Cybersecurity Emergency Action Plan for Local Entities in Comunitat Valenciana, Spain

2022 TF-CSIRT Meeting
& FIRST Regional
Symposium Europe

March 2nd, 2022

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

Fondo Europeo de Desarrollo Regional

Una manera de hacer Europa

UNIÓN EUROPEA

CSIRT-CV is the Cybersecurity Centre of the Regional Government in Comunitat Valenciana, Spain

Its constituency includes Regional Government, other public administration, SMB and citizens

Established in 2007

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Virtual SOC definition and test pilot started in 2018

Precedents (II)

Suscríbete

Levante
EL MERCANTIL VALENCIANO
Contenido exclusivo para suscriptores digitales

SECCIONES Lv+ › COMUNITAT VALENCIANA CV SEMANAL VALÈNCIA FALLAS COMARCAS SUCESOS ECONOMÍA CULTURA OPINIÓN

Lv+ Suscríbete a todos los contenidos Premium de Levante por 0,13 euros al día

La Generalitat elabora un plan contra los ciberataques en los ayuntamientos

e.p. valència 28·05·21 | 04:00

La Generalitat ha elaborado un plan de choque de ciberseguridad para las entidades locales de la Comunitat Valenciana tras los recientes ciberataques que han sufrido diferentes Administraciones que han generado «un gran impacto en la prestación de

CONTENIDO PREMIUM PARA TI

COMUNITAT VALENCIANA

Puig abre la puerta a implantar el

Cybersecurity Emergency Action Plan

Emergency contract

For 1 year (july 2021 to june 2022)

Awarded to S2 Grupo (HQ in Valencia)

Objectives:

- Deploy tools to protect municipalities from main types of cyberattacks they are suffering (ransomware).
- Deploy, where necessary, sensors to detect risky situations as soon as possible.
- Prepare municipalities so that if a cyberattack is successful, impact on essential services is minimal.

Scope of action

5M+ citizens in 542 municipalities

Bigger municipalities have bigger risk

Type	Micro	Small	Medium	Big
Criteria (Hab)	< 1.000	< 5.000	< 20.000	> 20.000
Municipalities	224	161	92	65
Population	88.061	365.554	907.707	3.696.731

Actions: Micro

Type	Micro	Small	Medium	Big
Criteria (Hab)	< 1.000	< 5.000	< 20.000	> 20.000
Municipalities	224	161	92	65
Population	88.061	365.554	907.707	3.696.731

MicroCLAUDIA: All computers

Backups: Instructions to review and check

Training & Awareness: Generic

Actions: Small

Type	Micro	Small	Medium	Big
Criteria (Hab)	< 1.000	< 5.000	< 20.000	> 20.000
Municipalities	224	161	92	65
Population	88.061	365.554	907.707	3.696.731

MicroCLAUDIA: All computers

Backups: Procedure review

External Visibility: Quarterly review

Training & Awareness: Generic and specific for TI Managers

Actions: Medium

Type	Micro	Small	Medium	Big
Criteria (Hab)	< 1.000	< 5.000	< 20.000	> 20.000
Municipalities	224	161	92	65
Population	88.061	365.554	907.707	3.696.731

MicroCLAUDIA: All computers

Backups: Periodic review and verification

External Visibility: Quarterly analysis, w/ focus on remote administration services

GLORIA Agent: All computers

Training & Awareness: Generic and specific for TI Managers

Actions: Big

Type	Micro	Small	Medium	Big
Criteria (Hab)	< 1.000	< 5.000	< 20.000	> 20.000
Municipalities	224	161	92	65
Population	88.061	365.554	907.707	3.696.731

MicroCLAUDIA: All computers

Backups: Periodic review and verification

External Visibility: Continuous analysis, w/ focus on remote administration services

GLORIA Agent: All computers

CARMEN/CLAUDIA: Local sensor deployment on 15 bigger ones

Online Reputation: Credential leak service

Training & Awareness: Generic and specific for TI Managers

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

S2 GRUPO
CERT

CCN-CERT
centro criptológico nacional

Red
Nacional de
SOC

Red Nacional de SOC

CSIRT.es
(53)

(13)

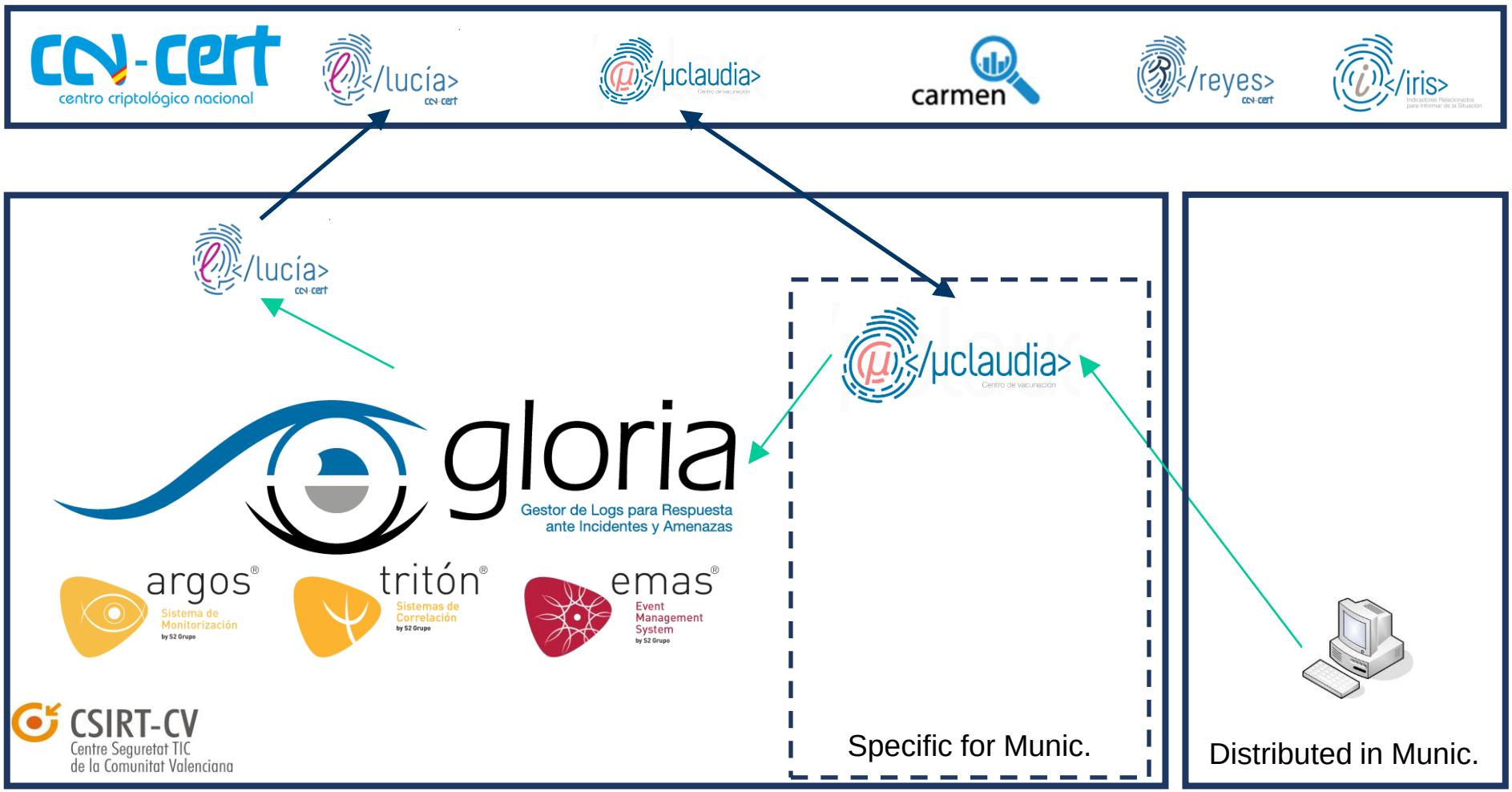
(6)

