INFORME D'AUDITORIA

Entitat Auditada	
Althaia Xarxa Assistencial Universitària de Manresa Fundació Privada	
Nom del Sistema	
Sistema Informático Althaia	
Data de l'Informe	**Elaboració**
03/07/2025	Dani Fontanilles Arbones
Categoria del Sistema	BÀSICA

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

ÍNDEX

1. OBJECTIU

L'objectiu d'aquest informe és expressar una opinió sobre el grau de compliment i nivell de maduresa segons els requeriments establerts pel Reial Decret 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat (en endavant, ENS).

2. RESUM EXECUTIU

Althaia	
Abast	
Sistemes que suporten la tramitació dels serveis descrits en el Perfil de Compliment Específic de Requisits Essencials de Seguretat (CCN-STIC 890C).	
Categoria	BÀSICA
Resultat de l'Auditoria	FAVORABLE

El dictamen final de la present auditoria de certificació, d'acord amb l'abast descrit, és de Favorable.

En aquest sentit, s'han identificat tres Observacions:

- Op.exp.1 (Inventari d'actius): En l'inventari d'actius proporcionat per Althaia, no s'observa un responsable assignat per a cadascun dels actius de manera individualitzada en el mateix arxiu, únicament s'han assignat tres responsables de manera general per a tots ells. És per aquest fet que, cal que l'inventari identifiqui clarament qui és el responsable de cadascun dels actius per tal de tenir traçabilitat i control d'aquests en cas d'incident.

- Op.exp.2 (Configuració de seguretat): Althaia ha demostrat que compta amb una guia tècnica sobre l'aplicació, en la qual s'identifiquen l'arquitectura, la configuració de les IPs, les versions de Software i Sistema Operatiu permeses, entre d'altres. No obstant això, no s'ha identificat cap document en el qual es defineixin aspectes a nivell de la configuració de la seguretat, com pot ser una checklist de verificació de seguretat prèvia a la entrada en producció que inclogui aspectes com la retirada de comptes i contrasenyes per defecte, la configuració de permisos tenint en compte el principi de mínim privilegi, els algoritmes de xifrat, la configuració de l'inici de sessió segur, entre d'altres. Aquesta checklist pot seguir les guies de configuració segura del CCN o d'altres guies de referència en el seu defecte.

- Mp.si.5 (Esborrat i destrucció): Entre les evidències proporcionades, s'observa la verificació de la destrucció d'actius. No obstant això, el registre que retorna el proveïdor indica la quantitat de pes destruïda, sense incloure el detall dels actius concrets destruïts o esborrats.

Resum de les Troballes				
Conformitats	No Conf. Majors	No Conf. menors	Observacions	Total
32	0	0	3	35

3. ABAST

L'abast de la present auditoria es centra en:

Sistemes que suporten la tramitació dels serveis descrits en el Perfil de Compliment Específic de Requisits Essencials de Seguretat (CCN-STIC 890C).

4. TIPOLOGIA D'AUDITORIA

Es tracta d'una auditoria ordinària.	Si
Es tracta de la primera auditoria ordinària de certificació per al sistema.	Si
Es tracta d'una auditoria extraordinària amb motiu de modificacions substancials en el sistema d'informació, ampliació de l'abast o increment de categoria del sistema.	NO
Es tracta d'una auditoria extraordinària per a verificar la correcció de NCs, per exemple, per resultat desfavorable de l'auditoria ordinària.	NO

5. LIMITACIONS DETECTADES EN LA REALITZACIÓ DE L'AUDITORIA

No s'ha identificat cap limitació per a la realització de l'auditoria.

6. EQUIP AUDITOR

L'equip auditor ha estat format per:

Rol	Persona
Auditor Cap / Líder d'equip auditor	Dani Fontanilles Arbones
Auditor	Jorge Rioja Lopez
Auditor	Daniel Serra Bernad

7. IDIOMA

L'auditoria s'ha realitzat en català.

8. CATEGORITZACIÓ DEL SISTEMA

- Categoria del sistema d'acord amb les dimensions de seguretat valorades (ALT/MITJÀ/BAIX):

Confidencialitat	Integritat	Traçabilitat	Autenticitat	Disponibilitat
BAIX	BAIX	BAIX	BAIX	BAIX

Categoria final del sistema: **BÀSICA**

9. DETALL DE L'AUDITORIA

- Comentaris al grau de confiança en les revisions de la Direcció i auditories internes de l'auditat (si n'hi hagués):

  No hi han hagut comentaris al respecte.

