

Votando entre tiburones

DIEZ AÑOS FORTALECIENDO LA CIBERSEGURIDAD NACIONAL


Internet voting… ¿ESTÁS SEGURO?
Hay mil maneras de hacerlo mal.
¡Pero también hay formas de **hacerlo BIEN!**

Quienes somos



Cryptography Researcher

PhD en Voto Electrónico

@sandra_guasch | sandra.guasch@scytl.com



Director of Security

+15 años trabajando en InfoSec

@jesuscholiz | jesus.choliz@scytl.com



Discutiendo sobre Internet Voting durante +6 años

Research & Security

@SCYTL_SA | www.scytl.com

Índice

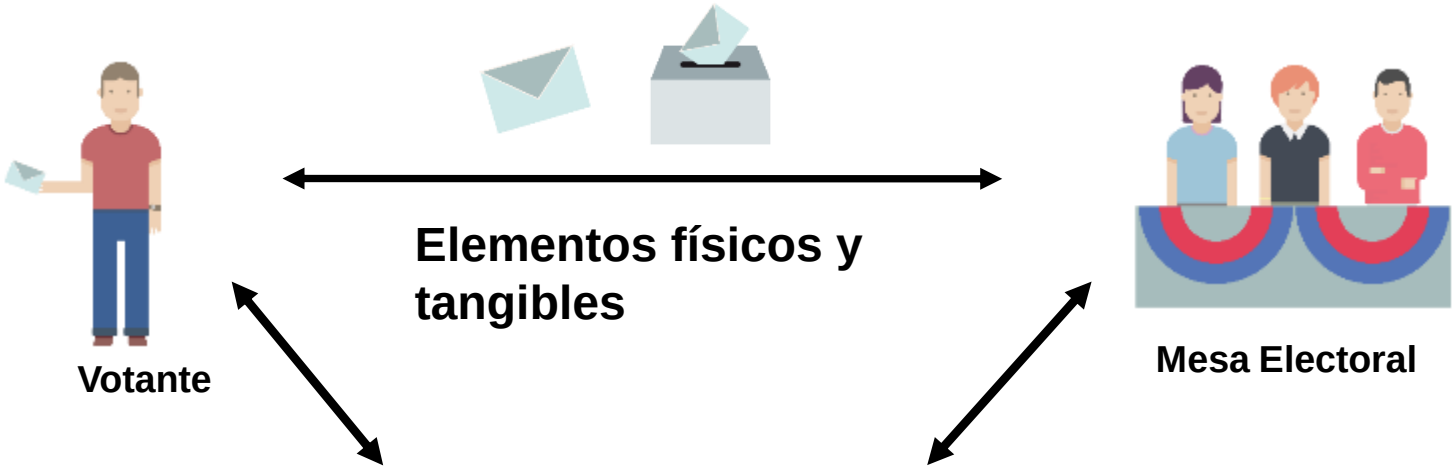
1. Introducción al voto por Internet
2. Principales preocupaciones de seguridad
3. Como proteger la privacidad
4. Verificabilidad
5. ¿Se puede hackear?

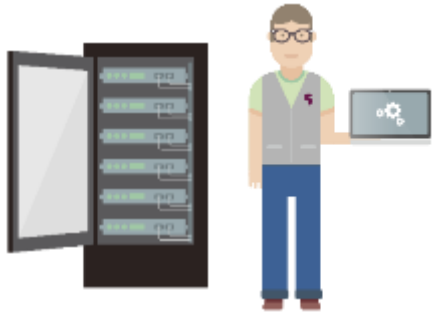
Introducción al voto por Internet

Motivación

- ¿Aumenta la **participación**?
- ¿Reduce el **coste**?
- ¿Más fácil para votantes con **discapacidades**?
- ¿Habilita a votantes **hospitalizados** o **convalecientes**?
- ¿Más eficiente para los ciudadanos residentes en el **extranjero**?
- ¿Posibilita elecciones o consultas **más a menudo**?
- ¿Provee resultados más **rápidos y libres de errores**?
- ¿Reduce las **colas y tiempos de espera** en los colegios electorales?

Introducción al voto por Internet





- Sysadmins
- Software developers
- Empresas de hosting
- Etc.

Nuevas relaciones indirectas implican nuevos riesgos de seguridad



PRIVACIDAD



INTEGRIDAD / CONFIANZA





SEGURIDAD / MALWARE

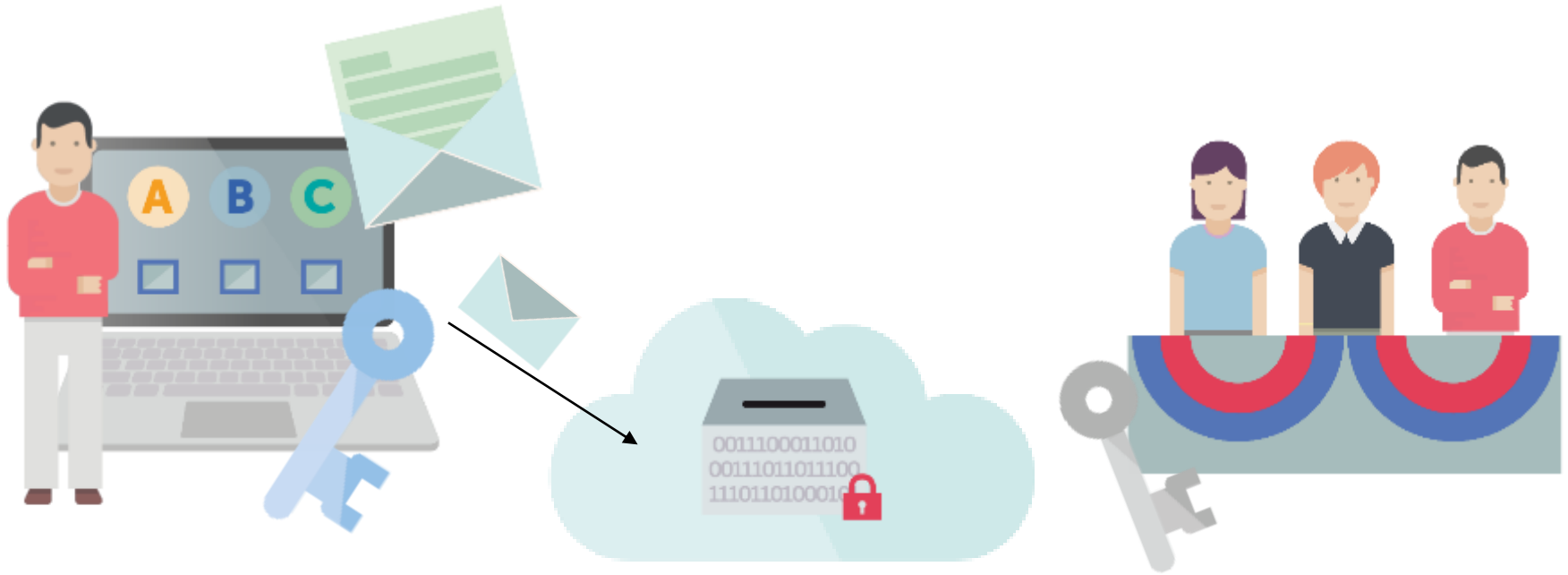


HACKING



¡¡La privacidad en Internet no existe!!

Cifrado extremo a extremo

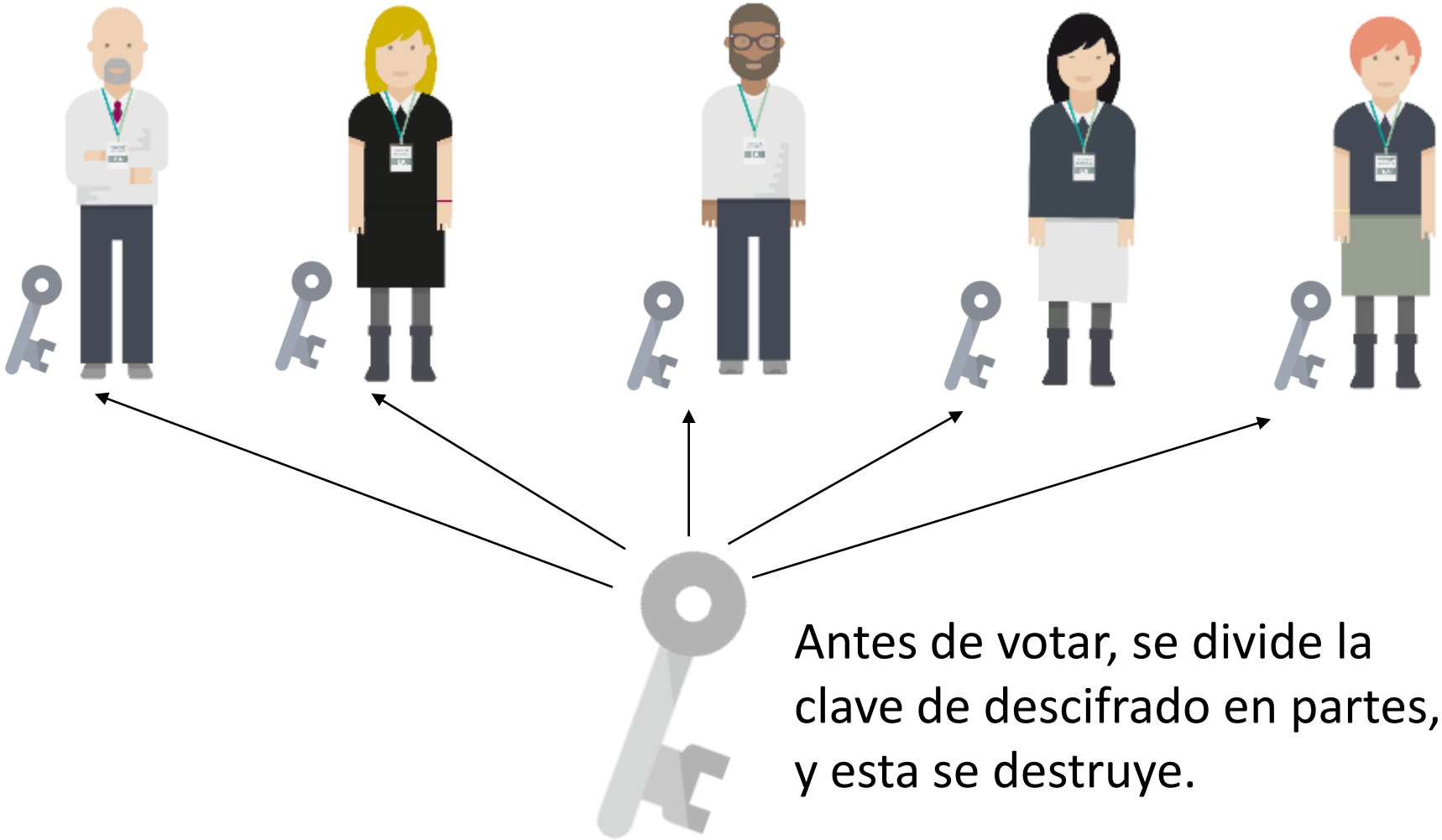


El voto se **cifra** en el PC del votante

End-to-end encryption

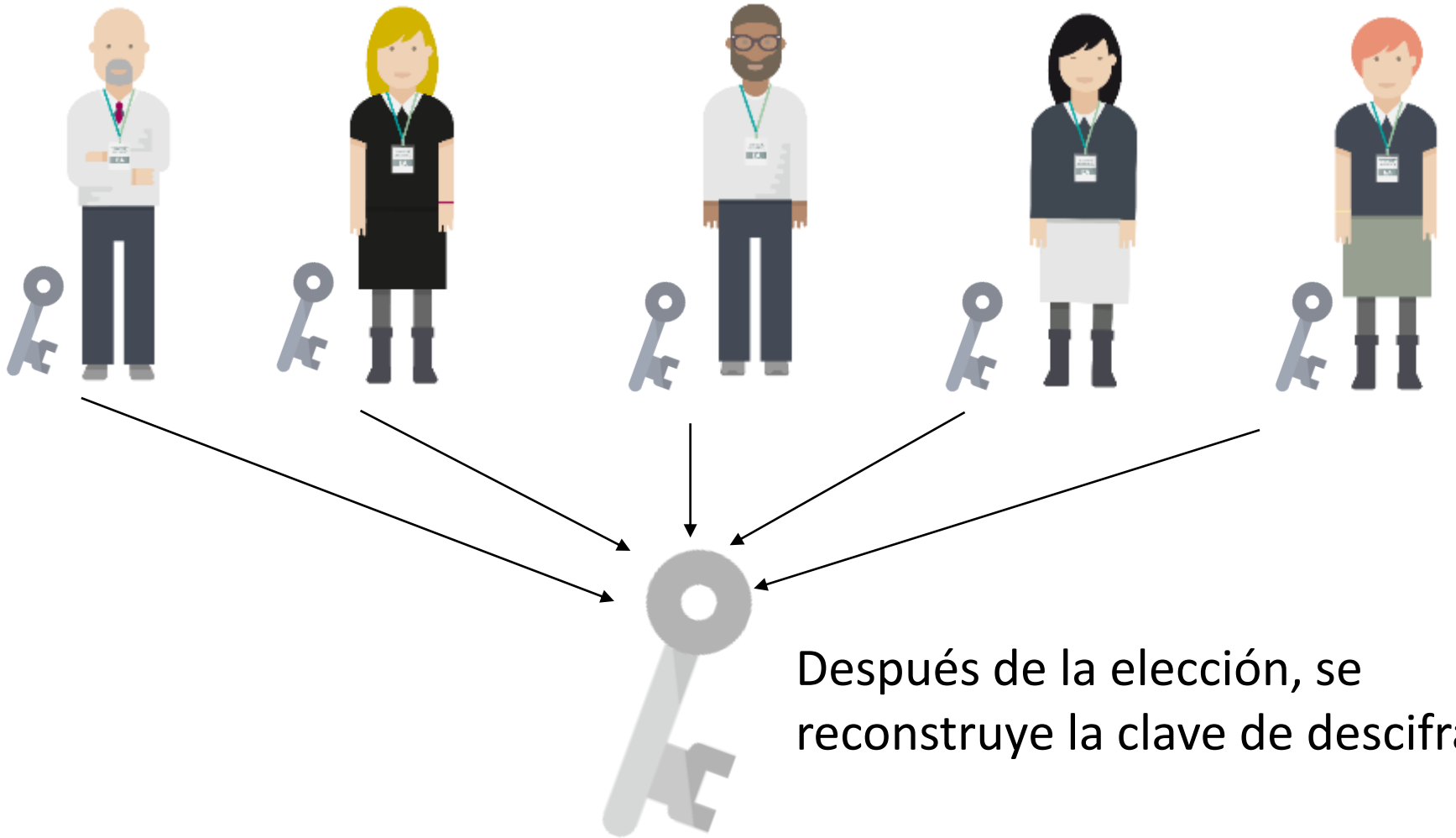
La mesa electoral posee la **clave de descifrado**

Dividir la confianza (I)



Antes de votar, se divide la clave de descifrado en partes, y esta se destruye.

Dividir la confianza (II)



Después de la elección, se reconstruye la clave de descifrado

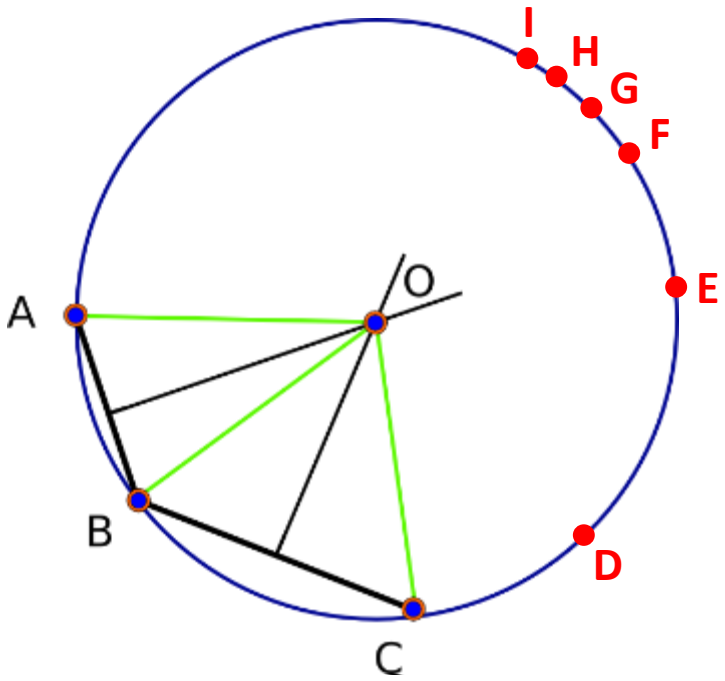
¿Cómo se protege la clave?

