



**Segurança Sistema
Eleitoral Webvoto**



Webvoto



Segurança do processo eleitoral

O que garante que meu voto...

- 01 É secreto
- 02 Será contado
- 03 ... conforme eu escolhi
- 04 Só pode ser feito por mim

E o que garante que agentes externos não podem interferir no resultado?





Segurança do processo eleitoral

O que garante que meu voto...

- 01 **É secreto**
- 02 Será contado
- 03 ... conforme eu escolhi
- 04 Só pode ser feito por mim



Sigilo do voto



E o que garante que agentes externos não podem interferir no resultado?



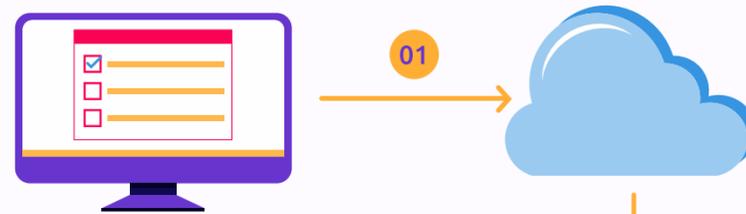


Sigilo do voto

Fluxograma sobre o sistema de votação

Votação

Os eleitores realizam e confirmam suas escolhas. Após esse processo, antes de deixarem o dispositivo, as informações do voto são encriptadas com o uso da chave pública disponibilizada pela comissão eleitoral, sendo uma das garantias de sigilo do voto.



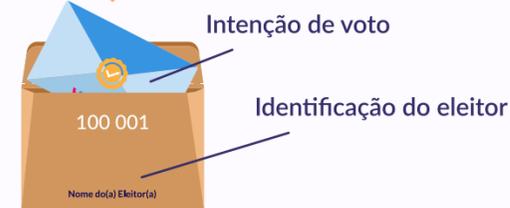
Internet / Nuvem

Os votos encriptados, advindos de quaisquer dispositivos dos eleitores, passam pela Internet em direção aos servidores da eleição, hospedados no Datacenter.

Intenção de voto e identificação do eleitor

Antes de ser armazenadas, as informações da identificação do eleitor e a intenção de voto são separadas, impedindo sua associação.

O voto permanece encriptado até o momento da apuração.



Comprovante de votação

O sistema gera o comprovante de voto que fica armazenado no banco de dados, impedindo que o eleitor vote múltiplas vezes.

Simulação de urna

Nessa etapa do processo, o voto é assinado digitalmente com a chave privada do servidor, em seguida, é embaralhado, de modo a simular o funcionamento de uma urna física.



Comissão eleitoral e auditor

A comissão eleitoral e o auditor são os responsáveis pelo fornecimento da chave privada correspondente à chave pública utilizada na criptografia dos votos.

Somente eles possuem acesso a essa chave e por consequência são responsáveis por garantir a lisura do processo.



Checagem de assinaturas e decriptação

Mediante o uso da chave pública dos servidores hospedados no datacenter, é possível assegurar a regularidade dos votos, uma vez que, apenas votos assinados digitalmente por servidores autorizados serão validados.

Após a confirmação de legitimidade dos votos a serem apurados, usa-se a chave privada fornecida pela comissão eleitoral para decriptar as intenções e computá-las, realizando assim a apuração dos votos.



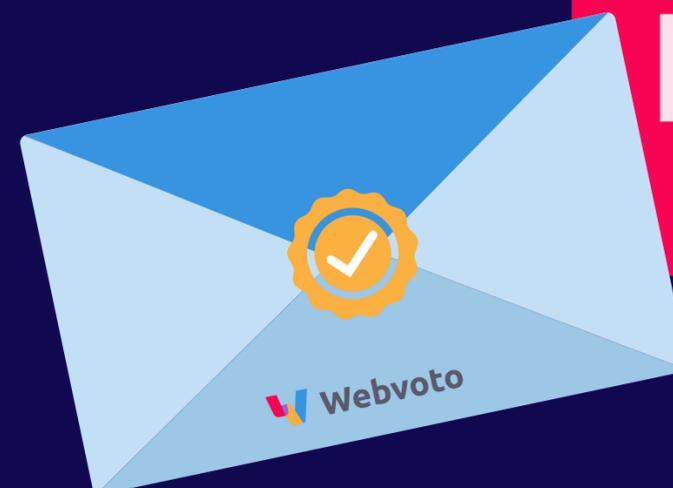
Resultado assinado

Após a checagem e decriptação dos votos, o resultado é emitido através de um documento pdf, que também é assinado digitalmente.



