CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

INFORME DE ACTIVIDADES, CIBERAMENAZAS Y TENDENCIAS

2022

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Fons Europeu de Desenvolupament Regional
Una manera de fer Europa
UNIÓ EUROPEA

Actuació susceptible de ser cofinançada per la Unió Europea a través del Programa Operatiu del Fons Europeu de Desenvolupament Regional (FEDER) de la Comunitat Valenciana 2014-2020

CLASIFICACIÓN

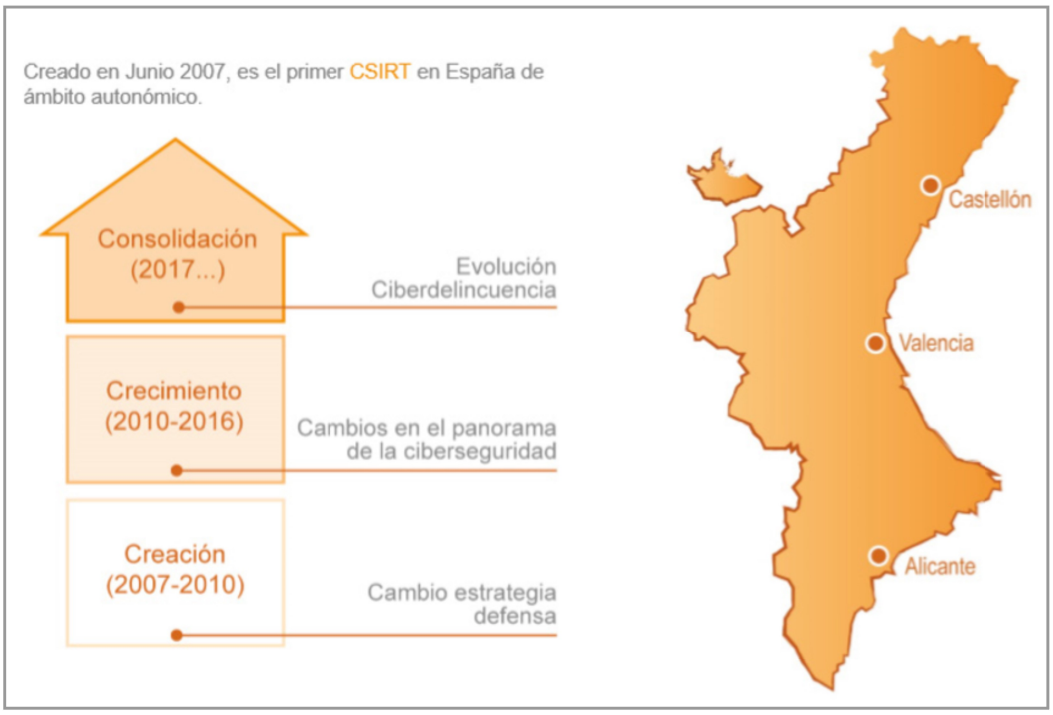
INDICE

SOBRE EL PRESENTE INFORME

La información recogida en este informe es, en gran medida, el resultado de la experiencia del CSIRT-CV durante 2022, en el desarrollo de sus competencias. Asimismo, se han tenido en cuenta otras fuentes documentales, nacionales e internacionales, públicas y privadas.

CSIRT-CV

CSIRT-CV es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007, como una apuesta de la Generalitat Valenciana por la seguridad en la red. En 2022, cumple 15 años de andadura, en los que se ha consolidado como un CSIRT de referencia a nivel nacional y con presencia internacional en foros como CSIRT.es, Trusted Introducer y FIRST.



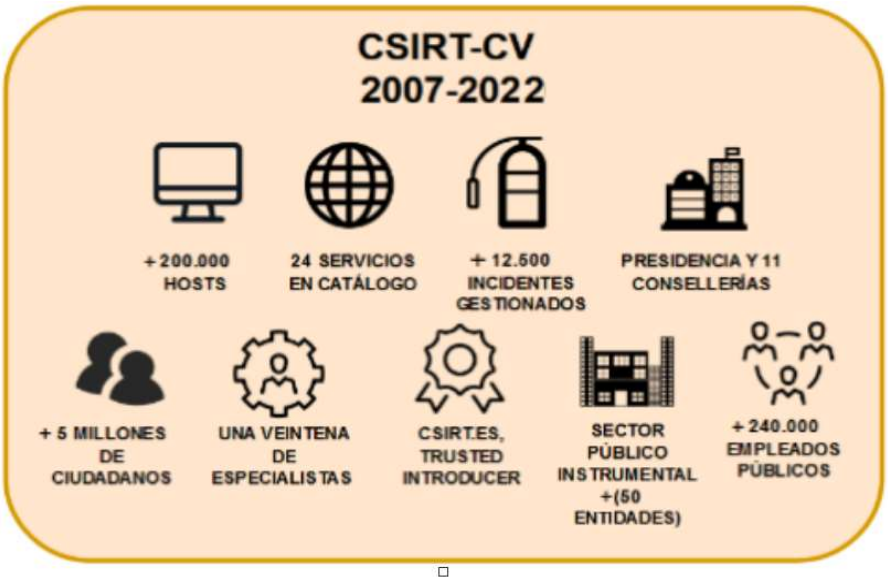
Se trata de una iniciativa pionera al ser el primer centro de estas características que se crea en España para un ámbito autonómico. Actualmente, **CSIRT-CV** está adscrito a la Dirección General de Tecnologías de la Información y las Comunicaciones (DGTIC) dentro de la Conselleria de Hacienda y Modelo Económico.

CSIRT-CV ofrece servicios dentro de la Comunitat Valenciana (Alicante, Castellón y Valencia), con vocación de servicio público y sin ánimo de lucro, por lo que sus servicios se ofrecen gratuitamente.

Los colectivos destinatarios de estos servicios son:

- Los ciudadanos de la Comunitat Valenciana.
- Los profesionales y empresas privadas, especialmente las de menor tamaño.
- La Administración Pública, tanto local como autonómica. Principalmente esta última por la ubicación del centro.

El ámbito de actuación del CSIRT-CV, como se observa, es muy amplio puesto que incluye a la Generalitat, que en la actualidad está formada por Presidencia y 11 Consellerias, entre las que se incluyen 2 Vicepresidencias. También se incluye el sector público instrumental[1], junto con medio centenar de entidades. En total, el número de empleados públicos en la Comunitat asciende a más de 240.000[2]. Por último, es preciso mencionar que la Comunitat Valenciana representa cerca de un 11% de la población nacional con más de 5 millones de habitantes (2022), siendo la 4ª comunidad autónoma de España en cuanto a población se refiere.



1 http://www.gvaoberta.gva.es/es/sector-publico-instrumental

2 Según datos publicados en el Boletín Estadístico del Personal al Servicio de las Administraciones Públicas, a fecha julio 2022.

Respecto a la infraestructura TI de la Generalitat Valenciana, es altamente heterogénea y compleja, dando servicio a más de 200.000 dispositivos, entre los que se incluye tanto equipamiento IT como OT.

El principal objetivo de CSIRT-CV es 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 pudieran surgir.

AÑO 2022: PRESENCIALIDAD Y TELETRABAJO

El confinamiento que provocó la pandemia de la COVID-19 supuso un aumento en el uso del teletrabajo, en ocasiones mal planificado, que provocó el riesgo de muchas organizaciones a ser atacadas de forma remota a través de esos canales de teletrabajo: VPN, escritorios remotos… Esto supuso un gran esfuerzo para configurar correctamente estas soluciones, así como monitorizar el uso de las mismas.

Aunque en muchos lugares ya se ha vuelto por completo a la presencialidad, en algunos sectores se continúa con un teletrabajo total o parcial.

HITOS Y SERVICIOS PRESTADOS DURANTE 2022

1 TEST DE INTRUSIÓN

Este servicio proporciona un análisis exhaustivo mediante una serie de pruebas manuales de intrusión, utilizando técnicas exhaustivas de identificación de vulnerabilidades contra aplicaciones y sistemas.

En el transcurso del año, el equipo Red-Team del CSIRT-CV ha realizado 63 test de intrusión, de los que 56 han sido sobre plataformas Web, 4 sobre aplicaciones móviles, 2 Web Services y 1 de Hacking Ético Interno.

Por último, comentar que fruto del trabajo de este servicio, durante 2022, se han reportado a INCIBE varias vulnerabilidades que están en proceso de publicación.

2 AUDITORÍAS DE VULNERABILIDADES

Este servicio consiste en la identificación de las vulnerabilidades presentes en los activos del solicitante analizando, gestionando y diseminando la información de la mejor manera posible mediante herramientas automáticas para que las debilidades detectadas sean corregidas antes de ser aprovechadas por un atacante real.

En 2022, se han realizado 107 auditorías de vulnerabilidades entre las habituales/rutinarias y otras ejecutadas bajo demanda.

En estas auditorías se han auditado 36 organismos pertenecientes al ámbito de la Generalitat en el primer semestre del año, y 36 en el segundo.

Comparado con el año 2021, donde hubo un incremento del 6,89% en el segundo semestre, no se han vuelto a observar cambios globales en cuanto al número de organismos con vulnerabilidades criticas.

A la hora de mantener la seguridad de los sistemas de información, un buen plan de actualizaciones es esencial para mantener la infraestructura en un estado óptimo, así como una configuración adecuada que logre minimizar la posibilidad de que un ataque pueda comprometer la seguridad del sistema.

Destacar también la importancia de la concienciación y prevención, que deben tener los administradores de los sistemas, para estar al corriente de las alertas de seguridad que podrían afectar a los servidores y equipos a su cargo.

3 AUDITORÍA DE SEGURIDAD SEMÁNTICA

Este servicio está centrado en la detección de posibles riesgos reputacionales, legales o técnicos en torno al uso de una marca o persona/s física/s en Internet.

No se han registrado peticiones de este servicio durante este año. Sin embargo, de forma proactiva se ha hecho un gran trabajo a raíz de varias situaciones de interés: campañas de desinformación relacionadas con la campaña de vacunación, uso de información sobre la pandemia para crear sitios webs maliciosos, orquestación de posibles ciberataques contra el gobierno autonómico, etc.

4 VALIDACIÓN DE CÓDIGO

Este servicio tiene como objetivo hacer una revisión de código y auditar la implementación de la metodología de seguridad en el ciclo de vida del desarrollo de software.

