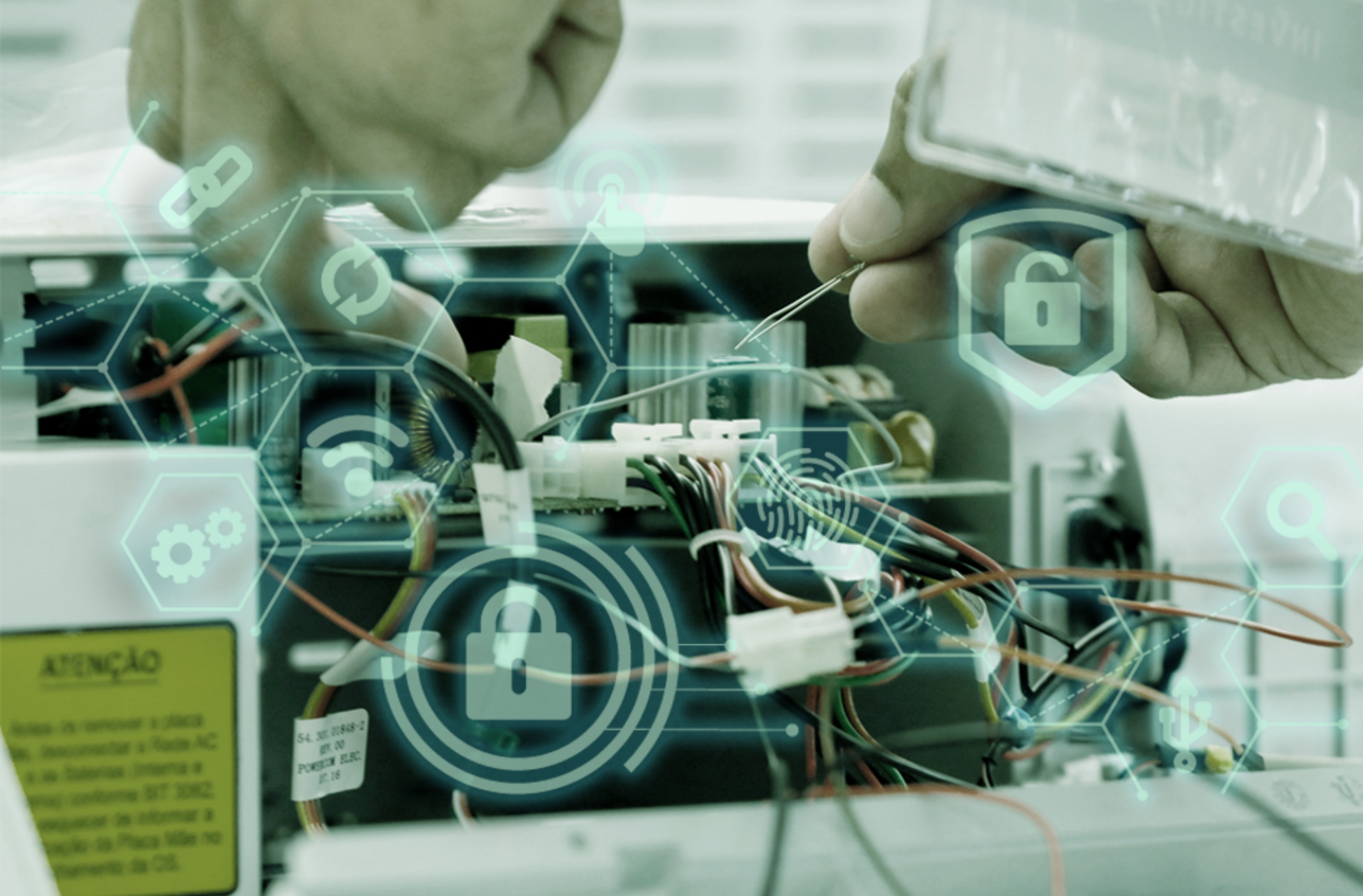




ATENÇÃO

Antes de remover a placa de documentação e Rede AC e da bateria interna e antes conforme NIT 1082, requerer de informar a equipe de Placa Mãe no momento de OS.

