ALTAIR-SIGVI: Descobreix les teves vulnerabilitats

Antonio Rodriguez - antonio.rodriguez.g@escert.upc.edu

Equip de Seguretat per a la Coordinació d'Emergències en Xarxes Telemàtiques - inLAB FIB - UPC

Identificació, valoració i classificació de vulnerabilitats del software

- *Common Platform Enumeration*.
- Definits per *MITRE* (www.mitre.org).
- "Nom" estàndard que s'assigna a un producte software o sistema.
- Permet identificar-lo de manera única.

- *Common vulnerabilities and Exposures*.
- També definits per *MITRE*.
- Identificador que s'assigna a una vulnerabilitat.

- El *National Institute of Standards and Technology (NIST)* disposa d'una base de dades amb totes les vulnerabilitats que han aparegut des del 2002.
- Permet la consulta directa o bé la descàrrega de totes les dades en format *XML*.
- S'actualitza diàriament.

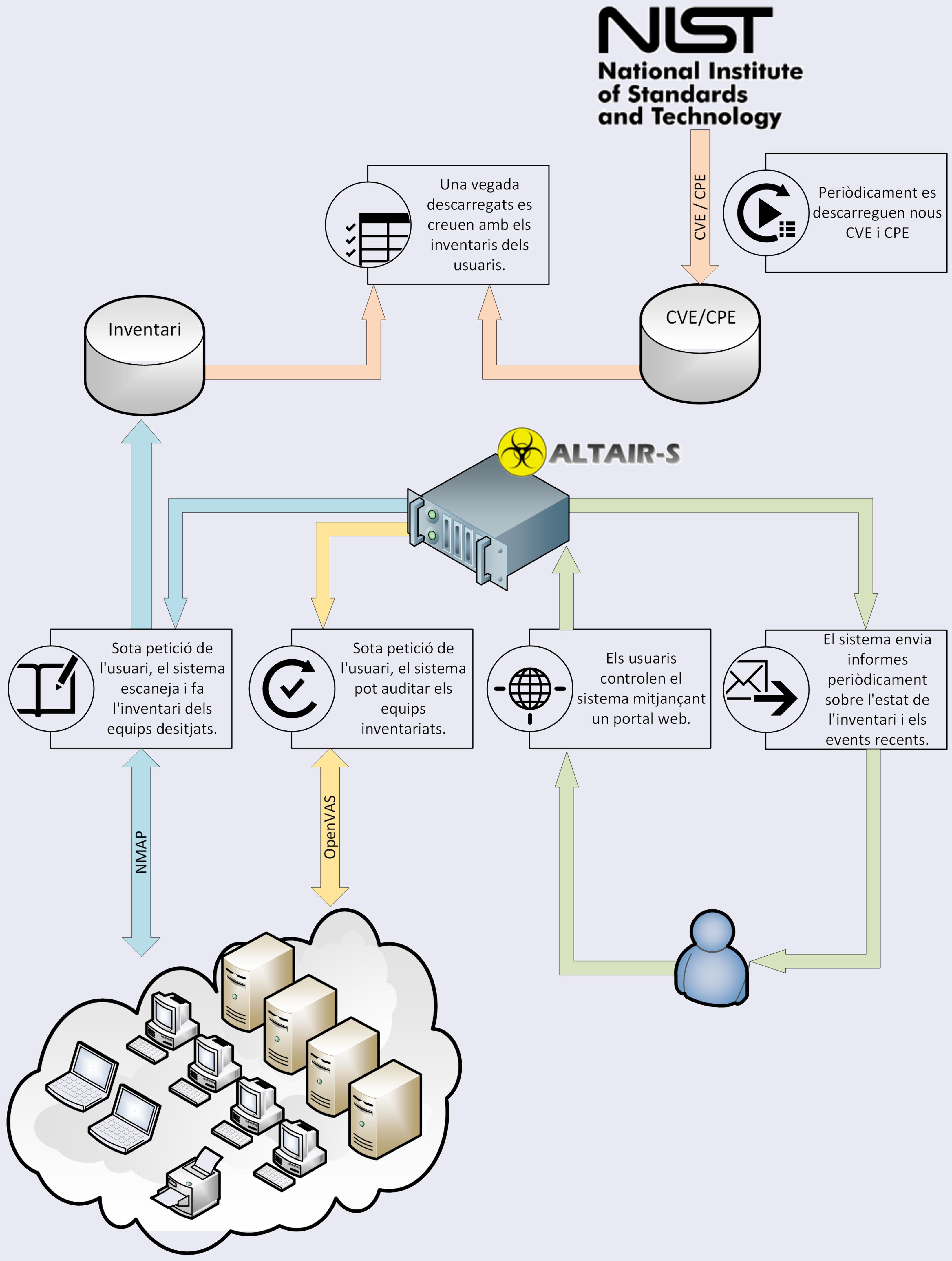
- *Common Vulnerability Scoring System*.
- Definit l'any 2004 pel conjunto d'equips de resposta a incidents i de seguretat del *Forum of Incident Response and Security Teams (FIRST)*.
- Pretén identificar i avaluar les vulnerabilitats en funció de la seva severitat.
- La NVD inclou *a posteriori* el CVSS de les vulnerabilitats.

