Un centro pionero en Ciberseguridad para todos los valencianos

GENERALITAT VALENCIANA

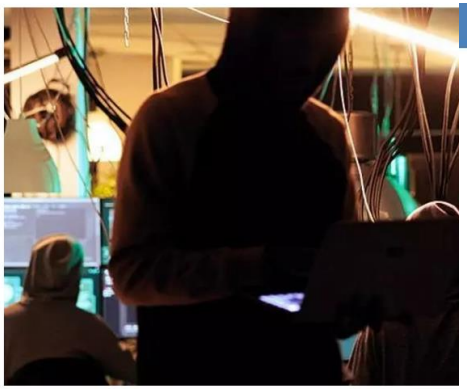
CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

¿A qué nos enfrentamos?

Levante
EL MERCANTIL VALENCIANO

La Generalitat evita 1.200 ciberataques a organismos y empresas en solo 5 meses

- El Centro de Seguridad TIC de la Comunitat Valenciana detecta un aumento de los incidentes promovidos por grupos prorrusos a los portales de diferentes Administraciones públicas y entidades
- El año pasado se registraron 1.788 casos



La Generalitat evita 1.200 ciberataques a organismos y empresas en solo 5 meses / ED

Escudodigital

Home / Ciberseguridad /

CIBERSEGURIDAD

Oleada de ciberataques contra España de los hackers rusos NoName: afectan incluso a la Casa Real

En los últimos tres días, los piratas han reivindicado más de una quincena de ofensivas contra instituciones y entidades españolas.

Silvia Montes Redactora especializada en Seguridad y Tecnología. 21 de julio de 2023 (14:11 CET) Actualizado: 24 de julio de 2023 (11:20 CET) Guardar

valenciaplaza

El grupo de 'hackers' prorrusos NoName057(16) 'tumba' la 'web' de Les Corts

VP Confidencial

COMPARTIR
TWEET
LINKEDIN
MENEAME

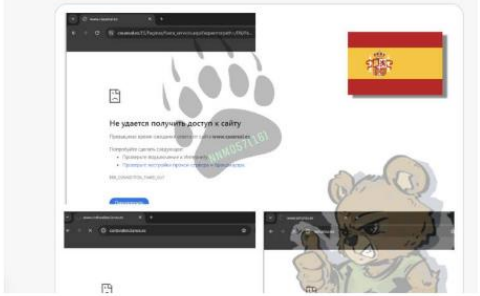
NoName057(16) @Noname05716 · 6min

We continuing attacks on Spanish internet infrastructure and putting down Russophobic government websites 😈 t.me/noname05716eng...

❌The royal family
check-host.net/check-report/1...

❌The website of the Valencian Regional Parliament
check-host.net/check-report/1...

❌Official website of the
Mostrar más



¿A qué nos enfrentamos?

Los ataques de ransomware se incrementan u 72 por ciento en España en apenas un año

Nuestro país ocupa el octavo puesto dentro del top 10 de países más atacados del mundo, y sufre un crecimiento muy superior a la media mundial, que es del 18 por ciento.

Zscaler, empresa líder en se
que analiza el panorama de
detalla las últimas tendenci

< VIVIRENELCHE.COM @ NOTICIAS PRENSA DIGITAL >

NOTICIAS DE PRENSA ELCHE Y COMARCA

INICIO | EDITORIAL | AGENDA | PRENSA | ADMINISTRACIÓN | EMPRESAS | EMPLEO | EDUCACIÓN | CULTURA | OCIO | SERVI
NATURALEZA | DEPORTES | CIENCIA | TÉCNOLOGÍA | AUDIOVISUALES | SUCESOS | COLUMNA LECTOR | CONTRATACION | CONTAC

Elche se enfrenta al ciberataque más grave en la historia del Ayuntamiento con servicios paralizados y respuesta manual

DEBATES: Ayuntamiento De Elche Ciberataque Elche Ciberseguridad Local Omac Elche
Pablo Ruz Alcalde Protección De Datos Ransomware Elche Servicios Municipales Elche

Seguridad

La Generalitat combate 100 millones de alertas y hasta diez ciberataques al día

Los ciberincidentes registrados en los organismos y servicios públicos dependientes del Consell ascienden a 3.512 el año pasado frente a los 1.504 de 2023nEl 'fraude' es la amenaza más común

Misión y objetivo

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

- Iniciativa pionera en España
- Nace en 2007: 1er CSIRT de ámbito autonómico en España
- Ámbito de actuación: Comunidad Valencia:
  - AAPP
  - Ciudadanos
  - Empresas

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

GENERALITAT VALENCIANA

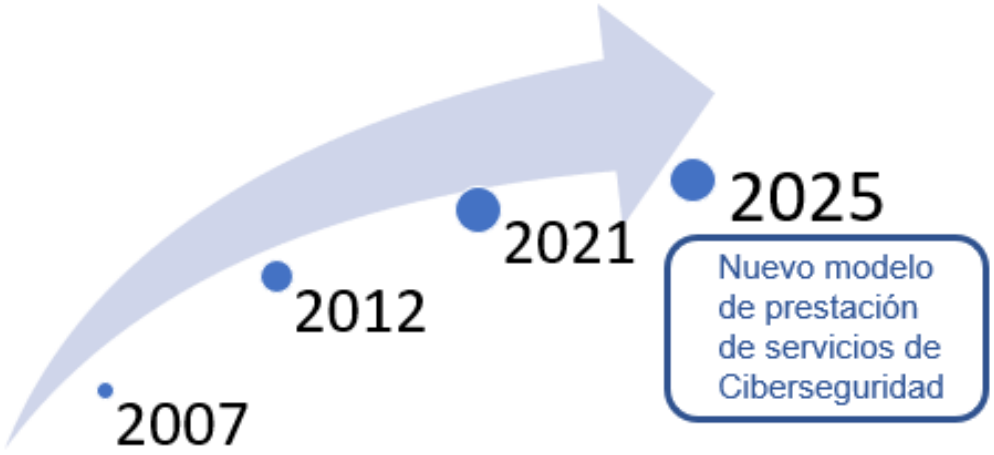
UNIÓ EUROPEA
UNIÓN EUROPEA

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Misión: convertirse en el **centro de referencia en seguridad** de la información y las nuevas tecnologías dentro de la Comunitat Valenciana, sirviendo de apoyo a los colectivos de su ámbito en base a los servicios ofrecidos.

Objetivo: contribuir a la **mejora de la seguridad de los sistemas de información dentro de su ámbito**, así como **promover una cultura de seguridad y buenas prácticas** en el uso de las nuevas tecnologías de forma que se minimicen los incidentes de seguridad y permita **afrontar de forma activa las nuevas amenazas** que pusieran surgir.

Origen y evolución



Visión Estratégica de la Ciberseguridad

GEN Digital 2025

- **CIBERSEGURIDAD:** Objetivo estratégico
- Impacto en la Sociedad: desarrollar y promocionar un **ecosistema digital seguro en la Comunitat**

> **LE 1.1 La ciberseguridad como pilar fundamental de la Administración y para el desarrollo de la cultura de seguridad**
>
> Promover la ciberseguridad como pilar fundamental de la infraestructura digital de la Administración y como facilitadora del desarrollo de la sociedad digital, permitiendo a la ciudadanía y a las empresas relacionarse entre ellas y con la Administración con confianza.

- Apoyar el **fortalecimiento y la mejora de la resiliencia** de las tecnologías como elemento necesario para su transformación digital, en colaboración con las **empresas**, el **sector público instrumental** y el resto **de Administraciones de la Comunitat Valenciana**.

Cuatro grandes objetivos estratégicos, alineados con la Misión del Centro

La misión de CSIRT–CV es convertirse en el centro de **referencia en ciberseguridad** de la Comunitat Valenciana, sirviendo de apoyo a los colectivos de su ámbito en base a los servicios ofrecidos.

Colaboración

CSIRT.es
(53)

(13)

(6)

(34)

Red Nacional de SOC

TF-CSIRT
Trusted Introducer

FIRST
Improving Security Together

¿A quiénes presta servicio CSIRT-CV?

5,2 Millones Ciudadanos

600.000 Usuarios educativos

35.000 Usuarios instit. sanitarias

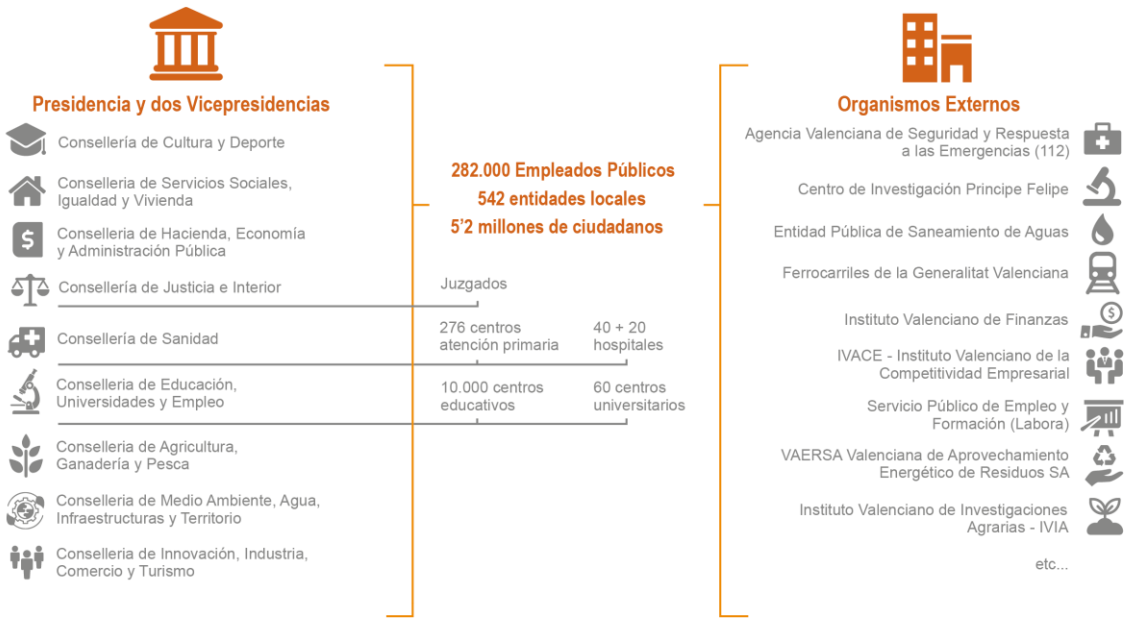
30.000 Usuarios Admon. Consell

10 Consellerias (+Presidencia y VPresidencia)

Entes SCC y Organismos Públicos

61 Entes SPI

584 Entidades locales



Incidentes gestionados

Balance de Actividad 2024

+3.500 incidentes gestionados

un 96% más que en 2023

es

Alcance

61 Entes de GVA y SPI

5.2 M de ciudadanos de la Comunitat Valenciana

550 Entidades Locales

282.000 empleados públicos

1 Presidencia

2 Vicepresidencias

8 Consellerias

Balance de Actividad 2024

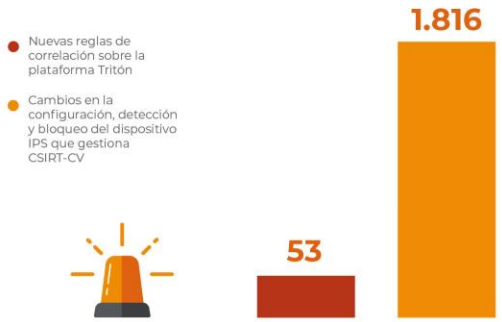
Servicios más destacados

Servicios de prevención

Conjunto de prácticas, tecnologías y medidas diseñadas para prevenir los sistemas informáticos de la Generalitat Valenciana contra amenazas y ataques cibernéticos ofrecidos por CSIRT-CV.

Servicios de detección

Este servicio pretende la detección temprana de intrusiones, la implementación de mecanismos de distracción para atacantes y análisis de tendencias y mejora de los mecanismos defensivos, entre otros.



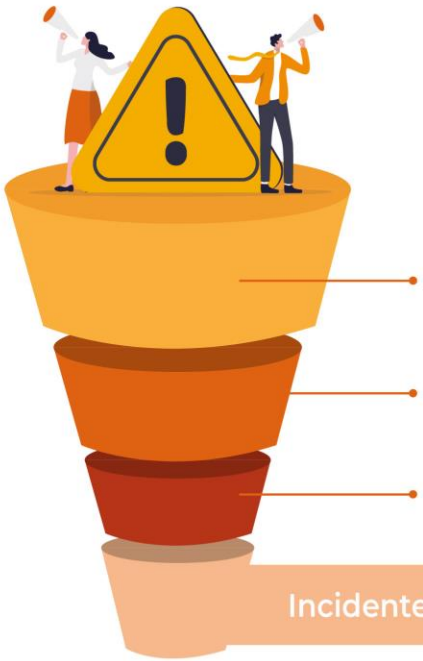
Servicios de respuesta

CSIRT-CV proporciona una solución integral a cualquier incidente de seguridad producido como: phishing, compromiso por malware, suplantación de identidad, robo de contraseñas, secuestro de información, etc.

CSIRT-CV en cifras

Balance de Actividad 2024

Alertas



Eventos generados en los dispositivos de seguridad integrados en CSIRT-CV previos a su correlación

36.400 M alertas anuales

100 M alertas diarias

1.150 alertas por segundo

Incidentes gestionados

3.512 incidentes gestionados
(un 96% más que en 2023)

Categorías de incidentes

1.951 fraudes online (55% del total)

Phishing

Suplantación

- **422** Intrusión (12%)
- **345** Contenido dañino (10%)
- **249** Vulnerable (7%)
- **184** Disponibilidad
- **183** Compromiso de la Información (18%)
- **102** Gestión de incidente
- **32** Contenido abusivo
- **25** Intento de Intrusión
- **11** Otros
- **8** Obtención de información

Balance de Actividad 2024

Formación y Concienciación

+9.700 personas formadas en 2024
39 sesiones
32 cursos online

1- Centros educativos

Desde 2017
+500 centros educativos
+46.000 personas formadas

En 2024:

+3.370 menores
+310 docentes
4 sesiones en otros entes
35 Jornadas de Concienciación sobre Ciberseguridad
+380 familiares del alumnado

2- Plataforma eFormación

En 2024: **+5.500** matrículas (⬆10%)
32 cursos

+25.000 personas matriculadas en cursos del CSIRT-CV desde 2009

Colectivos identificados

- Ciudadanos
  - Menores y jóvenes 
  - Violencia género 
  - Colectivos profesionales 
  - Personas mayores 
- Personal AAPP
  - Técnicos 
  - Altos Cargos 
  - Funcionarios 
- Empresas
  - Directivos 
  - CISOS 

PYME y SPI

Para la mejora e incremento del nivel de ciberseguridad de las organizaciones, se requiere de la implementación de medidas técnicas, el desarrollo de normativas y concienciar e implicar a las personas para que el factor humano se convierta en un pilar fundamental de la ciberseguridad.

Para ello, desde CSIRT-CV se ofrecen herramientas y servicios para incrementar el nivel de ciberseguridad de las organizaciones:

Cursos

Formación online dirigida a CEOS y técnicos de empresas.

Objetivos: conocer los nuevos riesgos y asumir "buenas prácticas" para mejorar la ciberseguridad.

Módulos Interactivos

Videos interactivos dirigidos a empleados.

Objetivos: concienciar en temas de ciberseguridad de una manera interactiva, donde el empleado debe ir respondiendo a las preguntas para poder avanzar los contenidos.

evalua'T

Herramienta de autoevaluación.

Objetivos: conocer los riesgos en ciberseguridad de la organización y obtener planes de mejora a implantar para aumentar el nivel de seguridad de la empresa.

Entidades locales de la Comunitat Valenciana

Plan de Choque de Ciberseguridad para Entidades Locales (EELL) - Retos y objetivos

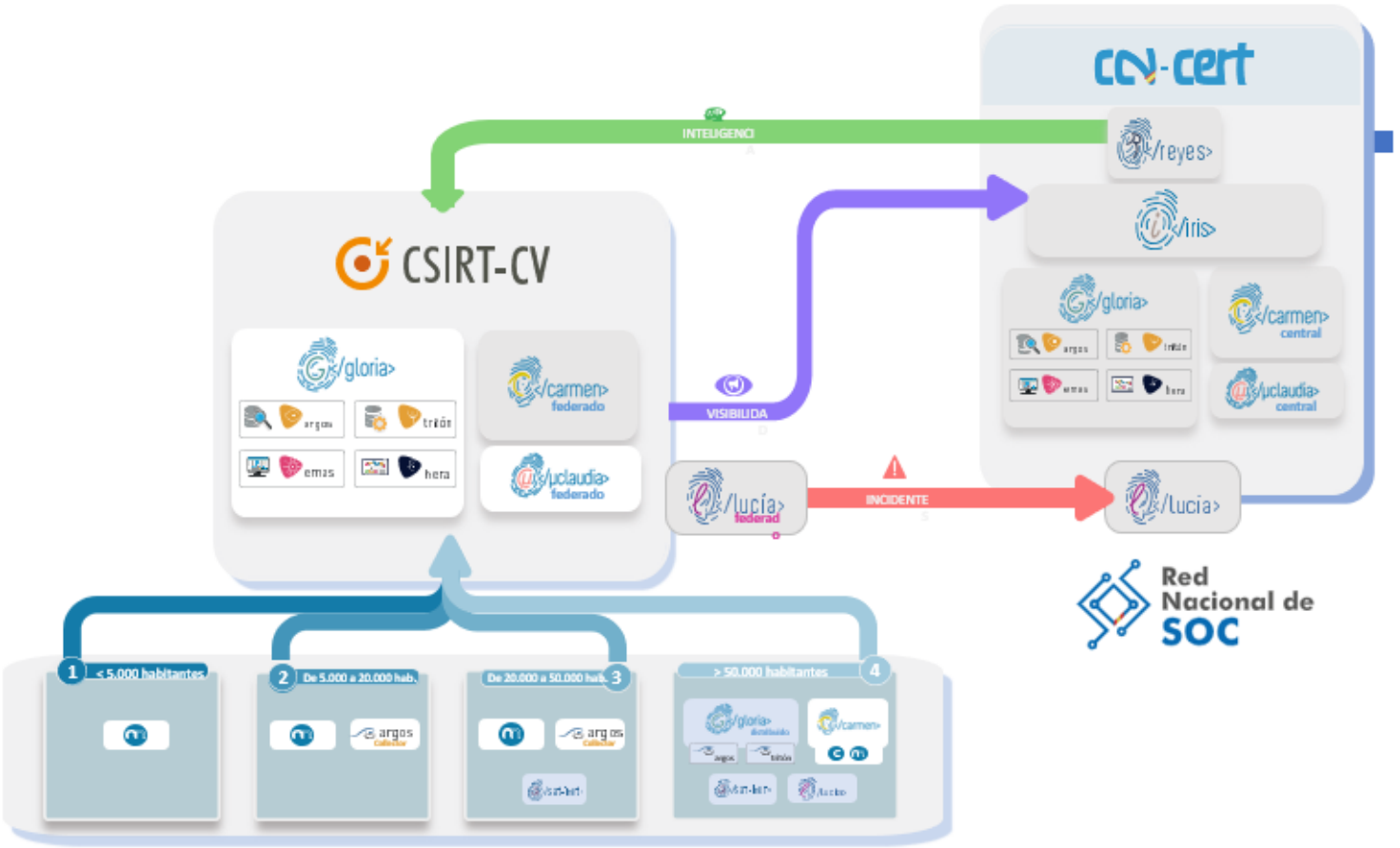
- Se lanzó con **carácter urgente** en 2021 para proteger a las **584 EELL** de la Comunitat Valenciana para frente a ciber amenazas.
- **Proporcionar gratuitamente a las EELL** de la Comunitat soluciones de **ciberseguridad y vigilancia** ante el creciente número de ciberataques (principalmente de ransomware) dirigidos contra ellas.
- Las EELL **carecen de los recursos necesarios** para abordar correctamente su ciberseguridad (escaso personal informático, diversidad de tareas, falta de especialización, etc.), **lo que las convierte en objetivos "blandos"**.
- Desplegar herramientas de protección para los municipios frente a ciberataques.
- Desafío que planteaba la **heterogeneidad y el elevado número de interlocutores** en las EELL y el **desconocimiento de la tecnología** de sus propios sistemas de información.

✓ Implementar **sondas para la detección** temprana de riesgos.

✓ **Reducir al mínimo el impacto** en los servicios esenciales de los ciberataques perpetrados con éxito.

✓ Ofrecer **soporte técnico y capacitación** en ciberseguridad y **asistencia en el cumplimiento** de las obligaciones derivadas del Esquema Nacional de Seguridad.

Modelo CCN-CERT Federado



Delega en la Comunidad Valenciana los servicios de Seguridad que presta el CCN-CERT, mediante el despliegue en **CSIRT-CV** de un nodo con herramientas **interconectadas con el propio CCN-CERT.**

Acciones sobre la industria conectada en la Comunitat Valenciana

- El proyecto se diseña a partir de la información obtenida en el I Estudio del Estado de la Ciberseguridad Industrial en la Comunidad Valenciana realizado en 2023 en el que se detectan las necesidades de la industria.
- El **Centro de Innovación y Competencia en Ciberseguridad** persigue convertir a la Comunitat Valenciana en un **referente en ciberseguridad industrial en España y la Unión Europea**
- Algunas de sus acciones más inmediatas relacionadas con la industria conectada son:
  - ✓ La elaboración de **nuevos entornos y demostradores** relacionados con la ciberseguridad industrial
  - ✓ Celebración de **jornadas de formación** dirigidas a estudiantes y profesionales relacionados con el sector de la ciberseguridad industrial mediante la demostración de posibles ciberataques a través de entornos portátiles
  - ✓ Celebración de la **II Jornada de Ciberseguridad Industrial** (19 de mayo de 2026)
  - ✓ **Estudios específicos** sobre OT (Tecnologías de la Operación)
  - ✓ **Jornadas de difusión** de los entornos en las instalaciones de CSIRT-CV

Planteamiento nuevo contrato: Objetivos estratégicos

¿Qué perseguimos?

- **Mejorar la ciberseguridad de la Administración Pública**: Se busca proteger las plataformas y sistemas de la Generalitat y las entidades locales (EELL), como se refleja en el Plan de Choque de Ciberseguridad para las Entidades Locales y las iniciativas del marco "GEN Digital 2025".
- **Proteger los servicios esenciales**: El objetivo principal es minimizar el impacto de los ciberataques, especialmente el ransomware, en los servicios públicos esenciales de los municipios y de la Administración en general.
- **Capacitar y concienciar**: Se desarrollan programas de formación para empleados públicos y cargos electos, así como para los ciudadanos y pequeñas empresas, con el fin de crear una Cultura de Ciberseguridad y dotarles de las herramientas necesarias para identificar riesgos, como fraudes y estafas y minimizar lo máximo posibles los efectos.

Planteamiento nuevo contrato: Objetivos estratégicos

Objetivos estratégicos de la Generalitat

- **Adoptar un enfoque proactivo**: Se incluyen acciones como el despliegue de sondas de detección de riesgos y la realización de auditorías y pentesting de plataformas para identificar vulnerabilidades y prevenir incidentes.
- **Impulsar la digitalización segura**: La estrategia de ciberseguridad es fundamental para la transformación digital de la Generalitat, asegurando que la implementación de sistemas e infraestructuras TIC se haga de forma segura y eficiente.
- **Fomentar la colaboración**: Se colabora con organismos como el CCN-CERT a nivel nacional, además de a nivel internacional, y se interactúa con las entidades locales para compartir conocimiento y mejores prácticas en ciberseguridad.

Aspectos clave del contexto de ciberamenazas

- **Cambio geopolítico y social**: Las tensiones internacionales y conflictos políticos
- **Aumento de la sofisticación**: Los ataques cibernéticos se han vuelto más complejos y dirigidos.
- **Amenazas emergentes**: Nuevas amenazas, como el ransomware, el cryptojacking y los ataques a la cadena de suministro, uso de la IA en los ciberataques
- **Escasez de habilidades**: La falta de profesionales capacitados.

Características principales

- **Aglutina los servicios de dos contratos** anteriores: el de CSIRT-CV y el Plan de Choque para las Entidades Locales, con un total de 47 profesionales y aumenta los recursos.
- **Aumento las capacidades** de defensa, de concienciación y de gestión de la Ciberseguridad del centro.
- **Incorpora una gestión de la directa** de las alertas de los grandes ayuntamientos de la Comunidad Valenciana y la gestión del plan de choque para la Entidades Locales.
- Con la **iniciativa RETECH** crea al Centro de Innovación y Competencia en Ciberseguridad de la Comunidad Valenciana, centrado en el tejido industrial y en la concienciación.
- Incluye **63 profesionales de la ciberseguridad**, **sede nueva, nuevos laboratorios y espacios formativos.**
- Presupuesto de licitación: 54.109.898,84 € (IVA incl.) por 4 años, de los cuales 12.414.773,25 € son RETECH.
- Presupuesto anual de los dos contratos a los que sustituye: 3.210.544,29€ (IVA incl.) anuales.

CSIRT-CV

Centre Seguretat TIC
de la Comunitat Valenciana

C/ Joan Reglà, 6 46010 Valencia (España)
Teléfono: +34-96-398-5300 Email: csirtcv@gva.es

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