

Andorra la Vella, 31 de maig de 2023

1. INTRODUCCIÓ

L'Autoritat de Certificació de les Administracions Públiques Andorranes (AC – APA) està subjecta al compliment del que s'indica a l'article 35.1 LSCE per la qual cosa ha de ser auditada anualment per un organisme independent reconegut per confirmar que tant l'AC-APA com els serveis de confiança electrònica que presta compleixen els requisits establerts en la LSCE .

En aquest sentit ADHOC.TECH ha rebut l'encàrrec per part del Govern d'Andorra de la realització de la present auditoria de conformitat. L'AC-APA està gestionada per l'Oficina de Serveis de Confiança Electrònica del Principat d'Andorra (OSCEPA), com a oficina responsable per part del Govern d'Andorra.

2. CONSIDERACIONS GENERALS

- **ENTITAT:** Oficina de Serveis de Confiança Electrònica del Principat d'Andorra (OSCEPA).
- **CREACIÓ:** segons decret de l'1-7-2015 pel qual s'aprova el Reglament de supervisió, control i servei públic de confiança electrònica, es crea l'Oficina de Serveis de Confiança Electrònica del Principat d'Andorra (Oscepa) en relació amb els serveis de confiança electrònica que presti l'Entitat de Certificació del Govern.
- **MINISTERI D'ADSCRIPCIÓ:** L'Entitat està adscrita al Ministeri de Presidència, Economia i Empresa.
- **EXPEDIENT ADMINISTRATIU:** NÚM. 8980848.
- **NORMATIVA REGULADORA OBJECTE DE L'AUDITORIA:**
 - LLEI 35/2014 DEL 27 DE NOVEMBRE, DE SERVEIS DE CONFIANÇA ELECTRÒNICA.
- **PERÍODE COBERT PER L'AUDITORIA:** del 1 de gener de 2022 fins el 31 de desembre de 2022.

3. ABAST DE L'AUDITORIA

L'abast de la Auditoria inclou la totalitat de les instal·lacions i sistemes de l'AC-APA i de l'OSCEPA ubicades al Principat d'Andorra i les dels prestadors de serveis d'infraestructura de firma electrònica ubicats a Espanya.

En línies generals, l'auditoria verificarà:

1. Que l'AC-APA té un sistema que garanteix la qualitat del servei prestat;

2. Que la CPS s'ajusta al que estableixen les polítiques, al que està acordat per l'autoritat aprovadora de la política i al que estableix la normativa vigent;
3. Que l'AC-APA gestiona de forma adequada la seguretat dels seus sistemes d'informació.

En línies generals, els elements objecte d'auditoria seran els següents:

1. Processos de l'AC-APA, AR i elements relacionats amb l'emissió de certificats i serveis de validació en línia OCSP;
2. Sistemes d'informació;
3. Documentació requerida per a cada tipus de certificat;
4. Verificació que els operadors d'AR coneixen la CPS de l'AC-APA.

L'àmbit de l'auditoria inclou les següents jerarquies:

1. Per una banda es demana conformitat de la jerarquia actual de l'AC-APA emesa a partir de la jerarquia pròpia signada amb el certificat arrel:
 - o http://pki.govern.ad/certificats/Govern_Andorra2021.crt
2. D'altra banda es demana conformitat només pels serveis de revocació i validesa dels certificats de l'anterior jerarquia signada amb el certificat arrel (des de juliol del 2019 no emet certificats):
 - o http://pki.govern.ad/certificats/Govern_Andorra2020.crt

4. NORMATIVA REGULADORA

- LLEI 35/2014 DEL 27 DE NOVEMBRE, DE SERVEIS DE CONFIANÇA ELECTRÒNICA
- Documentació annexa complementària:
 - DECLARACIÓ DE PRÀCTIQUES DE CERTIFICACIÓ PKI A L'ADMINISTRACIÓ PÚBLICA ANDORRANA - Versió 4.0.

5. IDENTIFICACIÓ I QUALIFICACIÓ DE L'EQUIP AUDITOR

Pel que fa als requisits exigits a l'equip auditor, ADHOC.TECH compleix amb l'especificat en les bases del concurs de la present auditoria:

- No existeix cap conflicte d'interessos entre l'auditor i la part auditada (AC-APA, OSCEPA, i proveïdor tècnic);
- L'equip auditor és independent de l'activitat auditada;
- Les troballes i conclusions del procés de l'auditoria es basen en només en evidències objectives;
- L'auditoria la realitza un equip auditor qualificat, tant en terme d'independència de l'auditoria com en terme de coneixements en l'examen de la tecnologia de la infraestructura de claus públiques, eines i tècniques de seguretat de la informació, auditoria de tecnologia i seguretat de la informació.

6. OBSERVACIONS

Per realitzar l'auditoria en els termes, abast i període definits en el plec de bases, i segons la normativa de referència, s'ha sol·licitat el Govern d'Andorra i l'AC-APA que gestiona els serveis de Certificació a Andorra per a les CA, per a què posi a disposició de l'equip auditor tota la informació necessària per poder realitzar l'examen correcte i suficient dels diferents procediments que fan referència a:

- Identificació i autenticació dels titulars dels certificats;
- Requisits d'operació del cicle de vida dels certificats;
- Controls de les instal·lacions, de gestió i operacionals;
- Controls de seguretat tècnica

En aquest sentit, després d'haver examinat les evidències aportades pel Govern Andorra i l'entitat gestora de l'AC-APA, es desprèn que:

- Existeixen i es mantenen els procediments i controls efectius i suficients per proporcionar una seguretat adequada pel que fa a la validació inicial de la identitat, identificació de l'entitat o persona jurídica;
- Les declaracions de pràctiques de certificació de l'AC-APA són coherents amb les seves polítiques de certificació;
- L'AC-APA presta els seus serveis de certificació en acord amb les seves polítiques i declaracions de pràctiques de certificació;
- Existeixen i es mantenen els procediments i controls efectius i suficients per proporcionar una seguretat adequada pel que fa a:
 - Sol·licitud de certificats, processament de les sol·licituds de certificats, emissió de certificats, acceptació de certificats;
 - Revocació de certificats;
 - Identificació i autenticació de sol·licituds de renovació;
 - Identificació i autenticació de la sol·licitud de revocació.

D'altra banda, l'examen de les evidències aportades permet posar de manifest que:

- Existeixen i es mantenen els procediments per garantir la integritat de les claus i dels certificats corresponents durant els seus cicles de vida;
- Existeixen i es mantenen els procediments per protegir la integritat de les claus i certificats de subscriptor que gestiona al llarg dels seus cicles de vida;
- La informació del subscriptor està degudament autenticada (per a les activitats de registre realitzades per l'AC-APA);
- Les sol·licituds de certificats de CA subordinades són adequades, autenticades i aprovades;
- La generació i instal·lació de claus, així com la protecció de les claus privades, corresponen adequadament i degudament als estàndards definits en els procediments corresponents per als mòduls criptogràfics.

A més, i en relació als controls de les instal·lacions i de seguretat tècnica, de l'examen de les evidències es desprèn que:

- L'accés lògic i físic als sistemes i a les dades de l'AC està restringit a persones autoritzades;

- Existeixen i es mantenen els procediments de continuïtat de les operacions de gestió de claus i certificats;
- El desenvolupament, el manteniment i les operacions de sistemes de l'AC estan autoritzats i realitzats adequadament per mantenir la integritat dels sistemes corresponents;
- Existeixen i es mantenen els procediments relatius als controls de seguretat dels diferents cicles de vida;
- Existeixen i es mantenen els procediments relatius als controls de seguretat de la xarxa, còpies de seguretat i arxius de les claus.

7. RECOMANACIONS

Els exàmens realitzats per l'equip auditor han portat a formular que no s'ha detectat cap no conformitat greu, ni cap no conformitat lleu, en cap dels aspectes analitzats, corresponents als procediments que fan referència a:

- Identificació i autenticació dels titulars dels certificats;
- Requisits d'operació del cicle de vida dels certificats;
- Controls de les instal·lacions, de gestió i operacionals;
- Controls de seguretat tècnica.

L'objectiu que ha de perseguir l'AC-APA és el de prevenir i evitar possibles errors, frauds, accessos no autoritzats a sistemes d'informació, o incompliments de polítiques o requisits interns i externs.

Els diferents procediments associats a l'objecte de l'auditoria han de procurar aproximar-se a proporcionar màxims nivells de seguretat, entenent-se que no existeix el nivell de seguretat absolut.

Amb tot això les evidències proporcionades per l'AC-APA i analitzades per l'equip auditor posen de manifest, tal i com queda exposat en l'apartat anterior 6-OBSERVACIONS que el conjunt de procediments presenten un nivell de seguretat adequat, no requerint-se per tant cap acció correctora urgent, greu o lleu.

Tot i així l'equip auditor posa de manifest que els sistemes de control implantats poden presentar en alguns casos algunes limitacions. Aquestes limitacions es poden relacionar amb una casuística general d'ús de controls interns que inclouen manualitats o bé amb interaccions amb els usuaris de claus i certificats que inclouen controls d'identitat amb un nivell de comprovació limitat.

Per aquest motiu es formulen les següents **recomanacions**:

- Suprimir o limitar les interaccions online no comprovables en les diferents transaccions amb el ciutadà o empresa, privilegiant o recomanant l'ús de la firma electrònica;
- Suprimir o limitar les interaccions físiques no comprovables, tal com firmes en paper o escanejades, en les diferents transaccions i interaccions amb el ciutadà o empresa, procurant incloure mitjans de comprovació quan és possible;

- Automatitzar i supervisar, en mesura raonable, els procediments manuals dels agents de l'AC-APA en la realització de les tasques d'identificació, autenticació; sol·licitud, emissió i revocació de certificats.

8. CONCLUSIONS

S'ha realitzat la present auditoria de manera a arribar a conclusions raonables pel que fa a les verificacions i anàlisis realitzades, de manera a poder contrastar de forma correcta les afirmacions i les evidències aportades per l'AC-APA, i en relació als diferents aspectes definits en la normativa reguladora corresponent.

Cal afegir a més que l'abast de la present auditoria no inclou cap anàlisi o control relatiu a factors presents a les ubicacions individuals dels subscriptors i de les parts de confiança.

L'opinió del present equip auditor, en relació als treballs definits en el plec de bases corresponent a l'AUDITORIA DE CONFORMITAT AMB LA LLEI 35/2014 DEL 27 DE NOVEMBRE, DE SERVEIS DE CONFIANÇA ELECTRÒNICA, expressa que els serveis oferts per l'AC-APA corresponen als principis i criteris que defineix la mencionada llei, són conformes als estàndards definits, i presenta uns principis i nivells de seguretat adequats.

Aquest informe no inclou cap anàlisi, recomanació, conclusió, referent a serveis del Govern d'Andorra i de l'AC-APA més enllà dels coberts per la LLEI 35/2014 DEL 27 DE NOVEMBRE, DE SERVEIS DE CONFIANÇA ELECTRÒNICA.

Signatura

ADHOC.TECH
Roland EROLES SENTENAC

ADHOC.TECH
Xavier PALACIOS ALBACAR

Information Security Management Systems Auditor
Lead Auditor (BS ISO/IEC 27001:2013)
(British Standard Institute)