No se han registrado peticiones de este servicio durante 2022, aunque es necesario matizar que en la mayoría de los test de intrusión ejecutados, se realiza una fase de validación del código de la aplicación objeto de análisis.

5 ANÁLISIS FORENSE

Tras un incidente de ciberseguridad, este servicio ofrece un análisis posterior con el objetivo de obtener toda la información pericial necesaria y elaborar un informe que pudiera ser requerido en procesos judiciales llevados a cabo por las autoridades competentes.

El equipo de CSIRT-CV ha realizado dos análisis forense durante 2022, derivados de la gestión de incidentes de seguridad contra ayuntamientos de la Comunitat Valenciana.

Cabe señalar que la gestión de muchos incidentes de seguridad, implícitamente, contempla un análisis forense de *logs* y registros que no se ha englobado como tal dentro de este servicio, sino que se ha considerado como parte del servicio de Gestión de Incidentes.

6 BASTIONADO DE ENTORNOS

Este servicio proporciona asesoramiento sobre las pautas y directrices adecuadas para fortalecer el entorno propuesto, bien sea de sistemas, redes, aplicaciones o dispositivos. Por ejemplo: protección de una red WiFi, bastionado de un servidor Windows, etc.

Durante 2022 se han registrado cuatro solicitudes de bastionado de diversos entornos, principalmente, relacionadas con el control de los accesos externos, aplicaciones de control remoto, Oracle Secure Global Desktop y servicios de copias de seguridad.

Es preciso comentar que muchas consultas técnicas que se atienden dentro del servicio de Consultoría, van ligadas al bastionado de sistemas o aplicaciones, y no se contabilizan en este servicio.

7 GESTIÓN DE INCIDENTES

Este servicio proporciona una solución integral a cualquier incidente de seguridad que se pueda producir, incluyendo entre ellos incidentes tales como: intento de fraude electrónico, phishing, compromiso por malware, detección de comportamiento sospechoso en el equipo o en las cuentas digitales, suplantación de identidad, robo de contraseñas, secuestro de información etc.

En 2022 se han gestionado un total de 1.144 incidentes. De estos, 138 están relacionados con “Intrusión”, 129 con “Intento de Intrusión”, 51 de “Obtención de Información”, 21 por “Disponibilidad”, 227 de “Compromiso de la Información” y, 578 por “Fraude”.

A continuación se muestra un gráfico con los datos mencionados en el párrafo anterior:

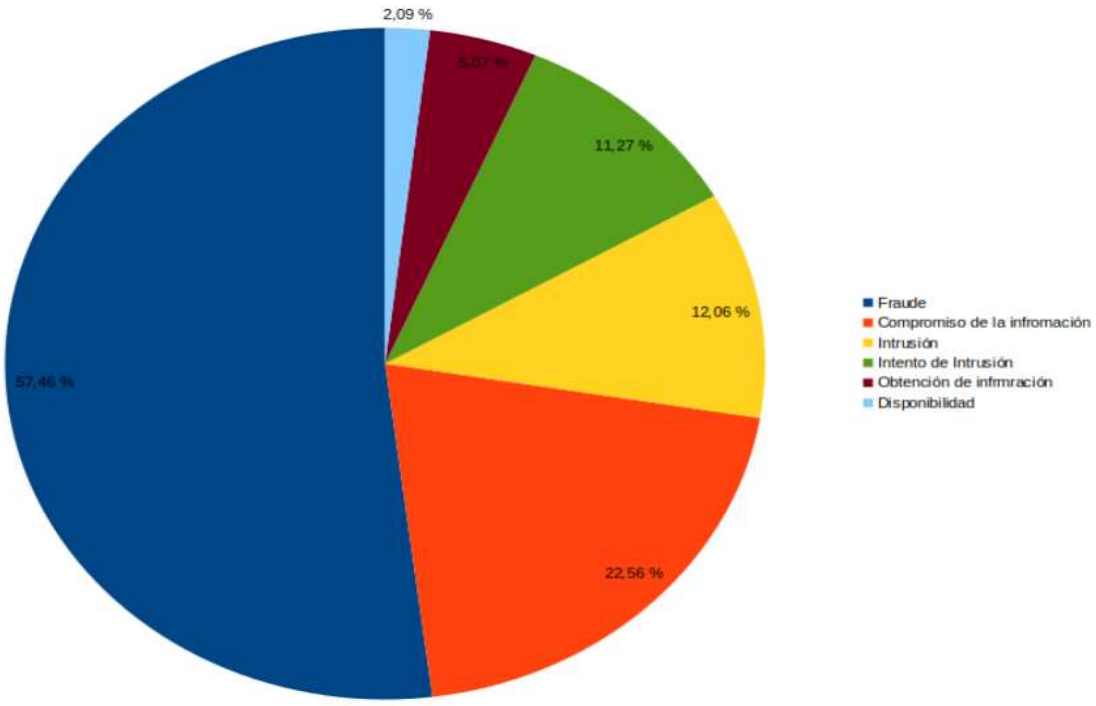


Figura 1: Desglose incidentes gestionados de en los últimos 12 meses por CSIRT-CV

En la información que muestra el gráfico anterior, se puede observar que prácticamente la mitad de los incidentes son de tipo Fraude, destacando aquí los correos de tipo phishing gestionados. Esto se debe a que se reciben campañas constantemente. Además de los correos de robo de credenciales se han producido casos de suplantación.

Destaca también la categoría Compromiso de la Información, debido a incidentes del proyecto vigilancia digital y brechas de seguridad en plataforma externas. Otros también relevantes en cuanto a volumetría son los de tipo Intrusión, principalmente son casos de compromiso de cuentas de usuario, derivados de incidentes de phishing, código dañino o fuerza bruta. Así como el Intento de Intrusión, donde se producen ataques relacionados con la explotación de vulnerabilidades conocidas.

La siguiente categoría a destacar es la Obtención de Información, donde se han producido varios incidentes de tipo escaneo. Este tipo de incidentes no representan un riesgo por sí solos, pero suele ser indicativo de acciones preliminares realizadas por los atacantes, para lanzar posteriormente otros tipos de ataques. La otra subcategoría que destaca, dentro de Obtención de Información, es Ingeniería Social, donde los atacantes suelen intentar estafar a los usuarios, habitualmente mediante el uso de correos malintencionados.

Por último, y con menor volumetría, mencionar la categoría de Disponibilidad, incidentes relacionados con ataques de denegación de servicio principalmente.

Se quiere remarcar en este punto que, a lo largo de este año, se han gestionado varios incidentes relevantes, que se detallaran en los siguientes epígrafes.

8 GIR, GESTIÓN DE CRISIS Y OTROS INCIDENTES RELEVANTES

CSIRT-CV ofrece al resto de Generalitat un Grupo de Intervención Rápida (GIR) ante incidentes de seguridad especialmente relevantes, prestando apoyo técnico y organizativo a Conselleríes u otros organismos para, ante cualquier problema, recuperar el servicio interno y para los ciudadanos en el menor tiempo posible.

En 2022 se ha activado el GIR en dos ocasiones, a causa de incidentes de seguridad en ayuntamientos de la Comunitat Valenciana. Además, se han gestionado algunos

incidentes de seguridad que merecen ser citados por su complejidad e impacto ocasionado.

8.1 GIR: RANSOMWARE Y EXFILTRACIÓN EN AYUNTAMIENTO

El incidente con más relevancia se produce en noviembre por la ejecución de una amenaza de ransomware en uno de los ayuntamientos de la Comunitat Valenciana.

El ayuntamiento se vio afectado por un ransomware perteneciente al grupo "ALPHV/BlackCat", extensión de cifrado ".rpppipo", viendo interrumpidos entorno al 90% de sus servicios. Tras el análisis por parte de CSIRT-CV, se determinó como vía de entrada un acceso VPN con usuario de credenciales débiles.

Lo más relevante de este incidente, aparte del compromiso de la información, es la exfiltración de información llevada a cabo por los atacantes, días después de la ejecución del Ransomware, los atacantes cumplen su amenaza y publican los datos robados al ayuntamiento en la red TOR. Esto condujo al reporte obligado del Ayuntamiento a la AEPD por los datos sensibles obtenidos y también se realizó denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

8.2 GIR: MÁS RANSOMWARE EN AYUNTAMIENTOS

Aparte del incidente anterior, cabe mencionar que se gestiona otro incidente relacionado con este tipo de amenaza y aunque fue afectado, no con el impacto y la repercusión que genera la publicación de datos sensibles. Estos incidentes no hacen más que confirmar la tendencia al alza, que ha sido observada desde el inicio de la pandemia, aprovechando deficiencias y malas configuraciones relacionadas con la seguridad.

En este otro caso, ocurrido en octubre, el ayuntamiento es afectado con ransomware de la familia Phobos y extensión de cifrado ".elbie", pero no concluye el proceso de cifrado y no se consigue obtener la nota de rescate ni la muestra del ransomware ante las acciones de contención realizadas por el ayuntamiento y las propias de los atacantes. No obstante, según el análisis llevado a cabo fue distribuido, como es la tendencia habitual en estos casos, desde los controladores de dominio para llegar a afectar la mayor cantidad de equipos y servidores. Además, la vía de entrada se da a través de servicios expuestos a Internet sin uso del doble factor de autenticación, en este caso el servicio RDP.

CSIRT-V colaboró con el ayuntamiento en el proceso de recuperación, así como en la revisión del entorno para cerrar las posibles vías de entrada y mejorar la seguridad de la infraestructura.

8.3 ATAQUE SQLI EFECTIVO A PORTAL DEL DOMINIO GVA

En agosto, se detecta un gran número de alertas de posible inyección SQL contra uno de los portales del dominio gva.es. Dicho portal tenía un CMS desactualizado y sin soporte, en el cual se intentaban listar las tablas de una base de datos. Además, la actividad reportada estaba distribuida en origen desde decenas de direcciones IP de la red TOR.

Desde CSIRT-CV, se determina que estos intentos de ataque eran efectivos al observar en las respuestas filtraciones de información que eran redirigidas a la página de error del portal. El ataque se produce mediante la herramienta SQLMap y se confirma que el servidor era vulnerable a ataques de inyección SQL por tiempo de respuesta, el cual permitía por fuerza bruta, listar información de la base de datos.