OpenVAS

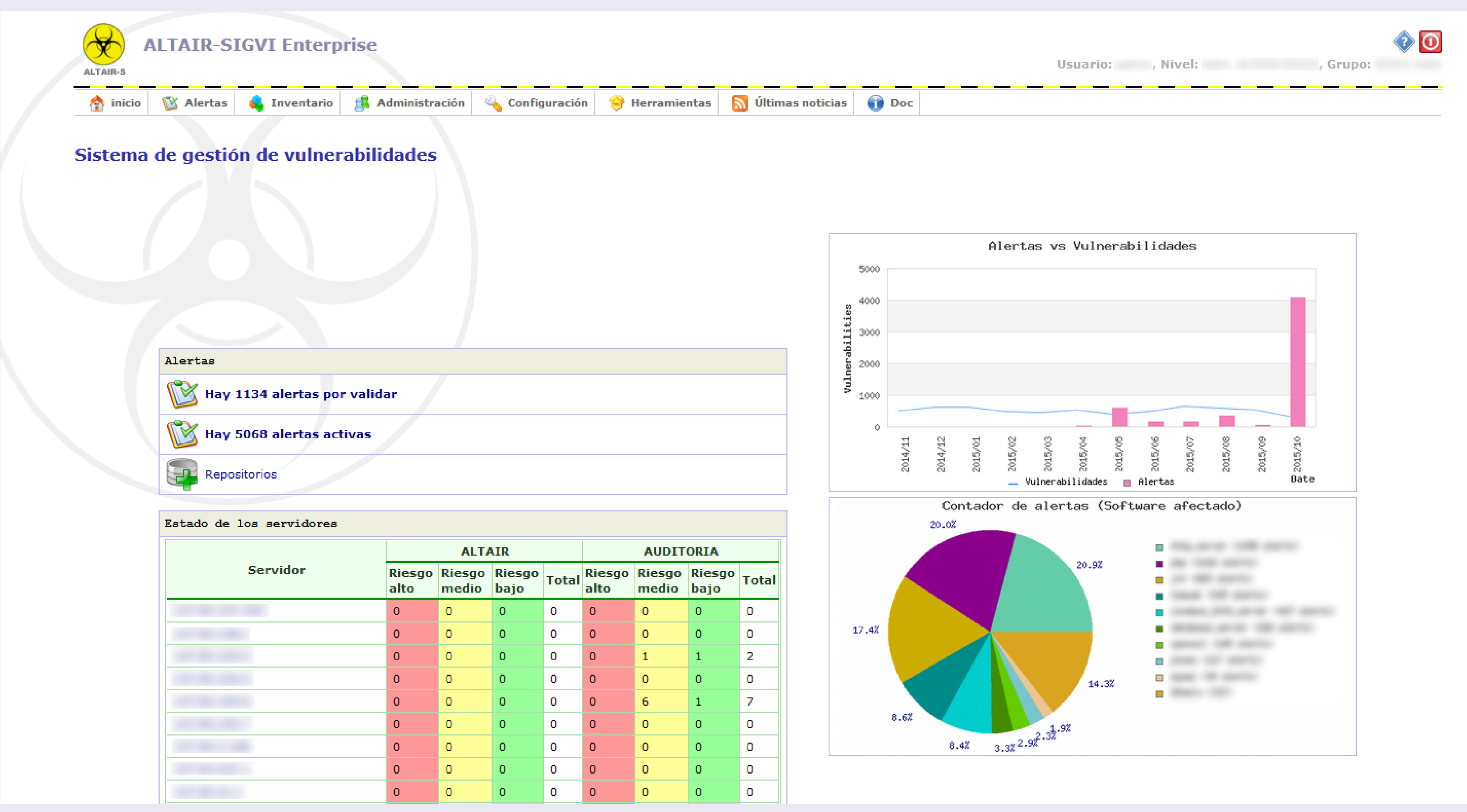
- Eina que permet escanejar una infraestructura, detectar els serveis que ofereix i automatitzar l'explotació de les seves vulnerabilitats.
- Integrada i preconfigurada a ALTAIR-SIGVI.
- En el cas d'auditoria no realitza explotació.

ALTAIR-SIGVI

- Característiques:
  - Inventari d'actius.
  - Auditoria de l'inventari.
  - Actualització diària de CVEs.
  - Avisos de les vulnerabilitats que afecten a l'inventari.



Interfície de l'eina ALTAIR-SIGVI



(a) Vista principal de l'aplicació.

Servidor	ALTAIR Riesgo alto	ALTAIR Riesgo medio	ALTAIR Riesgo bajo	ALTAIR Total	AUDITORIA Riesgo alto	AUDITORIA Riesgo medio	AUDITORIA Riesgo bajo	AUDITORIA Total
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	1	1	2
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	6	1	7
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0
[illegible]	0	0	0	0	0	0	0	0

(b) Relació de servidors amb vulnerabilitats detectades per ALTAIR-SIGVI o OpenVAS.