Sigilo do voto

- Voto encriptado no navegador com criptografia assimétrica de 2048 bits
- Chave privada em poder da comissão eleitoral
- Anonimização em tempo real





Segurança do processo eleitoral

O que garante que meu voto...

- 01 É secreto
- 02 Será contado**
- 03 ... conforme eu escolhi
- 04 Só pode ser feito por mim



Transparência da apuração

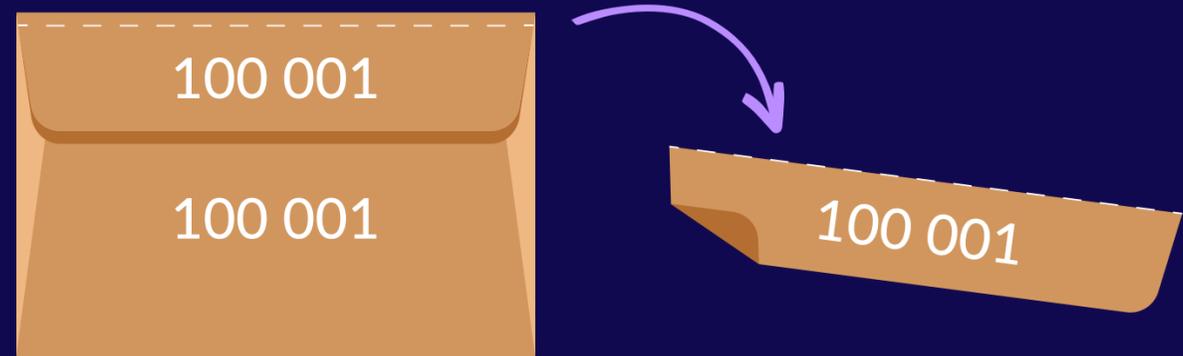
E o que garante que agentes externos não podem interferir no resultado?





Transparência da apuração

- Código verificador único
- Eleitores como testemunhas
- Logs imutáveis
- Documento de validação de logs



Comprovante de Voto

Nome: Nome completo do(a) eleitor(a)

CPF: XXX.XXX.XXX-XX

Eleição: Eleições CRM 2023

Data: 09/06/2023 11:54:13 GMT-3

Código verificador único: 0613c7a0ead3e8e7a01ea78447508763599bc28e16ab8ee7ede4da9014

Autenticação: 917c7a0ead3e8e7a01ea78447508763599bc28e16ab8ee7ede4da9014b64589

[Voltar ao início](#) [Imprimir / Salvar](#)

i Você poderá **reimprimir** o seu comprovante na seção **GERAR COMPROVANTE**



Segurança do processo eleitoral

O que garante que meu voto...

- 01 É secreto
- 02 Será contado
- 03 ... conforme eu escolhi**
- 04 Só pode ser feito por mim



Integridade do voto



E o que garante que agentes externos não podem interferir no resultado?



Integridade do voto

- Votos assinados digitalmente com certificado ICP-Brasil
- Assinatura conferida na apuração
- Código fonte 100% auditável
- Conferência tanto pela auditoria quanto pelas chapas
- Auditoria controla código fonte executando durante toda a eleição





Segurança do processo eleitoral

O que garante que meu voto...

- 01 É secreto
- 02 Será contado
- 03 ... conforme eu escolhi
- 04 Só pode ser feito por mim**

E o que garante que agentes externos não podem interferir no resultado?