En cuanto a las acciones tomadas, se solicita el bloqueo del recurso hasta que se corrigiese la vulnerabilidad explotada, y también, se recomienda la actualización del portal a una versión actualizada con soporte.

Adicionalmente, se pide una auditoría de código y un test de intrusión para dejar el entorno lo más securizado posible.

8.4 MÓVIL COMPROMETIDO EN UNA DE LAS CONSEJERÍAS DE GVA

En junio, un teléfono corporativo de una de las Consellerias de GVA recibió un mensaje a través de Facebook Messenger. El mensaje contenía una URL maliciosa cuyo acceso provoca la descarga de otra aplicación maliciosa que también se descarga y ejecuta por la víctima. Debido a esto, el móvil queda comprometido y se desplaza un técnico de CSIRT-CV para realizar varias acciones:

- Cambiar el patrón de desbloqueo
- Identificar la información que quería recuperar la usuaria
- Recogida del dispositivo para realizar un análisis forense
- También se dieron recomendaciones de cambio de credenciales y de instalar un antivirus.

El móvil no contaba con antivirus, pero sí una protección configurada con el MDM corporativo que impedía activar el modo de desarrollador y demás configuraciones para permitir el análisis forense, por lo que no se pudo completar. Del análisis del mensaje, se pudo determinar que se trataba de un gusano conocido que se propagaba de esa forma, por lo que otros contactos suyos pudieron verse afectados. Finalmente, se devuelve el dispositivo a su origen.

A raíz de este incidente, se impulsó un proyecto de configuración de un antivirus con el MDM corporativo.

8.5 WEBSHELLS

Cabe destacar también la tendencia continuada en el tiempo y relacionada con la explotación de aplicaciones o software con vulnerabilidades, que permiten subir y ejecutar código malicioso en un servidor vulnerable. Esto permite a los ciberdelincuentes controlar el servidor, así como emplearlo para perpetrar ataques contra terceros, ya sea empleando el servidor como el mando de control (C&C) o para realizar ataques vía phishing alojando las páginas fraudulentas en el mismo. Precisamente, durante 2022 se vuelve a observar la subida de una webshell en un servidor que utilizaba un componente vulnerable, y que posteriormente derivó en la inclusión de un phishing bancario para lanzar campañas maliciosas a otras entidades.

8.6 TROYANO VÍA APLICACIONES DE COMPARTICIÓN DE ARCHIVOS

Los sistemas de detección y prevención de intrusos desplegados en dicha red detectaron una alerta en un equipo de presidencia el pasado mes de marzo.

La fuente concreta de la detección fue una sonda IDS y la alerta hacia referencia al uso de una herramienta de compartición de archivos, avisando de un incumplimiento de la política de seguridad de la organización. Esta alerta, por sí misma, no supone un riesgo, pero a raíz de ella se identifica al equipo implicado y se analiza su actividad en otras fuentes. Es entonces cuando se observa en la consola del antivirus otra alerta que indica que se ha detectado y eliminado correctamente un troyano.

A través del canal de comunicación habitual en la gestión de incidentes nos remiten los archivos maliciosos que se encontraban en el equipo, se analizan y bloquean en el sinkhole los indicadores de compromiso con los que intentan contactar estos archivos.

Finalmente se eliminan los archivos del equipo, y queda libre de amenazas, sin llegar a afectar a otros equipos de la red.

Esto pone de manifiesto la necesidad de restringir y controlar las aplicaciones de compartición de archivos en una empresa u organización, ya que pueden ser usadas como vía de entrada a la infraestructura o para la exfiltrar datos, según las tendencias observadas en los incidentes gestionados por CSIRT-CV.

8.7 ATAQUE EFECTIVO A SERVIDORES DE UN ORGANISMO GVA

En enero, se detectan ciertas alertas por los sistemas de detección y prevención de intrusos de CSIRT-CV en servidores de un organismo de investigación. Estas alertas estaban relacionadas con el malware Cobalt Strike.

A raíz de estas alertas, se inició una investigación y se descubre que el antivirus detecta el malware mimikatz y lazagne en varios servidores de la red. Posteriormente, se observa que se trata de un ransomware que no llegó a desplegarse sobre el dominio de dicho organismo. Los atacantes comprometieron los servidores e instalaron herramientas maliciosas, típicas para la obtención de credenciales, pivotación dentro de la infraestructura y detonación de ransomware.

El incidente tuvo su origen en un proveedor de una aplicación instalada que tenía acceso de forma remota a los activos. Aprovecharon este acceso para desplegar el ransomware e intentar afectar a otros servidores. Afortunadamente, el ataque solo afectó a dichos servidores administrados por el proveedor y pudieron recuperar el servicio de la copia de seguridad. Esto no hace más que evidenciar la necesidad de tener un registro de proveedores y accesos externos permitidos y securizarlos al máximo.

Desde CSIRT-CV, se bloquearon los indicadores de compromiso encontrados en la investigación, como direcciones URL, direcciones IP y hashes de archivos.

9 AUDITORÍA RGPD

Este servicio se ofrece para dar cumplimiento a la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

A pesar de que no se ha realizado ningún servicio como tal, se ha continuado con la revisión de los aspectos contemplados en la nueva Ley que pudieran afectar a CSIRT-CV.

10 ANÁLISIS DE RIESGOS

Este servicio ofrece la realización de un análisis de riesgos mediante la metodología MAGERIT.

Durante 2022, se han llevado a cabo tres análisis de riesgos. Uno relacionado con un portal de grabaciones judiciales, otro con una revisión anual de riesgos en materia de ISO 27001 y ENS en un organismo concreto de GVA, y por último, un análisis de riesgos sujeto al nuevo Real Decreto 311/2022, del 3 de mayo, por el que se regula el Esquema Nacional de Seguridad sobre una aplicación de GVA.

11 AUDITORÍA ENS

Consta de una auditoría diferencial sobre el grado de cumplimiento del Esquema Nacional de Seguridad.

Durante 2022, aunque no se ha realizado una auditoría como tal en materia del Esquema Nacional de Seguridad (ENS), los análisis de riesgos se ejecutan en consonancia con la norma ENS.

A este respecto, se realiza una "pequeña" auditoría a través de formularios de preguntas y entrevistas con los distintos responsables con el objetivo de obtener toda aquélla información que nos permita abordar adecuadamente los análisis de riesgos.

En base a ello, se determina la aplicación de determinados controles y sus salvaguardas, así como el establecimiento del preceptivo Plan de Tratamiento de Riesgos (PTR).

12 CONSULTORÍA ISO 27001

Este servicio tiene como finalidad orientar para planificar una estrategia de mejora de la seguridad en base a una norma de referencia como es la ISO 27001:2013.

A lo largo de 2022 no se ha registrado ninguna consulta en materia del estándar ISO 27001. No obstante, dentro del CSIRT-CV se han llevado a cabo las actividades necesarias para el mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Asimismo, en la ejecución de los análisis de riesgos se tienen en cuenta las buenas prácticas en materia de seguridad de la información establecidas por la norma ISO 27002.

13 CONSULTORÍA GENERAL

Este servicio ofrece soporte especializado ante cualquier consulta en las diferentes vertientes de la seguridad de la información: técnica, organizativa y legal.

Durante este año se han atendido cerca de 191 consultas de diferente índole relacionadas con la ciberseguridad. La mayoría de las consultas están relacionadas con los informes diarios que se emiten a las Consellerías y Organismos, pero también se tratan temas como:

- Consultas de seguridad en navegadores Web
- Formación para ciudadanos en centros educativos
- Consultas de seguridad en aplicaciones
- Consultas sobre correos phishing/maliciosos

Cabe mencionar que las consultas procedentes de ciudadanos representan entorno al 80% del total de las consultas recibidas en CSIRT-CV.

14 PLAN VALENCIANO DE CAPACITACIÓN

Este servicio ofrece acciones formativas y de concienciación en ciberseguridad que puedan resultar de relevancia para el solicitante. Las acciones pueden ser cursos on-line o presenciales, jornadas, video-tutoriales, guías específicas, etc.

Para abordar el Plan Valenciano de Capacitación (PVC), se ha definido un calendario donde se contemplan acciones concretas de formación y capacitación en materia de ciberseguridad dirigidas a los diferentes colectivos identificados: **ciudadanos**, **GVA y organismos, empresas (PYMEs)**, **otras administraciones (Ayuntamientos etc.)**

Para realizar dichas acciones se han utilizado diferentes formatos y canales de comunicación: sesiones de concienciación, ponencias, publicaciones diarias en los portales de CSIRT-CV y ConcienciaT, jornadas de ciberseguridad en centros de secundaria, publicaciones en las redes sociales del centro (Facebook[3], Twitter[4]), boletines de seguridad para suscriptores, correos electrónicos, infografías, campañas de concienciación, etc..

Las principales acciones del Plan Valenciano de Capacitación durante el año 2022 se resumen a continuación:

14.1 INFORMES PUBLICADOS

Durante 2022, CSIRT-CV ha publicado su informe de actividad correspondiente al año 2021 en el portal principal.

Este año, el material publicado por CSIRT-CV en sus principales portales ha sumado mas de 4.078 descargas.

14.2 CAMPAÑAS DE CONCIENCIACIÓN

En 2022, CSIRT-CV ha lanzado cinco campañas de concienciación en las redes sociales en las que está presente, Facebook y Twitter así como en el portal ConcienciaT[5]:

- Campaña "**10 RECOMENDACIONES DE CIBERSEGURIDAD PARA EQUIPOS DOMÉSTICOS**". El objetivo principal de esta campaña es concienciar a los usuarios de los peligros que tiene disponer de un equipo en casa. Estas recomendaciones, están basadas sobretodo en la revisión de la privacidad del usuario, mantener actualizado el software que se usa, disponer de contraseñas robustas así como utilizar buenas herramientas.

3 https://es-es.facebook.com/CSIRTCV/
4 https://twitter.com/csirtcv?lang=es
5 https://concienciat.gva.es/

Figura 2: Detalle imagen utilizada para la campaña de concienciación "10 recomendaciones de seguridad para equipos domésticos"

- Campaña "**10 ciberamenazas que han marcado 2021**". El objetivo principal de esta campaña es hacer una recopilación de las 10 ciberamenazas mas importantes que tuvieron lugar en el año 2021 así como las medidas que debemos de tomar para hacerles frente.