- La clave se divide en **“shares”**.
- “Shamir Secret Sharing Scheme”
- Almacenadas en **smartcards** u otro hardware
- Custodiadas por la **Mesa Electoral.**
- Protegidas por un **código PIN** elegido por ellos.



¿Qué ocurre si una persona no aporta su clave?

¿Cuantos puntos de una circunferencia son necesarios para encontrar el centro?







ALERT!

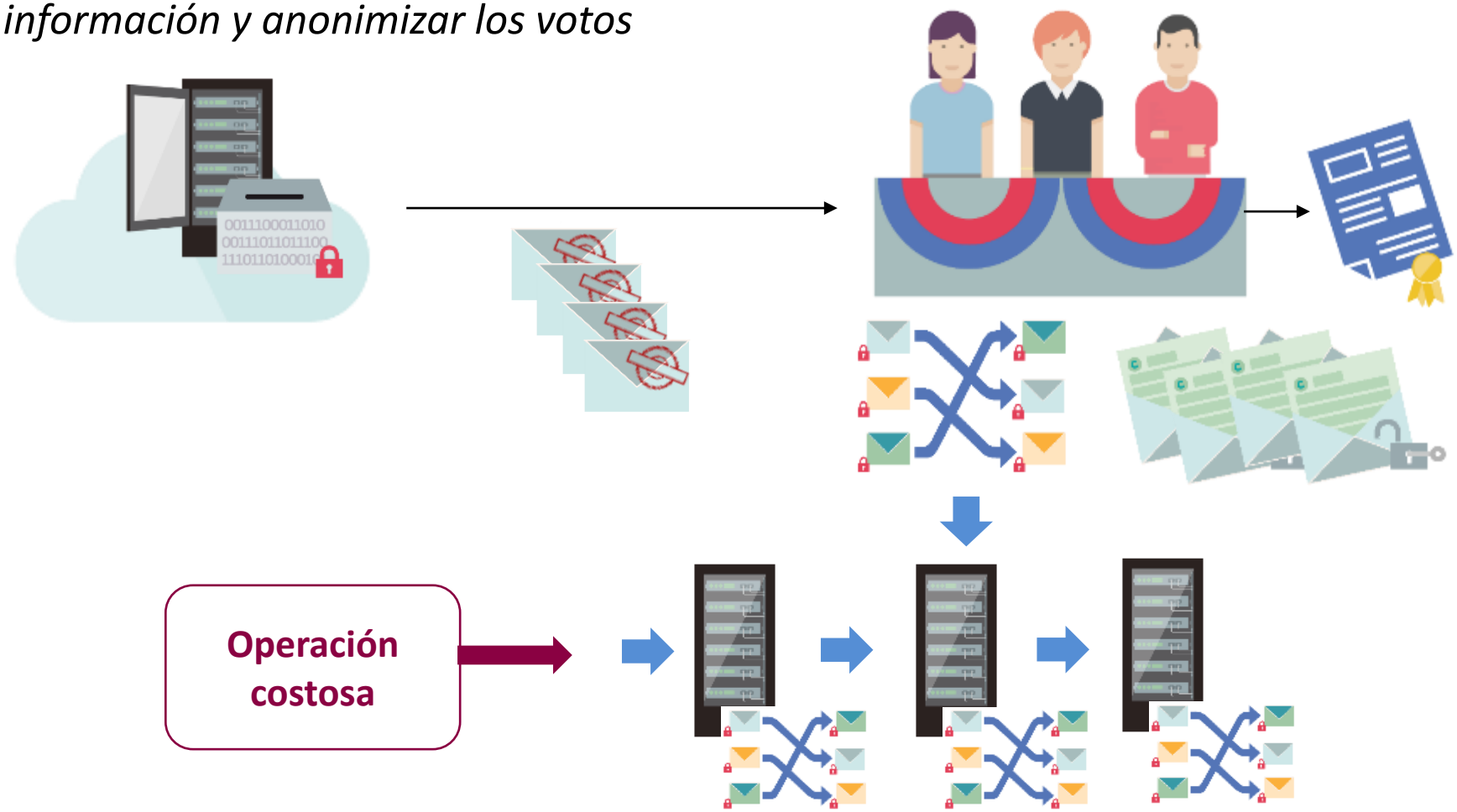


¡He perdido mi clave!

Pero entonces, la mesa electoral podrá ver mi voto, ¿cierto?... ¡NO!

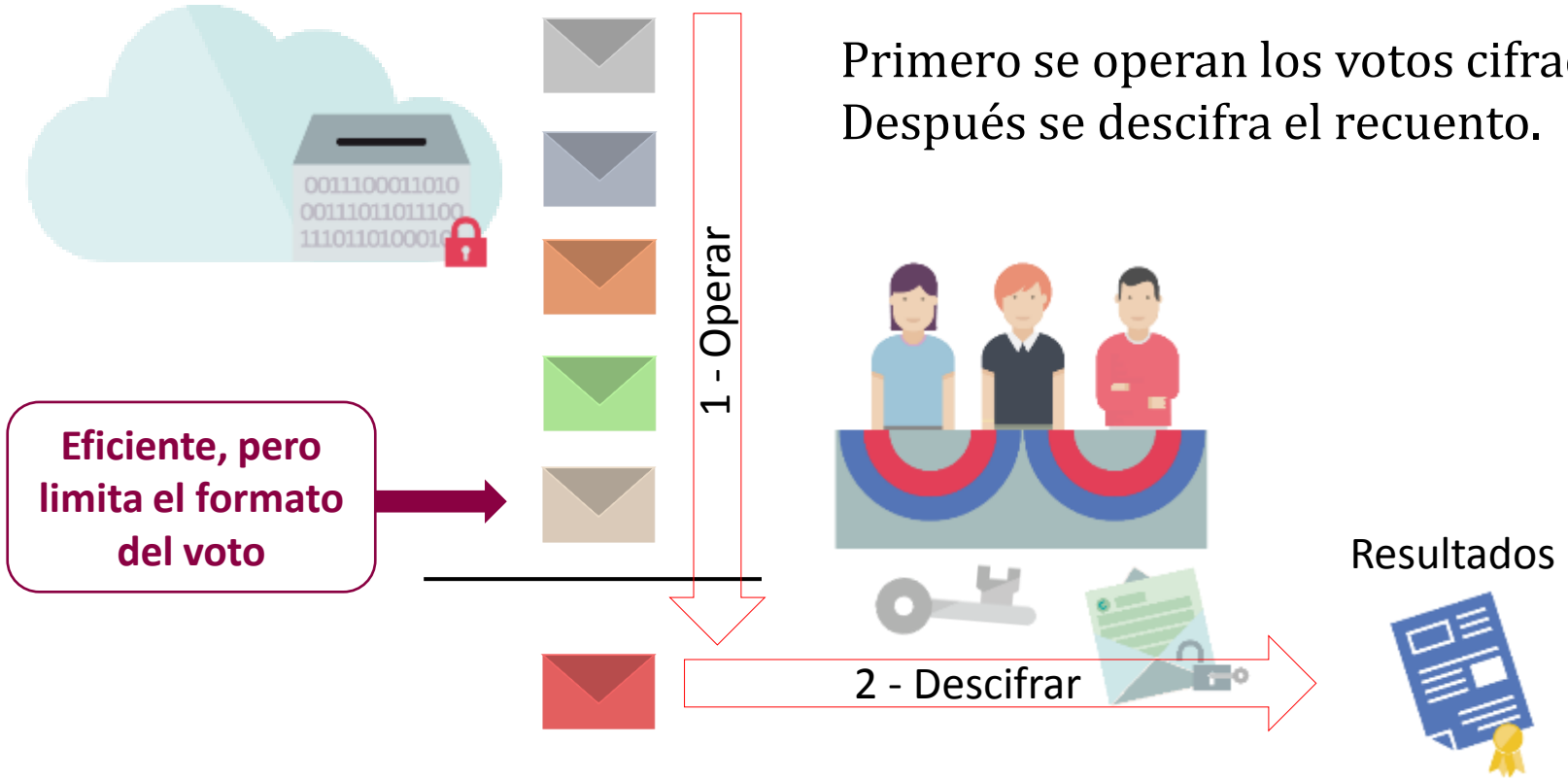
1. Uso de MixNets

Eliminar información y anonimizar los votos



2. Recuento homomórfico

No descifrar votos individuales



Primero se operan los votos cifrados.
Después se descifra el recuento.

Eficiente, pero limita el formato del voto

¿Como puedo estar seguro que mi voto se ha contado?

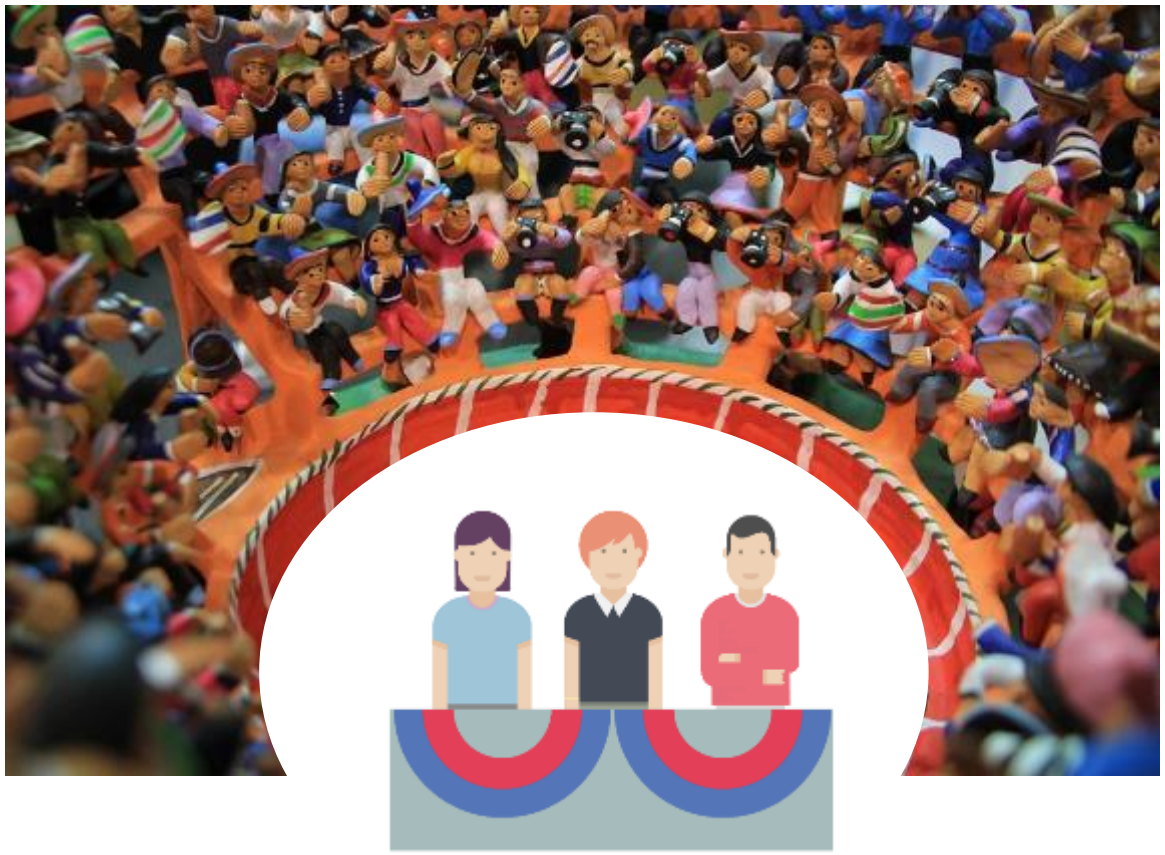


Verificabilidad en elecciones tradicionales

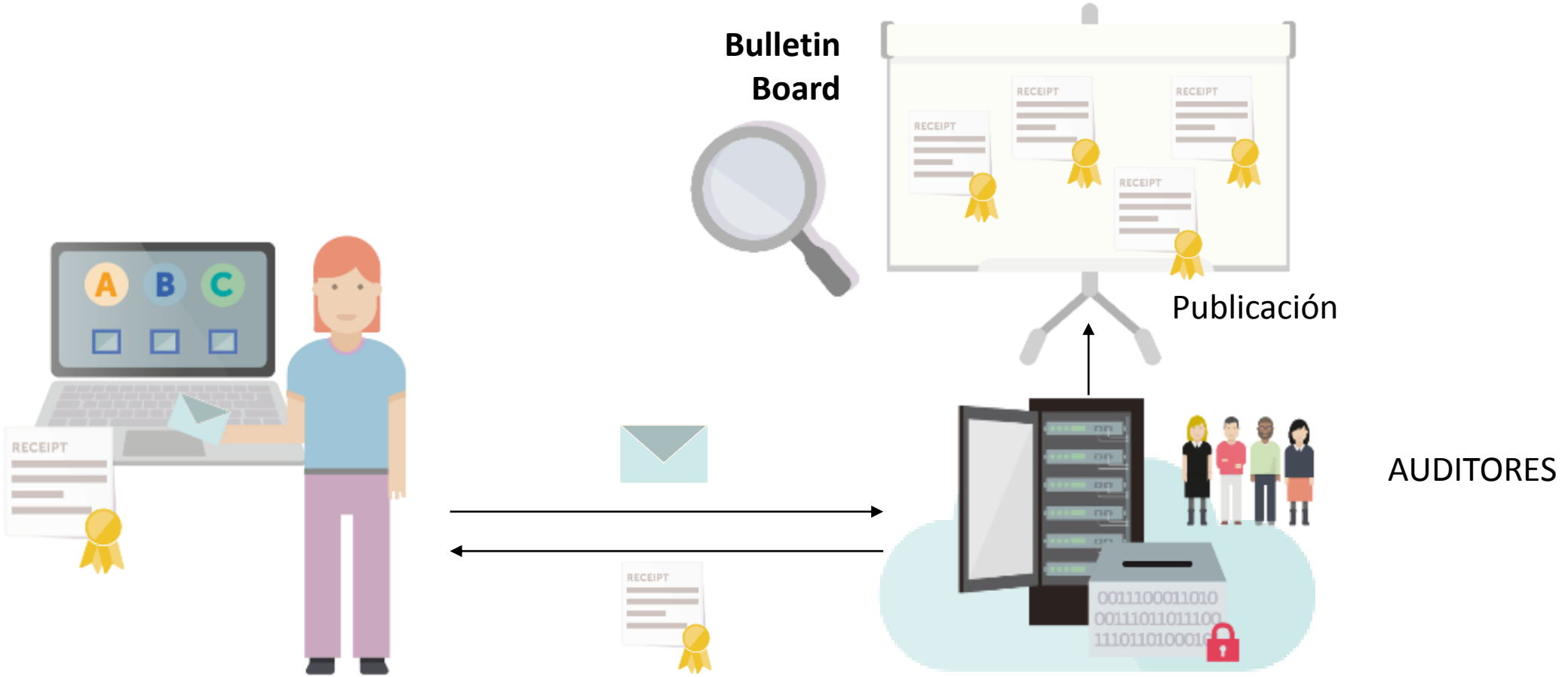
Podemos ver caer
nuestros votos en la urna