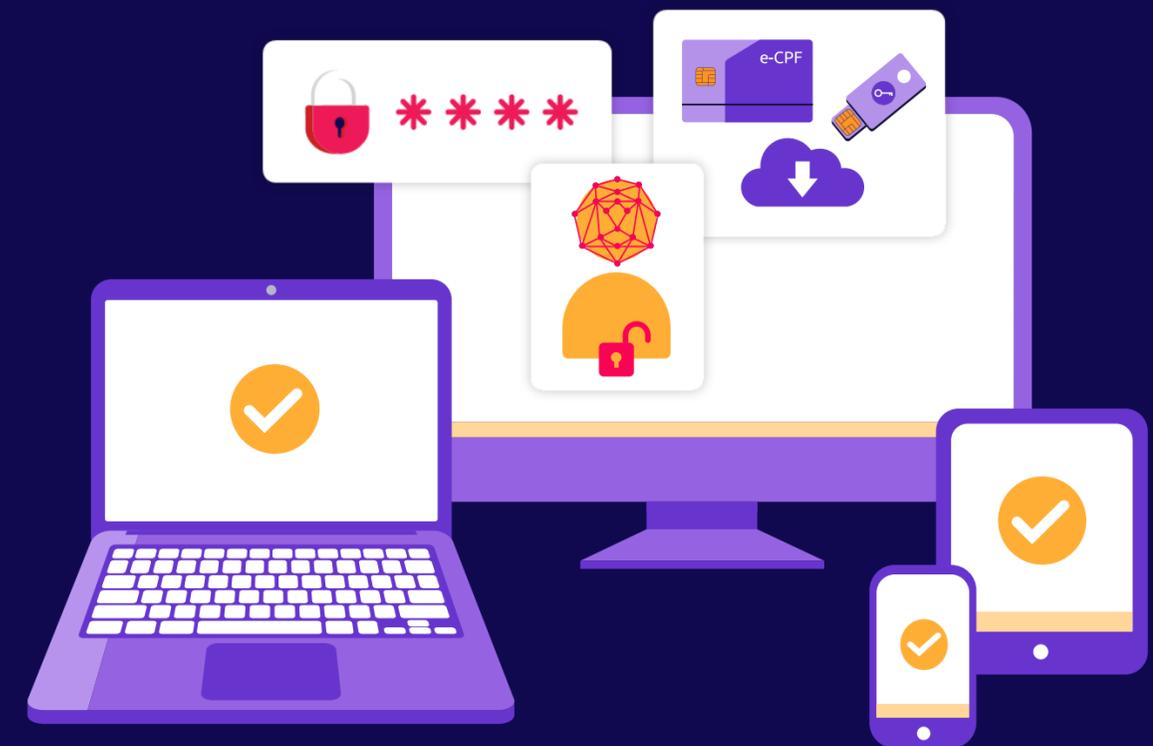
Autenticação





Autenticação

- Certificado ICP-Brasil (convencional ou nuvem)
- PIN enviado por email ou SMS
 - 2FA: data de nascimento
- Biometria facial



Importação de base

- Controle de acesso com certificado digital
- Rastreabilidade das ações
- Crítica da base com desativação de contatos duplicados
- Assinatura digital da base enviada



Segurança do processo eleitoral

O que garante que meu voto...

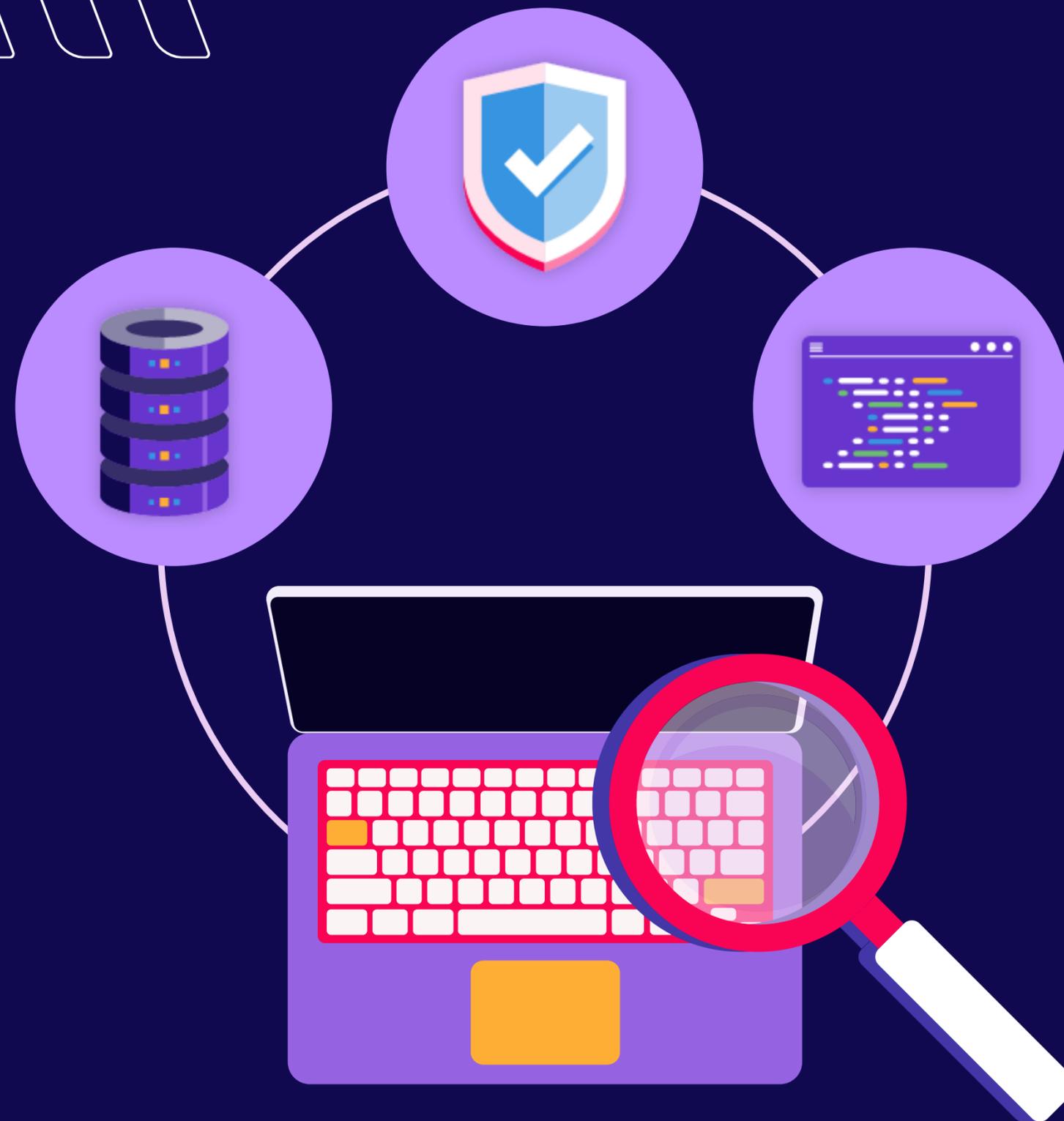
- 01 É secreto
- 02 Será contado
- 03 ... conforme eu escolhi
- 04 Só pode ser feito por mim

E o que garante que agentes externos não podem interferir no resultado?



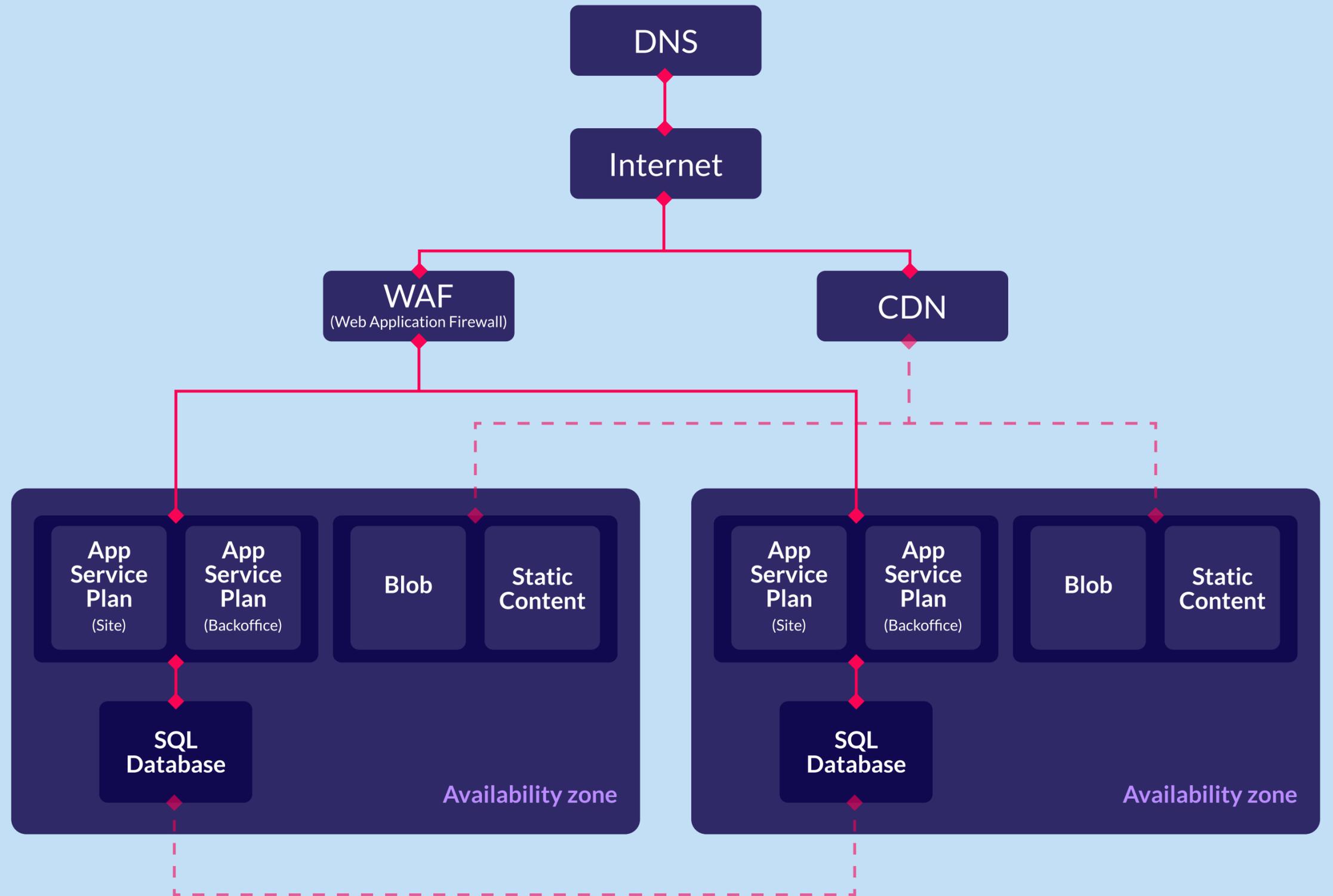
Infraestrutura

- Detecção de SQL/script injection
- Bloqueio automático de robôs
- Bloqueio por país de origem
- Prevenção de DDoS
- Data center de referência
- Redundância





Infraestructura redundante



Processo de desenvolvimento de software seguro

- 100% de revisão de código novo
- Revisões regulares
- Auditoria externa
- Boas práticas para evitar ataques (SQL injection, script injection, ...)
- Equipe especializada de criptógrafos



Sistema e processo auditados

- Todo o processo é auditado, desde o envio de credenciais para submissão de bases
- Auditoria realiza testes de intrusão
- Auditoria analisa código fonte e confere código que está executando no dia da eleição



Características adicionais

- Garantia de unicidade do voto
- Garantia adicional de integridade: assinatura RSA com chave efêmera do servidor
- Comunicação navegador-servidor encriptada
- Senha e voto encriptados com camada adicional de criptografia
- Garantia criptográfica da impossibilidade de incluir, alterar ou remover logs
- Todos os acessos são registrados com data, hora e endereço IP -- tanto para votar quanto administrativos
- Senhas geradas com gerador de números aleatórios criptograficamente seguro
- Senhas não são armazenadas, nem mesmo cifradas, sendo armazenado apenas dado que permite averiguação futura de acerto da senha
- Durante período de votação, servidores não podem ser acessados para administração
- Durante o período de votação, o único acesso permitido ao banco de dados é da própria aplicação
- Certificações da infraestrutura: ISO 20000-1:2011, ISO 22301, ISO 27001, Atestado CSA-STAR, Certificação CSA-STAR, Autoavaliação CSA-STAR, ISO 27701, ISO 27002, ISO 9001, ANSI/TIA-942



Webvoto

