



Consorti
Administració Oberta
de Catalunya

Informe d'auditoria d'Entitat de Registre T-CAT

Dades Generals	
Entitat de Registre	
Responsable del servei	
Auditor AOC	
Data auditoria	

Àrees	Id. Control	Control	Tipus Control	Valoració	Evidència / Observació
REQUISITS DE GESTIÓ DOCUMENTAL I ARXIU	1.1.	Tramitació dels expedients			
	1	Metodologia d'arxiu i traçabilitat	OBL	No avaluat	
	2	El contingut dels expedients és l'adequat (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 en que s'hagi tramitat en paper).	OBL	No avaluat	
	3	La informació dels expedients seleccionats es correspon amb la informació dels certificats emesos.	OBL	No avaluat	
	4	Els expedients estan impresos amb paper que compleix la Norma UNE-EN ISO 9706:1999.	OPT	No avaluat	
	1.2.	Arxiu de gestió			
	1	Els arxivadors i/o armaris de gestió romanen tancats amb clau quan el personal del servei no està present.	OBL	No avaluat	
	2	L'accés als arxivadors només es permet al personal autoritzat.	OBL	No avaluat	
	1.3.	Transferència a l'arxiu central			
	1	Existeix un procediment de transferència d'expedients que defineix la periodicitat, el responsable i el mode d'enviament físic a l'arxiu central.	OPT	No avaluat	
	1.4.	Arxiu Central			
	1	Els controls de seguretat física de l'arxiu són adequats.	OBL	No avaluat	
	2	Metodologia d'arxiu i traçabilitat	OBL	No avaluat	



Consorti
Administració Oberta
de Catalunya



REQUISITS OPERATIU

2.1.	Documentació Requerida				
1	Disposen d'una fitxa de subscriptor actualitzada i ha estat enviada en els darrers 2 anys		OBL	No avaluat	
2	Disposen d'una fitxa d'entitat de registre actualitzada i ha estat enviada en els darrers 2 anys		OBL	No avaluat	
3	Disposen de termes i condicions on hi consten:	Les obligacions dels subscriptors, període de temps d'arxiu de logs, marc legal i compromís sobre disponibilitat	OBL	No avaluat	
4	Disposen de termes i condicions on hi consten:	Procediment de queixes i resolució de conflictes	OBL	No avaluat	
5	L'entitat informa prèviament als subscriptors i parts interessades sobre els termes i condicions abans d'iniciar la relació contractual		OBL	No avaluat	
6	Els termes i condicions es troben disponibles en mitjans no peribles amb un llenguatge entenedor i es poden transmetre electrònicament.		OBL	No avaluat	
7	Els serveis han de ser accessibles a tots els sol·licitants		OBL	No avaluat	
8	Disposen de polítiques i procediments per a la resolució de conflictes o reclamacions de clients o altres parts interessades		OBL	No avaluat	
9	Es diposa de la Fitxa d'identitat i s'ha revisat el compliment		OBL	No avaluat	
10	Disposen d'un procediment de gestió d'incidents		OBL	No avaluat	
11	Disposen d'un procediment de compliment legal i normatiu (compliance)		OBL	No avaluat	
12	Mantenir un llistat actualitzat d'actius d'informació amb l'assignació de la classificació corresponent amb l'avaluació de riscos realitzada.		OBL	No avaluat	
13	Es disposa d'un procediment i registre de gestió de canvis per a versions, modificacions i desplegaments.		OBL	No avaluat	
14	Existeix un procediment de reinici i recuperació del sistema en cas que falli..		OBL	No avaluat	
15	L'Entitat de Registre està alineada amb el pla de continuïtat de l'AOC		OBL	No avaluat	
2.2.	Formació i repàs de coneixements				
1	Tots els operadors han realitzat el curs formatiu d'operador d'entitat de registre T-CAT de Consorci AOC.		OBL	No avaluat	
2	El responsable del servei mostra coneixement del procediment aprovat per tal de guardar la documentació a l'arxiu de gestió en forma d'expedient.		OBL	No avaluat	
3	Es disposa d'una fitxa personal actualitzada amb la formació rebuda del personal involucrat.		OBL	No avaluat	