(34)

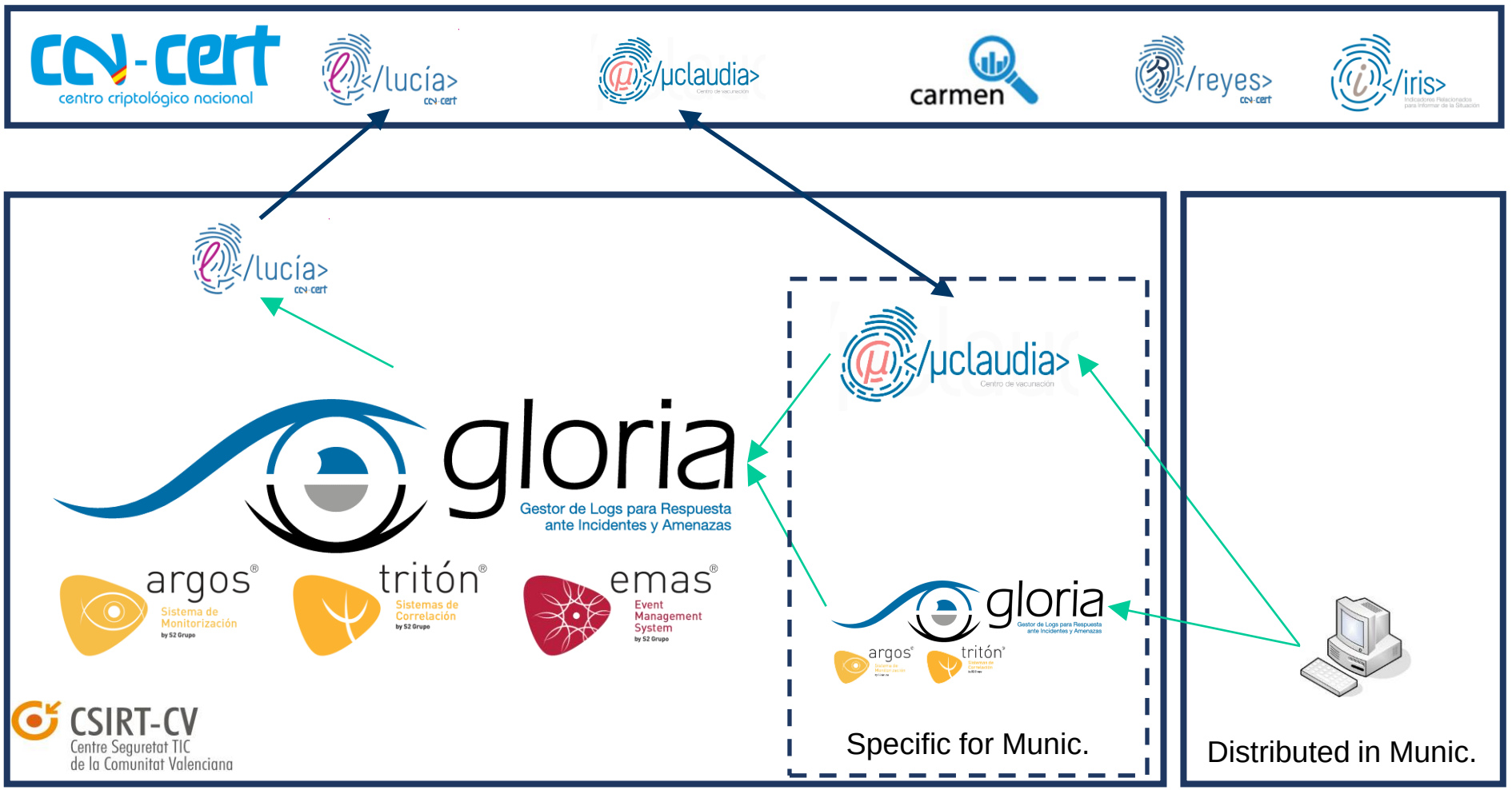
Red Nacional de SOC

Tooling Challenges

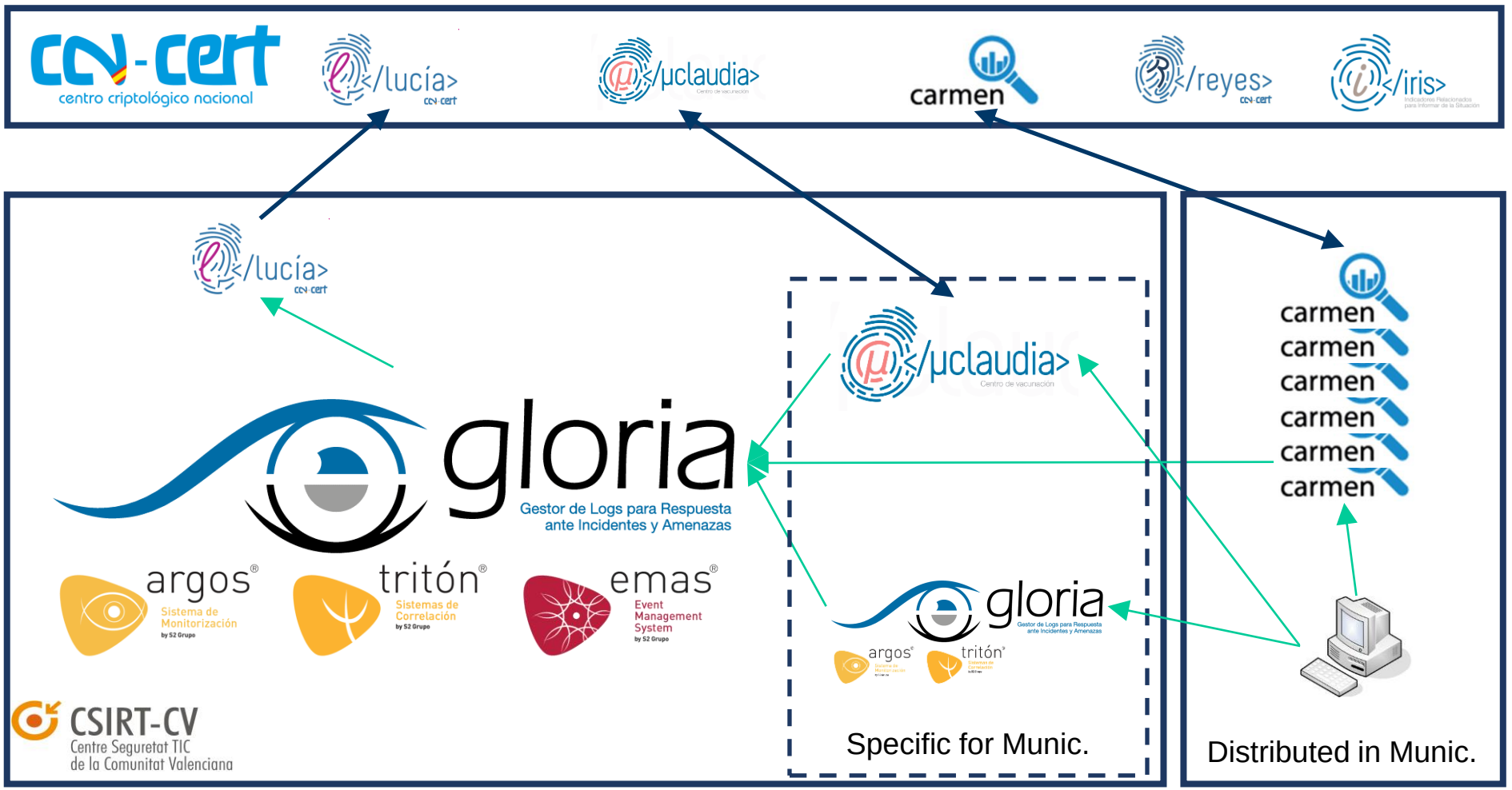
Tooling Challenges



Tooling Challenges



Tooling Challenges



Work Plan

July 2021

Design of procedures

Analysis of architecture

Training of the initial team

HW buy orders placed

August 2021

Initial contact with munic.