- Resum de mesures auditades:

CONF	NC	OBS	TOTAL
32	—	3	35

- Detall de les no conformitats identificades:

NC. MAJOR	NC. MENOR	OBS	TOTAL
—	—	3	3

ANNEX A: TROBALLES IDENTIFICADES

Nº	Descripció
1	Inventari d'actius (Op.exp.1)
Troballes	
En l'inventari d'actius proporcionat per Althaia no s'observa un responsable assignat per a cadascun dels actius de manera individualitzada en el mateix arxiu, únicament s'han assignat tres responsables de manera general per a tots ells. És per aquest fet que, cal que l'inventari identifiqui clarament qui és el responsable de cadascun dels actius per tal de tenir traçabilitat i control d'aquests en cas d'incident.	

Nº	Descripció
2	Configuració de seguretat (Op.exp.2)
Troballes	
Althaia ha demostrat que compta amb una guia tècnica sobre l'aplicació, en la qual s'identifiquen l'arquitectura, la configuració de les IPs, les versions de Software i Sistema Operatiu permeses, entre d'altres. No obstant això, no s'ha identificat cap document en el qual es defineixin aspectes a nivell de la configuració de la seguretat, com pot ser una checklist de verificació de seguretat prèvia a la entrada en producció que inclogui aspectes com la retirada de comptes i contrasenyes per defecte, la configuració de permisos tenint en compte el principi de mínim privilegi, els algoritmes de xifrat, la configuració de l'inici de sessió segur, entre d'altres. Aquesta checklist pot seguir les guies de configuració segura del CCN o d'altres guies de referència en el seu defecte.	

Nº	Descripció
3	Esborrat i destrucció (Mp.si.5)
Troballes	
Entre les evidències proporcionades, s'observa la verificació de la destrucció d'actius. No obstant això, el registre que retorna el proveïdor indica la quantitat de pes destruïda, sense incloure el detall dels actius concrets destruïts o esborrats.	

ANNEX B: DOCUMENTACIÓ ADDICIONAL REVISADA

Per a la correcta execució de l'auditoria, a banda de la documentació que l'entitat auditada ha pujat al portal de governança del CCN, l'equip auditor ha sol·licitat la següent documentació per correu, amb la finalitat d'obtenir evidència suficient del compliment de les mesures:

Política de Seguretat (Org.1)

- Arxiu DubtesENS-1: Document amb evidència de la publicació/difusió de la política a la intranet.

Procés d'Autoritzacions (org.4)

- Arxiu DubtesENS-2.1: Document amb exemples d'autoritzacions.
- Arxiu DubtesENS-2.2: Document amb el llistat del personal autoritzat per a transportar suports d'informació.

Inventari d'Actius (op.exp.1)

- Arxiu DubtesENS-3: Document amb l'inventari d'actius indicant els responsables dels actius.

Configuració de Seguretat (Op.exp.2)

- Arxiu DubtesENS-4: Document amb el detall de la configuració per a la implantació d'un Sistema Operatiu Linux.

Formació i Conscienciació (mp.per.4)

- Arxiu DubtesENS-5: Exemples de formacions dutes a terme en aquest any.
- Arxiu DubtesENS-5-Formacio_Informe: Document amb el pla de formació i conscienciació per al 2025.
- Arxiu DubtesENS-5-Formacio_ListaAlumnes: Document amb el llistat de participants en la darrera acció formativa.

Esborrat i destrucció (mp.si.5)

- Arxius DubtesENS-7-1 i DubtesENS-7-2: Documents amb el detall en kg del material destruït/esborrat.

Dades personals (Mp.info.1)

- Arxiu DubtesENS-8-Anàlisis de Riscos Mentimeter octubre 2024: Document amb la darrera versió de l'Anàlisi de riscos de Protecció de Dades.

Protecció de la navegació web (mp.s.3)

- Arxiu DubtesENS-9: Document amb el detall de la configuració de la navegació web.

Signatura entitat auditada

Signatura Agència de Ciberseguretat de Catalunya

Daniel Fontanilles Arbonés - 47326470Z (TCAT)

Digitally signed by Daniel Fontanilles Arbonés - 47326470Z (TCAT)
Date: 2025.07.03 14:45:13 +02'00'

Correu de contacte:
oat@ciberseguretat.cat

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya