auditoria, segue lista das bibliotecas de terceiros utilizadas:

- Linux Kernel versão 5.4.77
- Syslinux versão 6.04/3.62
- openssl versão 1.1.1l
- zlib versão 1.2.11
- libsodium versão 1.0.18
- boost versão 1.77.0
- sqlite3 versão 3.36.0
- gtest versão 1.11.0
- cepesc versão 8.3.4.2
- iiiasn1 versão 2.12
- liblzma versão 1.9
- e2fsprogs versão 1.44.5.2

- futronic versão 1.0.1.2
- libusblpfu versão 1.1
- libcap versão 2.26
- libjpeg versão 9d
- aes versão 1.0
- dppiv versão 3.0.14
- dpfd versão 1.1.2
- espeak-ng versão 1.50
- MBROLA versão 3.3
- mbrola-voices versão 3.02b.1
- libgpiod versão 1.2.1
- libbio versão 1.0.3.18
- libusb versão 1.0.24
- libusb-compat versão 0.1.7
- freetype versão 2.11.0
- libcap versão 2.26
- nbis versão 5.0.0
- libqrencode versão 4.1.1
- libalsa versão 1.2.5.1
- c-mock versão 0.4.0
- libssh2 versão 1.10.0
- libcurl versão 7.78.0
- qt versão 5.15.2
- antlr:antlr versão(ões) 2.7.6; 2.7.7
- aopalliance:aopalliance versão(ões) 1.0
- avalon-framework:avalon-framework versão(ões) 4.1.3
- biz.paluch.logging:logstash-gelf versão(ões) 1.14.1
- br.gov.cepesc.lib.linux-amd64:avclinux-x86-64:so versão(ões) 8.3.4
- br.gov.cepesc.lib.linux-amd64:avdlinux-x86-64:so versão(ões) 8.3.4
- br.gov.cepesc.lib.linux-amd64:avlinux-x86-64:so versão(ões) 8.3.4
- br.gov.cepesc.lib.win-amd64:avwinc-x86-64:dll versão(ões) 8.3.4
- br.gov.cepesc.lib.win-x86:avwinc-x86:dll versão(ões) 8.3.4

- cglib:cglib-nodep versão(ões) 3.2.9
- com.beust:jcommander versão(ões) 1.48; 1.72
- com.experlog:xapool versão(ões) 1.5.0
- com.fasterxml.jackson.core:jackson-annotations versão(ões) 2.11.4; 2.13.0; 2.13.1
- com.fasterxml.jackson.core:jackson-core versão(ões) 2.11.4; 2.13.0; 2.13.1
- com.fasterxml.jackson.core:jackson-databind versão(ões) 2.11.4; 2.13.0; 2.13.1
- com.fasterxml.jackson.datatype:jackson-datatype-hibernate5 versão(ões) 2.11.4; 2.13.1
- com.fasterxml.jackson.datatype:jackson-datatype-jdk8 versão(ões) 2.11.4; 2.13.1
- com.fasterxml.jackson.datatype:jackson-datatype-jsr310 versão(ões) 2.11.4; 2.13.0; 2.13.1
- com.fasterxml.jackson.module:jackson-module-jaxb-annotations versão(ões) 2.11.4; 2.13.1
- com.fasterxml.jackson.module:jackson-module-parameter-names versão(ões) 2.11.4; 2.13.1
- com.fasterxml:classmate versão(ões) 1.5.1
- com.github.ben-manes.caffeine:caffeine versão(ões) 2.8.8; 2.9.3
- com.github.paweladamski:HttpClientMock versão(ões) 1.5.0
- com.github.tuupertunut:powershell-lib-java versão(ões) 2.0.0
- com.google.code.gson:gson versão(ões) 2.8.7; 2.8.9
- com.google.collections:google-collections versão(ões) 1.0
- com.google.errorprone:error_prone_annotations versão(ões) 2.10.0; 2.4.0
- com.google.guava:guava versão(ões) 16.0.1; 18.0
- com.google.inject:guice versão(ões) no_aop:4.0
- com.google.zxing:core versão(ões) 2.3.0
- com.googlecode.javaewah:JavaEWAH versão(ões) 1.1.6; 1.1.7
- com.goterl.lazycode:lazysodium-java versão(ões) 4.0.1
- com.h2database:h2 versão(ões) 1.4.196; 1.4.200
- com.ibm.icu:icu4j versão(ões) 57.1
- com.jayway.jsonpath:json-path versão(ões) 2.6.0; 2.4.0

- com.jcraft:jsch versão(ões) 0.1.55; 0.1.49
- com.jcraft:jzlib versão(ões) 1.1.1; 1.1.3
- com.lowagie:itext versão(ões) 2.1.7.js2; 2.1.7.js7
- com.oracle.jdbc:ojdbc8 versão(ões) 18.3.0.0
- com.sshtools:j2ssh-maverick versão(ões) 1.5.5
- com.sun.activation:jakarta.activation versão(ões) 1.2.2
- com.sun.istack:istack-commons-runtime versão(ões) 3.0.12
- com.sun.xml.bind:jaxb-impl versão(ões) 2.1.13
- com.sun.xml.messaging.saaj:saaj-impl versão(ões) 1.5.3
- com.zaxxer:HikariCP versão(ões) 3.4.5; 4.0.3
- commons-beanutils:commons-beanutils versão(ões) 1.9.0; 1.9.3.redhat-1; 1.9.4
- commons-beanutils:commons-beanutils-core versão(ões) 1.8.0
- commons-cli:commons-cli versão(ões) 1.3.1
- commons-codec:commons-codec versão(ões) 1.11; 1.15
- commons-collections:commons-collections versão(ões) 3.2.1; 3.2.2
- commons-configuration:commons-configuration versão(ões) 1.6
- commons-digester:commons-digester versão(ões) 1.8; 2.1
- commons-fileupload:commons-fileupload versão(ões) 1.3.3; 1.4; 1.3.3
- commons-io:commons-io versão(ões) 2.1; 2.2; 2.4; 2.6
- commons-lang:commons-lang versão(ões) 2.6
- commons-logging:commons-logging versão(ões) 1.1; 1.1.1; 1.2
- commons-net:commons-net versão(ões) 3.0.1; 3.6
- dom4j:dom4j versão(ões) 1.6.1
- eu.europa.ec.joinup.sd-dss:dss-asic versão(ões) 4.6.0
- eu.europa.ec.joinup.sd-dss:dss-cades versão(ões) 4.6.0
- eu.europa.ec.joinup.sd-dss:dss-diagnostic-jaxb versão(ões) 4.6.0
- eu.europa.ec.joinup.sd-dss:dss-document versão(ões) 4.6.0
- eu.europa.ec.joinup.sd-dss:dss-model versão(ões) 4.6.0
- eu.europa.ec.joinup.sd-dss:dss-pades versão(ões) 4.6.0
- eu.europa.ec.joinup.sd-dss:dss-service versão(ões) 4.6.0
- eu.europa.ec.joinup.sd-dss:dss-spi versão(ões) 4.6.0
- eu.europa.ec.joinup.sd-dss:dss-test versão(ões) 4.6.0

- eu.europa.ec.joinup.sd-dss:dss-token versão(ões) 4.6.0
- eu.europa.ec.joinup.sd-dss:dss-tsl-jaxb versão(ões) 4.6.0
- eu.europa.ec.joinup.sd-dss:dss-xades versão(ões) 4.6.0
- eu.europa.ec.joinup.sd-dss:validation-policy versão(ões) 4.6.0
- fr.bmartel:http-endec versão(ões) 1.04
- fr.bmartel:jspeedtest versão(ões) 1.32.1
- io.craftsman:dozer-jdk8-support versão(ões) 1.0.3
- io.micrometer:micrometer-core versão(ões) 1.8.1
- io.netty:netty-all versão(ões) 4.1.9.Final-redhat-1
- io.netty:netty-buffer versão(ões) 4.1.67.Final; 4.1.72.Final
- io.netty:netty-codec versão(ões) 4.1.67.Final; 4.1.72.Final
- io.netty:netty-codec-http versão(ões) 4.1.67.Final; 4.1.72.Final
- io.netty:netty-codec-socks versão(ões) 4.1.67.Final; 4.1.72.Final
- io.netty:netty-common versão(ões) 4.1.67.Final; 4.1.72.Final
- io.netty:netty-handler versão(ões) 4.1.67.Final; 4.1.72.Final
- io.netty:netty-handler-proxy versão(ões) 4.1.67.Final; 4.1.72.Final
- io.netty:netty-resolver versão(ões) 4.1.67.Final; 4.1.72.Final
- io.netty:netty-tcnative-classes versão(ões) 2.0.46.Final
- io.netty:netty-transport versão(ões) 4.1.67.Final; 4.1.72.Final
- io.netty:netty-transport-classes-epoll versão(ões) 4.1.72.Final
- io.netty:netty-transport-classes-kqueue versão(ões) 4.1.72.Final
- io.netty:netty-transport-native-epoll versão(ões) linux-x86_64:4.1.67.Final; linux-x86_64:4.1.72.Final
- io.netty:netty-transport-native-kqueue versão(ões) osx-x86_64:4.1.67.Final; osx-x86_64:4.1.72.Final
- io.netty:netty-transport-native-unix-common versão(ões) 4.1.67.Final; 4.1.72.Final
- io.reactivex.rxjava3:rxjava versão(ões) 3.0.4
- io.undertow:undertow-core versão(ões) 2.2.10.Final; 2.2.14.Final
- io.undertow:undertow-servlet versão(ões) 2.2.10.Final; 2.2.14.Final
- io.undertow:undertow-websockets-jsr versão(ões) 2.2.10.Final; 2.2.14.Final
- jakarta.activation:jakarta.activation-api versão(ões) 1.2.2

- jakarta.annotation:jakarta.annotation-api versão(ões) 1.3.5
- jakarta.jms:jakarta.jms-api versão(ões) 2.0.3
- jakarta.json:jakarta.json-api versão(ões) 1.1.6
- jakarta.jws:jakarta.jws-api versão(ões) 2.1.0
- jakarta.persistence:jakarta.persistence-api versão(ões) 2.2.3
- jakarta.servlet:jakarta.servlet-api versão(ões) 4.0.4
- jakarta.transaction:jakarta.transaction-api versão(ões) 1.3.3
- jakarta.validation:jakarta.validation-api versão(ões) 2.0.2
- jakarta.websocket:jakarta.websocket-api versão(ões) 1.1.2
- jakarta.ws.rs:jakarta.ws.rs-api versão(ões) 2.1.6
- jakarta.xml.bind:jakarta.xml.bind-api versão(ões) 2.3.3
- jakarta.xml.soap:jakarta.xml.soap-api versão(ões) 1.4.2
- jakarta.xml.ws:jakarta.xml.ws-api versão(ões) 2.3.3
- jakarta-regexp:jakarta-regexp versão(ões) 1.4
- javassist:javassist versão(ões) 3.12.1.GA
- javax.activation:activation versão(ões) 1.1; 1.1.1
- javax.activation:javax.activation-api versão(ões) 1.2.0
- javax.annotation:javax.annotation-api versão(ões) 1.3.2
- javax.el:javax.el-api versão(ões) 3.0.0
- javax.inject:javax.inject versão(ões) 1
- javax.jms:jms versão(ões) 1.1
- javax.json:javax.json-api versão(ões) 1.1.4
- javax.persistence:javax.persistence-api versão(ões) 2.2
- javax.servlet.jsp:jsp-api versão(ões) 2.1
- javax.servlet:javax.servlet-api versão(ões) 3.1.0; 4.0.1; 4.0.1
- javax.servlet:servlet-api versão(ões) 2.5; 2.5
- javax.transaction:javax.transaction-api versão(ões) 1.3
- javax.transaction:jta versão(ões) 1.1
- javax.validation:validation-api versão(ões) 2.0.1.Final
- javax.xml.bind:jaxb-api versão(ões) 2.1; 2.3.1
- javax.xml.stream:stax-api versão(ões) 1.0-2
- jboss:jboss-common versão(ões) 3.2.3

- jboss:jbosssx versão(ões) 3.2.3
- junit:junit versão(ões) 4.12; 4.13.2
- libgcc_s_dw2:libgcc_s_dw2-x86:dll versão(ões) 1
- libgcc_s_seh:libgcc_s_seh-x86-64:dll versão(ões) 1
- libstdcplusplus:libstdcplusplus-x86:dll versão(ões) 6
- libstdcplusplus:libstdcplusplus-x86-64:dll versão(ões) 6
- libwinpthread:libwinpthread-x86:dll versão(ões) 1
- libwinpthread:libwinpthread-x86-64:dll versão(ões) 1
- log4j:log4j versão(ões) 1.2.12; 1.2.17
- logkit:logkit versão(ões) 1.0.1
- net.bytebuddy:byte-buddy versão(ões) 1.10.22; 1.11.22
- net.bytebuddy:byte-buddy-agent versão(ões) 1.11.22; 1.10.22; 1.11.22
- net.java.dev.jna:jna versão(ões) 4.4.0; 4.5.1
- net.jcip:jcip-annotations versão(ões) 1.0
- net.minidev:accessors-smart versão(ões) 2.4.7; 2.3.1
- net.minidev:json-smart versão(ões) 2.4.7; 2.3.1
- net.samuelcampos:usbdrivedetector versão(ões) 2.1.5-TSE
- net.sf.dozer:dozer versão(ões) 5.4.0
- net.sf.jasperreports:jasperreports versão(ões) 6.10.0; 6.3.0
- net.sf.jasperreports:jasperreports-fonts versão(ões) 6.12.1
- net.sourceforge.collections:collections-generic versão(ões) 4.01
- org.apache.activemq:activemq-client versão(ões) 5.16.3
- org.apache.activemq:activemq-jms-pool versão(ões) 5.16.3
- org.apache.activemq:activemq-pool versão(ões) 5.16.3
- org.apache.activemq:artemis-commons versão(ões) 2.15.0; 2.19.0; 2.8.1
- org.apache.activemq:artemis-core-client versão(ões) 2.15.0; 2.19.0; 2.8.1
- org.apache.activemq:artemis-jms-client versão(ões) 2.15.0; 2.19.0; 2.8.1
- org.apache.activemq:artemis-selector versão(ões) 2.15.0; 2.19.0; 2.8.1
- org.apache.ant:ant versão(ões) 1.7.0
- org.apache.ant:ant-launcher versão(ões) 1.7.0
- org.apache.commons:commons-collections4 versão(ões) 4.1; 4.4
- org.apache.commons:commons-compress versão(ões) 1.18; 1.21

- org.apache.commons:commons-exec versão(ões) 1.1
- org.apache.commons:commons-lang3 versão(ões) 3.11; 3.12.0
- org.apache.commons:commons-pool2 versão(ões) 2.11.1
- org.apache.geronimo.specs:geronimo-j2ee-management_1.1_spec versão(ões) 1.0.1
- org.apache.geronimo.specs:geronimo-jms_1.1_spec versão(ões) 1.1.1
- org.apache.geronimo.specs:geronimo-jms_2.0_spec versão(ões) 1.0-alpha-2
- org.apache.geronimo.specs:geronimo-json_1.0_spec versão(ões) 1.0-alpha-1
- org.apache.geronimo.specs:geronimo-jta_1.1_spec versão(ões) 1.1.1
- org.apache.httpcomponents:httpclient versão(ões) 4.5.13; 4.5.7
- org.apache.httpcomponents:httpcore versão(ões) 4.4.11; 4.4.14; 4.4.15
- org.apache.httpcomponents:httpmime versão(ões) 4.5.13; 4.5.7
- org.apache.johnzon:johnzon-core versão(ões) 1.2.14; 1.2.15
- org.apache.logging.log4j:log4j-api versão(ões) 2.13.3; 2.17.0
- org.apache.logging.log4j:log4j-core versão(ões) 2.13.3; 2.17.0
- org.apache.logging.log4j:log4j-jul versão(ões) 2.13.3; 2.17.0
- org.apache.logging.log4j:log4j-slf4j-impl versão(ões) 2.13.3; 2.17.0
- org.apache.lucene:lucene-analyzers-common versão(ões) 4.5.1
- org.apache.lucene:lucene-core versão(ões) 4.5.1
- org.apache.lucene:lucene-queries versão(ões) 4.5.1
- org.apache.lucene:lucene-queryparser versão(ões) 4.5.1
- org.apache.lucene:lucene-sandbox versão(ões) 4.5.1
- org.apache.mina:mina-core versão(ões) 2.0.1
- org.apache.pdfbox:fontbox versão(ões) 1.8.9
- org.apache.pdfbox:jempbox versão(ões) 1.8.9
- org.apache.pdfbox:pdfbox versão(ões) 1.8.9
- org.apache.santuario:xmlsec versão(ões) 2.0.2
- org.apache.sshd:sshd-core versão(ões) 0.5.0
- org.apache.tomcat.embed:tomcat-embed-el versão(ões) 9.0.56
- org.apache-extras.beanshell:bsh versão(ões) 2.0b6
- org.apiguardian:apiguardian-api versão(ões) 1.1.2; 1.1.0; 1.1.2
- org.aspectj:aspectjweaver versão(ões) 1.8.6; 1.9.4; 1.9.7

- org.assertj:assertj-core versão(ões) 3.21.0; 3.18.1; 3.21.0
- org.atteo:evo-inflector versão(ões) 1.3
- org.attoparser:attoparser versão(ões) 2.0.5.RELEASE
- org.beanshell:bsh versão(ões) 2.0b4
- org.bn:binarynotes versão(ões) 1.5.3
- org.bouncycastle:bcpkix-jdk15on versão(ões) 1.52; 1.55; 1.68
- org.bouncycastle:bcprov-jdk15on versão(ões) 1.52; 1.55
- org.checkerframework:checker-qual versão(ões) 3.19.0; 3.8.0
- org.codehaus.castor:castor-core versão(ões) 1.3.3; 1.4.1
- org.codehaus.castor:castor-xml versão(ões) 1.3.3; 1.4.1
- org.codehaus.woodstox:woodstox-core-asl versão(ões) 4.4.1
- org.dom4j:dom4j versão(ões) 2.1.3
- org.easymock:easymock versão(ões) 4.0.2
- org.eclipse.jdt.core.compiler:ecj versão(ões) 4.3.1; 4.4.2
- org.eclipse.jetty:jetty-continuation versão(ões) 7.4.5.v20110725
- org.eclipse.jetty:jetty-http versão(ões) 7.4.5.v20110725
- org.eclipse.jetty:jetty-io versão(ões) 7.4.5.v20110725
- org.eclipse.jetty:jetty-server versão(ões) 7.4.5.v20110725
- org.eclipse.jetty:jetty-util versão(ões) 7.4.5.v20110725
- org.eclipse.jgit:org.eclipse.jgit versão(ões) 5.1.3.201810200350-r; 5.12.0.202106070339-r
- org.eclipse.microprofile.config:microprofile-config-api versão(ões) 1.1
- org.eclipse.microprofile.rest.client:microprofile-rest-client-api versão(ões) 1.0.1
- org.fusesource.hawtbuf:hawtbuf versão(ões) 1.11
- org.glassfish.hk2.external:aopalliance-repackaged versão(ões) 2.6.1
- org.glassfish.hk2.external:jakarta.inject versão(ões) 2.6.1
- org.glassfish.hk2:hk2-api versão(ões) 2.6.1
- org.glassfish.hk2:hk2-locator versão(ões) 2.6.1
- org.glassfish.hk2:hk2-utils versão(ões) 2.6.1
- org.glassfish.hk2:osgi-resource-locator versão(ões) 1.0.3
- org.glassfish.jaxb:jaxb-runtime versão(ões) 2.3.5

- org.glassfish.jaxb:txw2 versão(ões) 2.3.5
- org.glassfish.jersey.core:jersey-client versão(ões) 2.32; 2.35
- org.glassfish.jersey.core:jersey-common versão(ões) 2.32; 2.35
- org.glassfish.jersey.ext:jersey-entity-filtering versão(ões) 2.32; 2.35
- org.glassfish.jersey.inject:jersey-hk2 versão(ões) 2.35
- org.glassfish.jersey.media:jersey-media-json-jackson versão(ões) 2.32; 2.35
- org.glassfish:jakarta.el versão(ões) 3.0.3
- org.glassfish:javax.enterprise.concurrent versão(ões) 1.0
- org.hamcrest:hamcrest versão(ões) 2.2; 2.2
- org.hamcrest:hamcrest-all versão(ões) 1.3
- org.hamcrest:hamcrest-core versão(ões) 1.3; 2.2; 2.2
- org.hdrhistogram:HdrHistogram versão(ões) 2.1.12
- org.hibernate.common:hibernate-commons-annotations versão(ões) 5.1.2.Final
- org.hibernate.validator:hibernate-validator versão(ões) 6.2.0.Final
- org.hibernate:hibernate-core versão(ões) 3.5.2-Final; 5.4.32.Final; 5.6.3.Final
- org.hibernate:hibernate-java8 versão(ões) 5.4.32.Final; 5.6.3.Final
- org.hibernate:hibernate-testing versão(ões) 5.6.3.Final
- org.infinispan.protostream:protostream versão(ões) 4.3.4.Final; 4.4.1.Final
- org.infinispan.protostream:protostream-types versão(ões) 4.4.1.Final
- org.infinispan:infinispan-commons versão(ões) 11.0.11.Final; 12.1.10.Final
- org.infinispan:infinispan-core versão(ões) 11.0.11.Final; 12.1.10.Final
- org.javassist:javassist versão(ões) 3.25.0-GA; 3.27.0-GA; 3.28.0-GA
- org.jboss.byteman:byteman versão(ões) 4.0.16
- org.jboss.byteman:byteman-bmunit versão(ões) 4.0.16
- org.jboss.byteman:byteman-install versão(ões) 4.0.16
- org.jboss.byteman:byteman-submit versão(ões) 4.0.16
- org.jboss.classfilewriter:jboss-classfilewriter versão(ões) 1.2.4.Final
- org.jboss.invocation:jboss-invocation versão(ões) 1.5.2.Final
- org.jboss.ironjacamar:ironjacamar-jdbc versão(ões) 1.2.6.Final
- org.jboss.logging:jboss-logging versão(ões) 3.4.2.Final; 3.4.2.Final
- org.jboss.logmanager:jboss-logmanager versão(ões) 2.1.14.Final
- org.jboss.marshalling:jboss-marshalling versão(ões) 2.0.9.Final

- org.jboss.marshalling:jboss-marshalling-river versão(ões) 2.0.0.Final
- org.jboss.metadata:jboss-metadata-common versão(ões) 13.0.0.Final
- org.jboss.metadata:jboss-metadata-ear versão(ões) 13.0.0.Final
- org.jboss.metadata:jboss-metadata-ejb versão(ões) 13.0.0.Final
- org.jboss.modules:jboss-modules versão(ões) 1.9.1.Final
- org.jboss.msc:jboss-msc versão(ões) 1.4.11.Final
- org.jboss.narayana.jta:narayana-jta versão(ões) 5.11.2.Final
- org.jboss.narayana.jts:narayana-jts-idlj versão(ões) 5.9.8.Final
- org.jboss.narayana.jts:narayana-jts-integration versão(ões) 5.9.8.Final
- org.jboss.openjdk-orb:openjdk-orb versão(ões) 8.1.4.Final
- org.jboss.remoting:jboss-remoting versão(ões) 5.0.15.Final
- org.jboss.resteasy:resteasy-cdi versão(ões) 4.0.0.Beta6
- org.jboss.resteasy:resteasy-client versão(ões) 4.0.0.Beta6
- org.jboss.resteasy:resteasy-client-api versão(ões) 4.0.0.Beta6
- org.jboss.resteasy:resteasy-client-microprofile versão(ões) 4.0.0.Beta6
- org.jboss.resteasy:resteasy-core versão(ões) 4.0.0.Beta6
- org.jboss.resteasy:resteasy-core-spi versão(ões) 4.0.0.Beta6
- org.jboss.resteasy:resteasy-validator-provider versão(ões) 4.4.3.Final
- org.jboss.security:jboss-negotiation-common versão(ões) 3.0.6.Final
- org.jboss.security:jboss-negotiation-extras versão(ões) 3.0.6.Final
- org.jboss.security:jboss-negotiation-spnego versão(ões) 3.0.6.Final
- org.jboss.spec.javax.annotation:jboss-annotations-api_1.2_spec versão(ões) 1.0.0.Final
- org.jboss.spec.javax.annotation:jboss-annotations-api_1.3_spec versão(ões) 2.0.1.Final
- org.jboss.spec.javax.ejb:jboss-ejb-api_3.2_spec versão(ões) 1.0.0.Final
- org.jboss.spec.javax.el:jboss-el-api_3.0_spec versão(ões) 2.0.0.Final
- org.jboss.spec.javax.enterprise.concurrent:jboss-concurrency-api_1.0_spec versão(ões) 2.0.0.Final
- org.jboss.spec.javax.interceptor:jboss-interceptors-api_1.2_spec versão(ões) 2.0.0.Final

- org.jboss.spec.javax.resource:jboss-connector-api_1.7_spec versão(ões) 2.0.0.Final
- org.jboss.spec.javax.security.jacc:jboss-jacc-api_1.5_spec versão(ões) 2.0.0.Final
- org.jboss.spec.javax.servlet:jboss-servlet-api_3.1_spec versão(ões) 1.0.0.Final
- org.jboss.spec.javax.servlet:jboss-servlet-api_4.0_spec versão(ões) 2.0.0.Final
- org.jboss.spec.javax.transaction:jboss-transaction-api_1.2_spec versão(ões) 1.1.1.Final
- org.jboss.spec.javax.transaction:jboss-transaction-api_1.3_spec versão(ões) 2.0.0.Final
- org.jboss.spec.javax.websocket:jboss-websocket-api_1.1_spec versão(ões) 2.0.0.Final
- org.jboss.spec.javax.ws.rs:jboss-jaxrs-api_2.1_spec versão(ões) 1.0.2.Final
- org.jboss.spec.javax.xml.bind:jboss-jaxb-api_2.3_spec versão(ões) 1.0.0.Final
- org.jboss.stdio:jboss-stdio versão(ões) 1.1.0.Final
- org.jboss.threads:jboss-threads versão(ões) 3.1.0.Final
- org.jboss.xnio:xnio-api versão(ões) 3.8.4.Final
- org.jboss.xnio:xnio-nio versão(ões) 3.8.4.Final
- org.jboss:jandex versão(ões) 2.2.3.Final
- org.jboss:jboss-dmr versão(ões) 1.5.0.Final
- org.jboss:jboss-transaction-spi versão(ões) 7.6.0.Final; 7.6.1.Final
- org.jboss:jboss-vfs versão(ões) 3.2.14.Final
- org.jboss:staxmapper versão(ões) 1.3.0.Final
- org.jfree:jcommon versão(ões) 1.0.23
- org.jfree:jfreechart versão(ões) 1.0.19
- org.jgroups:jgroups versão(ões) 3.6.13.Final
- org.json:json versão(ões) 20180813
- org.junit.jupiter:junit-jupiter versão(ões) 5.8.2; 5.7.2; 5.8.2
- org.junit.jupiter:junit-jupiter-api versão(ões) 5.8.2; 5.7.2; 5.8.2
- org.junit.jupiter:junit-jupiter-engine versão(ões) 5.8.2; 5.7.2
- org.junit.jupiter:junit-jupiter-params versão(ões) 5.8.2; 5.7.2; 5.8.2
- org.junit.platform:junit-platform-commons versão(ões) 1.8.2; 1.7.2; 1.8.2

- org.junit.platform:junit-platform-engine versão(ões) 1.8.2; 1.7.2
- org.jvnet.staxex:stax-ex versão(ões) 1.8.3
- org.keycloak:keycloak-adapter-core versão(ões) 15.0.0
- org.keycloak:keycloak-adapter-spi versão(ões) 15.0.0
- org.keycloak:keycloak-authz-client versão(ões) 15.0.0
- org.keycloak:keycloak-common versão(ões) 15.0.0
- org.keycloak:keycloak-core versão(ões) 15.0.0
- org.keycloak:keycloak-server-spi versão(ões) 3.4.3.Final-redhat-2
- org.keycloak:keycloak-spring-boot-2-adapter versão(ões) 15.0.0
- org.keycloak:keycloak-spring-boot-adapter-core versão(ões) 15.0.0
- org.keycloak:keycloak-spring-boot-starter versão(ões) 15.0.0
- org.keycloak:keycloak-spring-security-adapter versão(ões) 15.0.0
- org.keycloak:spring-boot-container-bundle versão(ões) 15.0.0
- org.latencyutils:LatencyUtils versão(ões) 2.0.3
- org.mitre.dsmiley.httpproxy:smiley-http-proxy-servlet versão(ões) 1.11
- org.mockito:mockito-core versão(ões) 4.0.0; 3.6.28; 4.0.0
- org.mockito:mockito-junit-jupiter versão(ões) 4.0.0; 3.6.28; 4.0.0
- org.modelmapper:modelmapper versão(ões) 2.3.2
- org.mortbay.jetty:jetty versão(ões) 6.1.26
- org.mortbay.jetty:jetty-embedded versão(ões) 6.1.26
- org.mortbay.jetty:jetty-sslengine versão(ões) 6.1.26
- org.mortbay.jetty:jetty-util versão(ões) 6.1.26
- org.objenesis:objenesis versão(ões) 3.2; 3.0.1; 3.1
- org.olap4j:olap4j versão(ões) 0.9.7.309-JS-3
- org.opentest4j:opentest4j versão(ões) 1.2.0; 1.2.0
- org.osgi:org.osgi.annotation.versioning versão(ões) 1.0.0
- org.ow2.asm:asm versão(ões) 9.1; 5.0.4
- org.picketbox:picketbox versão(ões) 5.0.3.Final
- org.picketbox:picketbox-commons versão(ões) 1.0.0.final
- org.picketbox:picketbox-infinispan versão(ões) 5.0.3.Final
- org.powermock:powermock-api-easymock versão(ões) 2.0.0
- org.powermock:powermock-api-support versão(ões) 2.0.0

- org.powermock:powermock-core versão(ões) 2.0.0
- org.powermock:powermock-reflect versão(ões) 2.0.0
- org.projectlombok:lombok versão(ões) 1.18.20; 1.18.22; 1.18.6
- org.projectodd.vdx:vdx-core versão(ões) 1.1.6
- org.projectodd.vdx:vdx-wildfly versão(ões) 1.1.6
- org.reactivestreams:reactive-streams versão(ões) 1.0.3
- org.skyscreamer:jsonassert versão(ões) 1.5.0; 1.5.0
- org.slf4j:jcl-over-slf4j versão(ões) 1.6.6; 1.7.32
- org.slf4j:jul-to-slf4j versão(ões) 1.7.32; 1.7.32
- org.slf4j:log4j-over-slf4j versão(ões) 1.7.32
- org.slf4j:slf4j-api versão(ões) 1.7.2; 1.7.32
- org.slf4j:slf4j-log4j12 versão(ões) 1.7.26; 1.7.32
- org.springframework.boot:spring-boot versão(ões) 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-actuator versão(ões) 2.6.2
- org.springframework.boot:spring-boot-actuator-autoconfigure versão(ões) 2.6.2
- org.springframework.boot:spring-boot-autoconfigure versão(ões) 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-starter versão(ões) 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-starter-actuator versão(ões) 2.6.2
- org.springframework.boot:spring-boot-starter-aop versão(ões) 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-starter-data-jpa versão(ões) 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-starter-data-rest versão(ões) 2.6.2
- org.springframework.boot:spring-boot-starter-jdbc versão(ões) 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-starter-json versão(ões) 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-starter-log4j2 versão(ões) 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-starter-security versão(ões) 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-starter-test versão(ões) 2.6.2; 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-starter-thymeleaf versão(ões) 2.6.2
- org.springframework.boot:spring-boot-starter-undertow versão(ões) 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-starter-validation versão(ões) 2.6.2
- org.springframework.boot:spring-boot-starter-web versão(ões) 2.4.10; 2.6.2

- org.springframework.boot:spring-boot-starter-web-services versão(ões) 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-test versão(ões) 2.6.2; 2.4.10; 2.6.2
- org.springframework.boot:spring-boot-test-autoconfigure versão(ões) 2.6.2; 2.4.10; 2.6.2
- org.springframework.cloud:spring-cloud-commons versão(ões) 3.0.3; 3.1.0
- org.springframework.cloud:spring-cloud-config-client versão(ões) 3.0.4; 3.1.0
- org.springframework.cloud:spring-cloud-context versão(ões) 3.0.3; 3.1.0
- org.springframework.cloud:spring-cloud-starter versão(ões) 3.0.3; 3.1.0
- org.springframework.cloud:spring-cloud-starter-bootstrap versão(ões) 3.0.3; 3.1.0
- org.springframework.cloud:spring-cloud-starter-config versão(ões) 3.0.4; 3.1.0
- org.springframework.data:spring-data-commons versão(ões) 2.4.12; 2.6.0
- org.springframework.data:spring-data-jpa versão(ões) 2.4.12; 2.6.0
- org.springframework.data:spring-data-rest-core versão(ões) 3.6.0
- org.springframework.data:spring-data-rest-webmvc versão(ões) 3.6.0
- org.springframework.hateoas:spring-hateoas versão(ões) 1.4.0
- org.springframework.plugin:spring-plugin-core versão(ões) 2.0.0.RELEASE
- org.springframework.security:spring-security-config versão(ões) 5.4.8; 5.6.1
- org.springframework.security:spring-security-core versão(ões) 5.4.8; 5.6.1
- org.springframework.security:spring-security-crypto versão(ões) 5.4.8; 5.6.1
- org.springframework.security:spring-security-rsa versão(ões) 1.0.10.RELEASE
- org.springframework.security:spring-security-test versão(ões) 5.6.1
- org.springframework.security:spring-security-web versão(ões) 5.4.8; 5.6.1
- org.springframework.ws:spring-ws-core versão(ões) 3.0.10.RELEASE; 3.1.2
- org.springframework.ws:spring-xml versão(ões) 3.0.10.RELEASE; 3.1.2
- org.springframework:spring-aop versão(ões) 4.1.7.RELEASE; 5.3.14; 5.3.9
- org.springframework:spring-aspects versão(ões) 4.1.7.RELEASE; 5.3.14; 5.3.9
- org.springframework:spring-beans versão(ões) 4.1.7.RELEASE; 5.3.14; 5.3.9
- org.springframework:spring-context versão(ões) 4.1.7.RELEASE; 5.3.14; 5.3.9
- org.springframework:spring-context-support versão(ões) 4.1.7.RELEASE
- org.springframework:spring-core versão(ões) 4.1.7.RELEASE; 5.3.14; 5.3.9

- org.springframework:spring-expression versão(ões) 4.1.7.RELEASE; 5.3.14; 5.3.9
- org.springframework:spring-jcl versão(ões) 5.3.14; 5.3.9
- org.springframework:spring-jdbc versão(ões) 5.3.14; 5.3.9
- org.springframework:spring-jms versão(ões) 5.3.14; 5.3.9
- org.springframework:spring-messaging versão(ões) 5.3.14; 5.3.9
- org.springframework:spring-orm versão(ões) 5.3.14; 5.3.9
- org.springframework:spring-oxm versão(ões) 5.3.14; 5.3.9
- org.springframework:spring-test versão(ões) 5.3.14; 5.3.14; 5.3.9
- org.springframework:spring-tx versão(ões) 5.3.14; 5.3.9
- org.springframework:spring-web versão(ões) 5.3.10; 5.3.14; 5.3.9
- org.springframework:spring-webmvc versão(ões) 5.3.14; 5.3.9
- org.testng versão(ões) 6.9.6; 6.14.3
- org.thymeleaf.extras:thymeleaf-extras-java8time versão(ões) 3.0.4.RELEASE
- org.thymeleaf:thymeleaf versão(ões) 3.0.14.RELEASE
- org.thymeleaf:thymeleaf-spring5 versão(ões) 3.0.14.RELEASE
- org.tukaani:xz versão(ões) 1.8
- org.unbescape:unbescape versão(ões) 1.1.6.RELEASE
- org.wildfly.client:wildfly-client-config versão(ões) 1.0.1.Final
- org.wildfly.common:wildfly-common versão(ões) 1.5.2.Final
- org.wildfly.core:wildfly-controller versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-controller-client versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-core-management-client versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-core-security versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-core-security-api versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-deployment-repository versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-domain-http-interface versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-domain-management versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-io versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-network versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-platform-mbean versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-process-controller versão(ões) 10.0.0.Final

- org.wildfly.core:wildfly-protocol versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-remoting versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-request-controller versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-server versão(ões) 10.0.0.Final
- org.wildfly.core:wildfly-version versão(ões) 10.0.0.Final
- org.wildfly.security.elytron-web:undertow-server versão(ões) 1.6.0.Final
- org.wildfly.security:wildfly-elytron versão(ões) 1.10.3.Final
- org.wildfly.transaction:wildfly-transaction-client versão(ões) 1.1.7.Final
- org.wildfly.wildfly-http-client:wildfly-http-client-common versão(ões) 1.0.16.Final
- org.wildfly.wildfly-http-client:wildfly-http-naming-client versão(ões) 1.0.16.Final
- org.wildfly.wildfly-http-client:wildfly-http-transaction-client versão(ões) 1.0.16.Final
- org.wildfly:wildfly-clustering-common versão(ões) 18.0.0.Final
- org.wildfly:wildfly-clustering-infinispan-spi versão(ões) 18.0.0.Final
- org.wildfly:wildfly-clustering-marshalling-api versão(ões) 18.0.0.Final
- org.wildfly:wildfly-clustering-marshalling-spi versão(ões) 18.0.0.Final
- org.wildfly:wildfly-clustering-service versão(ões) 18.0.0.Final
- org.wildfly:wildfly-ee versão(ões) 18.0.0.Final
- org.wildfly:wildfly-iiop-openjdk versão(ões) 18.0.0.Final
- org.wildfly:wildfly-naming versão(ões) 18.0.0.Final
- org.wildfly:wildfly-naming-client versão(ões) 1.0.11.Final
- org.wildfly:wildfly-security versão(ões) 18.0.0.Final
- org.wildfly:wildfly-transactions versão(ões) 18.0.0.Final
- org.xmlunit:xmlunit-core versão(ões) 2.8.4; 2.7.0; 2.8.4
- org.yaml:snakeyaml versão(ões) 1.27; 1.29
- oro:oro versão(ões) 2.0.8
- stax:stax versão(ões) 1.2.0
- stax:stax-api versão(ões) 1.0.1
- wsdl4j:wsdl4j versão(ões) 1.6.3
- xalan:serializer versão(ões) 2.7.2

– xalan:xalan versão(ões) 2.7.2

– xml-apis:xml-apis versão(ões) 1.0.b2; 1.3.04

25. Documentação do Processo de Verificação de Segurança de Software dos Sistemas que suportam o Processo Eleitoral.

Resposta: O processo de desenvolvimento dos sistemas eleitorais compreende um conjunto de etapas, incluindo aquelas em que a segurança, a integridade e a corretude dos produtos de software são verificadas. Essas etapas são:

– Testes durante a fase de desenvolvimento;

– Testes integrados, em que o conjunto dos sistemas são exercitados, validando o comportamento de cada produto individual dentro do processo eleitoral. Nesse momento sistemas mantidos por equipe distintas interoperam entre si, de forma a permitir que os dados de saída de uma fase sejam validados nas fases seguintes;

– Testes em campo e simulados nacionais. Oportunidade em que os sistemas são testados em ambiente de homologação, permitindo verificar os dados de saída e de entrada da mesma forma que ocorre nos testes integrados, além de validar o comportamento dos programas sob a perspectiva do usuário;

– Análise de código fonte por meio de processo de integração contínua utilizando as ferramentas SonarQube com "FindSecBugs", Depedency Track, Cppcheck, Flawfinder e clang-tidy;

– Teste estático, dinâmico e híbrido de aplicações por meio empresa contratada para prestação de serviço de análise de segurança;

– Análise de segurança dos softwares em parceria com instituições que prestam serviço de análise de segurança da informação. Atualmente o TSE mantém convênio com a Universidade de São Paulo – USP, que realiza esse tipo de atividade;

– Teste Público de Segurança: normatizado pela Res.-TSE nº 23.444/2015 (ANEXO 18), o evento é realizado no ano anterior ao das eleições ordinárias. Nesses testes o TSE abre para a comunidade acadêmica, científica e entidades os sistemas do processo eleitoral para avaliação, sugestão e busca de eventuais fragilidades, com o objetivo de possibilitar a implementação de melhorias e o reforço continuado da segurança. Ressalte-se que esse procedimento de contínuo aprimoramento de ferramentas tecnológicas é absolutamente normal

e desejável e ocorre justamente para evitar a identificação de vulnerabilidades nos processos de votação, antecipando-se a solução de potenciais problemas;

– Oito mecanismos de segurança preconizados na resolução de fiscalização e auditoria do sistema eletrônico de votação, as quais são executadas nos seguintes momentos: durante o desenvolvimento, a compilação, a assinatura digital, e a lacração dos sistemas eleitorais; durante as cerimônias destinadas à geração de mídias e preparação das urnas eletrônicas; durante a cerimônia destinada à verificação da integridade e autenticidade dos sistemas eleitorais instalados no TSE; na audiência destinada à verificação dos sistemas destinados à transmissão de BUs; durante os procedimentos preparatórios para realização de teste de integridade e no dia da votação; durante o Teste de Integridade das Urnas Eletrônicas; durante o Teste de Autenticidade dos Sistemas Eleitorais; após os procedimentos de totalização das eleições.

Por fim, cabe mencionar que a Portaria TSE nº 540/2021 (ANEXO 19), institui normas de desenvolvimento seguro de sistemas, relativa à política de segurança da informação deste Tribunal.

26. Lista de Ferramentas de análise de segurança de código utilizadas dos Sistemas que suportam o Processo Eleitoral.

Resposta:

– SonarQube e plugin "FindSecBugs";

– Depedency Track (para análise das bibliotecas de terceiros)

– Para o conjunto de software do Ecossistema da Urna são utilizadas as seguintes ferramentas: Cppcheck, Flawfinder e clang-tidy.

A aquisição de solução comercial para Análise Estática de Código Fonte (SAST) está em trâmite nos autos do Procedimento Administrativo SEI nº 2018.00.000014614-9, em que, até 5.1.2022, houve homologação da licitação e encontra-se na fase de formalização da Ata de Registro de Preços.

27. Documentação de Arquitetura da Solução, incluindo a topologia de rede que envolve os ativos de segurança (firewall, IDS, IPS, etc) dos Sistemas que suportam o Processo Eleitoral.

Resposta: A topologia de rede, incluindo a infraestrutura de mensagerias utilizadas na interoperabilidade de dados entre os sistemas eleitorais, compreende um conjunto de informações de alta sensibilidade no que tange aos aspectos de segurança da informação, razão pela qual estará disponível para conhecimento *in loco*, mediante agendamento.

De uma forma geral, a rede da Justiça Eleitoral é composta por enlaces privados que interligam os Cartórios Eleitorais aos TRE e estes ao TSE, com redundância provida por meio de SD-Wan. Adicionalmente, enlaces de internet redundantes chegam ao TSE para permitir a comunicação com a rede mundial de computadores. Internamente, há segmentação entre as redes externas, rede local e rede de datacenter. Na rede do datacenter há segmentações adicionais separando bancos de dados, servidores de aplicação e servidores de rede. São utilizadas tecnologias de web application firewall, IPS e NGF para proteção das comunicações.

Registre-se ainda que no final de semana das eleições são realizados bloqueios adicionais, dentre os quais citamos o impedimento de que usuários internos à rede da Justiça Eleitoral tenham acesso à internet.

RESPOSTAS AO OFÍCIO nº 002

1. Quais foram os parâmetros probabilísticos, entre eles o nível de confiança, utilizados nos cálculos do TSE para definir a quantidade de 6, 8 ou 10 urnas por Unidade da Federação, no Teste de Integridade das urnas eletrônicas, conforme o art. 58 e 59, da Minuta de Resolução Nr XX.XXX - Instrução Normativa Nr 0600747-28-2019.6.00.0000?

Resposta: O número de urnas por Unidade da Federação (UF) é definido proporcionalmente ao quantitativo de seções principais de cada UF, conforme previsto na Res.-TSE nº 23.673/2021 (que dispõe sobre os procedimentos de fiscalização e auditoria do sistema eletrônico de votação, ANEXO 17). Assim, Unidades Federativas com mais seções eleitorais farão jus a um número maior de testes de integridade.

Para o aumento da quantidade de urnas a serem submetidas aos testes, visando avaliar a relevância do plano amostral de Urnas Eletrônicas auditadas, foi realizado estudo estatístico pela unidade responsável do TSE, o qual atestou que o quantitativo existente antes da ampliação já era estatisticamente representativo. Esse estudo partiu da premissa verdadeira, considerada estatisticamente como um cenário favorável, de que todas as urnas utilizam o

mesmo sistema no país inteiro. Esse fato pode ser averiguado em diversas fases do processo eleitoral: nas Cerimônias de Lacração de Urnas, nas Cerimônias de Preparação das Urnas e nos Testes de Autenticidade dos Sistemas Eleitorais (que ocorrem no dia da eleição). Acrescente-se que a unicidade do sistema também pode ser averiguada em uma possível auditoria forense, por meio de comparações dos resumos digitais e verificação de assinaturas digitais geradas na cerimônia de lacração. Mesmo diante desse cenário, a Administração do TSE decidiu duplicar a quantidade de urnas a serem submetidas aos testes de integridade, implementação já presente na Res.-TSE nº 23.673/2021 (ANEXO 17).

Importante registrar que os partidos, candidatos e entidades fiscalizadoras depositam tanta confiança no sistema que, com frequência, não enviam quaisquer representantes a esses eventos.

2. Como foi feito o cálculo para chegar ao número máximo de 234 urnas submetidas ao teste de integridade, constante da medida 7 do Plano de Ação para Ampliação da Transparência do Processo Eleitoral 2022? Há relação com os art 8 e 59 da Minuta de Resolução Nr XX.XXX?

Resposta: Após o estudo realizado (descrito na resposta anterior), o qual já apontava a confiança do quantitativo de urnas submetidas ao processo de auditoria, foi decidida pela Administração do TSE dobrar o quantitativo de urnas a serem submetidas aos testes de integridades. Assim, o tema foi levado para apreciação do grupo de trabalho GT-Auditoria, responsável pela definição dos requisitos e processos de trabalho para os procedimentos de auditoria para as eleições de 2022, o qual propôs que fossem dobrados os quantitativos de urnas em cada faixa de eleitorado, o que foi acatado pela Administração do TSE, no julgamento da Res.-TSE nº 23.673/2021 (ANEXO 17), podendo chegar até o montante de 234 (duzentas e trinta e quatro) urnas eletrônicas submetidas aos testes de integridade (arts. 58 e 59 da Res.-TSE nº 23.673/2021):

https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021

3. Qual o nível de confiança nos casos em que há ação judicial relativa aos sistemas de votação e apuração, conforme estabelece o caput do art. 83, da Resolução nº 23.603/2019?

Resposta: Os percentuais, da forma como apontados na Res.-TSE nº 23.603/2019 (ANEXO 16), foram estabelecidos para a eleição de 2016 (Res. TSE nº 23.456/2015, art. 182, ANEXO 22), em substituição aos quantitativos definidos para a eleição de 2014 (Res TSE nº 23.399/2013, art. 235, § 3º, II, ANEXO 21).

O Grupo de Trabalho do Ecossistema da Urna (Portaria TSE nº 143/2013, ANEXO 20) estabeleceu que seria apresentado estudo estatístico sobre quantitativos máximos e mínimos de urnas que ficariam lacradas na pendência de desenlace de ações judiciais que questionassem o processo de votação. O referido trabalho utilizou os seguintes percentuais:

- Erro Amostral 3%
- Nível de Confiança 95%

Importante ressaltar que a análise em caso de ação judicial é complementada por todas as auditorias que já são executadas no processo eleitoral, tais como a inspeção do código-fonte, as cerimônias de Assinatura Digital e Lacração dos Sistemas Eleitorais, Preparação das Urnas, bem como os testes de autenticidade e integridade.

4. Qual a consequência para o processo eleitoral como um todo em face da observância de irregularidades na contagem dos votos da amostra utilizada no teste de integridade, a fim de não descaracterizar a auditoria por amostragem?

Resposta: A primeira medida a ser adotada em caso de divergência na contagem de votos no teste de integridade consta do art. 71 da Res.-TSE nº 23.673/2021 (ANEXO 17):

> Art. 71. Na hipótese de divergência entre o BU e o resultado esperado, serão adotadas as seguintes providências:
> I - localização das divergências; e
> II - conferência da digitação das respectivas cédulas divergentes, com base no horário de votação.
> Parágrafo único. Persistindo a divergência da votação eletrônica, proceder-se-á à conferência de todas as cédulas digitadas e ao registro minucioso em ata de todas as intercorrências, ainda que solucionadas.

Compreende-se que, persistindo divergência entre a votação em cédula e a eletrônica, estar-se-á diante da hipótese prevista no art. 222, c/c o art. 224, *caput*, do Código

Eleitoral, que definem respectivamente hipóteses nas quais a eleição é anulável e em quais situações eventual anulação dá ensejo a nova eleição. *In verbis*:

> Art. 222. É também anulável a votação, quando viciada de falsidade, fraude, coação, uso de meios de que trata o Art. 237, ou emprego de processo de propaganda ou captação de sufrágios vedado por lei.
>
> [...]
>
> Art. 224. Se a nulidade atingir a mais de metade dos votos do país nas eleições presidenciais, do Estado nas eleições federais e estaduais ou do município nas eleições municipais, julgar-se-ão prejudicadas as demais votações e o Tribunal marcará dia para nova eleição dentro do prazo de 20 (vinte) a 40 (quarenta) dias.

Destaca-se quanto ao tema que é dever da Justiça Eleitoral preservar todos os sistemas oficiais utilizados nas eleições informatizadas para que seja possível verificar se a origem da divergência na contabilização dos votos ocorreu a partir de falhas dos programas utilizados (Res.-TSE nº 23.673/2021, arts. 1º, IX, 26 e 52, parágrafo único).

5. Como será observada a mesma rotina de uma votação normal no Teste de Integridade, incluindo a identificação biométrica?

Resposta: Sobre o tema, inicialmente importante destacar que nenhuma eleição ocorre com identificação biométrica de 100% dos eleitores que compareceram à votação. Em primeiro lugar, devido ao fato de que algumas pessoas são desprovidas de membros superiores, o que impede a coleta de suas impressões digitais. Em segundo lugar, outra parte da população não buscou serviços eleitorais para coleta de sua biometria e, nem por isso, têm impedido o exercício do direito ao voto. Em terceiro lugar, há municípios que ainda estão em fase de coleta biométrica. Por fim, o processo de votação conta com medida de contingência para que eleitores tenham preservado o direito ao voto nas situações em que estejam impedidos de fazer a identificação digital (por exemplo, quando estejam com as mãos enfaixadas) ou que a digital não tenha sido reconhecida pela urna eletrônica.

Em todos esses casos, a identificação do eleitor ocorre mediante documento oficial com fotografia, conforme previsto na Lei nº 9.504/1997.

Portanto, compreende-se que atualmente o Teste de Integridade já preserva a rotina de uma votação normal, visto que é possível a votação com comprovação de identidade por via diversa da identificação biométrica.

Ainda assim, tramita no TSE proposta inicial para estudo de automação do teste de integridade, o que pode vir a facilitar a mobilidade para que o teste seja executado nas seções eleitorais, com eleitores reais, sendo necessário centrar esforços na comunicação com o eleitor para que sejam mitigadas eventuais incompreensões e receios sobre a preservação do sigilo do voto.

RESPOSTAS AO OFÍCIO nº 003

Esse documento reproduz o teor do Ofício nº 002, que já recebeu o devido tratamento.

RESPOSTAS AO OFÍCIO nº 004

6. É possível armazenar mais de um BU no aplicativo Boletim na Mão?

Resposta: O aplicativo Boletim na Mão, desde a sua primeira versão, permite que sejam armazenados tantos boletins quantos tenham sido lidos por meio dos respectivos QRCodes.

7. Em caso negativo, seria possível realizar uma alteração na aplicação Boletim na Mão de forma que mais de um BU seja armazenado no aplicativo?

Resposta: Não se aplica em razão da resposta da questão 6.

8. Seria possível realizar uma alteração na aplicação Boletim na Mão de forma que as informações do BU sejam enviadas para um servidor cujo endereço seja configurado pelo usuário?

Resposta: A versão atual do Boletim na Mão permite que os boletins de urna lidos possam ser compartilhados de forma individualizada por meio de vários aplicativos disponíveis no aparelho celular. Como exemplo: aplicativos de mensagens instantâneas, por e-mail, Google Drive etc. Dessa forma, por meio do aplicativo, os boletins de urna podem ser enviados para alguma central que acesse o destino do compartilhamento indicado pelo usuário. Também é

possível disponibilizar as informações necessárias para o desenvolvimento de versões próprias do aplicativo pelos interessados.

9. Qual foi a motivação para incluir uma porta USB na urna modelo 2020, a despeito que normalmente tal implementação reduz, em tese, a segurança da urna?

Resposta: O Uenux tem total controle sobre as portas USB da urna. Isso significa que o software valida cada dispositivo conectado a cada porta USB da urna. Somente os dispositivos conhecidos (periféricos que já integram a urna e suas mídias) são aceitos nas portas USB esperadas - a porta usada pelo teclado do eleitor só pode ser usada para esse periférico, por exemplo. Caso seja identificado um dispositivo não conhecido em qualquer porta, o sistema operacional da urna desliga a alimentação da porta USB. Dispositivos conhecidos conectados em portas diferentes da esperada resultam no bloqueio da urna pelo sistema operacional.

Em resumo, dispositivos USB desconhecidos ficam inutilizáveis quando conectados na urna. E a urna suspende a sua execução caso a sua montagem não esteja de acordo com as especificações.

Ademais, todo dado sensível que trafega pelo barramento USB é protegido por criptografia. Por exemplo, as teclas pressionadas no terminal do eleitor são cifradas. Dessa forma, não há a possibilidade de captura de ruído ou de pacotes de dados críticos em portas USB.

Assim, a presença de portas USB adicionais é uma oportunidade de evolução tecnológica da urna a um custo reduzido, ao mesmo tempo em que não fragiliza a segurança do sistema. De todo modo, as portas USBs adicionais na urna sempre existiram, tanto nos Terminais do Mesário, quanto na face traseira do Terminal do Eleitor, nas urnas modelo 2009 a 2015 e nas faces laterais do Terminal do Eleitor nas urnas modelo 2020 e 2022 (ainda em projeto).

10. Será realizada alguma auditoria externa nas novas urnas (modelo 2020), tendo em vista que as mesmas não estavam disponíveis durante o TPS 2021?

Resposta: O TSE audita a fabricação das urnas eletrônicas com servidores alocados diretamente na linha de produção, inspecionando todo o processo fabril, de maneira a verificar

se o produto acabado, urna eletrônica, está em conformidade com o projeto estabelecido e as demais especificações do edital de licitação.

Uma vez entregues aos tribunais eleitorais, as urnas eletrônicas estarão submetidas a todos os eventos de fiscalização e auditoria estabelecidos na Res.-TSE nº 23.673/2021 (ANEXO 17).

Os Testes Públicos de Segurança têm como objeto o último modelo de urna que teve seu sistema totalmente implementado e em produção. Assim, no caso do TPS 2021, a urna a ser testada foi o modelo 2015, pois o modelo 2020 ainda estava em desenvolvimento e os sistemas ainda estão em desenvolvimento.

O suporte de *software* para a urna 2020 estará disponível em março de 2022 para teste, momento em que este modelo de urna poderá participar de todos os eventos de verificação constantes na resolução supracitada e participar dos eventos de teste do calendário da Justiça Eleitoral.

11. Qual a previsão do quantitativo de urnas que serão utilizadas por Estado da Federação, para as eleições de 2022, considerando também as de contingência?

Resposta: O parque planejado para as Eleições 2022 está representado na tabela a seguir. Os quantitativos podem ser ajustados em função do fechamento do cadastro no início de maio do ano eleitoral e outras necessidades logísticas.

TRE	Parque previsto						
	UE2009	UE2010	UE2011	UE2013	UE2015	UE2020	TOTAL
AC	329	498	150	230	412	1.168	2.787
AL	962	1.776	550	716	1.202	2.959	8.165
AM	1.085	1.651	750	490	1.779	3.454	9.209
AP	237	356	144	171	274	828	2.010
BA	4.895	9.618	2.728	2.680	6.577	14.993	41.491
CE	2.957	4.921	2.356	720	3.685	10.424	25.063
DF	1.217	2.000	0	422	1.807	4.055	9.501
ES	1.209	2.255	332	760	1.947	3.741	10.244
GO	1.984	3.495	662	977	2.625	7.074	16.817
MA	2.297	3.677	1.681	876	2.942	7.989	19.462
MG	6.738	13.025	4.121	2.652	9.014	21.562	57.112

MS	972	1.890	222	510	1.140	3.502	8.236
MT	1.074	1.842	812	272	1.334	3.766	9.100
PA	2.818	4.915	1.630	1.058	3.695	9.760	23.876
PB	1.331	2.449	0	1.504	1.910	4.901	12.095
PE	2.978	5.969	1.717	1.359	4.149	9.064	25.236
PI	1.253	2.127	913	395	1.709	4.220	10.617
PR	3.532	6.690	670	2.050	4.784	12.221	29.947
RJ	5.022	9.011	1.100	2.150	8.700	16.586	42.569
RN	1.052	1.675	494	243	1.315	4.136	8.915
RO	522	961	0	370	716	1.832	4.401
RR	184	363	0	40	321	655	1.563
RS	3.862	7.089	2.373	2.871	4.880	11.665	32.740
SC	2.304	3.889	1.262	1.053	3.722	7.296	19.526
SE	818	1.257	450	488	972	2.949	6.934
SP	13.635	21.936	8.561	3.942	22.620	44.880	115.574
TO	559	1.031	349	143	654	2.005	4.741
TSE	7.458	1.451	971	1.000	1.000	7.314	19.194
TOTAL	73.284	117.817	34.998	30.142	95.885	224.999	577.125

12. Quais controles da ISO/IEC 27001:2013 foram implementados para verificar o código desenvolvido por programadores terceirizados?

Resposta: Partindo-se da premissa de que a pergunta se refere aos controles de segurança referentes ao desenvolvimento de software, especificados na norma ISO 27002 em seu item 14, informamos que o tribunal não se baseia diretamente nesta norma, mas adota como base para seu processo de desenvolvimento seguro o padrão OWASP SAMM (Security Assurance Maturity Model). A partir de um levantamento de conformidade entre as práticas implementadas e as recomendações do modelo, foi elaborada a Norma de Desenvolvimento Seguro (Portaria TSE nº 540/2021, ANEXO 19), que pode ser encontrada no endereço abaixo:

https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-540-de-23-de-agosto-de-2021

A referida norma tem como meta incrementar o nível de atendimento da realidade do TSE ao modelo, sendo dividida nos capítulos abaixo:

- Capítulo I – Da arquitetura e dos padrões de desenvolvimento de sistemas;
- Capítulo II – Dos ambientes de execução dos sistemas;
- Capítulo III – Do projeto de sistemas;
- Capítulo IV – Da codificação de sistemas;
- Capítulo V – Do ambiente de compilação e implantação de software;

- Capítulo VI – Da gestão de identidades, autenticação e certificação digital;
- Capítulo VII – Dos registros de log dos sistemas;
- Capítulo VIII – Do ciclo de vida dos sistemas;
- Capítulo IX – Do inventário de sistemas.

Em alinhamento às recomendações contidas na Portaria TSE nº 540/2021, o TSE adota a prática da realização de testes de segurança sobre seus sistemas, tanto por equipe interna quanto por equipe externa que atua sob contrato específico, acompanhada pelo respectivo ciclo de correção das vulnerabilidades eventualmente encontradas e da verificação dessas correções.

Adicionalmente, vem incrementando sua infraestrutura de segurança de aplicações, já tendo implementado solução de Web Application Firewall e Gerenciado de APIs, e licitado soluções para Análise Estática de Código Fonte e Gerenciamento de Acessos Privilegiados.

Em que pese o quadro de profissionais que participam do desenvolvimento dos sistemas eleitorais conter profissionais terceirizados, todas as etapas de construção dos softwares, desde a concepção até os testes, passando pelas especificações, projetos e implementações, são executadas utilizando os recursos, ferramentas e processos de engenharia de softwares do Tribunal Superior Eleitoral, bem como supervisionados, acompanhados e coordenados por servidores da corte. Sendo assim, todos os controles referentes ao processo de desenvolvimento de software, incluindo os testes e homologação, são aplicáveis, independente do vínculo do profissional. Ademais, os contratos de prestação de serviço preveem termo de confidencialidade, que resguarda o sigilo e a propriedade intelectual dos produtos sustentados pela empresa.

13. O Sistema de Gerenciamento da Totalização de votos permite auditar o momento em que cada Boletim de Urna é consolidado na totalização realizada pelo TSE?

Resposta: O processo de totalização dos votos pode ser entendido em três etapas.

– Etapa 1: transmissão e recebimento dos arquivos de urna, incluindo o boletim de urna;

– Etapa 2: processamento do boletim de urna. Nessa etapa o BU é lido, validado e seus dados inseridos no banco de dados;

– Etapa 3: totalização da seção eleitoral. Nesse momento, os votos de cada seção recebida são consolidados, aplicando-se as regras de totalização, e o resultado armazenado novamente em banco.

Em cada uma das etapas, são registradas data e hora da ocorrência do evento, sendo possível, portanto, conhecer, auditar e reconstruir a sequência de recebimento e totalização do BU.

14. Como é realizada a gerência das chaves criptográficas?

15. Como a chave privada é gerada, armazenada e protegida?

16. Trata-se de uma solução somente de hardware, somente de software ou híbrida?

17. Como as chaves públicas são carregadas no sistema central de validação de votos?

Resposta: A resposta abaixo abrange as questões 14, 15, 16 e 17.

A urna eletrônica e os sistemas correlatos, de preparação de dados e de transmissão e recepção de Boletins de Urna utilizam um sistema híbrido de chaves criptográficas.

O Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (Cepesc) que faz parte da estrutura da Agência Brasileira de Inteligência (Abin), órgão da Presidência da República, vinculado ao Gabinete de Segurança Institucional, foi escolhido desde o início da implantação do voto eletrônico no Brasil para a implementação de biblioteca criptográfica responsável por assegurar a troca de informações entre diversos sistemas eleitorais. Tal biblioteca, implementada em *software*, é a que tem maior abrangência e provê primitivas criptográficas de assinatura digital e verificação, além da cifração e decifração de dados.

O Cepesc foi escolhido por defender o uso de criptografia de Estado, produzida dentro do país e por órgãos governamentais, com o objetivo de assegurar a segurança das comunicações e, no caso, da integridade do voto eletrônico e dados correlatos. O Plenário do Tribunal Superior Eleitoral, por meio da Res.-TSE nº 22.597/2007 (ANEXO 23) decidiu, por unanimidade, "[...] *no sentido da continuidade da prestação de serviços pelo Cepesc* [...] *para apoiar a otimização, adaptação, correção e melhoria dos algoritmos criptográficos em uso na Justiça Eleitoral*".

De modo geral, cada sistema que gera informações garante a integridade dos dados intercambiados pelos sistemas de informação relacionados ao processo de cadastro eleitoral,

candidaturas, votação e totalização, e cifra inclusive informações personificadas do eleitor, tal como a biometria.

Para essa biblioteca, os respectivos pares de chaves assimétricos são gerados pela Assessoria do Gabinete da STI do TSE, com o uso também de biblioteca em *software* desenvolvida pelo Cepesc. Esse desenvolvimento é suportado pelo Termo de Execução Descentralizada TSE nº 07/2021 (ANEXOS 24 e 25), firmado com a Agência Brasileira de Inteligência. Uma vez geradas, as chaves são gravadas em mídia e distribuídas aos respectivos titulares das unidades responsáveis pelo desenvolvimento dos sistemas. Cabe destacar que as chaves privadas são criptografadas com senha pessoal do seu proprietário. Uma vez de posse da mídia, os titulares armazenam essas chaves em chaveiros (*key stores*), acessíveis somente pelas aplicações que as utilizam. Deve-se ressaltar que, embora a troca de informações entre sistemas faça uso de chaves públicas e privadas, há a segregação na distribuição de tais chaves entre as unidades responsáveis pelo desenvolvimento dos sistemas eleitorais. Como exemplo, mesmo a unidade responsável por decifrar uma determinada informação não detém a respectiva chave pública utilizada para cifração.

Especificamente para a urna eletrônica, o artigo intitulado "Protegendo o sistema operacional e chaves criptográficas numa urna eletrônica do tipo T-DRE" (ANEXO 26), disponível em https://sol.sbc.org.br/index.php/wte/article/view/14039, demonstra como a proteção das chaves da biblioteca do Cepesc é protegida pela infraestrutura de hardware da urna eletrônica, explicada mais adiante. Dessa forma, as chaves que originalmente estavam protegidas por senha, passam a ser protegidas pelo hardware da urna, num processo de empacotamento executado durante a Cerimônia de Lacração.

Além da biblioteca do Cepesc implementada em *software*, as urnas eletrônicas possuem um perímetro criptográfico, chamado de MSD (*Main Security Device*) nas urnas modelo 2009 a 2015 e depois rebatizado de MSE (Módulo de Segurança Embarcado) a partir das urnas modelo 2020. Nesse perímetro, há um processador ARM responsável por autenticar o conteúdo de toda a inicialização da urna (BIOS, *bootloader* e sistema operacional). Esse perímetro criptográfico também é capaz de gerar e armazenar chaves criptográficas assimétricas atendendo, no mínimo às diretivas do Manual de Condutas Técnicas nº 3 do Instituto Nacional de Tecnologia da Informação – ITI, correspondente a *tokens* criptográficos ICP-Brasil. No caso da UE2020, tal perímetro foi certificado ICP-Brasil. Nesse contexto, importante ressaltar que a aleatoriedade é garantida por um gerador de *números* aleatórios (TRNG) formado por componentes discretos e avaliado pelo CEPESC (ver resposta número 42). O MSE (ou MSD)

da urna foi inicialmente concebido para a urna modelo 2009 e sua arquitetura inicial foi objeto de artigo científico denominado T-DRE: a *hardware trusted computing base for direct recording electronic vote machines* (ANEXO 27), disponível em https://dl.acm.org/doi/10.1145/1920261.1920291.

Por fim, é importante frisar que os perímetros criptográficos das urnas emitem requisições de certificado que são validadas por uma Autoridade Certificadora das Urnas Eletrônicas, cujas chaves privadas estão armazenadas e protegidas em HSMs (*Hardware Secure Modules*) certificados ICP-Br, fabricado pela Kryptus (Empresa Estratégica de Defesa) e que também é um Produto Estratégico de Defesa.

As chaves públicas utilizadas pelos sistemas de recebimento de arquivos de urna e de totalização são carregadas e armazenadas nos servidores de aplicação que hospedam os sistemas por meio de um processo automatizado de *deploy*.

18. Quais os procedimentos de forense digital que a TI do TSE aplica de forma a garantir a integridade das evidências, de uma suposta intrusão aos sistemas proprietários do TSE?

Resposta: Os procedimentos compreendem a identificação do incidente; a custódia de evidências mediante "congelamento"/cópia do ambiente e preservação dos logs existentes; análise do incidente, visando identificação de fatos e evidências adicionais; elaboração de Relatório de Comunicação de Incidente de Segurança – RCIS ; restabelecimento de serviços após ajustes das falhas encontradas; Encaminhamento de relatório à alta gestão; e notificação à Polícia Federal e ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR.gov).

19. Quais são as rotinas de verificação da existência de programa indesejado em execução no sistema operacional da urna eletrônica?

Resposta: A urna só coloca em execução software assinado digitalmente. Há dois mecanismos de validação de assinatura digital de executáveis: um executado pelo kernel e outro em espaço de usuário.

O mecanismo executado pelo kernel é uma extensão desenvolvida pela equipe técnica do TSE. Consiste na integração de assinaturas digitais ECDSA P521 aos arquivos ELF

executados pelo Linux (aplicativos, bibliotecas e módulos de kernel). Essa assinatura é gerada durante a Cerimônia de Lacração e integrada ao binário. Quando o sistema operacional tenta colocar algo em execução (aplicativos, bibliotecas e módulos de kernel), a extensão desenvolvida pelo TSE valida a assinatura digital do executável, permitindo que somente software que contenha assinatura válida entre em execução. Binários não assinados ou com assinatura inválida não são executados e provocam o bloqueio da urna.

Essa extensão do Linux desenvolvida pelo TSE está em processo de integração ao kernel disponível para toda a comunidade (https://www.tse.jus.br/imprensa/noticias-tse/2021/Maio/tse-entra-no-seleto-grupo-de-incorporador-de-funcionalidades-no-linux, ANEXO 28).

A validação de assinatura digital feita em espaço de usuário é um mecanismo de verificação complementar àquele feito pelo kernel, pois permite a validação de binários que não entram em execução imediatamente. Também durante a Cerimônia de Lacração são geradas assinaturas digitais pela biblioteca fornecida pelo Cepesc/Abin para todos os arquivos de sistema incluídos na urna (aplicativos, bibliotecas, módulos de kernel, arquivos de configuração e recursos). Essas assinaturas são incluídas em arquivo específico, o qual geralmente integra todas as assinaturas digitais de um respectivo diretório do sistema de arquivos. Dessa forma, o *daemon* Sistema de Assinatura e Verificação – SAVD do Uenux é capaz de validar a assinatura digital de qualquer arquivo do sistema, mediante solicitação das aplicações, tais como o Gerenciador de Aplicativos – GAP e o Software de Carga – SCUE. Faz parte do processo de inicialização do GAP e do SCUE a validação de assinatura digital de todos os arquivos da urna (mídias interna e externa).

Mais detalhes podem ser encontrados no artigo científico https://sol.sbc.org.br/index.php/wte/article/view/14039 (ANEXO 26), de autoria da equipe técnica do TSE responsável pelo software da urna.

20. Existe algum processo de registro?

Resposta: Todas as validações feitas pelo kernel são registradas no mecanismo padrão de log do sistema (syslog), cujo arquivo fica disponível nas mídias interna e externa da urna. Todas as validações feitas pelo SAVD são registradas no log geral do Uenux, o qual fica disponível nas mídias interna e externa da urna, além de ser copiado para a mídia de resultados e transportado para os servidores do TSE. A partir das Eleições 2022 o log geral do Uenux será

publicado na internet (https://www.tre-mg.jus.br/imprensa/noticias-tre-mg/2021/Outubro/registro-digital-do-voto-e-logs-das-urnas-eletronicas-serao-publicados-na-internet-a-partir-de-2022, ANEXO 29).

21. Como são sincronizados os relógios das urnas eletrônicas?

Resposta: O relógio da urna eletrônica é ajustado pelo operador durante o processo de carga, com o auxílio do aplicativo SCUE. Além disso, também é possível utilizar o aplicativo Ajuste de Data-Hora – ADH para ajuste do relógio após a carga da urna. Em todos os casos, deve ser informada a hora local.

Destaca-se que o uso do ADH é restrito, havendo o registro da geração da sua mídia de ativação e uso da urna eletrônica (registro em log do Uenux e do Gedai-UE). Ademais, o ADH não pode ser executado na urna durante o período de votação, na medida em que há restrição em software controlada pelo GAP.

22. A data influencia a execução do sistema VOTA e dos testes de integridade ou somente é necessário a hora?

Resposta: O Software de Votação – Vota utiliza a data/hora para efetuar controles relativos ao processo de votação. O software pode ser executado independente da data, mas a operação de determinadas funcionalidades está condicionada ao relógio da urna. Existem os seguintes controles no Vota:

– Emissão da zerésima: somente a partir das 7h do dia do pleito;

– Início da votação: somente a partir das 8h do dia do pleito, caso tenha sido impressa a zerézima;

– Encerramento da votação: a partir das 17h do dia do pleito;

– Bloqueio da habilitação de eleitores: a partir das 4h do dia posterior ao pleito, em caso de inatividade da urna.

O sistema de apoio ao teste de integridade (SAVP-Votação) não possui controles baseados em data/hora.

23. Que órgão interno ou contratado realiza a auditoria dos códigos dos sistemas utilizados no processo eleitoral?

Resposta: O art. 66, § 2º, da Lei nº 9.504/1997, delega ao TSE a obrigação de apresentar aos representantes dos partidos políticos e das coligações os programas-fonte e programas executáveis, o que é regulamentado por meio da Res.-TSE nº 23.673/2021 (ANEXO 17), inclusive ampliando o rol de entidades fiscalizadoras, conforme art. 6º da referida norma:

> Art. 6º Para efeito dos procedimentos previstos nesta Resolução, salvo disposição específica, são consideradas entidades fiscalizadoras, legitimadas a participar das etapas do processo de fiscalização:
> I - partidos políticos, federações e coligações;
> II - Ordem dos Advogados do Brasil;
> III - Ministério Público;
> IV - Congresso Nacional;
> V - Supremo Tribunal Federal;
> VI - Controladoria-Geral da União;
> VII - Polícia Federal;
> VIII - Sociedade Brasileira de Computação;
> IX - Conselho Federal de Engenharia e Agronomia;
> X - Conselho Nacional de Justiça;
> XI - Conselho Nacional do Ministério Público;
> XII - Tribunal de Contas da União;
> XIII - Forças Armadas;
> XIV - Confederação Nacional da Indústria, demais integrantes do Sistema Indústria e entidades corporativas pertencentes ao Sistema S;
> XV - entidades privadas brasileiras, sem fins lucrativos, com notória atuação em fiscalização e transparência da gestão pública, credenciadas junto ao TSE; e
> XVI - departamentos de tecnologia da informação de universidades credenciadas junto ao TSE.

24. Quantas e quais foram as auditorias externas realizadas desde 2009?

Resposta: A verificação dos códigos-fonte é realizada rotineiramente, a cada pleito eleitoral, por peritos criminais da Polícia Federal. Os códigos-fonte foram também auditados por especialistas do Partido da Social Democracia Brasileira (PSDB), após as eleições de 2014; por equipe da Procuradoria-Geral da República, que compareceu em duas ocasiões no ano de

2020; recentemente, em 2021, recebemos o Partido Verde e o Partido Liberal; em janeiro de 2022, a Controladoria-Geral da União esteve no TSE durante uma semana para analisar os códigos-fonte; e a expectativa, a confirmar, é a de recebermos, em fevereiro e março de 2022, representantes da Ordem de Advogados do Brasil (OAB), do Conselho Federal de Engenharia e Agronomia (CONFEA), além de representantes da Universidade Federal do Rio Grande do Sul (UFRS) e da Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS).

25. Quais serão os controles e/ou formas de acompanhamento de que os códigos-fonte fornecidos, auditados e eventualmente corrigidos, serão os códigos utilizados durante as eleições de 2022?

Resposta: Os participantes da Cerimônia de Assinatura Digital e Lacração dos sistemas eleitorais poderão assinar digitalmente os sistemas e receber impressos os resumos digitais dos códigos assinados para fins de verificação de integridade e autenticidade dos sistemas eleitorais. Posteriormente, durante as diversas cerimônias previstas na Res.-TSE nº 23.673/2021 (ANEXO 17), poderão verificar a integridade dos sistemas por meio da comparação desses resumos digitais (*hashes*), ou seja, comparar se os resumos digitais recebidos na Cerimônia de Assinatura Digital e Lacração, publicados pelo TSE, correspondem aos dos sistemas utilizados pelos tribunais regionais eleitorais. Quanto a autenticidade dos sistemas as assinaturas poderão ser verificadas nas mesmas cerimônias, por todas as entidades fiscalizadoras, mediante utilização de sistema fornecido pelo TSE ou de sistema próprio desenvolvido pelas entidades.

Para garantir a efetiva verificação de autenticidade e integridade dos sistemas eleitorais, a Res.-TSE nº 23.673/2021 estabelece que durante a cerimônia de preparação de urnas, a verificação por amostragem será realizada em até 3% (três por cento) das urnas preparadas escolhidas por representantes das entidades fiscalizadoras presentes na cerimônia entre as urnas de votação e as de contingência, ou na ausência de escolhas, pela autoridade eleitoral responsável, observado o mínimo de: 1 (uma) urna por município para cada zona eleitoral nas eleições municipais, 1 (uma) urna por zona eleitoral nas eleições gerais.

Adicionalmente a essas verificações, a Res.-TSE nº 23.673/2021, também estabelece a obrigatoriedade de realização, no dia da eleição, do Teste de Autenticidade dos Sistemas Eleitorais, quando são verificados os resumos digitais (*hashes*) e as assinaturas nas urnas de 21 (vinte e uma) seções eleitorais distribuídas nas unidades da federação.

Finalmente, a urna eletrônica possui uma arquitetura de *hardware* e de *software* que garante que somente *software* assinado durante a Lacração pode ser executado na urna em modo Oficial. Essa verificação é feita pelo *hardware* e evidenciada pelo LED de Segurança, que precisa estar na cor verde. Todos os mesários e fiscais são orientados a fazer a verificação quanto ao estado desse LED.

26. Quais são os mecanismos que garantem a relação entre os códigos-fonte e binários que são assinados durante a cerimônia de assinatura digital e lacração dos sistemas eleitorais?

Resposta: O principal mecanismo é a própria cerimônia pública de Assinatura Digital a Lacração dos Sistemas Eleitorais, na qual os códigos-fontes são compilados diante dos representantes das entidades fiscalizadoras. Após a compilação, são gerados resumos digitais dos artefatos gerados, que são publicados na Internet, para permitir ampla auditabilidade. Todos os códigos-fontes e respectivos binários são lacrados em mídia não-regravável (DVD), que é preservada em cofre dentro de sala-cofre nas dependências no Tribunal Superior Eleitoral, para verificação das entidades fiscalizadoras a qualquer tempo. Adicionalmente, há estudos em curso em relação ao provimento de compilação determinística no que diz respeitos aos sistemas de urna eletrônica.

27. Os códigos-fonte relacionados com os binários assinados podem ser auditados após a cerimônia de assinatura digital e lacração dos sistemas eleitorais?

Resposta: Em que pese não haver em resolução uma cerimônia específica para auditar código-fonte após a sua assinatura e lacração, o TSE, mediante requerimento, pode autorizar essa auditoria. Inclusive, após as Eleições 2014, o PSDB, em 2015, auditou os códigos-fonte e binários utilizados naquelas eleições majoritárias.

28. Quais são os procedimentos de verificação e geração de alertas para tentativas de inserção de códigos, legítimas ou não, durante todo o processo do processo do sistema eleitoral?

Resposta: O código fonte dos sistemas eleitorais é armazenado e versionado na ferramenta de gestão de versão denominada Git. Nesta ferramenta, os sistemas são organizados

em repositórios, de forma que apenas os profissionais envolvidos em um projeto tenham privilégio de alteração de código. Todas as ações de alteração de código são registradas, possibilitando, a qualquer momento, identificar o responsável por uma alteração ou inserção de algum item no código-fonte dos produtos de *software*. Além disso, todas as necessidades de alteração identificadas são mantidas em *backlog*, planejadas e atribuídas à equipe de desenvolvimento, evitando que manutenções não conhecidas sejam incorporadas ao produto final.

O processo de desenvolvimento contempla também um conjunto de testes, desde testes unitários, passando por testes funcionais específicos, testes de integração, de homologação, teste público de segurança, simulados, possibilitando a identificação de inserção de novos comportamentos nos programas.

Por fim, a Res.-TSE nº 23.673/2021 prevê um conjunto de procedimentos, tais como inspeção de código-fonte, auditoria de teste de integridade das urnas eletrônicas, que permitem verificar a exatidão dos sistemas. As verificações podem ser realizadas pelos representantes das entidades fiscalizadoras relacionadas no art. 6º e já mencionadas na resposta da questão 23.

29. Qual o mecanismo de lacre utilizado para que não haja violação da urna eletrônica?

Resposta: Os lacres utilizados nas urnas eletrônicas são confeccionados pela Casa da Moeda do Brasil (CMB), a partir de um substrato de poliéster (amarelo para as Eleições 2022), revestido de adesivo tipo acrílico, de alta adesão inicial e final com sistema de evidência de violação que identifique a tentativa de remoção do lacre, sem deixar resíduos na superfície em que for aplicado. Ao ser retirado, é evidenciado o texto "TSE TSE TSE...".

Para a personalização, a CMB elabora um leiaute composto por requisitos de segurança como fundo numismático e microletras, com auxílio de ferramenta gráfica utilizada no design de cédulas de dinheiro. Também é empregado o uso de tinta reativa a luz ultravioleta.

Cabe ressaltar que a principal função do lacre é se apresentar como uma primeira camada de segurança, para auxiliar na análise forense posterior associando aos procedimentos e cerimônia de preparação das urnas. No caso do Teste Público de Segurança (TPS), as urnas são disponibilizadas sem lacres para as tentativas de invasão de forma a permitir que o

investigador possa atuar diretamente no propósito de seu plano de ataque, ou seja, que esse não tenha que vencer barreiras anteriores àquela(s) que pretende atacar.

30. Quando do recebimento de urna com lacre violado, quais são os procedimentos adotados no caso dela conter votos e no caso dela não conter?

Resposta: Caso haja a violação de lacre antes da eleição, essa urna deve ser investigada, ocorrendo uma nova carga e lacração desse equipamento. Agora, caso a violação ocorra após a eleição, igualmente recomenda-se a abertura de uma investigação, cabendo ao juiz eleitoral decidir se os votos serão validos ou não. Destaca-se, nesse ponto, que existe funcionalidade específica no sistema de totalização, para que os votos sejam totalizados em separado, ficando sub judice, até que haja uma decisão sobre a questão. Compete ao magistrado atuar em cada caso específico. Diante da conclusão da investigação, serão aplicadas as regras eleitorais quanto à anulação ou validação dos votos.

É importante destacar que um dos primeiros atos da Junta Eleitoral é o de verificar se os documentos estão idôneos, dentro desses, os lacres das urnas.

Outro ponto a ser reforçado é que em uma investigação de uma urna, que teve seus lacres violados, pode ser feita a análise de seus *logs*, averiguando se há registro de tentativas de manipulação desses equipamentos.

Por fim, salienta-se que, no que diz respeito a possíveis violações dos lacres das urnas antes da eleição, há dois momentos em que pode ser verificada a integridade desses lacres: na vistoria obrigatória na véspera do dia de votação, e no dia da eleição, no qual o mesário é orientado a verificar se tudo está de acordo com o equipamento para, caso esteja, junto com os presentes, iniciar a votação. Nessa última hipótese, havendo alguma suspeita quanto à integridade do equipamento, o juiz eleitoral deve ser chamando, sendo recomendada a troca do equipamento suspeito, por um de contingência.

31. Porque houve a mudança de procedimento quanto a totalização dos votos, enviando diretamente ao TSE?

Resposta: A centralização da totalização de votos no TSE é parte de um processo histórico de evolução da totalização dos votos. Historicamente, é preciso saber que, quando implementado o sistema eletrônico de votação, as primeiras totalizações automatizadas

ocorreram em computadores existentes nas juntas eleitorais, instaladas fisicamente nos Cartórios Eleitorais ou em locais designados para seu funcionamento. Após a totalização pelas zonas eleitorais, o resultado era transmitido e centralizado em cada Tribunal Regional Eleitoral, que totalizava o resultado da Unidade da Federação, nas eleições gerais, e encaminhava esse resultado ao TSE para realizar, por fim, a totalização nacional. Nas eleições municipais, todo o processo de totalização e resultado era processado nos servidores instalados na junta, sendo transmitidos, ao final, ao TRE, para fins de armazenamento e guarda. Essa arquitetura, porém, obrigava o TSE a manter para cada zona eleitoral um conjunto de equipamentos com configuração padrão, licenças de software, local com segurança física e lógica, equipe capacitada, entre outros elementos exigidos para que o processo transcorresse dentro do esperado.

Com a melhoria da capacidade de processamento dos equipamentos servidores e a melhoria dos links de comunicação no país, há mais de 15 anos foi possível centralizar nos tribunais regionais eleitorais a totalização das eleições no estado. Obviamente, essa medida proporcionou dois resultados positivos. Primeiro, obteve-se valorosa economia ao erário, em aquisição de máquinas, licenças de software, instalações físicas e serviços. Segundo, aumentou-se a segurança do processo de totalização na medida em que se passou de 3.073 locais de totalização para apenas 27.

De forma análoga, podemos trazer para a decisão da centralização da totalização no TSE as mesmas razões que levaram à centralização da totalização nos tribunais regionais. A essas razões soma-se a recomendação contida em relatório produzido pelos peritos da Polícia Federal, que aconselhou a centralização da totalização como uma forma de diminuição da superfície de ataque de hackers, ou seja, a redução do leque de potenciais ataques propiciados pelo ambiente tecnológico descentralizado quando comparado ao centralizado nas instalações físicas do TSE.

A recomendação de peritos da Polícia Federal ocorreu no âmbito dos Testes Públicos de Segurança, evento já conceituado na resposta da Questão 25 do Ofício nº 001. Não houve, assim, nenhum evento concreto de vulnerabilidade na totalização de resultados pelos Tribunais Regionais Eleitorais que tenha levado à alteração do sistema.

Após o TPS de 2017-2018, que começou em 2017 e foi concluído poucos meses antes da eleição de 2018, a Polícia Federal entregou, em outubro de 2018, um relatório elaborado por três peritos com análise dos códigos-fonte dos sistemas eleitorais nas Eleições

2018. O documento identifica que cada um dos 27 TREs realizava a totalização dos votos registrados a partir de um servidor instalado fisicamente em cada TRE, mas cuja administração e manutenção estava a cargo do TSE. O documento aponta que "*mudar a arquitetura de servidores para estarem fisicamente localizados no próprio TSE melhora[ria] consideravelmente a segurança operacional deste sistema*" e reduziria ponto de vulnerabilidade que poderia ser especialmente explorado em "*um ambiente com base de dados distribuída em cada TRE*". Por fim, conclui que *"[n]a arquitetura descentralizada, o fato de existir um banco de dados e um servidor de aplicações local em um computador em cada TRE aumenta o leque de potenciais ataques ao ambiente, que podem ser mitigados com a localização física destas máquinas no ambiente do TSE*".

Considerados os benefícios da centralização (maior economicidade e maior segurança) e a partir do relatório dos peritos da Polícia Federal corroborando os benefícios da medida, o TSE implantou a centralização da totalização dos resultados a partir das Eleições 2020.

32. Qual é a percentagem de sucesso no reconhecimento de eleitores pela biometria?

Resposta: Considerando que não foi utilizado o reconhecimento biométrico na urna nas eleições de 2020 em razão das medidas de combate à pandemia do Novo Coronavírus, os dados mais recentes de identificação biométrica do eleitor são das eleições de 2018.

Naquela ocasião, e considerando apenas o domínio de eleitores de municípios 100% biométricos e que compareceram à seção eleitoral, temos os seguintes números:

– Percentual de eleitores de municípios biométricos reconhecidos na urna no primeiro turno: 88,59%;

– Percentual de eleitores de municípios biométricos não reconhecidos na urna no primeiro turno: 11,41%;

– Percentual de eleitores de municípios biométricos reconhecidos na urna no segundo turno: 88,72%; e

– Percentual de eleitores de municípios biométricos não reconhecidos na urna no segundo turno: 11,28%.

33. Dado que o eleitor possui biometria cadastrada, qual a percentagem de verdadeiro positivo, verdadeiro negativo, falso positivo e falso negativo da detecção?

Resposta: Inicialmente, é necessário esclarecer que o processo de habilitação do eleitor por meio da biometria na urna é processo que ratifica a verificação da identidade do eleitor, feita pelo mesário. Portanto, é processo de verificação biométrica e não de identificação biométrica. Adicionalmente, em qualquer caso, as imagens das biometrias lidas no dia da eleição são preservadas no TSE para eventual investigação. Essa verificação na urna se dá da seguinte forma:

– O eleitor apresenta à mesa receptora de votos documento com foto;

– O mesário examina o documento, localiza o eleitor no caderno de votação, onde consta a foto do eleitor, e digita o número da sua inscrição eleitoral no terminal;

– O eleitor posiciona o dedo indicador ou polegar no leitor biométrico da urna;

– Havendo coincidência da biometria lida do eleitor com a cadastrada na urna, a habilitação estará completa;

– Não havendo coincidência, o eleitor pode repetir o procedimento por até quatro vezes;

– Após as quatro tentativas, não sendo possível identificar o eleitor por meio da biometria, o mesário deve indagar ao eleitor o seu ano de nascimento e digitá-lo no terminal;

– Estando o ano de nascimento correto, o eleitor é habilitado e o mesário deve coletar sua própria biometria na urna para fins de registro de autoria da operação.

Considerando tais procedimentos, para que houvesse um falso positivo, seria necessário que um eleitor mal-intencionado apresentasse uma documentação falsa, que esta não fosse percebida pelo mesário e que a biometria do falso eleitor fosse erroneamente identificada com sucesso.

34. Dentre as soluções de VPN disponíveis (de mercado, customizada, código aberto, gratuita, paga) qual a adotada para a transmissão dos dados das seções eleitorais para o sistema central de consolidação dos votos, localizado no TSE?

Resposta: A rede entre o TSE e os TRE denomina-se backbone principal. É provida por SDWan dedicada, contratada junto a operadoras de telecomunicações. A rede entre os TRE e os Cartórios Eleitorais é denominada backbone secundário e é provido por enlaces dedicados providos por operadoras de telecomunicações. Nos backbones da Justiça Eleitoral, as

tecnologias de VPN são utilizadas quando, por contingência, é necessário estabelecer comunicação por meio de links de internet. São utilizadas tecnologias dos fabricantes CheckPoint, FortiNet e SonicWall.

Adicionalmente, a solução JE-Connect (melhor detalhada na resposta à pergunta 38 abaixo) utiliza-se OpenVPN.

35. Como garantir que eleitores que apresentaram justificativa eleitoral em razão de impedimento para comparecer no dia da votação, não constem como votado numa determinada eleição?

Resposta: A urna eletrônica é desconectada de qualquer tipo de rede de dados, portanto não é possível conhecer no momento da votação se o eleitor já apresentou justificativa em outro município. Ao final da votação, a urna gera, dentre outros, arquivo contendo a informação dos eleitores que compareceram e daqueles que faltaram. Ao processar esse arquivo, o cadastro eleitoral verifica se houve eleitor que compareceu e justificou na mesma eleição. Diante desse cenário, a situação de comparecimento se sobrepõe à situação de justificativa, resultando em análise ou investigação superveniente. Quanto ao voto, é computado normalmente, uma vez que não é possível identificar o eleitor.
A principal garantia de que alguém não votará pelo eleitor é a existência da biometria dos eleitores no momento da habilitação para o voto. Hoje a biometria já alcança 80,5% do eleitorado, o que significa que a maior parte da população brasileira já tem o seu direito de voto assegurado por esse mecanismo. A hipótese ventilada de um possível voto à revelia do eleitor constitui crime eleitoral com pena de 1 a 3 anos (art. 309 do Código Eleitoral).

Consta do art. 114 da Res.-TSE nº 23.669/2021 (ANEXO 30), que dispõe sobre os atos gerais do processo eleitoral para as Eleições 2022:

> Art. 114. Na hipótese de não reconhecimento da biometria, após a última tentativa, o(a) presidente da mesa deverá conferir se o número do título digitado no Terminal do Mesário corresponde à inscrição da eleitora ou do eleitor e, se confirmado, indagará o ano do seu nascimento, digitando-o no Terminal do Mesário e:
> I - se coincidente, autorizará a eleitora ou o eleitor a votar;
> II - se não coincidente, em última tentativa, repetirá a pergunta quanto ao ano de nascimento e digitará no Terminal do Mesário;

III - se persistir a não identificação, a eleitora ou o eleitor será orientado(a) a contatar a Justiça Eleitoral para consultar sobre o ano de nascimento constante do Cadastro Eleitoral, para que proceda à nova tentativa de votação.

§ 1º Comprovada a identidade, a eleitora ou o eleitor:

I - assinará o Caderno de Votação ou premirá sua impressão digital, se não souber ou não puder assinar;

II - será habilitado(a) a votar mediante a leitura da digital da mesária ou do mesário; e

III - será orientado(a) a procurar posteriormente o cartório eleitoral para atualização de seus dados (Res.-TSE nº 23.659/2021, art. 8º, § 4º).

§ 2º As situações ocorridas neste artigo deverão ser consignadas na Ata da Mesa Receptora.

36. Há visualização de solução por parte do TSE para superar a possibilidade de perda de voto por falha de mídia eletrônica?

Resposta: A urna eletrônica trabalha com duas mídias durante o processo de votação: a mídia interna (MI) e a mídia externa, também chamada de mídia de votação (MV). Durante a votação, os votos são gravados no arquivo de Registro Digital do Voto – RDV, que em seguida é assinado digitalmente e validado (assinatura e conteúdo). A gravação do RDV se dá tanto na MI e na MV, repetindo-se o processo de assinatura e validação em ambas as mídias. Esse mecanismo de gravação redundante dos votos minimiza a possibilidade de perda de dados em caso de falha em uma das mídias.

Ao final da votação, os arquivos de resultado (boletim de urna, log, RDV e outros) são gravados na mídia de resultados (MR). Em caso de falha na MR, é possível utilizar o aplicativo Recuperador de Dados – RED para a cópia dos arquivos de resultado para uma nova MR. O RED também pode ser usado para a recuperação de dados em MIs ou MVs, na medida em que os arquivos de resultado são gravados também em ambas as mídias da urna.

Na impossibilidade de acesso aos resultados eletrônicos é possível proceder com a totalização do boletim de urna impresso. Para isso, é preciso utilizar o Sistema de Apuração – SA para que seja feita a digitação do boletim numa nova urna e, dessa forma, seja reproduzido o resultado em formato eletrônico para a totalização.

37. Caso uma eleição seja decidida por um número de votos menor do que o total que foi desconsiderado por falha na mídia eletrônica, como será resolvida uma possível incoerência que pode advir da desconsideração, total ou parcial, de votos?

Resposta: Na remota hipótese de impossibilidade de recuperação dos votos de uma urna eletrônica, cabe ao juiz eleitoral da respectiva zona eleitoral determinar a anulação integral da seção eleitoral. Num cenário em que os votos perdidos (anulados) façam diferença para a determinação do resultado, proceder-se-á conforme o disposto nos arts. 187 e 201 do Código Eleitoral (Lei nº 4.737/1965).

38. Que tipo de equipamento (computador, estação de trabalho) é utilizado para a transmissão dos dados das seções eleitorais para o sistema central de consolidação de votos localizado no TSE?

Resposta: A transmissão dos arquivos de urna é realizada por sistemas próprios da Justiça Eleitoral, conforme preconiza a resolução de atos gerais, que normatiza os procedimentos operacionais do pleito.

Os sistemas de transmissão, por sua vez, podem ser executados em dois ambientes:

a) em estação de trabalho da Justiça Eleitoral, com SIS; ou
b) a partir de máquinas virtuais estabelecidas pelo sistema JE-Connect.

O SIS (Subsistema de Instalação e Segurança) consiste de um software desenvolvido sob especificação da Justiça Eleitoral e que possui os respectivos módulos e características:

i. Módulo de Configuração de segurança: consiste na parcela do SIS instalada logo após o Windows ser instalado, antes, portanto, das demais partes do SIS. Responsável por inicializar o sistema de segurança, criar partição criptografada no disco e guarnecer o sistema operacional;

ii. Módulo de Instalação e atualização: responsável por instalar, atualizar e desinstalar as aplicações seguras nas máquinas da Justiça Eleitoral, bem como garantir a segurança nessas operações. Realiza controle de versões;

iii. Módulo de Controle de acessos: responsável por cadastrar usuários, validar logon e apresentar a janela que dá acesso às aplicações da Justiça Eleitoral, conhecida como "Gerenciador de Aplicações Seguras";

iv. Módulo de Proteção e auditoria: responsável por restringir acessos externos ao computador e controlar o histórico de operações. Utilizado ainda para detecção e investigação de tentativas de invasão ao sistema. Faz uso do VAP - Verificador de Autenticação de Programas, destinado à verificação dos resumos digitais (hash) dos programas instalados em

microcomputadores e bloqueando a execução de sistemas seguros cujo hash não seja equivalente ao esperado;

v. Módulo de Cópia de segurança: responsável por criar cópias de dados de usuários e sistemas, com objetivo de resguardar contra ocasional perda de arquivos originais.

Já o sistema **JE-Connect** consiste de um conjunto de soluções destinadas a prover a criação de máquinas virtuais sobre microcomputadores e estabelecer conexão segura com a rede de comunicação de dados da Justiça Eleitoral. É composto pelos seguintes sistemas:

i. **JEC-Admin**: é uma solução integrada ao sistema ODIN (sistema de autenticação, autorização e controle de acesso de usuários em sistemas WEB da Justiça Eleitoral), e responde pelo processo de gestão de grupos de geração de Kits JE-Connect, sendo também responsável pela requisição de criação de chaves e certificados para a autoridade certificadora da solução JE-Connect. É através deste sistema que são gerados certificados e definidas quais as configurações de conexão à rede da Justiça Eleitoral devem ser utilizadas. Além disso, é através deste sistema que são gerenciadas senhas de oficialização dos Kits JE-Connect. Sem a Oficialização, um Kit JE-Connect não funciona no dia da eleição. A solução JE-Connect se vale do uso de certificados digitais para identificar univocamente cada um dos clientes que ingressam na rede privada virtual estabelecida para o recebimento de dados. Desta forma, cada Kit JE-Connect deve possuir suas próprias chaves: pública e privada. A geração do conjunto de chaves públicas e privadas é solicitada pelo sistema JEC-Admin e é gerado na AC-JEC para que possa ser utilizada pelo Kit JE-Connect (cliente da rede privada virtual) para acesso ao JEC-Sense (provedor do serviço de rede privada virtual da solução).

ii. **AC-JEC**: autoridade certificadora centralizada no TSE. Recebe pedidos para geração de certificados digitais dos sistemas JEC-Admin, gera-os e os armazena em um repositório de dados da solução. Responsável por revogar certificados dos kits sob demanda da solução JEC-Admin. Toda geração de chaves públicas e privadas que serão inseridas nos Kits JE-Connect é realizada de forma centralizada, gerando certificados únicos e individuais para cada Kit JE-Connect. Usualmente, para cada um dos Kits JE-Connect, são geradas três pares de chaves para autenticação do kit nos sistemas JEC-Sense. Cada um destes certificados é específico para uma fase do processo eleitoral. São elas: fase simulado, fase oficial primeiro turno, fase oficial segundo turno.

iii. **JEC-Repo**: O JEC-Repo é o repositório centralizado de dados disponibilizados pelos demais sistemas para que possam ser utilizados no processo de geração de Kits JE-Connect. Neste repositório são mantidos os certificados gerados para os Kits que serão

utilizados pelo sistema JEC-Gerador para criação de Kits JE-Connect. O controle de permissões é realizado através dos grupos de geração de Kits e a autenticação é mantida pelo JEC-Admin, sendo-o armazenamento individualizado por Unidade Federativa. Por ser um sistema centralizado, permite o controle de versão e configuração de todo o processo de geração de Kits.

iv. **JEC-Gerador**: Realiza a gestão da geração dos Kits JE-Connect. Sua função principal é gerar os Kits JE-Connect e tem como pré-requisitos: O microcomputador deverá estar conectado à rede local; e comunicar-se com a base do JEC-Admin. **Cada um dos Kits JE-Connect é único de tal forma que deve ser gerado separadamente e de maneira individual**. Também é responsabilidade do sistema JEC-Gerador a geração de listas de correlação dos Kits gerados, em um processo que remete às tabelas de correspondência geradas no processo de carga de urnas eletrônicas.

v. **Kit JE-Connect**: O Kit JE-Connect é operacionalizado através de duas mídias do tipo pendrive. Uma que hospeda o sistema operacional que será inicializado na máquina e outro que hospeda uma chave que é utilizada como "keyfile" no processo de decifração de partições. A primeira mídia pendrive é chamada de Mídia de Sistema Embarcado - MSE e a segunda é chamado de Mídia-Chave - MC. Esse conjunto de pendrives realiza a carga de um sistema operacional GNU/Linux que por sua vez permite o ingresso à rede privada estabelecida na rede da Justiça Eleitoral para transporte de dados de urnas eletrônicas através do uso do sistema Transportador.

vi. JEC-Sense: O JEC-Sense é o sistema que estabelece a Rede Privada Virtual - VPN que permite o ingresso de computadores interconectados na rede de comunicação de dados da Internet na rede privada da Justiça Eleitoral. Baseado na distribuição PF-Sense, o JEC-Sense utiliza o sistema OpenVPN para gerar pontos de acesso nas infraestruturas de redes de comunicação de dados dos tribunais regionais e sede do TSE. O JEC-Sense também é responsável pela gestão das conexões não permitindo acessos simultâneos para mesmos certificados. Para o Regional que se interessar em implantar a infraestrutura de VPN com JEC-Sense, clicar aqui para obter acesso à documentação de implantação.

vii. JEC-Monitor: O sistema JEC-Monitor é aquele responsável pela gestão do ciclo de vida da solução JE-Connect. Ou seja, é utilizado para verificar quais "Kits" estão conectados nos pontos de entrada da rede privada virtual e permitir a troca de informações com os mesmos. Portanto, o sistema JEC-Monitor é importante para logística sobre quais sistemas estão homologados, não homologados e finalizados. Por exemplo, um ponto de transmissão "B" pode ser contingência de um ponto de transmissão "A" e neste caso não pode ficar com estado de

finalizado até que o ponto de transmissão "A" tenha transmitido todos os dados de suas seções. O sistema JEC-Monitor também possui a capacidade para realizar resposta ativa contra atividades suspeitas. Através do monitoramento de quais Kits JE-Connect estão conectados, das correlações esperadas, estado dos Kits JE-Connect e de informações recebidas dos próprios Kits o monitoramento pode finalizar conexões e bloquear acesso de Kits específicos.

39. Existe algum padrão ou norma de segurança para definir esse equipamento?

Resposta: Para as eleições de 2020, as características mínimas dos microcomputadores a serem adotados para a execução dos sistemas eleitorais foram levadas a conhecimento dos TRE por meio dos do Ofício-Circular GAB-DG nº 7/2020 (ANEXO 31), o qual estabelecia a obrigatoriedade de microcomputador com SIS e Windows 10, e, por meio do Ofício-Circular GAB-DG nº 281/2020 (ANEXO 32), que incluiu a exigência de Chip TPM nos microcomputadores.

40. Caso um equipamento (computador, estação de trabalho), utilizado para a transmissão dos votos de uma seção eleitoral, esteja comprometido, quais são os procedimentos adotados?

Resposta: Havendo falha do equipamento ou eventual suspeita de seu comprometimento, o envelope lacrado contendo a mídia de resultado da seção eleitoral é conduzido a outro ponto de transmissão ao tempo em que o equipamento é isolado para análise posterior.

No caso de uso de solução JEConnect e haja suspeita de comprometimento, o sistema JEC-Monitor revoga as credenciais daquela conexão e, de forma similar ao caso anterior, o envelope lacrado com a mídia de resultado é conduzido a outro ponto de transmissão.

É importante ressaltar que os resultados das eleições são conhecidos às 17h, quando as urnas eletrônicas são encerradas. Nesse momento, todas as urnas do país emitem um relatório de votação, o Boletim de Urna (BU), que é distribuído aos partidos políticos, afixado nos locais de votação e enviado às juntas apuradoras. Mesmo que um equipamento comprometido conseguisse alterar um BU durante a transmissão, isso seria identificado no processo de validação de assinatura no momento do recebimento, ou pela simples conferência entre os dados totalizados e o BU impresso pela urna.

41. Como ocorre o procedimento de descarte das urnas eletrônicas consideradas ultrapassadas?

Resposta: As urnas consideradas inservíveis (que ultrapassaram sua vida útil média de dez anos ou seis eleições) são alienadas a partir de um procedimento licitatório de maior preço por peso de material. São alienadas as urnas e os materiais correlatos (baterias, suprimentos etc.). As urnas modelo 2006 e 2008, por exemplo, estão sendo descartadas, por meio de contrato firmado a partir da Licitação TSE nº 01/2021 (ANEXO 33, e a documentação pode ser obtida a partir do site https://www.tse.jus.br/silic/pages/internet/licitacao/index.faces; "licitações concluídas").

O procedimento a ser seguido pela contratada se resume a: coletar as urnas nos tribunais eleitorais, desmontagem e separação dos materiais, descaracterização das partes exclusivas da urna, encaminhamento para reciclagem ou aterro sanitário adequado. Na coleta, uma comissão do tribunal eleitoral acompanha a pesagem do caminhão vazio, a pesagem após carregamento, a lacração do caminhão. No local de descarte, há uma equipe residente do TSE para acompanhar a deslacração do caminhão, desmonte e descaracterização do material e encaminhamento para reciclagem ou aterro sanitário. Conforme critérios definidos em edital, no mínimo 95% da urna deve ser reciclada, sendo que o restante deve ser encaminhado para o aterro sanitário adequado ao tipo de resíduo.

Cabe ressaltar que o principal processo relativo à segurança é a descaracterização, que garante que nenhuma placa eletrônica ou parte visual da urna esteja em uma dimensão que possa ser aproveitada para tal fim.

A título de exemplo, o edital de descarte exige que haja descaracterização completa das placas e outras partes, por trituração/moagem, no próprio local de desfazimento com o acompanhamento de servidores do TSE. Ainda, na fabricação de urnas eletrônicas, há o controle via sistema dos módulos a serem descartados, com perfuração antes de sair do ambiente fabril, dos principais chips que contém firmwares criptográficos. O fabricante das urnas encaminha tais módulos perfurados para descaracterização completa por empresas especializadas.

42. O TRNG é um chip de mercado ou de desenvolvimento customizado encomendado pelo TSE especialmente para as Urnas Eletrônicas?

Resposta: A arquitetura de segurança da urna eletrônica possui dispositivos seguros com funções criptográficas que se auxiliam de geradores de números aleatórios. Tais dispositivos são:

– MSE – Módulo de Segurança Embarcado, residente na placa-mãe;

– MSTE – Módulo de Segurança do Teclado do Eleitor, responsável pela cifração das teclas digitadas pelo eleitor;

– MSIR – Módulo de Segurança da Impressora de Relatórios, responsável pela segurança dos dados enviados pela urna para a impressão de relatórios; e

– MSLB – Módulo de Segurança do Leitor Biométrico.

Os principais dispositivos de segurança da urna eletrônica são o MSE, responsável pelas chaves de assinatura e cifração de cada urna e o MSTE, pela criticidade inerente à digitação da escolha do eleitor no teclado. Em tais dispositivos, o gerador de números aleatórios deve ser projetado e implementado com componentes discretos, não sendo admitidos estarem embutidos em um circuito integrado de mercado. Os circuitos desses TRNGs são também analisados pelo Cepesc, além da análise de testes de aleatoriedade conforme regras dispostas em edital.

No site https://www.tse.jus.br/silic/pages/internet/licitacao/index.faces, pode ser obtido o Edital de Licitação TSE nº 43/2019 (arquivo Lct. 043 - RP Urna Eletronica UE2020.zip). As especificações relativas ao TRNG e arquitetura de segurança da urna estão descritas principalmente no Anexo IV – Especificações técnicas – Segurança. Em especial, os itens mais importantes relativos aos TRNGs são os itens 4.6 e subitens; H.11 e subitens (ANEXO 34).

43. Como é constituído o sistema de monitoramento de infraestrutura de rede que apoia o sistema eleitoral?

Resposta: O Monitoramento de infraestrutura é realizado por unidade formalmente constituída no organograma do TSE, a Seção de Monitoramento da Produção (SEMOP). A SEMOP possui um NOC que funciona em regime 24x7, gerando alertas e chamados em atenção a incidentes e sobrecarga nas aplicações.

44. Como tais atualizações são incorporadas no UENUX?

Resposta: O Uenux é uma distribuição Linux criada pela equipe técnica do TSE. Dessa forma, a atualização dos seus componentes de software não está condicionada à integração feita por terceiros. A equipe técnica do TSE tem absoluto controle sobre a integração de atualizações de segurança aos componentes do Uenux. A equipe adota sistemática de atualização frequente e monitora a evolução do software de terceiro integrado ao Uenux. As atualizações são integradas em tempo hábil para a condução de testes de integração de larga escala antes da Cerimônia de Lacração, com vistas à garantia da estabilidade e corretude do software.

45. Existe algum registro que mostre o tempo levado para que uma atualização na distribuição Linux seja incorporada no UENUX?

Resposta: O Uenux possui um ciclo de 2 anos para entrada em produção, o que ocorre a cada Cerimônia de Lacração. A cada ciclo, o kernel do Linux é atualizado para a última versão com suporte de longo prazo disponível (LTS) e recebe os incrementos e atualizações de segurança periodicamente. Essa periodicidade ocorre em média a cada seis meses, encerrando-se poucos dias antes da Lacração, ainda a tempo da condução de testes de integração em larga escala, com vistas à garantia da estabilidade e corretude do software.

46. Quais são os mecanismos de controle utilizados para prevenir que um ataque de negação de serviço (DoS/DDoS) possa interferir na transmissão dos dados de votação para o sistema totalizador do TSE?

Resposta: A transmissão dos dados de votação não utiliza os enlaces de comunicação do TSE com a internet. Tais dados chegam ao TSE por meio de dois caminhos:

a) Por meio dos backbones da Justiça eleitoral (vide resposta à pergunta 34), constituindo-se de conjunto de enlaces dedicados que interligam os Cartórios Eleitorais ao TSE;

b) Por meio de VPN estabelecida por meio da Soluçao JEConnect (vide resposta à pergunta 38).

No primeiro caso, o trânsito de informações utiliza-se apenas de enlaces internos. No segundo caso, a Solução JEConnect é configurada para que cada Tribunal Regional Eleitoral possua outro Tribunal como contingência às suas conexões. Caso tanto a conexão primária (o

próprio TRE) quanto a secundária (o TRE de contingência) estejam indisponíveis, os envelopes lacrados contendo as mídias de resultado são conduzidas até o Cartório Eleitoral para transmissão por meio da rede interna da Justiça Eleitoral.

Adicionalmente, mesmo que os enlaces de comunicação com a internet não sejam usados para transmissão de dados de totalização, os contratos efetivados pelo TSE preveem que os SOC das operadoras devam mitigar todos os ataques DDoS. Isso é feito por meio da integração de equipamentos ARBOR Pravail do TSE com ARBOR PeakFlow das operadoras.

Adicionalmente, no período eleitoral, o TSE estabelece centrais de comando e controle com os SOC das operadoras para que possam ser realizadas ações de bloqueios geográficos nos backbones das operadoras (se possível fora do Brasil), conforme necessidade de interrupção de tráfego. Fazem ainda parte dessa central de comando e controle representantes das Operadoras de Telecomunicações, ANATEL, ANEEL, Operador Nacional do Sistema Elétrico e INPE (meteorologia).

47. Já foram realizados testes para avaliar os controles configurados e em consequência estabelecer o nível de confiabilidade?

Resposta: Os ataques de DDoS em direção à Justiça Eleitoral não são raros, tendo ocorrido inclusive no 1º Turno das Eleições Municipais de 2020. Durante um ataque de DDoS, as equipes técnicas das operadoras interagem com equipes do TSE para efetivação dos bloqueios e restabelecimento de serviços. Trata-se de prática bastante operacionalizada e, portanto, testada de modo a aferir sua efetividade.

48. No processo de licitação das urnas, como é exigido dos fornecedores uma comprovação/certificação de que eles seguem as melhores práticas de segurança e de conformidade bem como aplicam as mesmas exigências para as respectivas cadeias de produção?

Resposta: A seleção de fornecedor feita pela licitação de urnas eletrônicas se baseia principalmente na apresentação de um protótipo de urna, denominado Modelo de Engenharia, que deve ser submetido a dezenas de testes para aferir a capacidade da empresa em desenvolver uma urna, tanto do ponto de vista de projeto eletrônico (eficiência energética, estabilidade etc), quanto do ponto de vista de segurança, pois o protótipo deve atender com sucesso a vários testes

que consistem em desafios criptográficos. Os critérios de seleção de fornecedor estão definidos principalmente no Anexo I do Edital de Licitação TSE nº 43/2019 (ANEXO 35, e o edital e seus anexos podem ser obtidos no sistema SILIC, "licitações concluídas", disponível em https://www.tse.jus.br/silic/pages/internet/licitacao/index.faces).

Na cadeia de produção, há exigência de rastreabilidade total dos componentes da BOM (*Bill of Material*) de todos os módulos da urna eletrônica. Especificamente quanto aos *firmwares* criptográficos embarcados nos dispositivos de segurança, há a exigência de que a gravação seja feita apenas na fábrica de integração das urnas, em que há uma equipe de servidores do TSE realizando auditorias.

No contexto dos fornecedores das urnas eletrônicas, é importante ressaltar que o Módulo de Segurança Embarcado – MSE (MSD nas urnas modelo 2009 a 2015) provê uma segregação de função importante. O equipamento possui cinco níveis distintos de inicialização, que permitem que testes de *software*, atualização de *firmwares* e diagnósticos de *hardware* sejam realizados sem que haja privilégios de acesso que possam permitir ataques ao sistema. Como exemplo, a seção de desenvolvimento consegue testar diversas versões de sistema com mídias assinadas pelos modos DESENVOLVIMENTO e SIMULADO. A versão final dos sistemas é assinada pela chave OFICIAL. Tais modos permitem a utilização completa da urna, com exceção de atualização de *firmware*. Em cada um desses modos, o MSE também provê assinaturas digitais com não repúdio e outras garantias conforme as melhores práticas elencadas pelo Instituto Nacional de Tecnologia da Informação (ITI). Contudo, cada modo possui seu próprio par de chaves de assinatura e o *firmware* do MSD não provê acesso às chaves privadas de outro modo. Deste modo, uma urna inicializada com DESENVOLVIMENTO, somente permite a assinatura com a respectiva chave de desenvolvimento.

Os outros dois modos, denominados INICIALIZADOR e MANUTENÇÃO são utilizados, respectivamente, para atualização de *firmware* dos dispositivos de segurança da urna (tal como o próprio MSE) e para que o próprio fabricante desenvolva e utilize *softwares* de diagnóstico na urna. Esses dois modos, contudo, não oferecem acesso às chaves privadas e somente permitem o uso das teclas BRANCO e CORRIGE da urna, não sendo possível que um software falso de votação fosse utilizado com mídias assinadas nesses modos. Para testes de teclado, é utilizada uma primitiva de teste sequencial que faz parte do próprio *firmware* de segurança do teclado do eleitor. Somente a chave privada de MANUTENÇÃO está de posse da empresa fabricante, sendo que as chaves DESENVOLVIMENTO, SIMULADO, OFICIAL e

INICIALIZADOR estão de posse do TSE, com utilização exclusiva na sala cofre do TSE, e fazem parte da cadeia de certificação da Autoridade Certificadora das Urnas Eletrônicas.

Assim, considerando que há controles na fábrica para a gravação dos *firmwares* de segurança, que após a fabricação apenas o TSE pode substituir os *firmwares* de segurança, e que o fabricante apenas pode executar *software* de diagnóstico, não seria possível que mídias assinadas pelo fabricante consigam executar *softwares* distintos dos oficiais, desenvolvidos pelo TSE. Deste modo, nem mesmo o próprio fabricante dos equipamentos tem poder para fraudar o *hardware* ou executar qualquer *software* que comprometa a votação.

Portanto, a arquitetura de segurança da urna eletrônica, combinada com as exigências de cadeia de produção e demais avaliações feitas pela equipe do TSE durante o planejamento da produção, garantem que haja segurança nas urnas produzidas independentemente do fornecedor dos componentes eletrônicos e independente da contratada, que projeta e integra a urna eletrônica.