Podemos ver como recuenta la mesa electoral



Recibo de voto



El votante obtiene un **recibo de voto**

Trazabilidad hasta la urna digital

Verificación del recuento

Proceso de recuento al finalizar la elección



MEZCLAR con una **permutación secreta**

DESCIFRAR con una **clave privada**

CONTAR

Comprobar que los votos no han sido **modificados / añadidos / borrados**

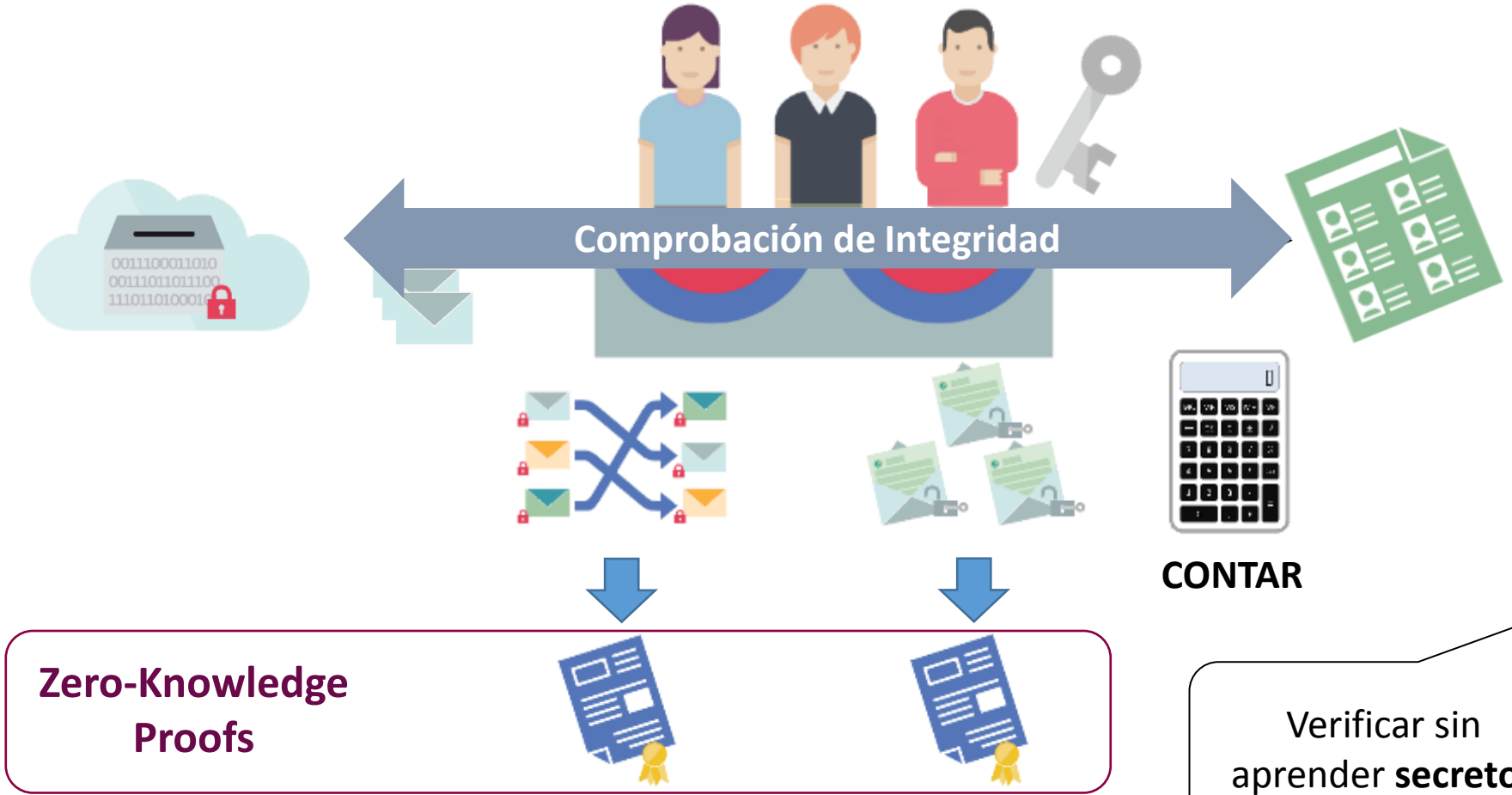


AUDITORES

Verificar sin aprender **secretos**

Verificación del recuento

Proceso de recuento al finalizar la elección



Comprobar que los votos no han sido **modificados / añadidos / borrados**



AUDITORES

Verificar sin aprender **secretos**



URNA ORIGINAL





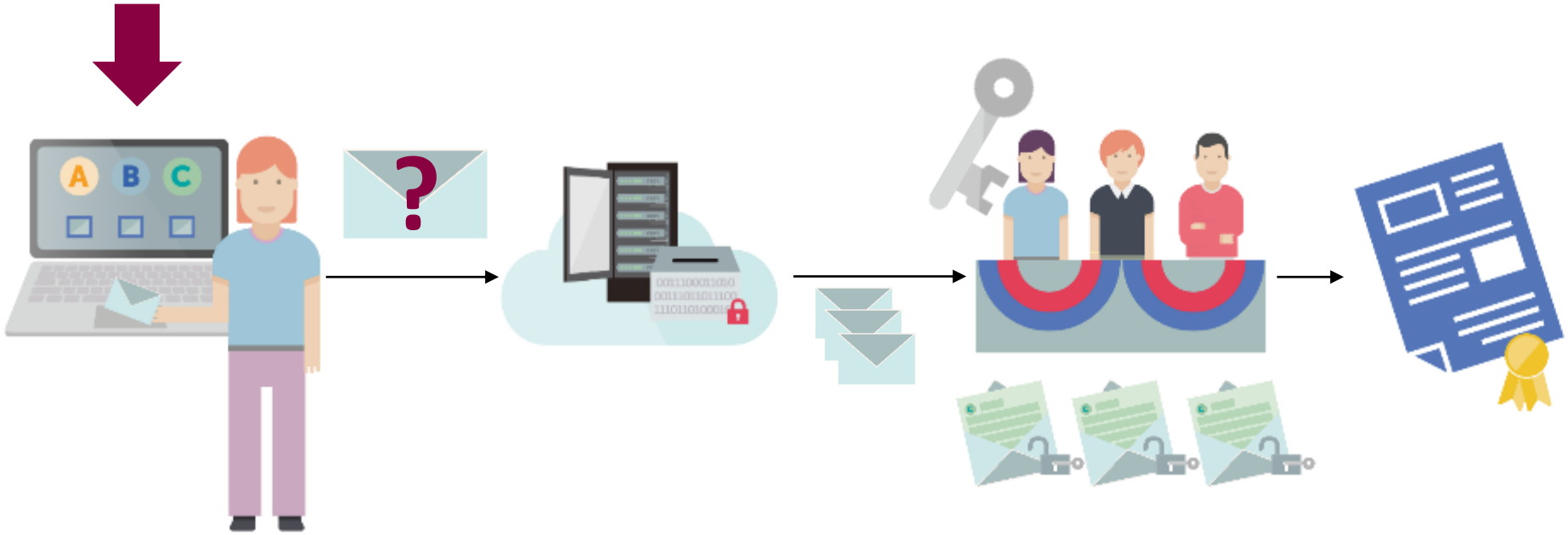




ZKPS – Demuestran que contienen lo mismo



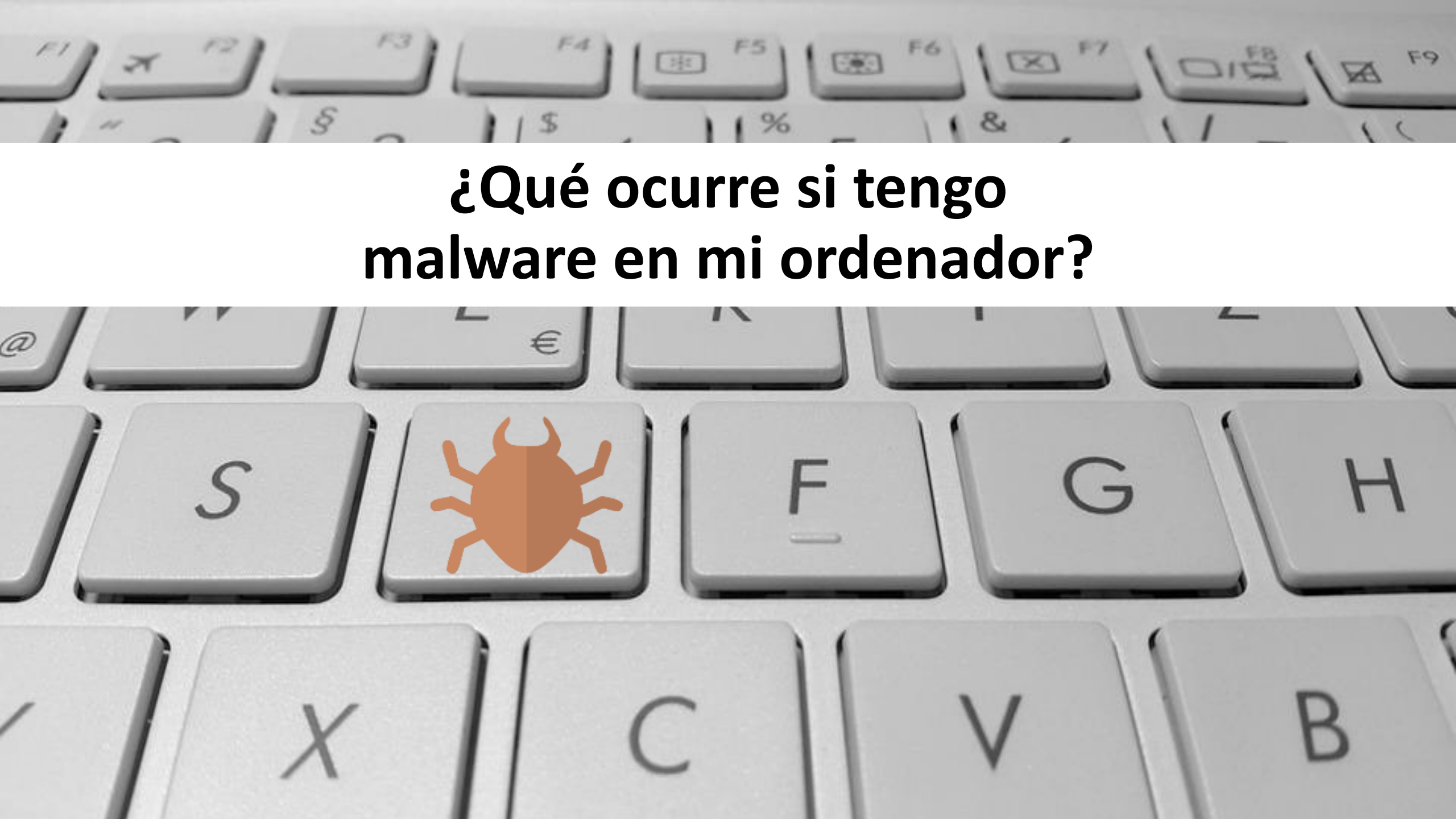
URNA DESPUES DEL MIXING

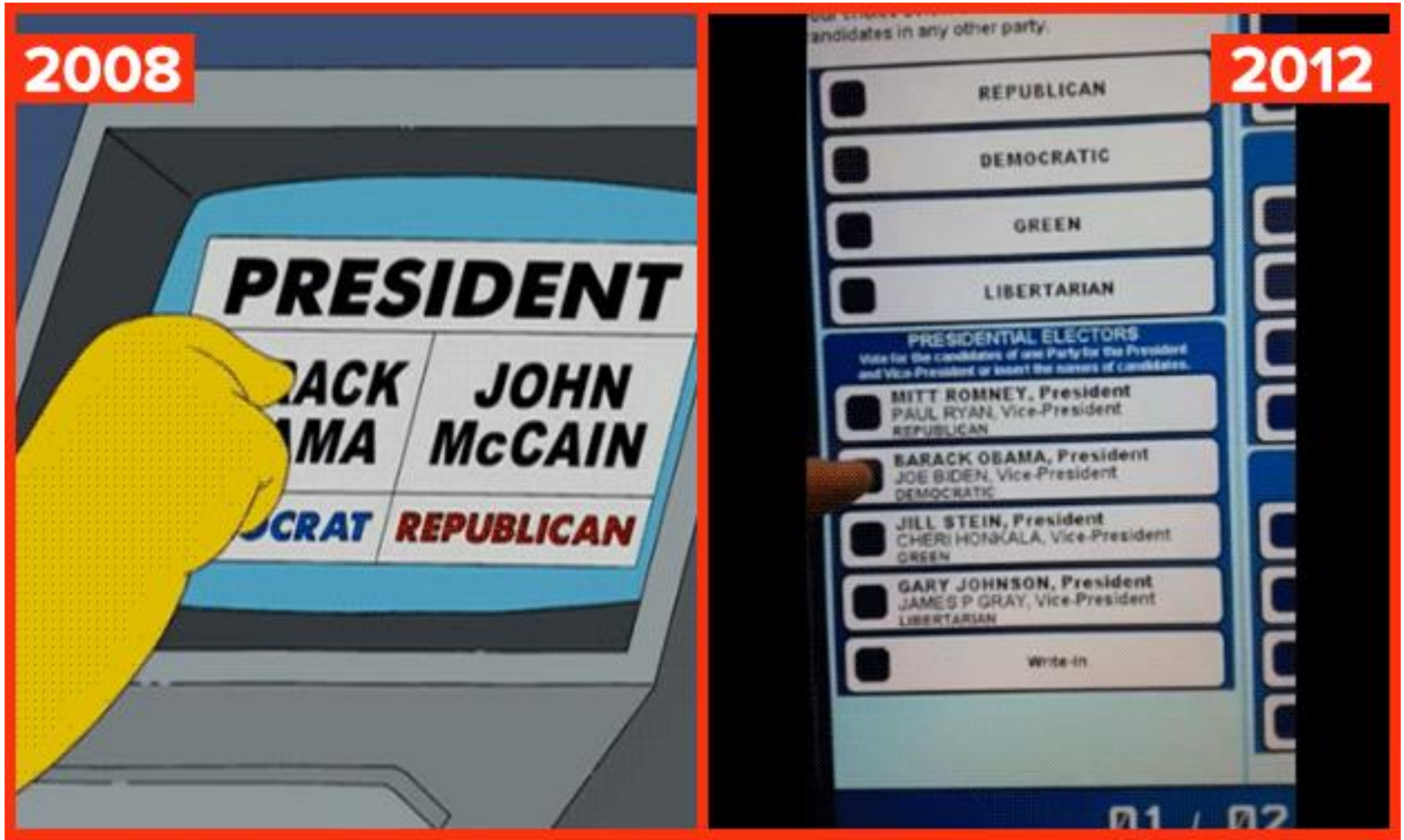


Trazabilidad hasta la urna digital

Comprobación de Integridad

¿Qué ocurre si tengo malware en mi ordenador?




2008
PRESIDENT
JOHN
McCAIN
REPUBLICAN
2012
REPUBLICAN
DEMOCRATIC
GREEN
LIBERTARIAN
PRESIDENTIAL ELECTORS
MITT ROMNEY, President
PAUL RYAN, Vice-President
REPUBLICAN
BARACK OBAMA, President
JOE BIDEN, Vice-President
DEMOCRATIC
JILL STEIN, President
CHERI HONKALA, Vice-President
GREEN
GARY JOHNSON, President
JAMES P GRAY, Vice-President
LIBERTARIAN
Write-in

1. Códigos de Retorno

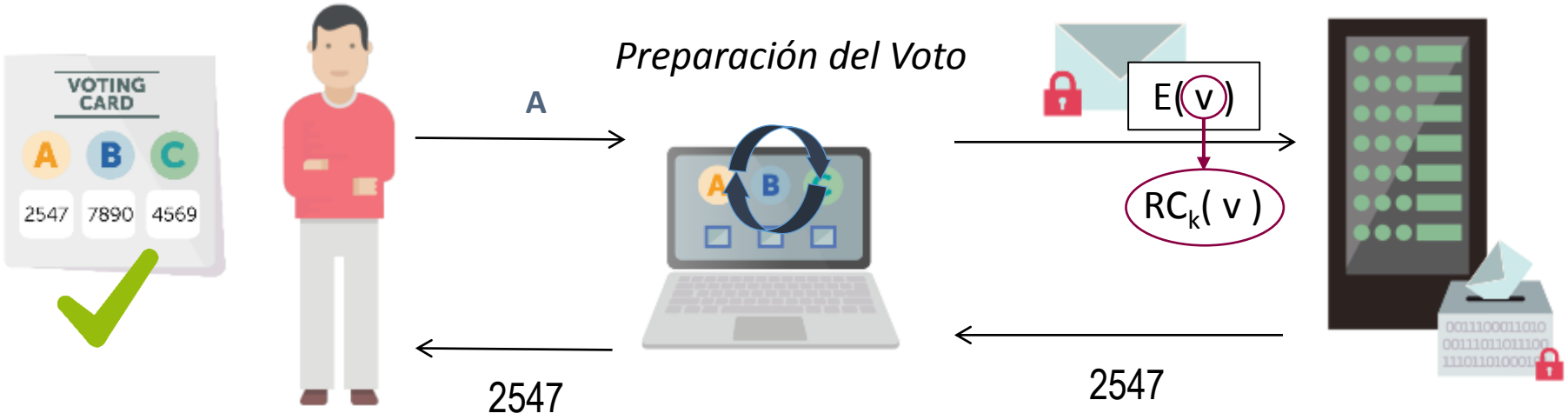
Dine personlige returkoder

- Du skal *alltid* få en tekstmelding med returkode etter at du har stemt via Internett.
- Det *eneste* du skal bruke returkodene på dette arket til, er å sjekke at du får riktig returkode via tekstmelding.
- Du skal *aldri* taste inn eller oppgi returkodene på dette arket til noen, heller ikke til en nettside.

Parti- /gruppenavn	Returkode	Parti- /gruppenavn	Returkode
Blank stemmeseddel	2887	Rødt	4469
Det norske Arbeiderparti	0700	Senterpartiet	0681
Demokratene	0239	Sosialistisk Venstreparti	4288
Det Liberale Folkepartiet	0519	Venstre	3014
Høyre	6564	Fremskrittspartiet	4946
Kristelig Folkeparti	5494		
Kystpartiet	4274		
Miljøpartiet De Grønne	6720		
Pensjonistpartiet	4536		

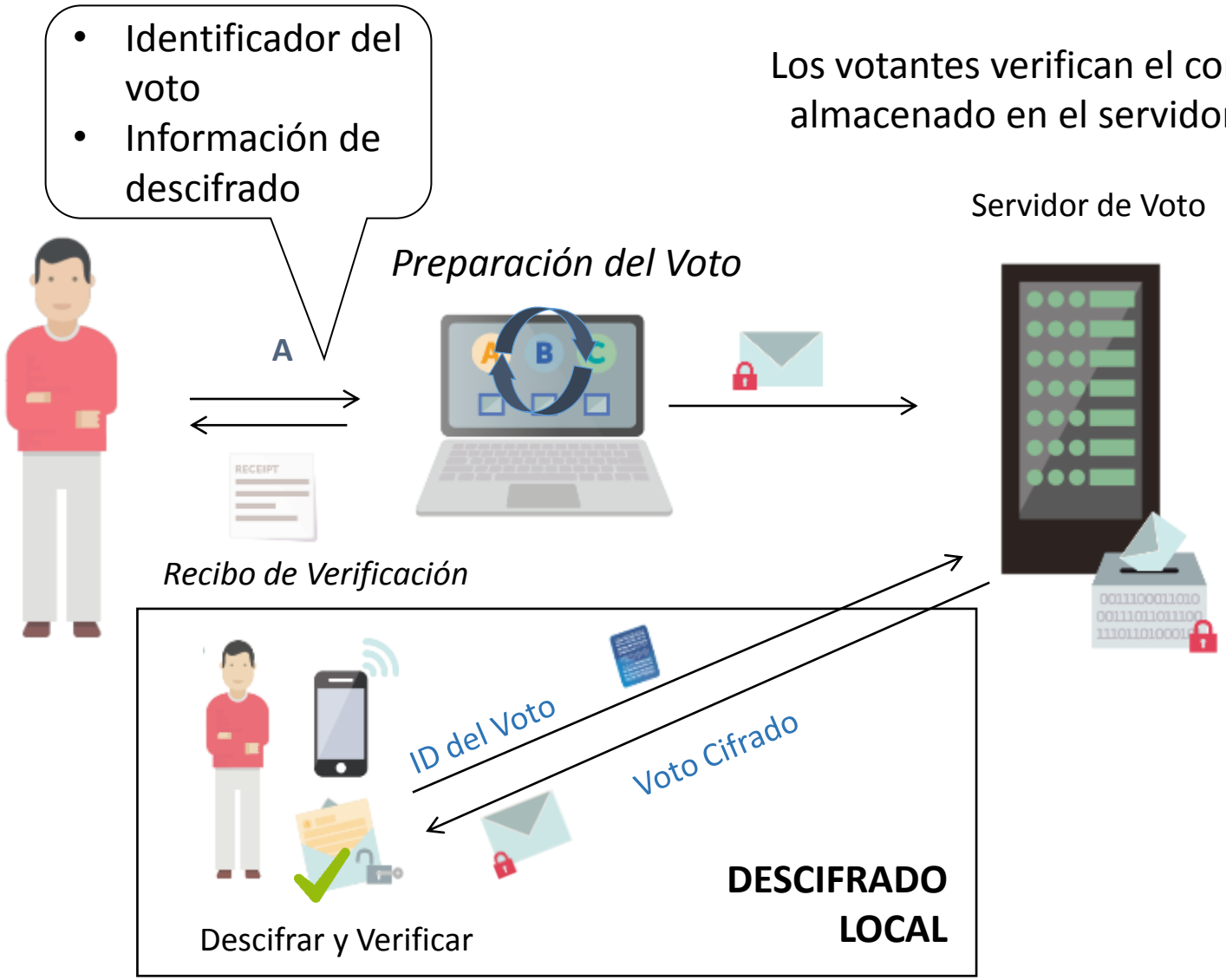
1. Códigos de Retorno

Los votantes utilizan la Voting Card que han recibido previamente en papel, para verificar el voto después de enviarlo



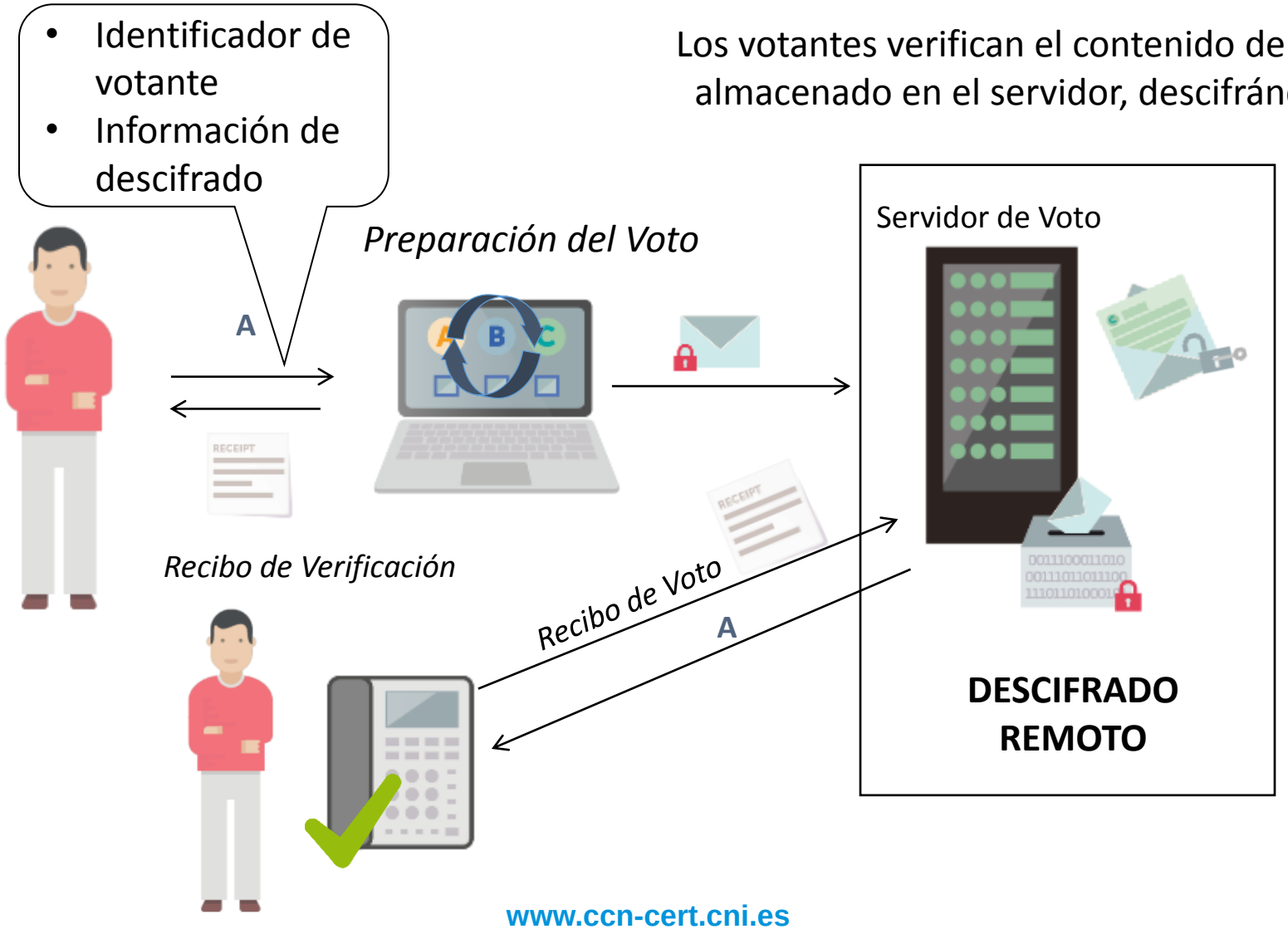
2. Descifrar el voto emitido (I)

Los votantes verifican el contenido del voto almacenado en el servidor, descifrándolo