54.30.01848-2
R7.00
POWER ELEC.
R7.16



Software do Ecossistema da Urna



Sumário

- Nomenclatura e escopo
- Procedimentos
 - Preparação das urnas
 - Votação
 - Apuração
- Segurança
- Estrutura do código-fonte

Nomenclatura e escopo



Nomenclatura



- 2012: nomes de estrelas
- 2014: nomes de rios brasileiros
- 2016: nomes de árvores brasileiras
- 2018: nomes de livros da literatura brasileira
- 2020: nomes de doces típicos do Brasil
- 2022: nomes de animais da fauna brasileira
 - **TPS 2021: “Carcará”**

Escopo



- UENUX - Linux na Urna Eletrônica
 - Software de Votação – VOTA
 - Sistema de Apuração – SA
 - Recuperador de Dados – RED
 - Software de Carga – SCUE
 - Gerenciador de Aplicativos – GAP
 - Verificador Pré-Pós Eleição – VPP
 - Verificador de Assinaturas – AVPART
- Software básico da urna - *bootloader, kernel* do Linux, *drivers* e bibliotecas

Escopo

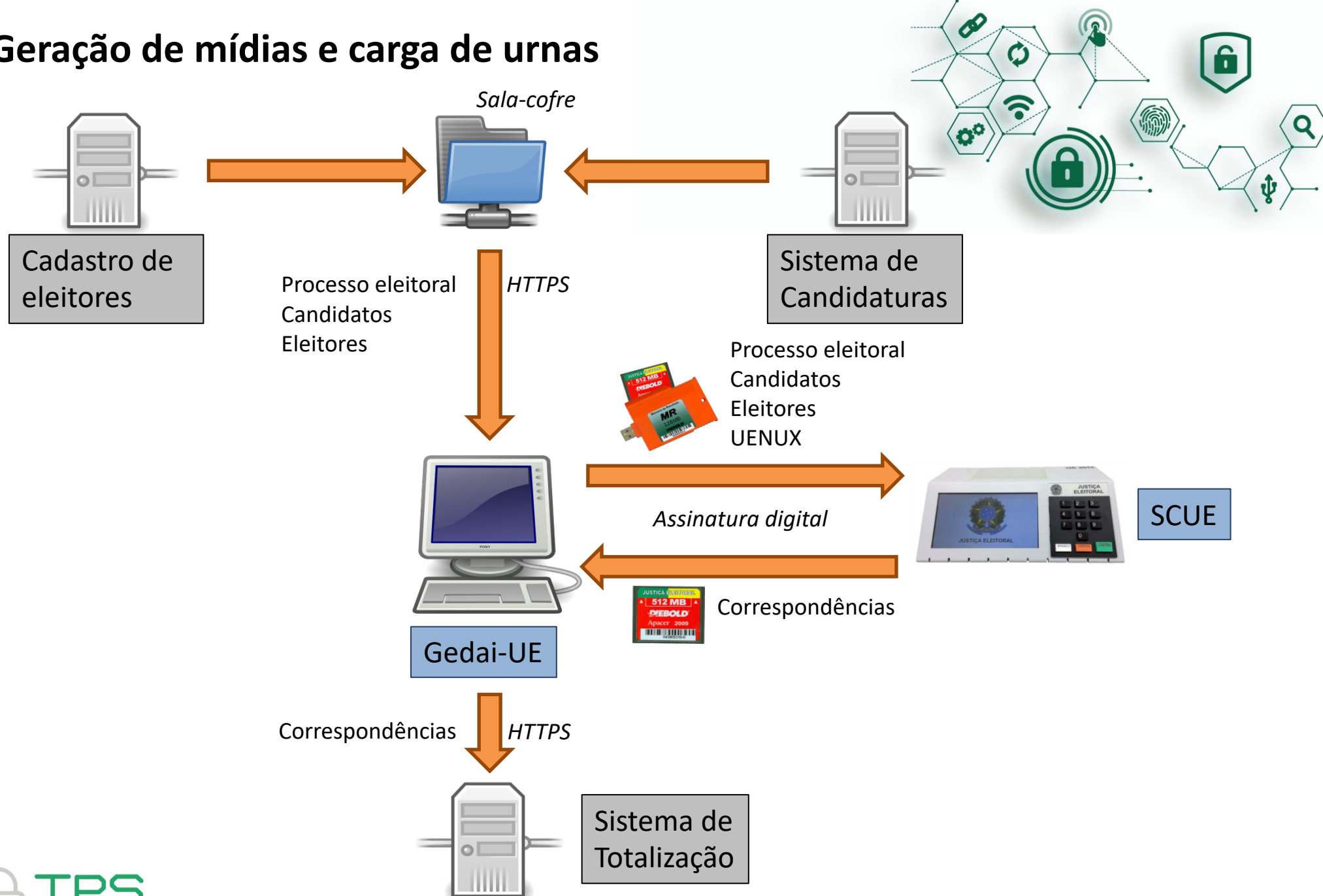


- Plataforma desktop
 - Aplicativos de apoio à preparação das urnas
 - Gedai-UE
 - HotSwapFlash
 - Aplicativos de apoio aos processos de auditoria
 - SAVP-Sorteio e SAVP-Votação
 - Infraestrutura de segurança
 - CriptoSevin
 - Holocron

Preparação da urna



