Premios SOCINFO Digital: Ciberseguridad AAPP

TITULO: “Plan de Ciberseguridad para las 584 Entidades Locales de la Comunidad Valenciana”

Candidatura GENERICA (al recaer en varias de las categorías especificadas)

Descripción del proyecto

Introducción

Como consecuencia del creciente número de ciberataques, principalmente de ransomware, que estaban sufriendo los municipios de la Comunitat Valenciana, la Generalitat adoptó hace dos años el compromiso de elaborar un Plan de Choque de Ciberseguridad para las Entidades Locales (EELL), adaptado a las características y riesgos de los municipios de la Comunitat, con el fin de desarrollar medidas de protección, mejora de la seguridad, implantación y soporte técnico, además de ayudar a dichas entidades en el cumplimiento de las obligaciones derivadas del Esquema Nacional de Seguridad (ENS).

El reto consistía en proporcionar gratuitamente, a las 584 entidades locales (EELL) de la Comunitat Valenciana, soluciones de ciberseguridad y vigilancia frente a los ciberataques. 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”, fácilmente atacables. Con la gestión óptima de los recursos ofrecidos mediante el Plan de Ciberseguridad para las Entidades Locales de esta región, los municipios han podido contar con herramientas y soluciones que normalmente les son inaccesibles y elevar su protección frente a los ciberataques.

La Dirección General de Tecnologías de la Información y las Comunicaciones (DGTIC) de la Generalitat Valenciana, a través del Servicio de Confianza Digital y del CSIRT-CV (Centro de Ciberseguridad de la Comunitat Valenciana), ha abordado la problemática de forma unificada frente al desafío que planteaba la heterogeneidad y el elevado número de interlocutores en las EELL, así como el desconocimiento por parte de algunas de estas entidades, de la tecnología de sus propios sistemas de información.

Objetivos del proyecto:

- desplegar herramientas de protección para los municipios frente a ciberataques, principalmente de ransomware.
- implementar sondas para la detección temprana de riesgos.
- reducir al mínimo el impacto en los servicios esenciales municipales de los ciberataques perpetrados con éxito.
- ofrecer soporte técnico, capacitación en ciberseguridad y apoyo en el cumplimiento de las obligaciones derivadas del Esquema Nacional de Seguridad.

La DGTIC ha implementado este plan a través de CSIRT-CV, el más veterano de los centros de respuesta ante incidentes de ámbito autonómico en toda España, con la colaboración del centro de respuesta a incidentes de ciberseguridad del Centro Criptológico Nacional (CCN-CERT), el máximo organismo competente en materia de ciberseguridad para las Administraciones Públicas, además de las tres diputaciones provinciales, las 584 EELL y la empresa valenciana S2 Grupo, adjudicataria del plan bajo la dirección del Servicio de Confianza Digital. La tecnología empleada ha sido proporcionada por el CCN-CERT, siendo, además, S2Grupo quien ha desarrollado para el centro nacional algunas de las herramientas empleadas.

El plan ha supuesto la extensión del modelo de prevención, detección y respuesta ya implantado en CSIRT-CV a las 584 EELL, mediante la ampliación de sus capacidades y la federación de herramientas del CCN-CERT.

Para implementar las acciones incluidas en este proyecto, ha sido necesaria la ampliación tanto de las infraestructuras TIC como de las capacidades preexistentes en CSIRT-CV, incluyendo el reenfoque de algunas de las herramienta del CCN-CERT, para poder hacer una gestión federada, tanto de las herramientas desplegadas como de las alertas generadas, lo que ha supuesto todo un reto: una inversión en infraestructuras y recursos que ha abierto la puerta a que las EELL valencianas puedan gozar de unos niveles de protección en ciberseguridad como las de ninguna otra Comunidad Autónoma de toda España y ser las primeras en integrarse de facto en la Red Nacional de SOC. Esta red es una plataforma liderada por el CCN-CERT que interconecta a los principales centros de respuesta ante incidentes de España, públicos, privados y de distintos sectores, con el fin de compartir inteligencia e intercambiar información de ciberincidentes a nivel nacional.

Con el fin de priorizar acciones y optimizar recursos, se ha agrupado a las EELL en bloques, según el número de habitantes, debido a la correlación entre esa cifra y los niveles de riesgo a los que se enfrentan.

Soluciones tecnológicas y servicios implantados:

- **microCLAUDIA**: instalación de la herramienta microCLAUDIA del CCN-CERT en los servidores y puestos de trabajo de todas las EELL de la Comunitat, lo que incluye el soporte y seguimiento del despliegue de la herramienta, la operación, notificación de alertas, vigilancia y posibles recomendaciones. Su implantación ha estado destinada a todas las EELL, las 584, independientemente de su tamaño.

- Documentación sobre el procedimiento de **backup**: distribución de información relativa a la implantación de buenas prácticas en materia de realización de backups y su seguimiento y asesoramiento. Destinada a todas las EELL.

- **TRILLION**: alta en el servicio proporcionado por el CCN-CERT de los dominios indicados por cada EELL en busca de fugas de credenciales. Análisis de los informes de la herramienta y notificación de las cuentas comprometidas. Destinada a todas las EELL.

- **Análisis de visibilidad**: realización de análisis automáticos de puertos expuestos en las IP públicas notificadas. Informe de recomendaciones a partir de los datos obtenidos en el análisis. La medida ha estado destinada a los cerca de 320 ayuntamientos de más de 5.000 habitantes.

- **Vigilancia digital**: revisión en redes sociales de los dominios de la entidad local, complementada con búsquedas por palabras clave de posibles “leaks” en Internet. Envío

de informe periódico de riesgos encontrados, con recomendaciones para su mitigación. La medida ha ido destinada a los 65 ayuntamientos de más de 20.000 habitantes

- **ARGOS COLLECTOR**: despliegue de un agente de la herramienta GLORIA del CCN-CERT, un recolector de eventos derivados de la actividad TIC de la entidad que se consideren significativos para la correlación en busca de amenazas y posibles ataques. El servicio incluye la distribución de documentación referente a la configuración del entorno y apoyo técnico durante el despliegue de la herramienta y la configuración, así como la contextualización de cada instalación con la información del entorno TIC de la entidad. Se dispone de analistas para la revisión y cribado de los eventos obtenidos. La entidad local recibe el reporte de resultados junto con las recomendaciones pertinentes para la mejora de su ciberseguridad. Medida destinada a las 146 EELL de entre 5.000 y 50.000 habitantes.

- **CARMEN/CLAUDIA**: para aumentar los niveles de vigilancia en los quince ayuntamientos de más de 50.000 habitantes de la Comunitat, potenciales destinatarias de APT (Amenazas Persistentes Avanzadas, las más letales de todas las existentes), el proyecto incluye, para cada uno de ellos, un servidor con la instalación y configuración completa de la herramienta CARMEN del CCN-CERT, más el apoyo a la puesta en marcha y operaciones de vigilancia y "thread hunting" necesarias, así como la herramienta CLAUDIA del CCN-CERT (el end-point de CARMEN). Medida destinada a los 15 ayuntamientos de más de 50.000 habitantes.

- **Formación y concienciación**: para minimizar el riesgo de sufrir un incidente de ciberseguridad y tratar de que su impacto sea el mínimo posible, se han diseñado varios itinerarios formativos destinados al personal directivo de las EELL, al personal técnico TIC y al resto de empleados. Igualmente se han emitido varias jornadas on-line de concienciación de alto impacto, para mostrar en directo los principales riesgos a los que todo el personal está expuesto en el uso de las TIC y dar unas sencillas pautas para mitigarlos. Esta actuación ha ido destinada a todas las EELL, independientemente de su tamaño.

Fases del proyecto:

- ampliación de las capacidades y la infraestructura TIC de CSIRT-CV.
- procedimentación de las acciones.
- difusión de la iniciativa a los municipios para su adhesión.
- inicio del despliegue de la herramienta microCLAUDIA en las EELL.
- difusión de buenas prácticas de backup.
- implementación del "modelo CCN-CERT federado", mediante el cual el CCN-CERT delega en la Comunitat los servicios de seguridad que presta a las EELL, mediante el despliegue en CSIRT-CV de un nodo con herramientas interconectadas con el CCN-CERT (microCLAUDIA, ARGOS Collector, Trillion, GLORIA, CARMEN/CLAUDIA, etc.).
- inicio de los análisis de visibilidad y de las operaciones de vigilancia digital.

- definición y puesta en marcha de las acciones de formación y concienciación para altos cargos, personal municipal y personal técnico.

Metodología

El proyecto nace con dos características principales: la urgencia por conseguir ciertos hitos y la alta dispersión de infraestructuras y tecnologías.

Así, se definieron tres fases estratégicas:

1. En la primera, se utilizó el método de ruta crítica, en el que se marcan los hitos críticos, priorizando desplegar vacunas (microCLAUDIA) y ordenar la información sobre tecnologías. Se marcó un plazo para obtener la información de los organismos y su tecnología, así como para evaluar su grado de madurez. En paralelo, se priorizó el despliegue de la herramienta microCLAUDIA como medida inicial de protección. Se definieron tres entregables: mapa de infraestructura, documento de infraestructura por organismo y un entregable mensual, el informe de seguimiento del despliegue de microCLAUDIA.
2. La segunda fase comprendía la ejecución del resto de iniciativas, mediante un modelo de cascada, con iniciativas en paralelo, fechas definidas y entregables pactados previamente.
3. En la tercera fase, la fase de servicio, se aplican fundamentalmente metodologías LEAN para maximizar la eficiencia de los recursos del proyecto, ya que, derivado de la dispersión de infraestructuras, se producen muchos "desperdicios" (Muda).

Indicadores de implantación

El indicador óptimo, por ser el que en mayor medida ayuda a conseguir el principal objetivo del proyecto, es el grado de implantación de microCLAUDIA, herramienta que vacuna a los sistemas contra el ransomware. La situación de partida no ha sido cuantificada pero el CCN-CERT calificó la implantación inicial de la herramienta en la Comunitat como “baja”.

Actualmente, el despliegue se ha iniciado ya en el 77% de las EELL. Sin embargo, no es posible cuantificar el número de infecciones evitadas, ya que la herramienta, pese a ser muy eficaz evitando ejecución de ransomware, no proporciona estimación numérica sobre ello.

Otros indicadores relevantes

- el 82% de las EELL se ha dado de alta en el servicio Trillion, con 500 dominios registrados.
- en 14 de los 15 ayuntamientos de más de 50.000 habitantes, se ha completado el despliegue de la herramienta CARMEN y están recibiendo informes de análisis de “threat hunting”, con las pertinentes recomendaciones.
- en las 65 EELL de más de 20.000 habitantes, se han realizado 47.272 actuaciones de vigilancia digital, con más de 1.150 alertas notificadas.

- sobre el análisis de visibilidad, en las 320 EELL de más de 5.000 habitantes, se han detectado 449 eventos relevantes y se han notificado más de 12.500 alertas a 169 ayuntamientos.
- El despliegue de ARGOS-EPC cuenta con un 82% de adhesión y, solo en el pasado mes de diciembre, ha permitido gestionar 5.879 eventos de seguridad y resolver 5.763, con un saldo de 0 eventos críticos y 0 incidentes.

Resumen del alcance de las iniciativas

En la tabla siguiente se expone el resumen numérico de las entidades a las que aplica cada una de las medidas y el grado de implantación, a fecha de emitir este informe, evidenciando así tanto el alcance del proyecto, como la gran acogida que ha tenido desde su lanzamiento. Más del 82% de las EELL valencianas ha implantado ya alguna de las medidas ofrecidas.

	microCLAUDIA	Documento Backup	Analisis visibilidad	Argos Collector	Carmen	Vigilancia Digital	Trillion
Alcance	584	584	323	147	15	66	584
Adherido	446	536	169	121	14	65	480
No Adherido	138	48	154	26	1	1	184

Repercusión para el ciudadano y las Administraciones

Beneficios

Como se mencionaba en el apartado anterior, en unos pocos meses desde su puesta en marcha, este plan consiguió elevar los niveles de ciberseguridad de las EELL participantes, de forma que están gozando ya de unos niveles de protección en ciberseguridad como las de ninguna otra Comunidad Autónoma de toda España, lo que redunda en una mejora global de la protección de los datos de los ciudadanos que están bajo la custodia las EELL de la Comunitat en sus sistemas de información.

El principal beneficio ha sido, sin duda, el descenso drástico de los niveles de infecciones por ransomware en las Entidades Locales de esta Comunitat, objetivo prioritario del proyecto, sin olvidar lo mucho que ha contribuido al cumplimiento del Esquema Nacional de Seguridad en todas ellas, especialmente en aquellas medidas que atañen a la protección contra código dañino, a la vigilancia del perímetro y a la formación y concienciación del personal.

Satisfacción de las EELL participantes

A lo largo de la ejecución de este plan, se ha podido constatar la enorme aceptación que este proyecto ha suscitado entre las entidades destinatarias de sus acciones, muchas de ellas huérfanas hasta ahora de cualquier apoyo en la mejora de su ciberseguridad. Hay que tener en

cuenta que las EELL, especialmente las de menor tamaño, carecen de los recursos necesarios para abordar, por sí solas, las obligaciones que en cuanto a la mejora de su ciberseguridad les impone el Esquema Nacional de Seguridad (ENS). Muchas de estas obligaciones han sido parcialmente cubiertas a través de la puesta en marcha de las iniciativas del plan, como ya se ha especificado.

La acogida por parte de las EELL destinatarias ha sido encomiable, a pesar de que se les ha exigido un relevante esfuerzo para la implantación de las medidas que, en ocasiones, ha excedido con mucho de su capacidad. No habría sido posible lograr las cifras de despliegue actual solo con la implicación de la DGTIC, por lo que conviene destacar la motivación y el esfuerzo de las EELL y de las tres diputaciones provinciales que, cada una con sus distintas aportaciones, han contribuido al éxito del proyecto. Cabe, por tanto, poner en valor el alto grado de colaboración obtenida.

La satisfacción puede también deducirse fácilmente de los indicadores de implantación y despliegue mostrados en el apartado anterior que, sin el esfuerzo realizado por parte de los empleados municipales tampoco habría sido posible.

Ejemplaridad y relevancia

La DGTIC ha implementado el plan a través de su centro especializado en ciberseguridad CSIRT-CV, bajo la dirección del Servicio de Confianza digital. Se ha conseguido generar economías de escala y extender la experiencia y madurez del centro hacia las EELL, gracias a la colaboración del CCN-CERT, con el que se ha definido un modelo federado para desplegar sus herramientas interconectadas.

CSIRT-CV ha sido elegido por el CCN-CERT, por su trayectoria y posición de liderazgo actuales, como el primer centro autonómico que se integrará en la Red Nacional de SOC, siendo a su vez el primero que integra en dicha red a las 584 EELL del territorio, proporcionándoles la cobertura de ciberseguridad y vigilancia necesarias, con una gestión óptima de los recursos de ciberseguridad, que tan costosos e inaccesibles resultan para dichos organismos, carentes de personal especializado.

El resultado de este esfuerzo colectivo es conocido por el CCN-CERT como el "modelo valenciano de ciberseguridad", en el que el CCN-CERT delega en CSIRT-CV los servicios de seguridad que presta, mediante el despliegue en el centro especializado valenciano de sus herramientas, interconectadas, para que desde CSIRT-CV se ofrezca servicio tanto a la Generalitat Valenciana y todas sus consellerías y organismos, como a todas las EELL del territorio, a su ciudadanía y a las empresas.

Este modelo ha sido expuesto por el CCN-CERT con frecuencia a todas las Comunidades Autónomas españolas, como caso de éxito y como un modelo de excelencia a implementar por todas ellas, acreditando así la máxima ejemplaridad que un proyecto liderado por una Comunidad Autónoma puede alcanzar en España.

Repercusión para el ciudadano como mejora en la protección de sus datos

Las corporaciones locales son las administraciones más cercanas a la sociedad y albergan, en sus sistemas de información, gran cantidad de datos de la ciudadanía que es necesario proteger. Sin

embargo, al carecer de recursos especializados y de la concienciación necesaria de sus empleados para poder protegerlos adecuadamente, han sido blanco de frecuentes ciberataques. Con demasiada frecuencia han venido precedidos de ataques de ingeniería social, que han aprovechado dicha falta de concienciación como vector de entrada para lograr sus objetivos.

Por esta razón, ha sido necesario reforzar la concienciación del personal empleado público de estas entidades, poniendo a disposición de todas las personas itinerarios auto-formativos diferenciados por perfiles profesionales y llevando a cabo acciones formativas on-line de alto impacto, a través de jornadas. En ellas se ha expuesto, mediante ejemplos y ataques reales ejecutados por un hacker presente en la sesión, la facilidad con la que nuestras acciones cotidianas pueden poner en riesgo los sistemas de información municipales y los datos que albergan.

Tal ha sido el éxito de estas últimas que, pese a emitirse on-line con reiterada convocatoria previa, han tenido que ser repetidas a petición de las EELL, en tres ocasiones distintas. Hasta la fecha se han registrado más de 2.500 conexiones a estas jornadas, no sólo con usuarios individuales, sino con aulas de formación, salas de plenos o bibliotecas, resultando imposible cuantificar cuántos usuarios de esas 2.500 conexiones asistían a cada una de ellas. Está previsto reiterar esta medida durante el año entrante.

Equipo de desarrollo y proveedores

Selección del proveedor y equipo de trabajo

Este plan se instrumentalizó, en sus inicios, a través de un contrato de emergencia que permitió la elección del proveedor. Todas las acciones del plan debían enmarcarse en las estructuras de servicio de CSIRT-CV, aprovechando así la experiencia y madurez del centro, lo que ha resultado determinante para obtener un alto grado de sinergias entre ambos equipos y una velocidad en los despliegues bastante notable. Por esta razón y dado que la mayoría de las actuaciones estaban basadas en herramientas del CCN-CERT, se buscaban perfiles similares a los ya existentes en CSIRT-CV, capaces de integrarse con rapidez en sus estructuras de servicio y conocedores de las herramientas, para minimizar el tiempo de adaptación.

Se eligió, por tanto, a la empresa valenciana S2Grupo, por su experiencia y posición de liderazgo actuales, así como por el conocimiento del centro y por contar con los perfiles adecuados. Actualmente, se dispone de casi una veintena de técnicos de distintos perfiles y dedicaciones, la mayoría ingenieros informáticos y de telecomunicaciones, expertos en formación y concienciación y en el ENS, con amplia experiencia contrastada.

Valoración económica

El montante inicial de la ampliación de la infraestructura TIC preexistente en el CSIRT-CV, para albergar el despliegue y operación de todas estas actuaciones supuso una inversión cercana a

los 200.000 €. El coste de los perfiles técnicos para la prestación de los servicios de despliegue, operación y vigilancia que contempla el plan, ha alcanzado hasta la fecha los 2.000.000 €.

El éxito de este modelo se ha basado en la coordinación entre todos los agentes implicados, en la implantación de mecanismos de respuesta centralizada contando con la experiencia y madurez del CSIRT-CV, lo que ha aumentado la eficiencia de la respuesta, al generar economías de escala.

La valoración económica prevista para poder seguir prestando estos y otros servicios de ciberseguridad a las EELL valencianas en los años venideros, no puede ser revelada en este momento, por no haber sido publicada la licitación a fecha de redactar esta memoria, pero va a superar con creces la asignación actual, para mantener en el tiempo la vigencia del proyecto.

Plazos de cumplimiento

Como ya se ha mencionado, la Generalitat Valenciana adoptó el compromiso de elaborar un Plan de Choque de Ciberseguridad para las Entidades Locales. En junio de 2021 se acordó la adjudicación de un contrato de emergencia para prestar los servicios del plan, con una duración inicial de un año.

Pese a que el objetivo inicial de disponer de un plan de emergencia estuvo plenamente conseguido en los meses iniciales de su lanzamiento, su desarrollo puso de manifiesto que las necesidades de protección en materia de ciberseguridad de las Entidades Locales valencianas iban mucho más allá de lo que un plan de emergencia podía abarcar en tan sólo un año, por muy ambicioso que éste fuera.

Por ello, todas estas acciones han sido sostenidas y ampliadas en el tiempo a través de figuras contractuales distintas de la emergencia con la que se inició, evidenciando tanto el compromiso del Gobierno valenciano con la ciberseguridad de las EELL -las administraciones más cercanas al ciudadano- como la trascendencia y continuidad de todo el proyecto en su conjunto, que no tiene, por tanto, plazo de finalización, al tratarse de un servicio continuado.

Información relevante, adicional a los elementos básicos deseables que mencionaba la convocatoria

Resumen de los aspectos más relevantes

A lo largo de la exposición anterior, han sido muchos los aspectos enumerados que podrían resultar relevantes e incluso únicos:

- se ha logrado extender el modelo de prevención, detección y respuesta ya implantado en CSIRT-CV a las 584 EELL del territorio y ser la primera Comunidad Autónoma de España en conseguirlo.
- la Comunitat Valenciana ha sido elegida por el CCN-CERT para ser la primera Comunidad en integrarse en conjunto en la Red Nacional de SOC.

- se han logrado elevar, en términos globales, los niveles de cumplimiento del Esquema Nacional de Seguridad, especialmente en aquellas medidas que atañen a la protección contra código dañino, a la vigilancia del perímetro y a la formación y concienciación del personal.
- la anticipación de la DGTIC en la definición y puesta en marcha de las acciones que se iban a ofrecer a los ayuntamientos de más de 50.000 habitantes ha resultado, asimismo, determinante para que todos ellos, sin excepción, hayan podido justificar en tiempo y forma, a través de la adhesión a este proyecto, los requisitos obligatorios para el acceso a las subvenciones europeas destinadas a la transformación digital y modernización de las Administraciones de las Entidades Locales (en el marco del Plan de Recuperación, Transformación y Resiliencia publicadas en el BOE el 6 de Noviembre del 2021), complementando estos, tan solo con alguna herramienta adicional del CCN-CERT, que desde la dirección del proyecto, con el apoyo del centro nacional, se ha ayudado a definir.
- el descenso drástico de los niveles de infección por ransomware en las Entidades Locales de la Comunitat Valenciana, objetivo prioritario del proyecto.
- el proyecto es, actualmente, un referente para el resto de Comunidades Autónomas españolas, un modelo de excelencia a impulsar en todas ellas.

Aspectos a mejorar:

Pese a que el plan fue presentado en sus comienzos por la Conselleria de Hacienda, Economía y Administración Pública, convocando a las tres diputaciones provinciales y a la mayoría de los alcaldes de los municipios de mayor tamaño de la Comunitat, hubiera sido deseable insistir en el aspecto de la insuficiente dotación de personal especializado en los departamentos TIC municipales. De haber conseguido un aumento, en términos globales, en la dotación de personal de TI en las entidades, se hubiera aligerado el esfuerzo empleado en los despliegues por parte del equipo del proyecto.

Las corporaciones municipales valencianas han sufrido muchos cambios en su composición tras las últimas elecciones municipales. Así pues, se ha previsto volver a convocar a todas ellas, con el fin de presentar los resultados del proyecto y seguir recabando su apoyo a las iniciativas presentes y futuras.

Recomendaciones ante iniciativas similares

Durante los meses de vigencia del proyecto han sido muchas las consultas recibidas por parte de otras comunidades autónomas, interesándose por los pormenores de la solución adoptada. La recomendación, en cada caso, ha estado muy ligada a la evaluación de la situación de partida. Si hubiera que escoger unas pocas recomendaciones que pudieran aplicarse a todas ellas sería, sin duda, la de elegir las herramientas y soluciones aportadas por el CCN-CERT y contar con una empresa y equipo de trabajo con la suficiente solvencia técnica y experiencia acreditada.

Otros premios

Desde la puesta en marcha del proyecto, la Generalitat ha cosechado los tres premios a los que ha optado con esta iniciativa:

- ha sido reconocido por la Asociación Española de Usuarios de la Sociedad de la Información, AUTELSI, quien otorgó al proyecto, en el año 2022, el "Premio a la mejor iniciativa o proyecto tecnológico del sector público" de España.
- el pasado 22 de noviembre, la Generalitat Valenciana recogía el premio otorgado al proyecto por CIONET y Vocento, en la categoría "Cybersecurity, Risk Management & Business Continuity", alcanzando la condición de Digital Leader 2024.
- el 14 de diciembre de 2023, la Generalitat era galardonada con el CIO 100 Awards Spain 2023, en la categoría de mejor proyecto de tecnologías de la información para la seguridad y la resiliencia, por el plan de ciberseguridad de la Comunitat Valenciana en apoyo a las administraciones valencianas.

Referencias

Premios mencionados:

- Los Premios AUTELSI 2022, ya tienen Ganadores (autelsinsights.es)
- https://concienciat.gva.es/sabias_que/el-plan-de-choque-de-ciberseguridad-para-las-eell-de-la-comunitat-valenciana-de-la-direccion-general-de-las-tecnologias-de-la-informacion-recibe-el-premio-autelsi/
- Premios CIONET Vocento 2023
- La Generalitat recibe el premio CIO 100 Awards Spain 2023 al proyecto del año de innovación tecnológica en ciberseguridad - Valencia Plaza

Algunas menciones a este plan, aunque pueden encontrarse muchas más:

- https://cadenaser.com/emisora/2022/01/05/radio_valencia/1641396717_216108.html
- https://dgtic.gva.es/va/actualidad/-/asset_publisher/0YobAjUX6lT2/content/la-generalitat-forma-a-m%25C3%25A1s-de-500-personas-que-trabajan-en-ayuntamientos-para-prevenir-ciberataques
- https://dgtic.gva.es/es/home/-/asset_publisher/0YobAjUX6lT2/content/el-plan-de-choque-de-ciberseguridad-de-la-generalitat-para-las-entidades-locales-se-convierte-en-modelo-de-excelencia-para-el-resto-de-las-autonom%25C3%25ADas
- https://cybersecuritynews.es/el-informe-anual-de-csirt-cv-revela-aumento-de-ciberamenazas-y-tendencias-preocupantes-en-2022/
- https://valenciaplaza.com/deshabilitar-conexiones-inalambricas-recomendaciones-sobre-ciberseguridad
- https://www.levante-emv.com/comunitat-valenciana/2022/01/07/c-valenciana-sufrio-1-500-61329831.html
- https://www.elperiodic.com/villena/villena-acoge-xxii-encuentro-anual-tecnicos-informaticos-municipales_862718