MicroCLAUDIA installed

Analysis of GLORIA convergent architecture

Initial set of KPI created

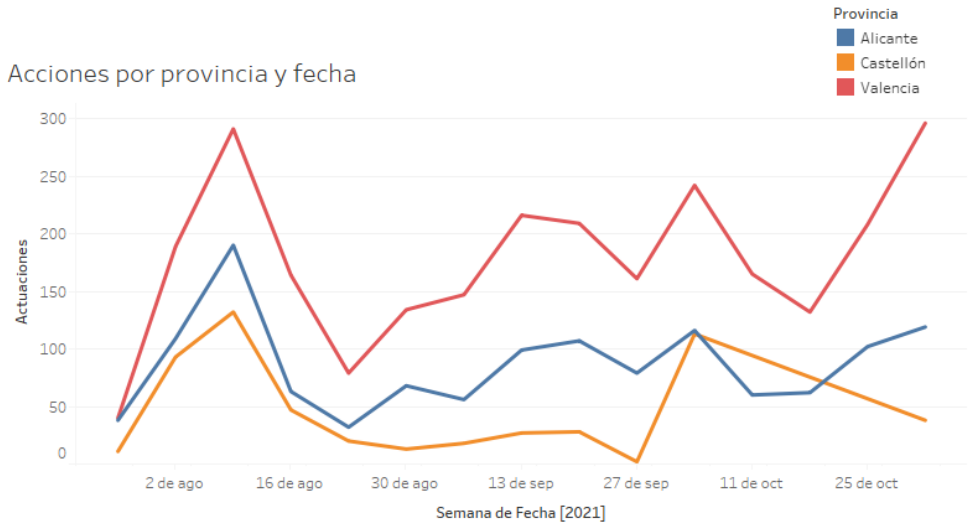
Número de Actuaciones realizadas

Provincia	Tamaño					
	Grandes	Medianos	Pequeños	Micro	Mancomunidad	Total general
Alicante	204	338	311	349	98	1.300
Castellón	31	81	105	319	6	542
Valencia	266	457	1.103	772	75	2.673
Total gener..	501	876	1.519	1.440	179	4.515

Se incluyen llamadas telefónicas y envio de correos electrónicos de CONTACTO, pero no el resto de comunicaciones dirigidas a prestar soporte a los organismos

Numero de Organismos

Provincia	Tamaño					
	Grandes	Medianos	Pequeños	Micro	Mancomunid..	Total general
Alicante	26	32	32	53	15	158
Castellón	8	12	25	91	7	143
Valencia	31	47	107	85	13	283
Total general	65	91	164	229	35	584



Total Actuaciones
4.515

Llamadas Telefonicas
3.408

Correos electrónicos
1.077

Organismos contactados
544

Organismos sin Contactar
40

Consideramos como contactados todos los organismos de Castellon gestionados por la diputación tras contactar con la misma

Work Plan (II)

September 2021

GLORIA installed and configured

CARMEN Machines received and preconfiguration started

New service Password Leaks added to pool of services

IT Questionnaire sent

Online Reputation service setup

November 2021

First CARMEN deployed to municipality

GLORIA configuration and use cases finished

September 2021

GLORIA installed

CARMEN Machin
preconfiguratio

New service Pass
added to pool

IT Questionnaire s

Online Reputation

deployed to

uration and use
ed

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

Plan de choque en Ciberseguridad para las EELL Valencianas

El Plan de choque en Ciberseguridad para entidades locales está siendo **diseñado para ayudar a los Ayuntamientos a sentar un mínimo común y contar con unas bases sólidas en materia de ciberseguridad** que permitan no solo el cumplimiento del Esquema Nacional de Seguridad, ENS, sino también minimizar en la medida de lo posible el impacto que un ciberincidente pueda tener en la organización.

El presente formulario pretende recopilar información de los medios tecnológicos de que dispone el Ayuntamiento, para poder priorizar la ejecución de acciones que aporten una mayor mejora en términos globales del nivel de madurez en ciberseguridad. En ningún momento se pretende controlar el licenciamiento del software utilizado, ni acceder a ningún dato que pudiera estar alojado en cualquiera de los sistemas de información que la entidad utilice.

Formulario de recogida de datos inicial

Datos de contacto:

Ayuntamiento	
Datos persona de contacto / responsable informática	
Nombre y apellidos	
Teléfono	
Correo electrónico	
Fecha cumplimentación encuesta	

Información global del ayuntamiento:

Número de líneas de datos (Internet) diferentes y función:	___ Ayuntamiento ___ Servicios sociales ___ Policía ___ Biblioteca ___ Casa de Cultura / Casa de Juventud ___ Otros, indicar cual(es): _____
Número de estaciones de trabajo existentes:	
Sistema operativo principal de las estaciones de trabajo:	___ Anterior a Windows XP, Vista ___ Windows XP, Vista ___ Windows 7, 8, 8.1 ___ Windows 10 ___ Cualquier versión de Linux ___ Otros, indicar cual(es): _____
Número de servidores existentes:	
Sistema operativo de los servidores:	Anterior a Windows Server 2008

Work Plan (III)

January 2022

GLORIA Agent deployment started

70% MicroCLAUDIA deployed

March 2022

Finished definition of training paths for each type of munic.

Online reputation and SIEM services growth as more agents/devices deployed

How is it going so far? MicroCLAUDIA deployment

Total Organismos:584

Alicante	Castellón	Valencia
27,05%	24,49%	48,46%

Organismos Por provincia y Tamaño

Provincia	Grandes	Medianos	Pequeños	Micro	Mancomunid..	Total general
Alicante	26	32	32	53	15	**158**
Castellón	8	12	25	91	7	**143**
Valencia	31	47	107	85	13	**283**
Total general	**65**	**91**	**164**	**229**	**35**	**584**

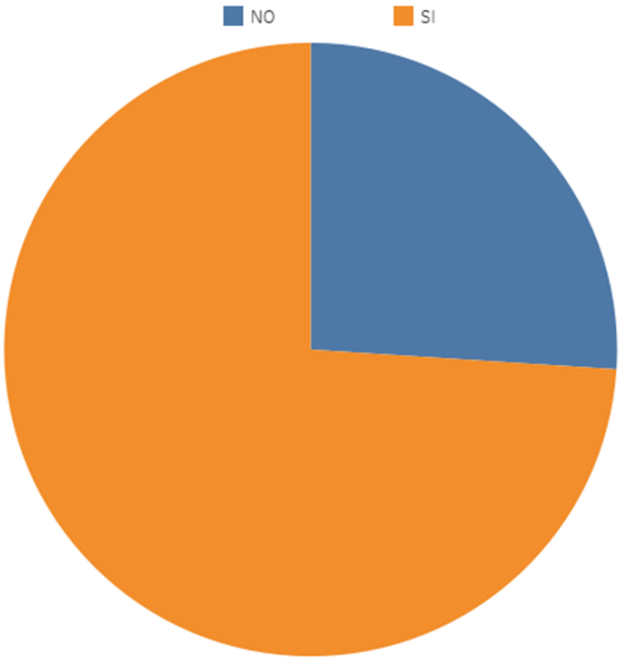
Organismos por consola y provincia

Consola	Alicante	Castellón	Valencia	Total general
Alta en Csirt	129	17	207	353
Alta en CCN	29	16	76	121
Alta en CCN (DipCastellon)		110		110
Total general	**158**	**143**	**283**	**584**

Organismos en despliegue

En despliegue	Valencia	Alicante	Castellón	Total general
NO	68	77	11	**156**
SI	215	81	132	**428**
Total general	**283**	**158**	**143**	**584**

How is it going so far? MicroCLAUDIA deployment per region

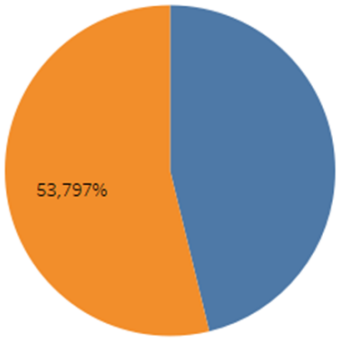


En despliegue	%	Total
NO	26,03%	152,0
SI	73,97%	432,0

ALICANTE

NO
SI

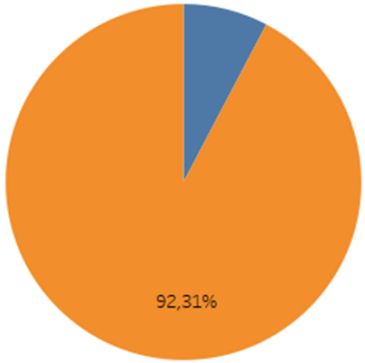
En despliegue	%	Total
NO	46,20%	73,00
SI	53,80%	85,00



CASTELLON

NO
SI

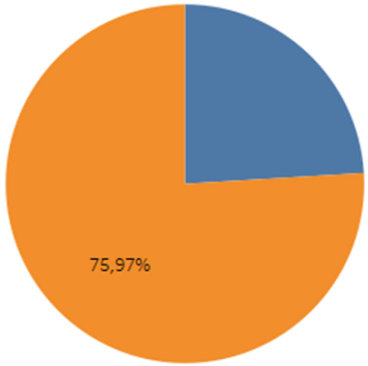
En despliegue	%	Total
NO	7,69%	11,0
SI	92,31%	132,0



VALENCIA

NO
SI

En despliegue	%	Total
NO	24,03%	68,0
SI	75,97%	215,0



How is it going so far? MicroCLAUDIA deployment per region (II)

Totals	Alacant	Castelló	Valencia
Total municipalities	158	143	283
Deployment in process	85 (53,80%)	132 (92,31%)	215 (75,97%)
Computers deployed	6201	2145	10796

With depth information	Alacant	Castelló	Valencia
Municipalities w/ depth	94 (59,49%)	139 (97,20%)	222 (78,45%)
Computers informed	11199	3776	17917
Computers deployed	5826	2145	10522
KPI Depth Achieved	52,02%	56,81%	58,73%

How is it going so far? Password Leaks

Numero de Organismos	Dominios dados de alta
584	403

Informes Recibidos	Cuentas reportadas con incidencias	Incidencias individuales reportadas
9	4.521	8.942

Notificación de alertas a organismos.

Organismos Notificados	Notificaciones realizadas	Cuentas notificadas a los organismos
224	421	4.521 (100%)

cada notificación lleva múltiples cuentas siempre que sean del mismo organismo

How is it going so far? Summary

	MicroCLAUDIA	Backups	External Visibility	GLORIA Agent	CARMEN	Online Reputation	Password Leaks
Applies to	584	584	319	141	15	65	584
Applied	446	534	84	6	8	64	466
In process	0	0	115	8	2	0	0
Not applied	138	50	120	128	5	1	118

Conclusions

Benefits for Municipalities

Improvement of cybersecurity baseline

Creation of trusted network of contacts

Centralised incident notification

Perimetral assessment

Better backup procedures

Better ENS coverage

Starting point to ask for Europe's recovery funds

Benefits for CSIRT-CV

Unified management

Capacities improvement

Independent input channel

Synergies

¡ Thank you very much !

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

C/ Ramiro de Maeztu Nº9 46022 Valencia, España
Teléfono: +34-96-398-5300 Email: csirtcv@gva.es

www.csirtcv.gva.es | csirtcv@gva.es
facebook.com/csirtcv | twitter.com/csirtcv