Geração de mídias e carga de urnas

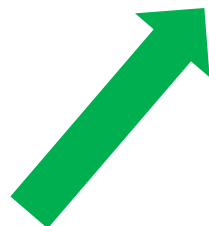




SCUE



GAP



ATUE



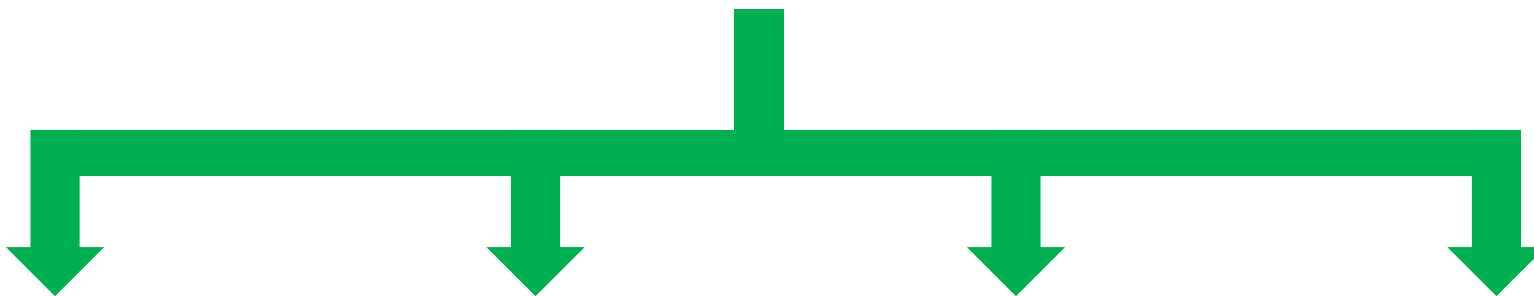
GAP



VOTA



GAP



VOTA



RED



SA



Outros

Votação



Votação



Apuração

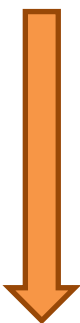


Apuração, totalização e divulgação

Boletim de urna impresso



VOTA

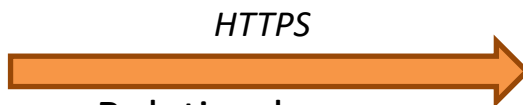


Boletim de urna
Comparecimento
Log
RDV
Assinaturas



Transportador

Valida assinaturas



HTTPS

Boletim de urna
Comparecimento
Log
RDV
Assinaturas



Sistema de
Totalização



Valida assinaturas
e correspondência



Divulgação

Segurança



Hardware de segurança das urnas



- Interface PKCS11 – ECDSA P521
 - Verificação de assinatura do BIOS
 - Verificação de assinatura do *bootloader*
 - Verificação de assinatura do *kernel*
 - Desafio do initje
 - Assinatura da correspondência
 - Assinatura de todos os arquivos de resultado que saem da urna

Hardware de segurança das urnas



- Uso do TRNG
 - Geração de chaves
 - Geração do código da carga
- Uso da chave de *kernel*
 - Criptografia da chave de SO (cifração do *kernel* do Linux)
 - Derivação de chaves (RDV e envelopes de chave)

