

Codi Segur de Verificació:
d8041667-dab1-4c78-a9d9-6980faef112c
Origen: Ciutadà
Identificador document: ES_L01171609_2023_3125545
Data d'impressió: 30/06/2026 20:38:53
Pàgina 1 de 6

SIGNATURES
1.- CIPISR-2 Núria Faura Pujol, 09/02/2023 12:33



Versió 1



Consorci
Administració Oberta
de Catalunya

INFORME D'AUDITORIA DE CONFORMITAT

Ajuntament de Sant Feliu de Guíxols

Codi Segur de Verificació:
d8041667-dab1-4c78-a9d9-6980faef112c
Origen: Ciutadà
Identificador document: ES_L01171609_2023_3125545
Data d'impressió: 30/06/2026 20:38:53
Pàgina 2 de 6

SIGNATURES
1.- CIPISR-2 Núria Faura Pujol, 09/02/2023 12:33



Consorci
Administració Oberta
de Catalunya

Versió 1

1. DADES DE L'ORGANITZACIÓ

NOM: Ajuntament de Sant Feliu de Guíxols

TIPUS: Ens Subscriptor

RESPONSABLE: Alfred Mont de Rojas

DATA: 28/11/2022 5:57:42

2. OBJECTE I ABAST

L'objecte d'aquest document és desenvolupar els requisits de les Auditories relacionades amb els organismes que executen part del Servei de Certificació Digital concretament a l'àmbit de les Entitats de registre o Ens subscriptors: és un ens o departament que col·labora amb el Consorci AOC en els tràmits d'identificació, registre i autenticació per a l'emissió de certificats digitals, seguint els procediments i les relacions amb els titulars dels certificats.

L'abast de l'auditoria contempla diversos elements objecte d'aquesta:

- **Termes i condicions**
- **Operació i gestió del servei**
- **Recursos humans involucrats**
- **Gestió d'actius:** L'ens s'haurà d'assegurar del nivell apropiat de protecció dels actius, incloent-hi els actius d'informació.
- **Control d'accés digital:** L'accés al sistema estarà limitat al personal autoritzat.
- **Control d'accés físic:** S'ha de controlar l'accés físic als components del sistema de l'ens, la seguretat dels quals és crítica per a la provisió del servei de confiança i minimitzar els riscos relacionats amb la seguretat física.
- **Seguretat operacional:** L'ens ha d'utilitzar sistemes de confiança i productes protegits contra modificacions i s'ha d'assegurar de la seguretat tècnica i fiabilitat dels processos realitzats per ells.
- **Seguretat de les xarxes:** L'ens ha de protegir la seva xarxa i els seus sistemes dels atacs.
- **Gestió d'incidents:** S'ha de controlar l'activitat del sistema relacionada amb l'accés als sistemes informàtics, l'ús de sistemes informàtics i les sol·licituds de servei.
- **Alineació amb el Pla de continuïtat de negoci de l'AOC:** L'ens ha de tenir definit i mantenir un pla de continuïtat que promulgarà en cas de desastre.
- **Compliment legal i normatiu:** L'ens s'ha d'assegurar que opera dins el marc legal aplicable
- **Gestió de la identificació.**
- **Gestió del canvi:** Procediment transversal on es planifiquin els canvis, es registrin i es dugui un seguiment.

3. METODOLOGIA

La metodologia emprada per a la realització d'aquesta auditoria és la següent:

- S'ha fet un mostreig dels certificats personals, de dispositiu i aplicació generats. Establint un valor no superior al 10% o un mínim de 10 certificats si és possible.
- S'ha comprovat que les dades del certificat generat són les mateixes que el certificat sol·licitat o que el DNI. En els casos de full de lliurament de T-CAT es comprovarà mitjançant l'aplicació que el full de lliurament no s'ha imprès en el moment de l'auditoria sinó quan es va realitzar el certificat, i que la data de signatura del full de lliurament és anterior a l'enviament dels codis PIN i PUK.
- S'ha comprovat la seguretat del tractament de dades personals en compliment de la legislació vigent.
- S'han avaluat una sèrie de controls relatius a requisits de gestió documental i arxiu, requisits de seguretat i requisits operatius.