	4	Tot el personal (temporal o fixe) disposa de la seva descripció del lloc de treball on hi consta la sensibilització de posició en funció dels drets i nivell d'accés, formació i sensibilització.	OBL	No avaluat	
	5	L'Entitat de Registre té descrites sancions disciplinàries per aquells treballadors que incompleixin les polítiques o procediments establerts.	OBL	No avaluat	
	6	L'Entitat de Registre disposa de procediments i processos de gestió alineats amb els de seguretat de la informació.	OBL	No avaluat	
	7	Tots els operadors han d'estar lliures de conflictes d'interessos que puguin perjudicar la imparcialitat de les operacions del servei.	OBL	No avaluat	
	8	El personal no tindrà accés a les funcions d'operador del sistema fins que no s'hagin complert tots els controls necessaris.	OBL	No avaluat	
	9	Tots els operadors mostren coneixement del procediment per registrar i comunicar incidents de seguretat de la informació.	OBL	No avaluat	
	10	Tots els operadors han rebut una formació sobre actualitzacions sobre noves amenaces i pràctiques de seguretat actuals en els darrers 12 mesos.	OBL	No avaluat	
3.1. Seguretat física					
	1	La sala d'operacions ha de disposar d'un sistema electrònic d'obertura o, com a mínim, d'una porta amb pany i clau. En el cas que això no fos possible, la LRA ha d'estar ubicada en un lloc reservat on només hi tingui accés el personal de l'ER i en cap cas personal aliè al Ens subscriptor.	OPT	No avaluat	
	2	L'Entitat de Registre emmagatzema les targetes verges en una ubicació amb accés restringit.	OBL	No avaluat	
	3	El següent material es custodia a l'interior de la sala d'operacions: PC, impressora de targetes, caixa forta, estoc de targetes generades i la documentació de processos i sistemes.	OBL	No avaluat	
	4	Els components crítics per a la prestació del servei estan localitzats en un perímetre de seguretat protegit físicament contra la intrusió i es controla l'accés a través d'un perímetre de seguretat i alarma.	OBL	No avaluat	
	5	L'Entitat de Registre realitza prova de penetració a les infraestructures i la registra.	OBL	No avaluat	
	6	L'entitat té implementats controls per evitar el compromís o robatori d'informació i de les instal·lacions de processats de la informació.	OBL	No avaluat	
3.2 Seguretat lògica					
	1	La Entitat de Registre disposa d'un sistema antimalware instal·lat, està actiu i actualitzat (almenys de forma diària).	OBL	No avaluat	
	2	L'Entitat de Registre disposa de polítiques d'accés, qualitat de contrasenyes i estalvi de pantalles	OBL	No avaluat	
	3	La Entitat de Registre disposa d'un SAI amb una autonomia suficient per finalitzar un tràmit en condicions segures.	OPT	No avaluat	

REQUISITS DE SEGURETAT	4	A la LRA no s’hi ha detectat cap programari instal·lat sense l’aprovació deL Consorci AOC	OPT	No avaluat		
	5	A la LRA no s’hi ha detectat cap programari instal·lat que permeti accedir-hi de forma remota.	OPT	No avaluat		
	6	L'entitat de registre únicament fa servir la LRA per realitzar tasques relacionades amb el servei de certificació T-CAT.	OPT	No avaluat		
	7	Totes les informacions es tractaran de manera segura segons la seva classificació de risc.	OBL	No avaluat		
	8	L'Entitat de Registre es protegeix contra l'obsolescència i el deteriorament durant el temps en que s'hagin de conservar els registres.	OBL	No avaluat		
	9	L'accés a la informació i a les funcions del sistema d'aplicació estan restringits d'acord amb la política d'accés.	OBL	No avaluat		
	10	Els desplegaments de seguretat que estan disponibles, s'apliquen en un temps raonable.	OBL	No avaluat		
	11	L'Entitat de Registre es sotmet a simulacres de vulnerabilitats periòdics en adreces IP publicades, privades i sistemes i registra les proves realitzades.	OBL	No avaluat		
	12	El personal de l'Entitat de Registre s'identifica i autentica abans d'utilitzar aplicacions crítiques relacionades amb el servei.	OBL	No avaluat		
	3.3	Seguretat del personal				
		1	Els operadors custodien amb diligència les seves targetes d’operador, així com el PIN i el PUK.	OBL	No avaluat	
		2	En cas de participació de personal extern, aquests han signat una clàusula de confidencialitat amb l'Entitat de Registre	OBL	No avaluat	
		3	En el cas dels operadors que han causat baixa, el responsable del servei ha procedit a comunicar-ho a Consorci AOC i s’ha revocat el certificat de l’operador en qüestió.	OBL	No avaluat	
		4	Els operadors no tenen accés a les funcions de confiança (trusted functions) fins que no es compleixen tots els requisits.	OBL	No avaluat	
	3.4	Seguretat de l'arxiu				
		1	L’entitat de registre disposa de procediment d'arxiu.	OPT	No avaluat	
		2	Les targetes inutilitzades es garanteix la destrucció.	OPT	No avaluat	
		3	Existeix un protocol o política d'esborrat segur de dades confidencials en dispositius per tal d'evitar l'accés no autoritzat	OBL	No avaluat	

Resum d'avaluació

	Compleix	No compleix	No aplica
Controls obligatoris	0	0	0
Controls optatius	0	0	0

Avaluació:

APTA

0

PLA D'ACCIÓ	Id. Control	Descripció del control	Id. Acció	Acció	Responsable	Termini Resolució

OBSERVACIONS DE L'ENS	Primer.
	Segon.
	Tercer.

Barcelona, dia, mes any

Responsable del servei

Auditor Consorci AOC: