Informe d'auditoria tecnològica del procés electoral "Eleccions a la Presidència 2025" del Consell de la República

16 de febrer de 2025

Antecedents i objectius

El present informe té per objectiu consolidar en un únic document l'anàlisi realitzada del sistema de votacions electròniques emprats per a donar sortida a l'esmentada comtessa electoral, així com verificar que, en relació a la proclamació dels resultats provisionals, s'han proporcionat els elements tècnics necessaris per a la seva certificació de manera definitiva.

Sistema de votacions electròniques

Donat que les votacions s'han realitzat exclusivament per mitjans electrònics, ha estat cabdal determinar si les tecnologies emprades a tal efecte a l'entorn de *back-end* proveïen les garanties necessàries per a la certificació dels resultats electorals de manera que es poguessin garantir tant els drets dels electors com els de les persones candidates. En aquest sentit, i com a part de l'auditoria tecnològica global del Consell de la República, ha estat determinat que s'ha disposat de la solució Amazon Web Services Quantum Ledger Database (AWS QLDB), que **es caracteritza per permetre verificar criptogràficament la integritat de les dades, registrant automàticament totes les operacions d'escriptura i actualització de dades, de tal manera que qualsevol modificació que vulneres la integritat del procés electoral hauria estat degudament detectada en una cadena de blocs, que, precisament gràcies al fet que aquesta és immutable, hauria permès constatar qualsevol intent d'ingerència externa.** Cal assenyalar que, aquesta base de dades **no s'ha de confondre amb una cadena de blocs pública** *a l'ús* com ho és, per exemple, Ethereum, i que, per tant, la interacció amb aquesta es realitza de manera programàtica mitjançant API, emprant els SDK proporcionats pel mateix *vendor*. En aquest sentit, indicar que, de fet, **aquest és el mateix sistema que s'ha vingut emprant pel Consell de la República en nombrosos processos electorals (inclòs el de la Presidència de l'any 2024)**, sense que consti que en cap cas s'hagi produït cap mena incidència, el que confirma que, més enllà de l'anàlisi teòrica del sistema, el seu desplegament en l'entorn de producció compleix amb els requisits necessaris en termes de seguretat i idoneïtat per al desplegament de processos electorals en el marc del Consell de la República.

Cal assenyalar, complementàriament, que s'ha pogut constatar que **el programari emprat** per a la validació dels electors i l'emissió dels vots **va ser actualitzat per darrer cop en data de 24 de novembre de 2023**, precisament per a l'actualització del SDK proporcionat per AWS per a la interacció amb l'esmentat servei AWS QLDB.

Procés electoral

En data de **8 de febrer de 2025, a les 9:00h** (GMT+1:00 - Barcelona) es va activar automàticament, segons estava previst, l'accés al servei de votació electrònica, sense que fos detectada cap incidència tècnica rellevant.

Durant el procés es van registrar 359 consultes d'incidències relatives a la votació, i, de l'anàlisi del contingut d'aquestes, **es certifica que en cap cas es van produir incidències relatives al sistema de votació**, ans al contrari, essencialment es van registrar consultes relatives a les incidències habituals en l'operació de qualsevol sistema informàtic. Cal assenyalar, en tot cas, que **la xifra d'incidències detectades és residual, per quant aquestes representen un impacte en el 0,40% del cens, i, en termes dels electors que van exercir el seu dret a vot, un 4,44%**.

Addicionalment, es va realitzar un monitoratge de ciberseguretat emprant les solucions a disposició del Consell de la República (en particular, CloudFlare), detectant-se **un intent de DoS (*Denial of Service*)** aïllat i que no va tenir impacte en cap de les infraestructures digitals del Consell de la República. Aquest atac **es va detectar i mitigar mitjançant WAF**, sense que fos detectat cap altre intent de degradar els serveis.

Complementàriament, cal assenyalar que a causa d'atacs informàtics rebuts en el passat pel Consell de la República, **en un nombre molt reduït de casos, alguns programaris d'antivirus informaven erròniament que l'adreça en la que s'allotja el servei de votacions electròniques podria contenir programari maliciós**. Les incidències de votació relatives a aquest extrem van ser mitigades suggerint la votació mitjançant dispositiu mòbil o la desactivació temporal dels esmentats programaris d'antivirus.

El període de votacions va finalitzar normalment el 12 de febrer de 2025, a les 9:00h (GMT+1:00 – Barcelona).

No es va detectar cap altre circumstància rellevant i, especialment, **no es va detectar cap anomalia que poses en risc la integritat del procés electoral**.

Certificació de resultats

En data de 12 de febrer de 2025, es va procedir a la certificació automatitzada dels resultats electorals, sense que detectes cap incidència o ingerència que hagués tingut per objectiu manipular els resultats. El resultat s'extreu del JSON corresponent, del que es transcriu literalment el resultat:


```
"PRP-20250207142236507-MWq//DBT-20250207144034151-dV8//EQS-20250207153927401-gPP": {
        "numVots":          8108,          "RSP-
        20250207153928186-5jr":   5340,   "RSP-
        20250207153931965-BMO":  1846,  "RSP-
        20250207153932445-Fu9":   745,   "RSP-
        20250207153932440-6Q0":  161,  "blanc":
        16
    }
```


Per referència, els identificadors únics assignats per candidatura, son:


```
{
    "RSP-20250207153928186-5jr": "Jordi Domingo",
    "RSP-20250207153931965-BMO": "Montserrat Duran",
    "RSP-20250207153932445-Fu9": "Toni Comín",
    "RSP-20250207153932440-6Q0": "Antoni Walter"
}
```


Consideracions addicionals

Deprecació del servei AWS QLDB

El sistema emprat actualment compleix amb tots els estàndards de seguretat i transparència, i, per tant, és possible recomanar que aquest se segueixi emprant en el futur, però, tot i això, ha estat informat pel *vendor* del mateix que aquest ha estat *deprecat*, i que es cessarà en prestar el servei associat el mes de juliol de 2025, moment en el que s'haurà d'haver desenvolupat un nou sistema que permeti la realització de processos electorals electrònics al Consell de la República. **Aquesta circumstància no té cap impacte en el procés electoral realitzat, però sí, com s'indica, ho és pel futur, ja que no es podrà emprar per a la realització de votacions electròniques més enllà del juliol de 2025.**

Jordi Planas Bielsa
Smart Contract Engineer

Digitally signed by JORDI PLANAS BIELSA - DNI [redacted]
Date: 2025.02.16 22:30:16 +01'00'