2. Descifrar el voto emitido (II)

Los votantes verifican el contenido del voto almacenado en el servidor, descifrándolo



2. Descifrar el voto emitido



Example: **Estonian election**

DESCIFRADO LOCAL

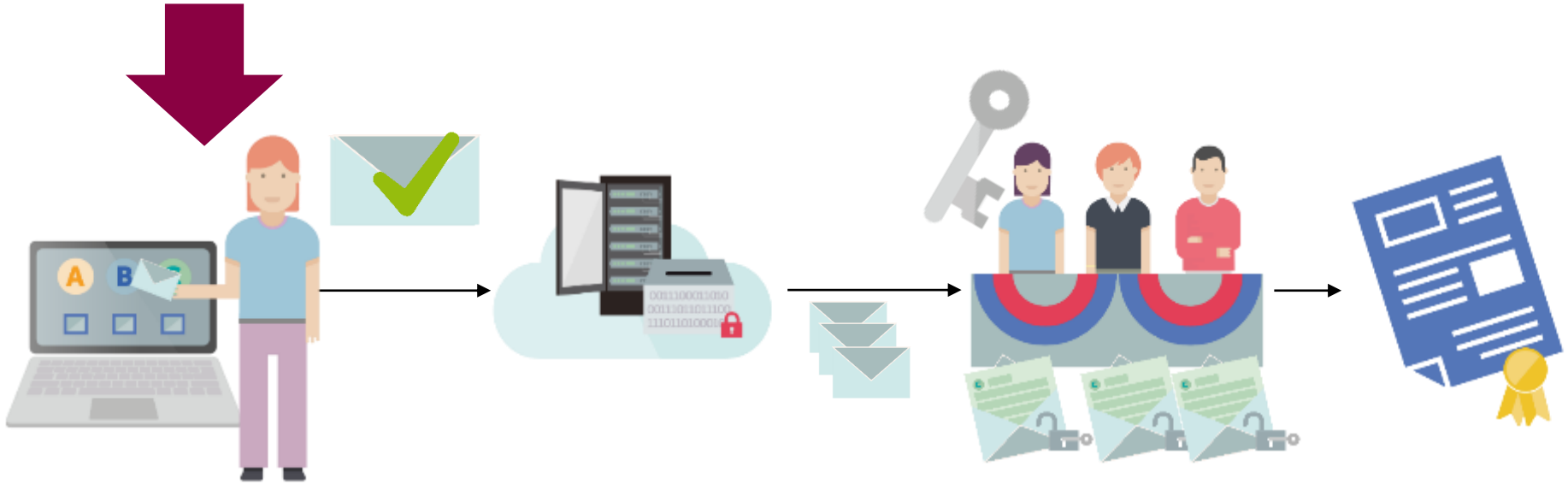
VOTE RECEIPT

Thank you for using the iVote® for Web demonstration system. Your practise vote is complete and the demonstration **Receipt Number** is:

3111 6228 8894

Example: **New South Wales iVote system**

DESCIFRADO REMOTO


Comprobación del contenido
Trazabilidad hasta la urna digital
Comprobación de Integridad
End-to-end verifiability

Todo en la wild wild web puede ser hackeado…





Reduce tu superficie de ataque

- Ordenadores aislados para las actividades más críticas
- Sólo son unas pocas llamadas web
- Corto espacio de tiempo
- Todo parcheado a la última versión
- Bastionado y adecuadamente probado

Pero en cualquier caso, tenemos que asumir que podemos ser hackeados

Los sysadmins siempre tienen acceso a todo…



El terminal de voto



Servidores

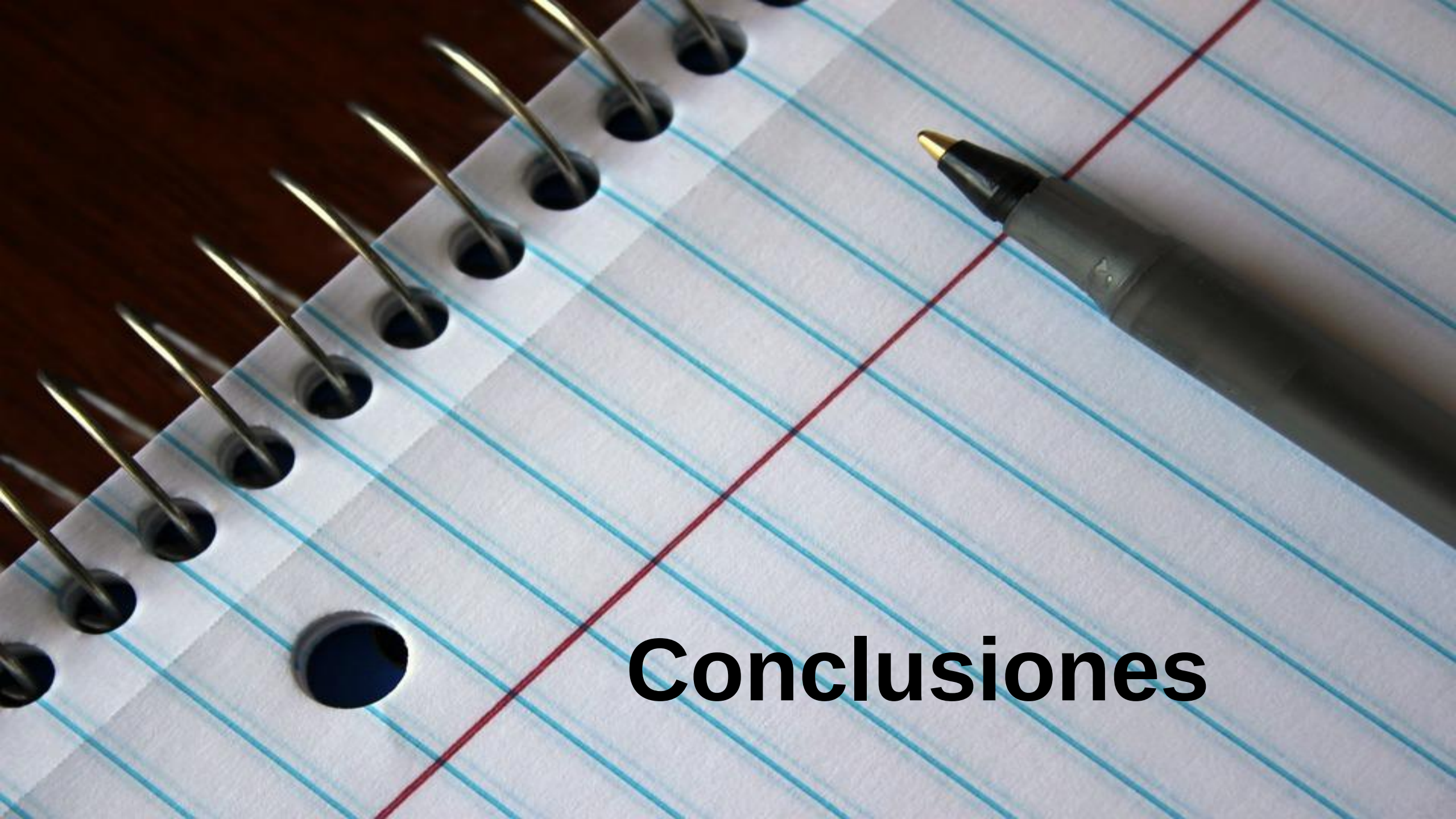


Ordenadores aislados



- ¿Ver los votos y romper la privacidad? Cifrado end-to-end, anonimización en mixnets, recuento homomórfico…
- ¿Añadir o modificar votos? Votos firmados digitalmente, verificabilidad end-to-end…
- ¿Malware puede modificar el voto? Códigos de retorno, descifrado del voto enviado…
- ¿Una persona con el control? Claves repartidas en la mesa electoral
- ¿Manipular el recuento de votos? Zero-Knowledge proofs, ceremonias de recuento con ordenadores aislados…
- ¿Cambiar los logs de todo el sistema? Logs inmutables
- …

La confianza reside en la Mesa Electoral y la Mesa de Administración, con auditores y observadores.



Conclusiones

- Hay muchos controles de seguridad basados en criptografía aplicables a Internet Voting, aunque sean desconocidos para los ciudadanos.

- La seguridad es similar a la de **elecciones tradicionales**. Y mucho más avanzada que la del voto postal.

- Que un ordenador remoto gestione tu voto no significa que debas confiar en él, debe haber **verificabilidad** de todo el proceso.




¿Alguna
pregunta?

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en