Codi Segur de Verificació:
d8041667-dab1-4c78-a9d9-6980faef112c
Origen: Ciutadà
Identificador document: ES_L01171609_2023_3125545
Data d'impressió: 30/06/2026 20:38:53
Pàgina 3 de 6

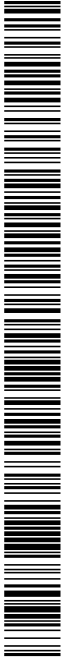
SIGNATURES
1.- CIPISR-2 Núria Faura Pujol, 09/02/2023 12:33



Versió 1

4. AVALUACIÓ

Control	Avaluació	Observacions
El contingut dels expedients és l'adequat i es correspon amb la informació dels certificats emesos (Sol·licitud d'emissió, acusament de rebuda de correus i còpia del full de lliurament i acceptació de certificats signada pel titular, en els casos que s'hagi tramitat en paper).	Sí	
1.1.1 Existeix un procediment de transferència d'expedients a l'arxiu central que defineix la periodicitat, el responsable i el mode d'enviament en cas que hagi de ser traslladat?	Sí	Comentari ENS: Els arxius electrònics es transfereixen mitjançant accions configurades al programa de gestió d'expedients. Els arxius en paper es digitalitzen d'acord amb la normativa La periodicitat va en funció de la disponibilitat de l'àrea gestora
1.2.1 Els controls de seguretat física de l'arxiu són adequats? (No deixar cap document fora del seu expedient; Tancar amb clau l'arxivador i/o armari; Permetre l'accés a l'arxiu o al mobiliari d'arxiu només al personal autoritzat, etc.)	Sí	Comentari ENS: Els controls d'accés físics són els adequats per tot l'arxiu però en aquest cas no s'apliquen perquè tota la gestió derivada del servei es tramita íntegrament en digital. Els aplicatius digitals tenen les mesures de seguretat adequades al nivell mitjà de l'Esquema Nacional de Seguretat
Evidències dels CERTIFICATS seleccionats	Sí	R_2zx0CSq6shnhz0mO_R4.108.rar
2.1.1 Disposeu d'una fitxa d'ENS actualitzada a la situació actual i que d'aquesta manera, que garanteixi el compliment i hagi estat enviada en els darrers 2 anys?	No	Comentari ENS: Estem en procés d'implantació de l'ENS però a nivell operatiu complim amb tots els requeriments de la documentació que s'ha de requerir als usuaris
2.2.1 Totes les persones que tenen algun rol en la sol·licitud i revocació de certificats tenen suficients coneixements sobre els procediments a seguir?	Sí	
3.1.1 Les targetes es custodien diligentment abans de l'entrega als titulars en una ubicació amb accés restringit, de tal manera que permetin la traçabilitat?	Sí	Comentari ENS: Actualment es lliuren molt pocs certificats en dispositiu targeta però aquestes només passen per 3 serveis: OAC que les recepcionen de correus i les registren al programari informàtic. les guarden en una oficina d'accés restringit i arxivadors tancats amb clau informàtica, que les recepciona i les guarda fins que les porta al destinatari. oficines amb accés restringit amb porta d'accés destinatari
3.2.1 Disposeu d'un sistema antimalware instal·lat a tots els equips de treball, està actiu i actualitzat (almenys de forma diària)?	Sí	R_2zx0CSq6shnhz0mO_EVIDENCIA AV.pdf



Codi Segur de Verificació:
d8041667-dab1-4c78-a9d9-6980faef112c
Origen: Ciutadà
Identificador document: ES_L01171609_2023_3125545
Data d'impressió: 30/06/2026 20:38:53
Pàgina 4 de 6

SIGNATURES
1.- CIPISR-2 Núria Faura Pujol, 09/02/2023 12:33



Consorci
Administració Oberta
de Catalunya

Versió 1

3.2.2 Teniu implementats controls per evitar l'accés indegut als sistemes d'informació (doble factor per l'autenticació de sistemes, impossibilitat d'accedir depenent del rol assignat, etc.)?	Sí	Comentari ENS: Tot l'accés als expedients corporatius tenen restriccions per usuaris, rols, àrea/departament , etc. Les connexions des de l'exterior van encriptades i via accés vpn
3.2.3 Disposeu de polítiques de control d'accés lògic: rols i responsabilitats, qualitat de contrasenyes, de taules netes (bloqueig de pantalles) i de bones pràctiques en seguretat?	Sí	R_2zx0CSq6snhz0mO_Instrucció mesures de seguretat.pdf
3.2.4 Disposeu d'un procediment de gestió d'incidents propi de l'ENS?	Sí	R_2zx0CSq6snhz0mO_Gestió incidents.pdf
3.2.5 Disposeu d'un pla o procediment de continuïtat per poder assignar i revocar els certificats en cas que el sistema falli? (p. ex. SAI per poder finalitzar un tràmit en cas de fallida, procediments alternatius per sol·licitar les revocacions de certificats, etc.)	Sí	Comentari ENS: Les emissions no solen ser serveis crítics i si fallen els sistemes informàtics no té massa importància no poder sol·licitar nous certificats, que, a més a més, trigaran uns dies en emetre'ls. en tot cas, els mecanismes del nostre ajuntament tenen un pla de continuïtat basat en alimentació (SAI) i redundància de la majoria de sistemes Tan les emissions com revocacions, donat que només requereixen la signatura digital dels operadors, es podria efectuar des d'ordinadors corporatius independents (portàtils dels serveis informàtics) i, per tan, servirien per continuar el servei en el cas de fallada generalitzada dels serveis centrals municipals
3.3.1 Els titulars dels certificats custodien amb diligència les seves targetes, així com el PIN i el PUK de les mateixes?	Sí	Sí, segons els procediments de seguretat
3.3.2 Tots els titulars de certificats que hagin estat baixa han estat comunicats al Consorci AOC a través del responsable i s'ha revocat el certificat en qüestió?	Sí	
3.3.3 De tots els titulars de certificats amb càrrec s'ha verificat la vigència d'aquest càrrec durant la vigència del certificat o s'ha sol·licitat la revocació del mateix?	Sí	
3.3.4 Es garanteix la destrucció de les targetes inutilitzades de manera diligent?	Sí	Comentari ENS: Sí, però només en el cas que ens les lliurin als serveis informàtics. de totes maneres, actualment l'emissió de certificats en targeta és pràcticament nul·la



Codi Segur de Verificació:
d8041667-dab1-4c78-a9d9-6980faef112c
Origen: Ciutadà
Identificador document: ES_L01171609_2023_3125545
Data d'impressió: 30/06/2026 20:38:53
Pàgina 5 de 6

SIGNATURES
1.- CIPISR-2 Núria Faura Pujol, 09/02/2023 12:33



Consorci
Administració Oberta
de Catalunya

Versió 1

3.3.5 Existeix un protocol o política d'esborrat segur de dades confidencials en dispositius per tal d'evitar l'accés no autoritzat?

Sí

Comentari ENS: els treballadors no haurien de tenir informació confidencial fora dels sistemes centralitzats però quan es canvia un ordinador, es passa "imatge" que destrueix tota la informació antiga.

Els disc durs qe es substitueixen es destrueixen físicament també

5. PUNTS DE MILLORA

ID	Recomanacions
1	Recomanem que guardeu tota la informació relativa als certificats, ja que s'ha de custodiar 15 anys des de la data de caducitat del certificat.
2	Recordem que tal com indiquen les condicions del servei s'ha d'enviar cada dos anys encara que no hi hagi canvis.

6. NORMATIVA APLICABLE

- UNE-EN-ISO 19011:2011 Directrices para la auditoria de los sistemas de gestión.
- UNE-EN-ISO/IEC 17065:2012 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.
- Reglament (UE) N° 910/2014 del Parlament Europeu i del Consell de 23 de juliol de 2014 relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i per la que es deroga la Directiva 1999/93/CE.
- DIRECTIVA (UE) 2016/1148 DEL PARLAMENT EUROPEU I DEL CONSELL de 6 de juliol de 2016 relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i sistemes d'informació a la Unió.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment-Requirements for conformity assessment bodies assessing Trust Services Providers.
- I tota la relacionada amb la prestacions de serveis de certificació.

7. RESULTAT

1. L'organització es quedarà amb una còpia de l'informe.
2. Tenint en compte les no conformitats constatades i indicades en aquest informe, l'entitat de registre es compromet a presentar accions correctives en el termini d'un any, de cara a la següent auditoria.
3. L'equip auditor informa que aquesta auditoria s'ha realitzat a través d'un mostreig pel qual poden existir altres no conformitats no identificades en aquest informe.
4. Les no conformitats es refereixen a incompliments dels requisits de la Regulació eIDAS a través de les normes ETSI.
5. **OPINIÓ DE L'AUDITOR: L'auditora considera adequada la situació actual.**

Nota:

A causa dels resultats favorables i superar aquesta auditoria, emplacem una nova auditoria l'any 2024.



Codi Segur de Verificació:
d8041667-dab1-4c78-a9d9-6980faef112c
Origen: Ciutadà
Identificador document: ES_L01171609_2023_3125545
Data d'impressió: 30/06/2026 20:38:53
Pàgina 6 de 6

SIGNATURES
1.- CIPISR-2 Núria Faura Pujol, 09/02/2023 12:33



Versió 1

Lloc: Barcelona

Signatura/s auditor/s

Signatura del representant de l'organització

Date:
2023.02.09
12:33:12 +01'00'