Segurança em software



- Imagem do *kernel* criptografada com AES-CTR 256 bits
- Executáveis, bibliotecas dinâmicas e módulos de *kernel* com assinatura ECDSA P521 embutida
- Assinatura com curvas elípticas de 256 bits (Cepesc):
 - todos os arquivos de dados que entram na urna
 - todos os arquivos de resultado que saem da urna
 - *kernel* e todos os executáveis, bibliotecas e demais arquivos

Segurança em software



- Criptografia com curvas elípticas de 256 bits (Cepesc):
 - arquivo de boletim da urna
 - biometria do eleitor
- Assinatura do QR Code do BU com EdDSA (Curve25519) de 256 bits
- Derivação de chaves com HKDF
- Envelopes de chave cifrados com AES CBC 256 bits
- Código verificador do BU e do log baseado em SipHash

Segurança em software



- Uso do TPM na plataforma desktop
 - Conjugado com driver monitor do ambiente
 - Criptografia RSA 2048 bits para os chaveiros
 - Autoridade certificadora de estações de trabalho
 - Serviço (*daemon*) para funções de segurança
 - Autenticação das aplicações
 - Serviços de assinatura, criptografia e MAC
 - Guarda de chaves

Registro Digital do Voto – RDV



- Novo formato do arquivo – ASN.1
 - Aprimora auditabilidade
- Novo modo de gravação dos votos
 - Votos ordenados lexicograficamente
 - Ordenação por inserção na lista do cargo
 - Preserva o sigilo da votação e a digitação do eleitor
- Criptografia com AES-CBC 256 bits durante a votação

Código-fonte

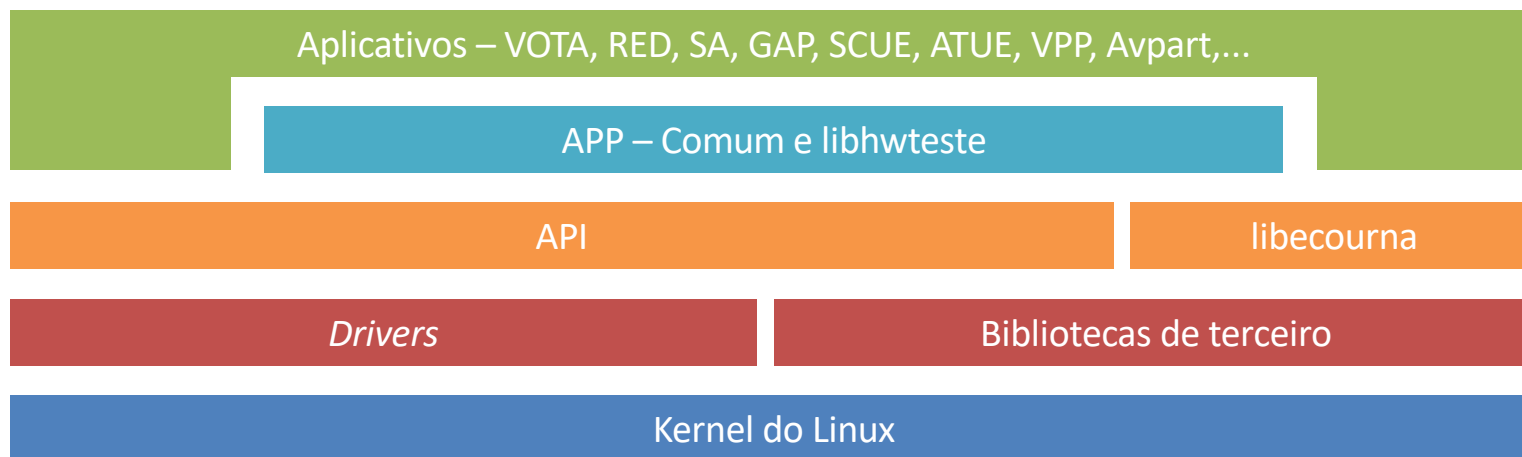


Tecnologias e ferramentas

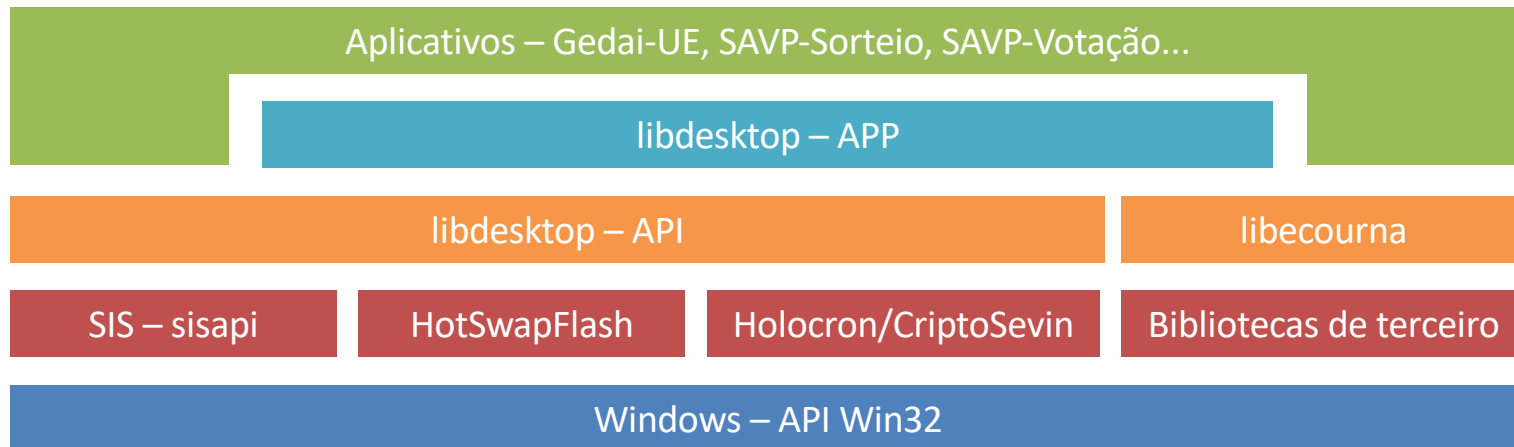
- C, C++, Assembly x86 e ASN.1
- Linux 5.4.77
- GNU Make e GCC 9.2
- Conan e Artifactory
- Bibliotecas de terceiros
- Eclipse CDT e Visual Studio Code
- PlantUML e Markdown
- Cppcheck
- Flawfinder
- Doxygen



Estrutura do Uenux



Estrutura dos aplicativos desktop

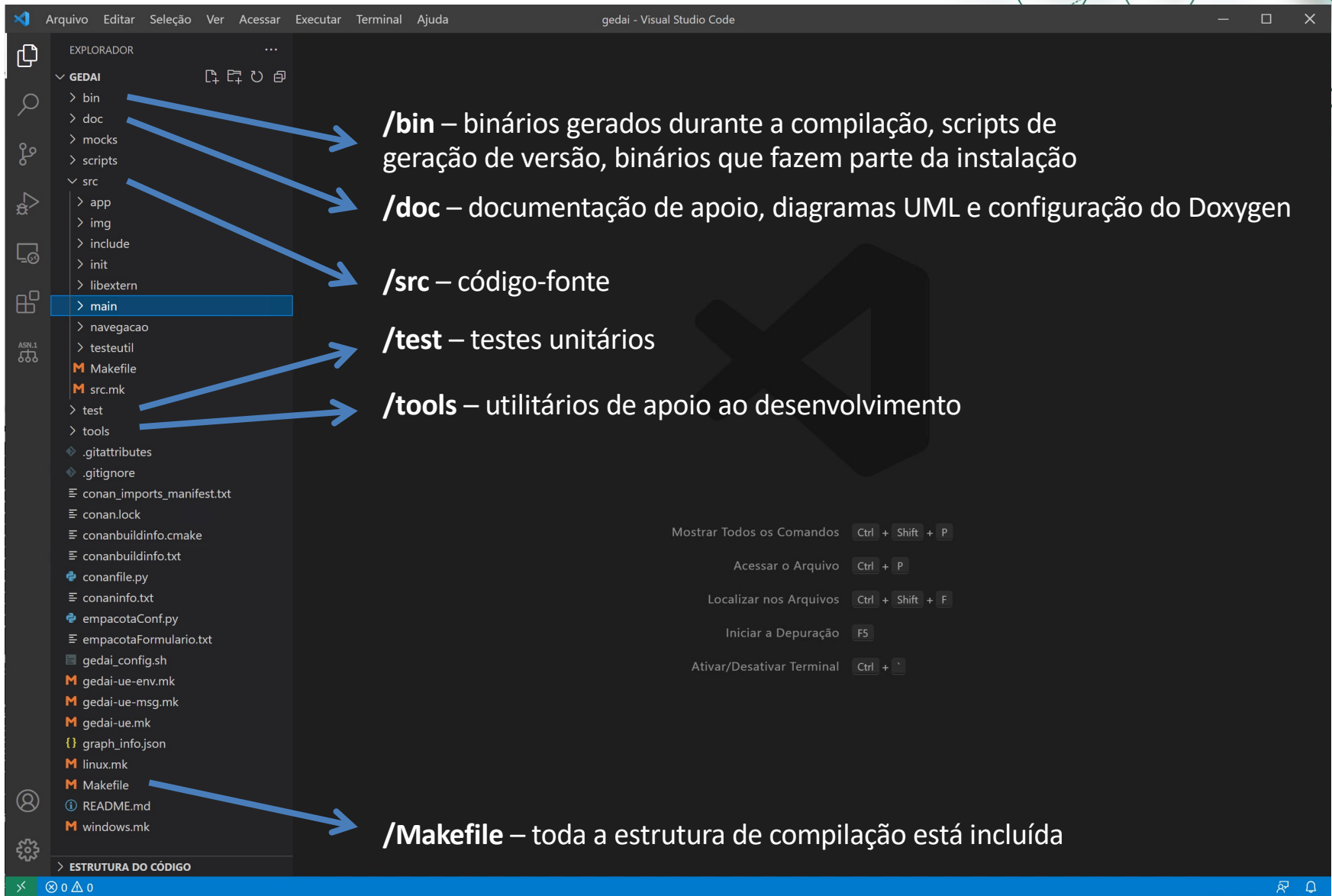


Visual Studio Code interface showing the file explorer for the **uenux** project. The explorer lists the following files and folders:

- bin** – binários gerados durante a compilação
- build** – scripts de geração de versão
- doc** – documentação de apoio, diagramas e configuração do Doxygen
- mock**
- pkg** – binários que fazem parte do pacote de instalação ou utilizados para apoio ao desenvolvimento
- src** – código-fonte
 - api
 - app
 - include
 - so
- Makefile** – toda a estrutura de compilação está incluída
- src.mk**
- test** – testes unitários
- tools** – utilitários de apoio ao desenvolvimento
- vm**
- .clang-format**
- .gitattributes**
- .gitignore**
- .gitmodules**
- .syntastic_cppcheck_config**
- .todo**
- conanfile.py**
- Makefile**
- README.md**
- uenux_config.sh**
- uenux.mk**
- uenuxcodequality.mk**
- uenuxdebuggoals.mk**
- uenuxenv.mk**
- uenuxmaingoals.mk**
- uenuxmsg.mk**
- uenuxrun.mk**
- uenuxtargets.mk**
- uenuxtools.mk**
- uerules.mk**

Additional commands shown in the bottom right:

- Show All Commands: **Ctrl + Shift + P**
- Go to File: **Ctrl + P**
- Find in Files: **Ctrl + Shift + F**
- Start Debugging: **F5**
- Toggle Terminal: **Ctrl + `**



The screenshot shows the Visual Studio Code interface with the GEDAI project open. The Explorer sidebar on the left lists the project's directory structure. Blue arrows point from specific folders/files in the Explorer to their descriptions on the right. The descriptions are as follows:

- /bin** – binários gerados durante a compilação, scripts de geração de versão, binários que fazem parte da instalação
- /doc** – documentação de apoio, diagramas UML e configuração do Doxygen
- /src** – código-fonte
- /test** – testes unitários
- /tools** – utilitários de apoio ao desenvolvimento
- /Makefile** – toda a estrutura de compilação está incluída

At the bottom right of the editor area, a list of keyboard shortcuts is displayed:

- Mostrar Todos os Comandos: **Ctrl + Shift + P**
- Acessar o Arquivo: **Ctrl + P**
- Localizar nos Arquivos: **Ctrl + Shift + F**
- Iniciar a Depuração: **F5**
- Ativar/Desativar Terminal: **Ctrl + `**



FIM

Tribunal Superior Eleitoral
Seção de Voto Informatizado
sevin@tse.jus.br