Figura 3: Detalle imagen utilizada para la campaña de concienciación "10 Ciberamenazas que han marcado 2021"

- Campaña "**Protege tu movil de ciberataques**". El objetivo principal de esta campaña era la protección de nuestros dispositivos móviles frente a ciberataques, así como las medidas que debemos de tomar para hacerles frente.

Figura 4: Detalle imagen utilizada para la campaña de concienciación "Protege tu móvil de ciberataques"

- Campaña "**10 recomendaciones de ciberseguridad para las vacaciones**". El objetivo principal de esta campaña es indicar una serie de medidas de seguridad que debíamos de tomar en la época de las vacaciones de verano para evitar sufrir algún ciberataque .

Figura 5: Detalle imagen utilizada para la campaña de concienciación "10 recomendaciones de ciberseguridad para las vacaciones"

- Campaña "**Aprende, durante el mes europeo de la ciberseguridsad, a protegerte del Phishing y del Ransomware**". El objetivo principal de esta campaña es indicar una serie de medidas de seguridad que debíamos de

tomar en la época de las vacaciones de verano para evitar sufrir algún ciberataque.

Figura 6: Detalle imagen utilizada para la campaña de concienciación "Aprende, durante el mes europeo de la ciberseguridad, a protegerte del Phishing y del Ransomware"

14.3 SAPS: formación online a ciudadanos

Durante 2022, en la plataforma SAPS se han formado 4.304 alumnos. En total, son 25 los cursos que CSIRT-CV ofrece en su catálogo.

El curso que más alumnos ha concentrado durante este año ha sido el de "**Reglamento General de Protección de Datos (RGPD)**"[6] con 744 alumnos, casi un 17% del total de usuarios que han realizado alguno de nuestros cursos durante el 2022. El segundo curso con más éxito ha sido "**Introducción a la seguridad informática**"[7].

14.4 PLAN DE CAPACITACIÓN EN CIBERSEGURIDAD PARA EMPRESAS

Tras poco más de un año desde la puesta en marcha del "**Plan de Capacitación en Ciberseguridad para Empresas**", CSIRT-CV sigue ofreciendo desde su portal de concienciación, la posibilidad de que las organizaciones se registren de manera

6 https://concienciat.gva.es/cursos/reglamento-general-de-proteccion-de-datos/
7 https://concienciat.gva.es/cursos/introduccion-a-la-seguridad-informatica/

gratuita para evaluar su nivel de madurez en ciberseguridad en los diferentes aspectos que engloban a una organización.

A través de la herramienta AvaluaT, se puede llevar a cabo un seguimiento y mejora continua en ciberseguridad, gracias a los consejos ofrecidos en la propia plataforma y que pueden programarse como tareas que se irán llevando a cabo para conseguir los objetivos recomendados. Además de esta herramienta, se ofrecen diferentes cursos online y videos interactivos.

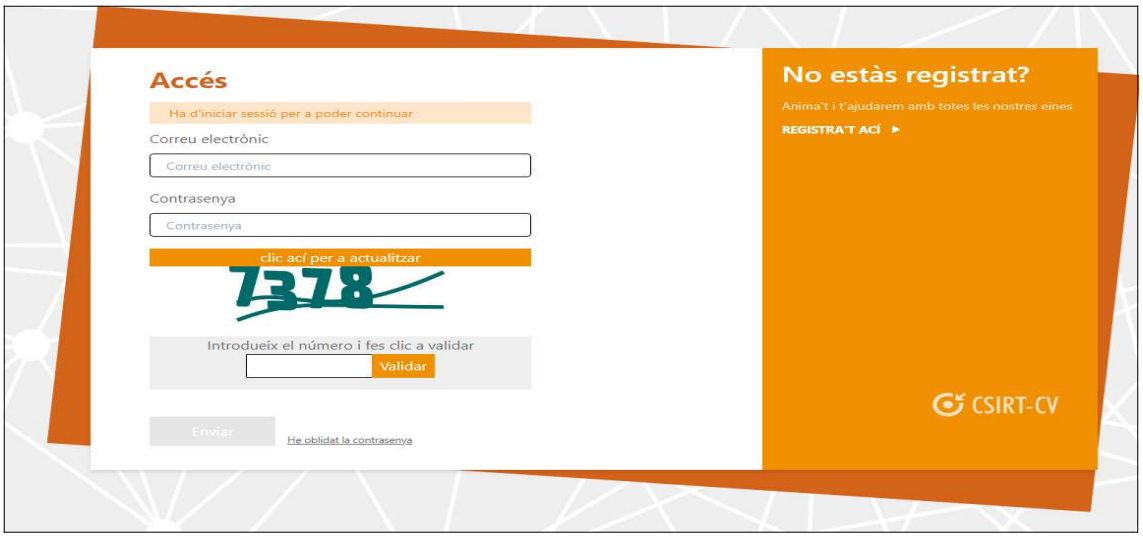


Figura 7: Acceso a AvaluaT

Asimismo, se ha llevado a cabo un estudio sobre **Ciberseguridad Industrial**[8] a nivel autonómico para medir el nivel de madurez de las empresas en la Comunitat y se están subiendo en ConcienciaT contenidos con los que se pretende ayudar a mejorar la concienciación en este sector tan creciente.

Por ultimo, se crearon **itinerarios formativos para las Entidades Locales (EELL)**[9]. Estos itinerarios tienen como objetivo capacitar a los empleados municipales, independientemente de cuál fuera su perfil, para que se convirtieran en parte activa de la ciberseguridad de su organización.

8 https://concienciat.gva.es/estudio-de-ciberseguridad-industrial/
9 https://concienciat.gva.es/entidades-locales/

14.5 JORNADAS DE CIBERSEGURIDAD EN CENTROS DE SECUNDARIA

Durante 2022 se han seguido realizando las Jornadas de Concienciación sobre Ciberseguridad en diferentes centros de educativos de la Comunitat Valenciana.

Este año se han formado un total de 7.172 personas durante estos doce meses (5.452 menores, 918 familiares y 802 docentes).

14.6

14.7 JORNADAS DE CONCIENCIACIÓN EN OTROS CENTROS

A lo largo de 2022, se han realizado otras seis jornadas de concienciación con la finalidad de mejorar el nivel de ciberseguridad. Dos de ellas en la Asociación Patronato Intermunicipal Francisco Esteve, otras dos en el SPI (Sector Público Instrumental) e instituciones, una en la casa de la cultura de Gandía dirigida a padres y otra en la organización Plena Inclusión.

14.8 MATERIAL GRÁFICO

Con motivo del "Día de Internet Segura", que se celebra anualmente el segundo martes de febrero, y que este año tenía como lema "Juntos por una Internet mejor", CSIRT-CV preparó un **video**[10] en el que se da a conocer las diferentes **campañas de concienciación**[11] elaboradas para fomentar el uso de una Internet más segura y que están accesibles desde el portal de ConcienciaT.

10 https://concienciat.gva.es/sabias_que/dia-de-internet-segura-2022/
11 https://concienciat.gva.es/tips_de_seguridad/

Además, se ha ido re-publicando en los días señalados, las **infografías**[12] que ya se tenían sobre consejos específicos, para facilitar el alcance a las mismas a un mayor número de visitantes de nuestro portal.

14.9 PORTALES PRINCIPALES Y REDES SOCIALES

Durante este 2021, el portal de **CSIRT-CV**[13] ha contado con 12.646 visitas. Se trata del portal más representativo del Centro durante años y, por tanto, cuenta con un gran número de lectores.

Durante todo el año se ha continuado con la publicación de las principales noticias y alertas relacionadas con la ciberseguridad, así como el envío mensual de los boletines a sus suscriptores.

12 https://concienciat.gva.es/infografias/
13 https://www.csirtcv.gva.es/

Figura 9: Detalle sección "Actualidad" del portal CSIRT-CV

Por otra parte, el portal enfocado a la concienciación en ciberseguridad (**concienciaT**) también ha mantenido y ampliado su actividad con nuevas publicaciones, donde destacan las campañas "**10 Recomendaciones de ciberseguridad para equipos domésticos**[14]", "**10 Ciberamenazas que han marcado 2021**[15]", "**Protege tu móvil de ciberataques**[16]", "**10 recomendaciones de ciberseguridad para las vacaciones**[17]" y "**Aprende, durante el mes europeo de la ciberseguridad, a protegerte del Phishing y del Ransomware**[18], los múltiples post mensuales publicados en la sección "**¿Sabías que…?**[19]", relacionados con la "**ataques a tarjetas de crédito**[20]", "**Estudio de ciberseguridad industrial**[21]", "**CSIRT-CV pone en marcha el plan de formación para Entidades Locales**[22]", "**El plan de choque de Ciberseguridad para las EELL de la Comunitat Valenciana, de la dirección general de las Tecnologías de la**

14 https://concienciat.gva.es/tips_de_seguridad/campana-csirt-cv-diez-recomendaciones-de-ciberseguridad-para-equipos-domesticos/
15 https://concienciat.gva.es/tips_de_seguridad/10-ciberamenazas-que-han-marcado-2021/
16 https://concienciat.gva.es/tips_de_seguridad/protege-tu-movil-de-ciberataques/
17 https://concienciat.gva.es/tips_de_seguridad/diez-recomendaciones-de-ciberseguridad-para-las-vacaciones/
18 https://concienciat.gva.es/tips_de_seguridad/aprende-durante-el-mes-europeo-de-la-ciberseguridad-a-protegerte-del-phishing-y-del-ransomware/
19 https://concienciat.gva.es/sabias_que/
20 https://concienciat.gva.es/sabias_que/manos-arriba-esto-es-un-carding-tu-dinero-en-peligro/
21 https://concienciat.gva.es/sabias_que/estudio-de-ciberseguridad-industrial/
22 https://concienciat.gva.es/sabias_que/csirt-cv-pone-en-marcha-el-plan-de-formacion-para-entidades-locales/

Información recibe el premio AUTELSI[23]", "**CSIRT-CV PARTICIPA EN EL MES EUROPEO DE LA CIBERSEGURIDAD (ECSM)**[24]", donde además se preparó un vídeo donde se da a conocer las diferentes campañas de concienciación que se ha elaborando para fomentar el uso de una Internet más segura, así como una campaña de CSIRT-CV **"Protege tu móvil de ciberataques"**[25]" con la que se quería enfocar en los diferentes ataques que pueden sufrir los dispositivos móviles. Este portal ha tenido 22.164 visitas durante el periodo.

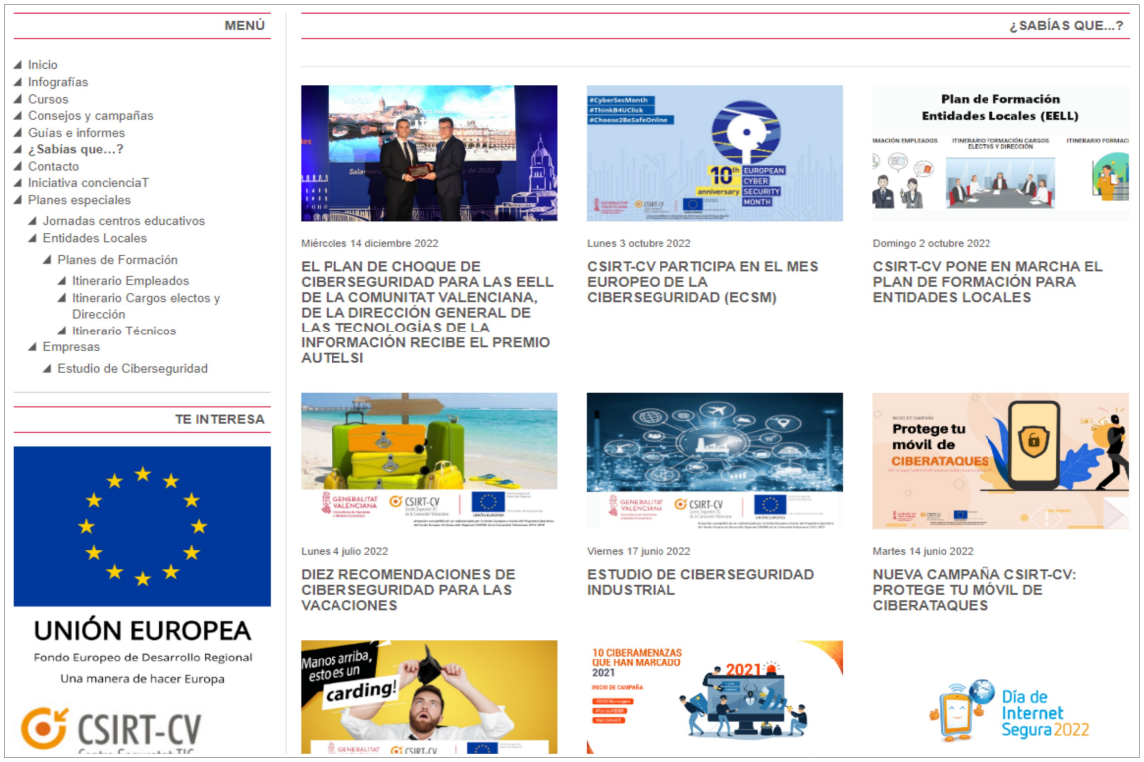


Figura 10: Detalle sección "¿Sabías que...?" del portal concienciaT

Respecto a redes sociales, CSIRT-CV cuenta en "**Facebook** [26]" con 2.287 seguidores y cerca de 6.481 en "**Twitter** [27].

23 https://concienciat.gva.es/sabias_que/csirt-cv-participa-en-el-mes-europeo-de-la-ciberseguridad-ecsm/
24 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/
25 https://concienciat.gva.es/sabias_que/nueva-campana-csirt-cv-protege-tu-movil-de-ciberataques/
26 https://es-es.facebook.com/CSIRTCV/
27 https://twitter.com/CSIRTCV

15 DETECCIÓN DE INTRUSOS

Este servicio detecta los intentos de intrusión o incidentes que afecten a equipos y servicios del dominio protegible de la Generalitat.

15.1 FUENTES INTEGRADAS Y MEJORAS EN EL SIEM

Este año se han continuado integrado distintas fuentes según las necesidades del centro o de las distintas Consellerias u organismos para mejorar la detección, fiabilidad y, al mismo tiempo, dotar de más contexto a los posibles incidentes de seguridad.

Por último, indicar que se ha realizado una serie de mejoras significativas en el SIEM, sobre todo en el motor de correlación avanzada permitiendo, por ejemplo, aplicar excepciones más precisas en ciertas reglas, mejorar la visualización del contenido de las alertas procedentes de determinadas fuentes, añadir campos para valores adicionales que permitan aumentar el nivel de complejidad de las reglas de correlación, etc.

16 TENDENCIAS EN CIBERATAQUES

El año pasado se produjeron varios incidentes críticos en nuestro ámbito, algunos de ellos fueron incidentes de ransomware y tuvieron un gran impacto en las administraciones. Como respuesta a este aumento de incidentes críticos, especialmente afectando a los ayuntamientos, se llevó a cabo un plan de choque para reforzar la seguridad. De este plan nació un equipo específico para gestionar incidentes en las entidades locales, que aunque forma parte de CSIRT-CV, está especializado y puede dar un servicio más rápido y eficiente a ellos a la vez que colabora con el equipo del proyecto original.

En cuanto a los tipos de ataques que se han dado, se encuentran aquellos que afectan a recursos PHP, como por ejemplo el xmlrpc.php, ataques utilizando exploits que se aprovechan de vulnerabilidades en Apache, así como ataques de ejecución remota de código. Cabe destacar los ataques recibidos intentando explotar la vulnerabilidad de ejecución remota de código que afectaba al módulo log4j.

También se han producido ataques web con el objetivo de obtener información, como los ataques SQL Injection, y en menor medida los ataques cross-site scripting.

Respecto a los ataques de denegación de servicio, se ha recibido menos cantidad respecto al año anterior, sin que ninguno tuviera impacto en la organización, debido al bajo volumen de tráfico generado en el ataque y a las medidas delegadas en el proveedor de Internet.

Se ha recibido multitud de campañas de phishing, que ya vienen siendo habituales en nuestro ámbito, suplantando instituciones como la Agencia Tributaria, Seguridad Social, Correos, empresas de mensajería, bancos, e incluso la propia Generalitat Valenciana. Estos últimos son los que prestamos mayor atención, por su impacto y peligrosidad.

Entre la multitud de casos de phishing, cabe destacar uno de ellos que simulaba una página de login de Generalitat. Utilizaba logos oficiales y pedía las credenciales al usuario. Afortunadamente, ningún usuario cayó en el engaño y ninguna cuenta fue comprometida.

En cuanto a la procedencia de los ciberataques por países, se ha identificado como los cinco principales a China, Estados Unidos, España y Rusia, seguidos por Holanda y Alemania. Es importante recordar que la geolocalización desde la que se recibe el ataque no necesariamente corresponde con el origen del atacante, y que en la atribución a esos cinco países influye también el hecho de que en los mismos se concentre un mayor volumen de equipos y de servicios, por lo que existe una también mayor probabilidad de recibir ataques desde allí.

17 DETECCIÓN DE APT

El servicio de detección de Amenazas Persistentes Avanzadas (APT) se gestiona mediante la herramienta CARMEN desarrollada por el Centro Criptológico Nacional (CCN) y S2 Grupo. La herramienta ha sido actualizada a su última versión y los analistas de CARMEN del CSIRT-CV asisten de manera periódica a formación especializada para explotar dicha herramienta con la mayor eficacia.

Este año se ha reportado un total de 19 incidentes originados detectados vía “Threat Hunting” en CARMEN, siendo 3 de ellas de nivel alto y 25 de criticidad media.

Mencionar que la capacidad de detección de CARMEN sigue aumentado, ya que se continua desplegando Claudia, el endpoint de CARMEN. Además, durante este año se ha vuelto a dotar de más capacidades para la ingesta y conservación de datos.

Cabe indicar también que durante el transcurso del año, se ha continuado trabajando en la herramienta mediante la configuración de analizadores, plugins e IOCs, ajustándolos al modelado de amenazas que más afectan dentro del alcance. Esto supuso un incremento en la inteligencia de análisis de Carmen al pasar de 1.360 a 1.420 indicadores de Compromiso (IOC), de 2.206 a 2.295 analizadores y de 2.118 a 2.226 plugins, con el objetivo de identificar más amenazas y más dirigidas contra GVA.

18 INFORMES Y ALERTAS. OBSERVATORIO

CSIRT-CV, en su función de Centro de Alerta Temprana, elabora una serie de informes sobre tendencias en seguridad y otros aspectos de interés para su ámbito entre los que destacan boletines de alerta puntuales, boletines públicos de seguridad mensual, emisión diaria de informes personalizados a cada organismo o informes sobre malware.

Este año, CSIRT-CV ha enviado un total de 14 boletines mensuales y 171 boletines de alertas.

18.1 OBSERVATORIO DE SEGURIDAD

El año 2022 supuso el regreso a la normalidad tras los periodos de confinamiento y restricciones en la actividad cotidiana y en el trabajo. En este periodo, se ha tenido tiempo de revisar la seguridad en aquellos accesos remotos que se tuvieron que preparar con tanta celeridad y que supuso un riesgo y el punto de entrada de importantes incidentes de seguridad en algunas organizaciones.

Vinculado a esto, se ha seguido trabajando en controlar y reforzar el uso de los accesos remotos a los sistemas internos de GVA, así como la compartición de archivos, VPN no autorizadas o P2P, enfocadas en evitar el robo o la fuga de información sensible.

Otro punto a destacar viene a raíz de la invasión de Ucrania por parte de Rusia. Se creó un comité de crisis de ciberseguridad en el que participaron los responsables de seguridad de la administración central y las comunidades autónomas. De este comité

salió un documento que estableció un conjunto de medidas a aplicar. A fecha de redacción del presente informe, destacamos el uso de 2FA en los servicios de acceso remoto, monitorización de VPN y el cambio de credenciales de todas las cuentas del dominio.

Por otro lado, en mayo de 2022 se pasó la auditoría de seguimiento para el cumplimiento de la UNE-ISO/IEC 27.001:2014. A este respecto, CSIRT-CV sigue trabajando y mejorando continuamente su seguridad en cumplimiento de los controles y requisitos de la Norma, ampliando y abordando nuevos riesgos emergentes, coadyuvando en la adecuación al ENS de los sistemas horizontales de la DGTIC, y siendo una referencia como centro de alerta temprana ante cualquier amenaza.

Para mejorar la calidad de los desarrollos propios, se lanzó junto con el Servicio de Proyectos TIC y Calidad de la DGTIC un proyecto de mejora del Sello de Excelencia, donde se está desarrollando un procedimiento de validación del código en función del nivel ENS que se le asigne. En concreto, se está trabajando en mejorar el análisis estático con la herramienta SonarQube y se ha desplegado el portal ANA, del CCNCERT, para consultar y gestionar las vulnerabilidades detectadas por CSIRT-CV.

Siguiendo con indicadores de calidad, se está trabajando en trasladar los KPI que se manejaban manualmente en CSIRT-CV para llevarlos de forma más automática a la herramienta de Business Intelligence de la DGTIC.

Respecto a los incidentes que han podido tener un mayor impacto, junto a los ransomware en ayuntamientos, destacar un incidente de ransomware que afectó a varios centros de investigación y que tuvo su origen en un proveedor de una aplicación instalada que tenía acceso de forma remota a los activos. Aprovecharon este acceso para desplegar el ransomware e intentar afectar a otros servidores. Afortunadamente, al no estar en el mismo dominio de Windows, el ataque solo afectó a dichos servidores administrados por el proveedor y pudieron recuperar el servicio de copia de seguridad. Esto no hace más que evidenciar la necesidad de tener un registro de proveedores y accesos externos permitidos y securizarlos al máximo.

Siguiendo por las tareas de mejora continua en el refuerzo de la seguridad y buscando ampliar los puntos donde se está monitorizando, se abordó un plan de despliegue de una solución endpoint, que permite tener una visión más completa de lo que ocurre dentro de una red, siendo su objetivo principal la detección de malware complejo y movimiento lateral relacionado con APT.

Entre los eventos internacionales, destacamos la participación en el CyberEurope 2022, evento bienal organizado por ENISA y que reúne a cientos de participantes europeos en un ejercicio completo y complejo de dos días de duración. Esta edición puso el foco en el sector sanitario, por lo que también participaron en él la Conselleria de Sanidad Universal y Salud Pública, representados por la Oficina de Seguridad de la Información y diversos hospitales y centros de salud, así como representantes de la industria farmacéutica y algunos proveedores de servicios Cloud.

Completaban la participación española los CERTs nacionales de referencia y el DSN, quien representó a España en el ejercicio y seleccionó a los participantes.

El segundo evento internacional a destacar fue la Cumbre de la OTAN 2022 en Madrid, marcado por el aumento del riesgo de ciberataque debido a la invasión de Ucrania por parte de Rusia. Se estableció un operativo en el que se aplicaron unas cuarentenas a una lista de direcciones IP maliciosas. Se reforzó la monitorización de alertas que pudieran venir de Rusia y Bielorrusia, así como los correos que tuvieran relación con dicha cumbre. Afortunadamente, no se detectó ninguna amenaza al respecto y el operativo se canceló después de dos semanas tras la finalización de la cumbre.

Entre las actividades públicas de CSIRT-CV, destaca la XXIII Reunión de Ciberseguridad de la Comisión Sectorial de Seguridad, organizada por el Centro Criptológico Nacional (CCN) en la que se puso de nuevo a CSIRT-CV y al proyecto de EELL como modelos de referencia para el resto de comunidades autónomas en la prestación de servicios de seguridad para las administraciones públicas.

Otro acto público de relevancia fue la visita de la ministra de Ciencia e Innovación, la valenciana Diana Morant, con motivo de la XI Conferencia Española del programa Horizonte Europa. El objetivo de la visita fue conocer de primera mano el trabajo realizado en la protección y respuesta a incidentes de seguridad que se realiza en CSIRT-CV.

Finalmente, el ransomware sigue siendo la mayor preocupación de las organizaciones (especialmente en las que forman parte de las infraestructuras críticas) y ha tenido repercusión en ciertos organismos nacionales. Destacar un posible cambio en estos incidentes, pasando de cifrar la información y solicitar un rescate para recuperarla a amenazar con publicarla si no se satisface el pago en el plazo requerido.

19 CIBERSEGURIDAD INDUSTRIAL

Este servicio busca mejorar el nivel de ciberseguridad industrial de los sistemas SCADA gestionados por organismos de la Generalitat y las II.CC. De la Comunitat Valenciana.

Durante 2022 se ha seguido con proyectos que se empezaron en el año 2021 y se han iniciado nuevos, que darán forma a la ciberseguridad industrial dentro del CSIRT-CV. Con este fin, se han iniciado siete proyectos, cuatro de ellos principalmente enfocados en I+D+i, el desarrollo de capacidades dentro del CSIRT-CV y en su establecimiento como referente en materia de ciberseguridad industrial.

Los proyectos iniciados son:

1. Entorno médico
2. Honeynet
3. SmartCity
4. Publicación Vulnerabilidades OT
5. Estudio de ciberseguridad industrial en la Comunitat Valenciana
6. Infografías
7. Formación
8. eSondas SAT-ICS

El primero de los proyectos, **"Entorno médico"**, consiste en el desarrollo de un entorno de pruebas basado en una unidad de radiología de un hospital. El entorno consta de una simulación de las diferentes modalidades (dispositivos médicos dedicados a la imagen médica) y su uso mediante el protocolo DICOM.

El segundo de los proyectos, **"Honeynet"**, consiste en el desarrollo de 8 honeypots de las diferentes industrias representativas de la Comunitat Valenciana. Además, análisis de los intentos de ataques realizados a la honeynet y formación respectiva.

El tercero de los proyectos, **"SmartCity"**, contará con un entorno físico que simula diferentes módulos representativos de una ciudad inteligente como son la gestión de: tráfico, residuos urbanos, luminarias y cargadores de vehículos eléctricos.

El cuarto de los proyectos, **"Publicación Vulnerabilidades OT"**, tiene como objetivo, la creación de un nuevo servicio en la página web de CSIRT-CV donde se publicarán las vulnerabilidades críticas relacionadas con los sistemas industriales.

El quinto de los proyectos, **"Estudio de ciberseguridad industrial en la Comunitat Valenciana"**, tiene como objetivo la realización de encuestas a diferentes empresas con sede en la Comunitat Valenciana para conocer eel grado de madurez de dichas empresas a través del análisis de los resultados.

El sexto de los proyectos, **"Infografías"**, consiste en la elaboración de material relacionado con la industria. Las infografías realizadas son: programas de ayudas de ciberseguridad industrial e IoT para organizaciones.

El séptimo de los proyectos, **"Formación"**, tiene como objetivo el desarrollo de formación relacionada con los sistemas industriales. Estos proyectos se encuentran en un estado inicial.

El ultimo de los proyectos, **"eSondas SAT-ICS"**, tiene como objetivo la colaboración con diferentes organizaciones para comenzar a implantar sondas de monitorización de protocolos industriales.

20 SISTEMAS DE DECEPCIÓN

Este servicio busca la detección temprana de intrusiones, la implementación de mecanismos de distracción y retraso para posibles atacantes, análisis de tendencias y mejora de los mecanismos defensivos a partir de la información recopilada.

La plataforma de *deception* de CSIRT-CV se encuentra en una fase estable, aunque todavía se continua con los procesos de ocultar el fingerprint, diseño y despliegue de nuevos dockers.

Por otra parte, comentar que desde CSIRT-CV se sigue trabajando en la definición de la información más importante que se desea obtener y cual es la mejor forma de procesarla.

Figura 11: *Dashboard Honeynet CSIRT-CV*

21 SERVICIO I+D+i

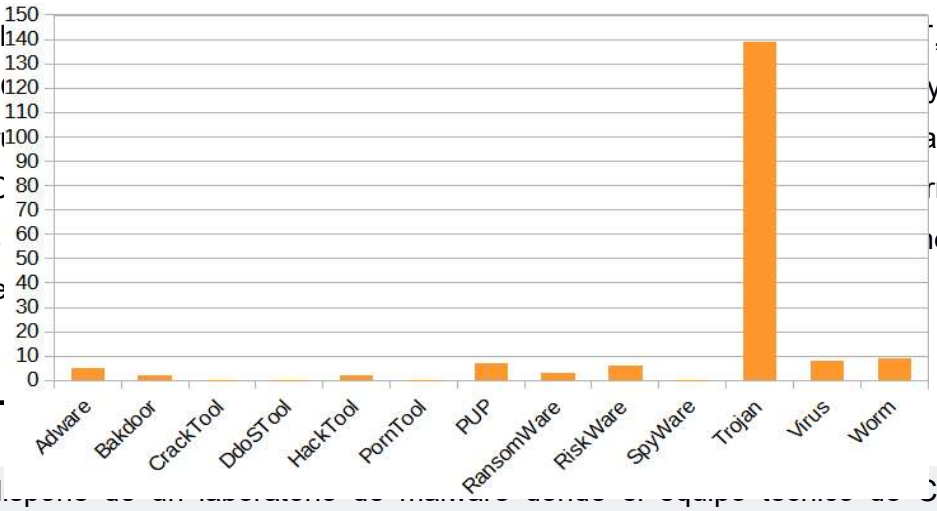
Durante 2022, el equipo de CSIRT-CV ha participado en diferentes proyectos internos de investigación con el objetivo de mejorar nuestros servicios. Destacan los siguientes:

- Mejoras en el servicio de correlación avanzada con el desarrollo de un piloto de correlador multifuente basado en programación orientada a objetos que aporta mayor flexibilidad en la integración de fuentes y diseño de reglas de correlación así como en el diseño de excepciones.
- En la plataforma de Ciber Threat Intelligence (CTI) MISP, debido a diversos problemas de rendimiento se realizó un exhaustivo trabajo en cuanto a su configuración para que operase de la forma más eficientemente posible. Los cambios llevados a cabo se tradujeron en modificaciones en tiempos de respuesta de Apache/PHP, así como en mejoras en la gestión de peticiones y

bloques en la base de datos. Por otro lado, a nivel de inteligencia, a lo largo de este primer semestre se ha trabajado en la generación de listas de indicadores de compromiso para ponerlas a disposición de los interesados.

22 INTERCAMBIO DE INFORMACIÓN

Servicio intercambio de información relativa a ciberseguridad tanto en la Generalitat Valenciana como en empresas de la Comunitat.



Entre l , a través de LU y también S2 Gr alizadores para C rmación a través ensajería despl

23 L

Se d CSIRT-CV puede analizar artefactos para medir de un modo preciso el impacto y consecuencias reales de posibles códigos maliciosos en los activos de la Generalitat y de este modo diseñar las medidas de contención y erradicación más adecuadas en cada caso.

Este servicio vio incrementadas sus capacidades notablemente en 2018 con el despliegue de un laboratorio físico y una Sandbox. Durante 2019 se ha continuado el trabajo de automatización y extracción de inteligencia y en 2020 alcanza su estabilidad como servicio con una mayor capacidad de procesado y automatización de datos. Durante 2022, se continua mejorando y adaptando dichos sistemas a las nuevas técnicas y necesidades detectadas.

23.1 TENDENCIAS DE MALWARE

El estudio de los resultados obtenidos por el laboratorio de malware proporciona al equipo de seguridad, las nuevas tendencias empleadas por los ciberatacantes, como:

- La utilización de nuevas vulnerabilidades que están siendo aprovechadas.
- Nuevos formatos de fichero para la distribución de malware.
- Mejoras en los mecanismos de detección y categorización de amenazas.

En el transcurso del año 2022, el laboratorio ha analizado 1.476 archivos, la mayoría provenientes de la plataforma de antivirus corporativo.

De los 1.476 ficheros analizados, 181 archivos han sido detectados como maliciosos y categorizados dependiendo de la funcionalidad de cada uno. En la siguiente tabla se puede comparar la cantidad de programas maliciosos detectados por tipología:

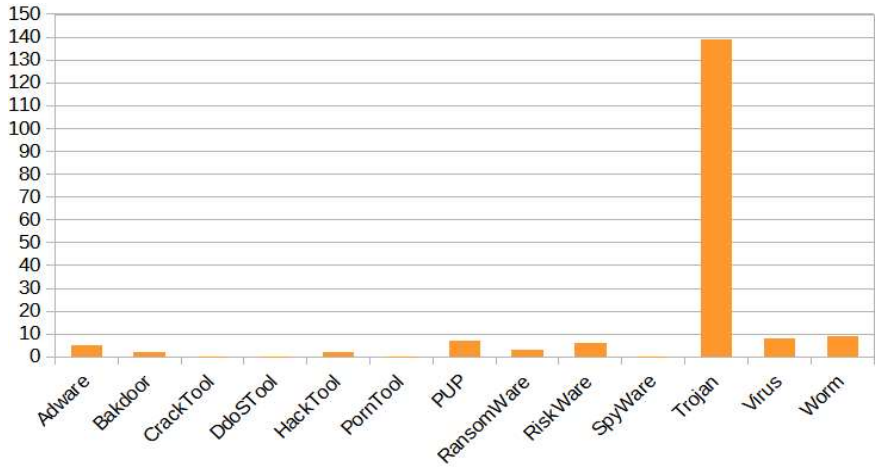


Figure 12: Cantidad de programas maliciosos detectados por tipo.

En la mayoría de estos ficheros analizados, se han encontrado capacidades de tipo *stealer*, las cuales buscan robar credenciales de aplicaciones instaladas en el equipo (clientes FTP, correo, conexiones remotas, etc.), credenciales almacenadas por los diferentes navegadores y captura de credenciales introducidas por el usuario en formularios web.

El resto de los ficheros analizados son documentos detectados en primera instancia cómo posibles ficheros maliciosos, en los cuales se ha comprobado al realizar el análisis, que no contenían código dañino.

Del mismo modo, los formatos y extensiones de los documentos analizados suelen ser en su mayoría ficheros ofimáticos y ficheros ejecutables PE.

Durante 2022, se ha continuado observando la misma tendencia del año anterior en la cual se utilizan los documentos ofimáticos, tanto en formato PDF como Office, para la descarga de malware. Esto representa entorno al 91% del total de documentos analizados.

Respecto a los ficheros ejecutables, se ha detectado una gran cantidad de código malicioso con capacidad de monitorización de equipos, *stealers*, cómo pueden ser Emotet, Mekotio y Grandoeiro que tiene el objetivo de robar usuarios y contraseñas de los equipos que infectan mediante robo de archivos y capacidades de *keylogging*. Otro de los malwares, que mayor incremento ha tenido, ha sido el malware de tipo gusano llamado Raspberry Robin. El propósito de este malware es el de tomar el control parcial o total de un dispositivo, mantener el acceso e incluso la distribución de ransomware.

A continuación, en la gráfica se puede comprobar qué tipos de ficheros son los más usados a la hora de distribuir código malicioso.

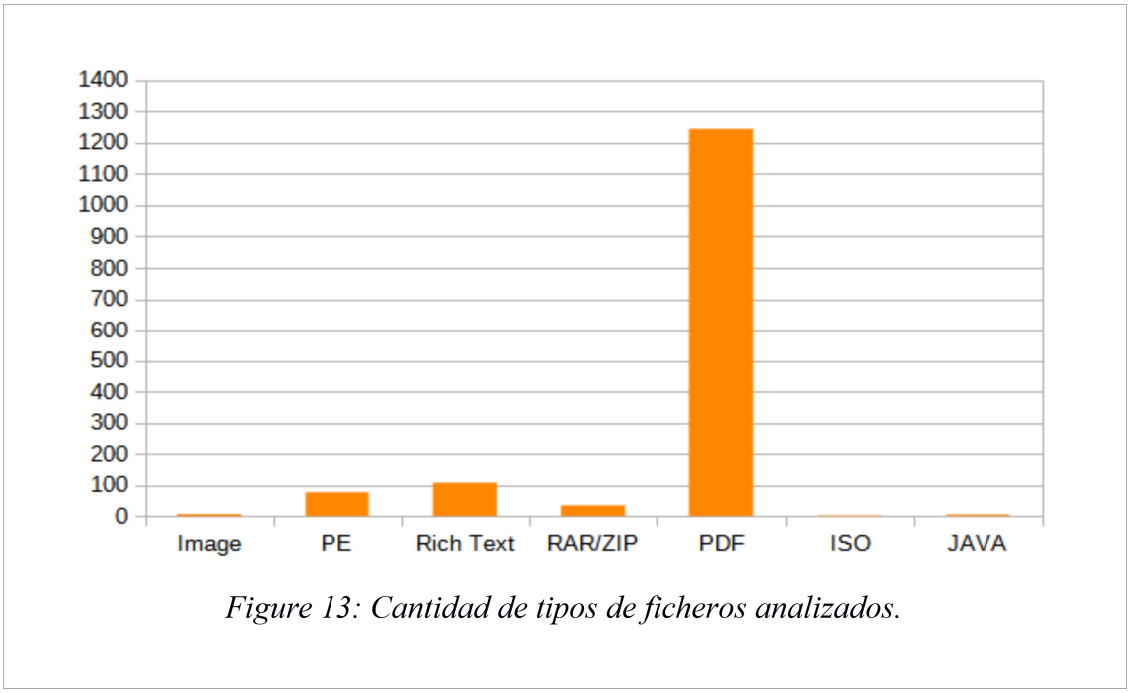


Figure 13: Cantidad de tipos de ficheros analizados.

Por otro lado, en los incidentes de tipo phishing o relacionados con el correo electrónico, gestionados por el equipo de CSIRT-CV, se ha detectado una gran

cantidad de ficheros ofimáticos de tipo PDF tratando de engañar al usuario que lo recibe para navegar por diferentes URL maliciosas, evitando así que las direcciones IP o dominios puedan ser verificadas con herramientas de seguridad automáticas existentes en las soluciones de correo electrónico, dificultando su análisis. Por esta razón, los ficheros de tipo PDF son también uno de los ficheros más detectados como vía de entrada de malware.

A grandes rasgos, si se analiza la cantidad de ficheros detectados por tipo, se puede comprobar que las tendencias empleadas por los atacantes denotan el uso de diferentes técnicas, siendo la principal el correo, cómo puerta de entrada en la organización. En 2021, los documentos ofimáticos como PDF y ejecutables eran la principal vía de entrada de malware, y esta tendencia se mantiene durante 2022.

Respecto a las capacidades de detección y análisis de ficheros maliciosos, durante el pasado ejercicio, se ha dedicado un gran esfuerzo en la optimización de herramientas automatizadas de análisis dinámico y en la integración con el resto de herramientas del parque.

24 MONITORIZACIÓN DE SERVICIOS WEB

Este servicio ofrece respuesta en tiempo real ante cualquier tipo de manipulación ilícita a los servicios web de la Generalitat.

Este servicio monitoriza los principales sitios web de la Generalitat, tanto por alcance de los mismos, como por su criticidad. Dada la naturaleza de la información de este servicio, no se ofrecen más detalles públicamente.

25 PROMOCIÓN DEL CENTRO Y PLAN DE COMUNICACIÓN

Servicio enfocado a la comunicación y conocimiento de la actividad de CSIRT-CV a diferentes colectivos de la Comunitat Valenciana para fomentar un cambio de hábito general en la sociedad valenciana en pro de una mejora de la seguridad global de la ciudadanía.

Este servicio se ha desarrollado en 2022 a través de diferentes acciones, que se enumeran a continuación.

25.1 EVENTOS Y JORNADAS

CSIRT-CV ha participado en 2022 en los siguientes eventos:

- XI Conferencia Española del Programa Marco de Investigación e Innovación de la Unión Europea Horizonte Europa (Abril, 2022). La ministra de Ciencia e Innovación, **Diana Morant**, visita CSIRT-CV aprovechando la ocasión.
- El director general de Tecnologías de la Información y las Comunicaciones, José Manuel García Duarte, y la jefa de servicio de Confianza Digital, Lourdes Herrero realizan una ponencia en ATIAL (Junio, 2022).
- CSIRT-CV participa en el Cyber Europe 2022 organizado por ENISA y que reúne a cientos de participantes europeos en un ejercicio completo y complejo de dos días de duración (Junio, 2022):

12/06/2022

- Cyber Europe 2022 està organitzat per Enisa, l'Agència de la Unió Europea per a la Ciberseguretat
- El Centre de Seguretat TIC de la Comunitat Valenciana i la Conselleria de Sanitat participen en aquesta edició, centrada en el sector sanitari
- Els ciberexercicis simulen incidents a gran escala de ciberseguretat per a provar i entrenar la cooperació transeuropea i nacional

La Generalitat ha participat aquest mes de juny en Cyber Europe 2022, l'esdeveniment més important de simulació de ciberatacs o ciberexercici que té lloc a tot el món i que en aquesta edició s'ha centrat en el sector sanitari.

La Generalitat, a través del Centre de Seguretat TIC de la Comunitat Valenciana (CSIRT-CV) i la Conselleria de Sanitat Universal i Salut Pública, ha sigut una de les entitats públiques i privades europees que han participat en el ciberexercici. Cyber Europe persegueix posar a prova la cooperació nacional i europea mitjançant una simulació de resposta a incidents informàtics a gran escala i davant de crisis de ciberseguretat, així com aplicar els coneixements adquirits sobre coordinació entre els equips de resposta a incidents de seguretat, CSIRT en el cas de la Comunitat Valenciana.

Tal com ha apuntat el conseller d'Hisenda, Arcadi España, "la participació de la Generalitat en Cyber Europe suposa una oportunitat única de col·laborar amb centres especialitzats de tot Europa en la lluita contra els ciberdelinqüents, però també un important aprenentatge".

Així, el responsable d'Hisenda ha destacat "la importància de la cooperació institucional en matèria de ciberseguretat, ja que ens ajuda al fet que els nostres equips siguen coneixedors dels últims procediments existents per a protegir les dades de la ciutadania que custodia l'Administració i donar el suport necessari a empreses privades i altres administracions i institucions, com ara diputacions i entitats locals, en la lluita per la ciberseguretat".

Per part seua, el conseller de Sanitat, Miguel Mínguez, ha assegurat que "amb els resultats obtinguts i després de l'exercici d'anàlisi podrem estar preparats davant de possibles bretxes de seguretat i reforçar en el que calga la nostra capacitat de resposta". "La ciberseguretat dels nostres serveis i infraestructures de salut és crítica, especialment en un món connectat com ara l'actual, que viu noves amenaces davant de les quals hem de continuar protegint les dades i la salut de la ciutadania", ha conclòs el conseller de Sanitat.

Recentment, la Conselleria de Sanitat ha rebut el premi Isaca València 2022 en la categoria de seguretat de sistemes d'informació.

El ciberexercici ha sigut organitzat per l'Agència de la Unió Europea per a la Ciberseguretat (Enisa) i hi han participat més de 800 experts europeus en ciberseguretat per a avaluar la disponibilitat i la integritat dels sistemes d'informació.

- Lourdes Herrero participa en el XXII Encuentro de Técnicos Informáticos en Villena y habla sobre el I Plan de Choque de Ciberseguridad de la Generalitat para las Entidades Locales Valencianas (Noviembre, 2022).

- CSIRT-CV participa en el mes europeo de la ciberseguridad (ECSM) (octubre, 2022).

26 PRESENCIA EN MEDIOS

Tal y como se ha comentado anteriormente, CSIRT-CV ha estado presente en varios eventos a lo largo del año, por lo que ha aparecido en diferentes medios de comunicación:

Celebración de la XI Conferencia Española del Programa Marco de Investigación e Innovación de la Unión Europea Horizonte Europa con la participación de la ministra de Ciencia e Innovación, **Diana Morant**, y visita a las instalaciones del centro:

- Ministerio de Ciencia e Innovació [28]

Participación en la **VII Jornada ATIAL "Retos de la Ciberseguridad en la Administración Local**", donde Lourdes Herrero habló de ciberseguridad y de las ayudas que el CSIRTCV está aportando a las AAPP:

- Twitter [29]

Asistencia al **Cyber Europe 2022** organizado por ENISA:

- ENISA [30]
- ENISA [31]
- INCIBE [32]

Participación en el "**XXII Encuentro de Técnicos Informáticos en Villena**", donde Lourdes Herrero habló sobre el I Plan de Choque de Ciberseguridad de la Generalitat para las Entidades Locales Valencianas :

- Cadena Ser [33]
- El periódico de Villena [34]

28 https://www.ciencia.gob.es/Noticias/2022/Abril/Diana-Morant-destaca-el-impulso-de-Horizonte-Europa-a-la-cultura-del-conocimiento-y-la-innovaci-n-en-el-tejido-productivo-espa-ol.html
29 https://twitter.com/ATIAL_ES/status/1540460551201034250
30 https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme
31 https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2022
32 https://www.incibe.es/sala-prensa/notas-prensa/incibe-participa-los-cyber-europe-2022-organizados-enisa
33 https://cadenaser.com/comunitat-valenciana/2022/11/28/el-xxii-encuentro-de-tecnicos-municipales-informaticos-en-villena-analiza-la-introduccion-de-la-robotica-en-la-administracion-publica-y-los-mecanismos-de-seguridad-cibernetica-radio-villena/
34 https://elperiodicodevillena.com/villena-punto-de-encuentro-de-los-tecnicos-informaticos-municipales-de-la-comunidad/

- Villena [35]

El Consell recibe el premio **Autelsi** al sector público por el plan de choque de ciberseguridad para entidades locales:

- Valencia Plaza [36]
- ConcienciaT [37]

La Generalitat lanza una **campaña para combatir los ciberataques de 'phishing' y 'ransomware':**

- Europa Press [38]
- Entre las provincias que más ciberdelitos sufren destacan Valencia y Alicante:
  - La Vanguardia [39]
- Las mejoras y los cursos de valenciano suben las matriculaciones un 50% en el portal SAPS:
  - Valencia Plaza [40]

Las campañas de concienciación, como es habitual, también tienen mucha repercusión en prensa. La primera campaña de concienciación puesta en marcha por CSIRT-CV este año se tituló "***10 Recomendaciones de CiberSeguridad para equipos domésticos***", cuyo objetivo principal de esta campaña era concienciar a los usuarios de los peligros que tiene disponer de un equipo en casa. Prensa GVA y varios medios se hacen eco de esta nueva campaña:

- ConcienciaT [41]
- Blog Lexgoapp [42]

A mediados de año se lanzaron otras campañas, como por ejemplo, "***10 Ciberamenazas que han marcado 2021***", cuyo objetivo principal de esta campaña

35 https://www.villena.es/noticia/villena-acoge-el-xxii-encuentro-anual-de-tecnicos-informaticos-municipales-para-abordar-los-retos-en-ciberseguridad-y-automatizacion-robotica-de-la-administracion/
36 https://valenciaplaza.com/consell-recibe-premio-autelsi-sector-publico-plan-choque-ciberseguridad-entidades-locales
37 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/
38 https://www.europapress.es/comunitat-valenciana/noticia-generalitat-lanza-campana-combatir-ciberataques-phishing-ransomware-20221004120834.html
39 https://www.lavanguardia.com/local/valencia/20220830/8490339/valencia-alicante-provincias-mas-ciberdelitos-sufren.html
40 https://valenciaplaza.com/mejoras-cursos-valenciano-suben-matriculaciones-50-portal-saps
41 https://concienciat.gva.es/tips_de_seguridad/campana-csirt-cv-diez-recomendaciones-de-ciberseguridad-para-equipos-domesticos/
42 https://lexgoapp.com/blog/el-50-de-los-ciberataques-que-sufren-las-empresas-ya-llevan-el-sello-del-software-malicioso-ransomware/

era hacer una recopilación de las ciberamenazas mas importantes que tuvieron lugar en el año 2021 así como las medidas que debemos de tomar para hacerles frente. "***Protege tu móvil de ciberataques***", cuyo objetivo principal de esta campaña era la protección de nuestros dispositivos móviles frente a ciberataques, así como las medidas que debemos de tomar para hacerles frente. "***10 recomendaciones de ciberseguridad para las vacaciones***", cuyo objetivo principal de esta campaña era las medidas que debíamos de tomar en la época de las vacaciones de verano para evitar sufrir .

También en esta ocasión, prensa de GVA y varios medios se hacen eco de la campaña:

- La Vanguardia [43]
- Europa Press [44]
- Diario de Alicante [45]
- ConcienciaT [46]
- ConcienciaT [47]

A finales de año, se lanzó una ultima campaña, "***Aprende, durante el mes europeo de la ciberseguridsad, a protegerte del Phishing y del Ransomware***", cuyo objetivo principal de esta campaña era hacer una recopilación de las medidas que debemos de tomar para hacerles frente. También en esta ocasión, prensa de GVA y varios medios se hacen eco de la campaña:

- ConcienciaT [48]

A continuación, se muestra una serie de capturas de pantalla que reflejan la difusión en la red social Twitter de la presencia en medios de CSIRT-CV:

43 https://www.lavanguardia.com/local/valencia/20220613/8336276/generalitat-lanza-campana-mostrar-ciudadania-como-proteger-movil-frente-ciberataques.html
44 https://www.europapress.es/comunitat-valenciana/noticia-proteger-movil-ciberataques-generalitat-lanza-uan-campana-ciudadania-20220613142650.html
45 https://diariodealicante.net/generalitat-campana-ciberataques-phishing-ransomware/
46 https://concienciat.gva.es/tips_de_seguridad/diez-recomendaciones-de-ciberseguridad-para-las-vacaciones/
47 https://concienciat.gva.es/tips_de_seguridad/protege-tu-movil-de-ciberataques
48 https://concienciat.gva.es/tips_de_seguridad/aprende-durante-el-mes-europeo-de-la-ciberseguridad-a-protegerte-del-phishing-y-del-ransomware/

GVA Hisenda
@GVAhisenda

La ministra de Ciència @CienciaGob, @DianaMorantR, visita les instal·lacions de @CSIRTCV i @GVADgtic per a conèixer el treball de l'equip de ciberseguretat de @generalitat, eixemple pel seu treball i coordinació entre administracions i entitats privades

Traducir Tweet

CSIRT-CV
@CSIRTCV

Finaliza la campaña de @CSIRTCV: "Diez recomendaciones de #ciberseguridad para #equiposDomésticos". Esperamos que haya sido útil para identificar #ciberpeligros y tomar las medidas necesarias para proteger nuestra información.

#Ciberprotección #concienciaT #FondosFeder

CSIRT-CV
@CSIRTCV

En esta nueva campaña de CSIRT-CV nos queremos centrar en la protección de nuestros dispositivos #móviles. No te pierdas los 10 consejos sobre #ciberseguridad en móviles que te daremos durante las próximas semanas.
#ProtegeTuMóvil #FondosFeder #concienciaT


CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana