Informe de Actividad 2023

V1

GENERALITAT VALENCIANA
Conselleria d'Hisenda, Economia i Administració Pública

AENOR ER Seguridad Información UNE-ISO/IEC 27001

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

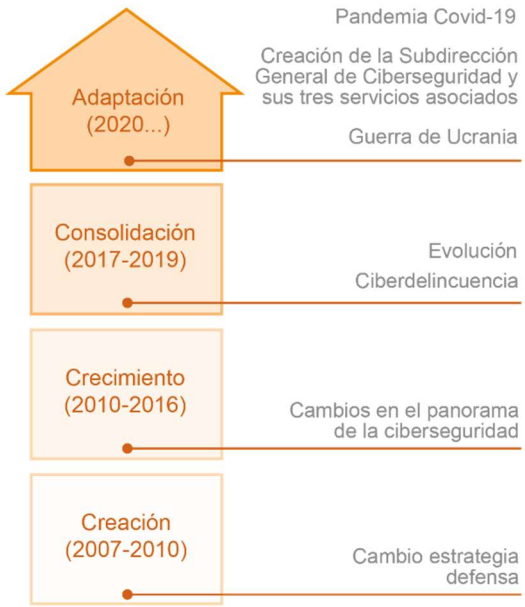
CLASIFICACIÓN

La información recogida en este informe corresponde, en su mayoría, a la experiencia del CSIRT-CV durante 2023 en el desarrollo de sus competencias. Además, se han tenido en cuenta otras fuentes documentales, de índole nacional e internacional, públicas y privadas para la elaboración del documento.

ÍNDICE

1 CSIRT-CV

CSIRT-CV es el Centro de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Comunitat Valenciana. Nace en junio de 2007 como una apuesta de la Generalitat Valenciana por la seguridad de la información en los sistemas de la red autonómica. En sus 16 años de existencia, se ha consolidado como un CSIRT de referencia a nivel nacional, y con presencia internacional en foros como CSIRT.es, Trusted Introducer y FIRST.



CSIRT-CV es una iniciativa pionera al ser el primer centro de estas características creado en España para un ámbito autonómico. Actualmente, CSIRT-CV está adscrito a la Dirección General de Tecnologías de la Información y las Comunicaciones (DGTIC) perteneciente a la Conselleria de Hacienda, Economía y Administración Pública.

CSIRT-CV ofrece sus servicios en las tres provincias de la Comunitat Valenciana (Castellón, Valencia y Alicante) 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:

- Administración Pública, tanto local como autonómica.
- Ciudadanos de la Comunitat Valenciana.
- Empresas privadas, especialmente las de menor tamaño.

Como se observa, el ámbito de actuación del CSIRT-CV es muy amplio, ya que incluye:

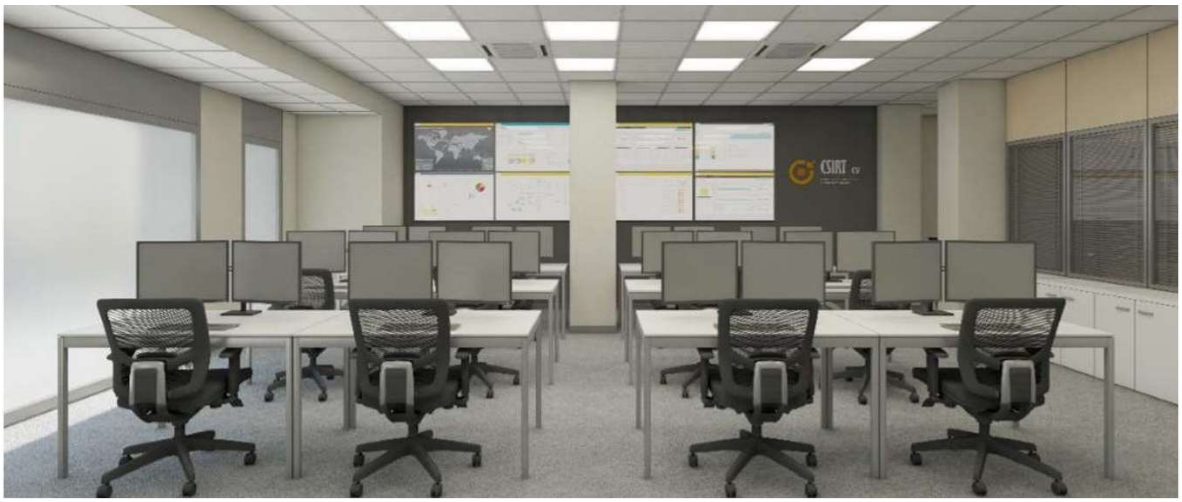
La Generalitat Valenciana, formada por Presidencia, dos Vicepresidencias y siete Consellerias.

- Entes de la Generalitat Valenciana y el Sector Público Instrumental[1]
- Un total de 584 Entidades Locales (EELL) de la Comunitat Valenciana.

En total, el número de empleados públicos en las tres provincias asciende a más de 282.000[2]. La Comunitat Valenciana representa cerca del 11% de la población nacional con más de 5,2 millones de habitantes (2023), siendo la 4ª comunidad autónoma de España en cuanto a población se refiere.

Respecto a la infraestructura informática de la Generalitat es altamente heterogénea y compleja, dando servicio a más de 200.000 dispositivos, entre los que se incluyen tanto equipamiento IT (tecnología de la información) como OT (tecnología de la operación).

El principal objetivo del 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 en el territorio autonómico y permita afrontar de forma activa las nuevas amenazas que pudieran surgir en este área.



Sala de Operaciones del CSIRT-CV

(1) Sector Público Instrumental - GVA Oberta 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 2023.

2 Servicios de Prevención

En este apartado, se refleja la actividad de los servicios ofrecidos por CSIRT-CV en su catálogo base solicitados bajo petición.

A continuación, se muestra una tabla con algunos de los datos de los servicios más destacados realizados por CSIRT-CV en el año 2023.

Servicios realizados	Total 2023
Test de intrusión	57
Auditorías de vulnerabilidades	162
Gestión de incidentes	1.788
Boletines de alertas a usuarios suscritos	291
Jornadas de Ciberseguridad en centros educativos	56
Consultas genéricas	168
Intercambio de información	210

2.1 TEST DE INTRUSIÓN

Este servicio proporciona un análisis exhaustivo de los activos del solicitante elaborando planes de acción a corto, medio y largo plazo con los que se puedan mitigar los riesgos descubiertos. Se realizará una serie de pruebas manuales de intrusión, utilizando técnicas exhaustivas de identificación de vulnerabilidades contra aplicaciones y sistemas. Las vulnerabilidades serán validadas por el equipo auditor y serán presentadas en un informe junto con una prueba de concepto de su explotación e información sobre cómo solucionarlas.

En el transcurso del año 2023, el equipo Red-Team de CSIRT-CV ha realizado un total de 57 test de Intrusión, de los que 51 han sido sobre plataformas web, cuatro sobre aplicaciones móviles y dos Web Services.

Asimismo, resaltar que fruto del trabajo de este servicio, durante 2023, el Instituto

Nacional de Ciberseguridad (INCIBE) ha publicado 12 vulnerabilidades[3] reportadas por el equipo de seguridad ofensiva de CSIRT-CV.

Las siete vulnerabilidades detectadas en 'QSige' de IDM Sistemas, llevó al Red-Team a la primera posición del ranking de investigadores de problemas de seguridad[4], perteneciente al programa CVE (Common Vulnerabilities and Exposures), coordinado por el CNA (Computer Network Attack) de INCIBE, y del que CSIRT-CV participa desde 2020.

2.2 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, informes sobre malware o publicación de papers sobre investigaciones. Adicionalmente, el Centro dispondrá de un Observatorio de Seguridad, que establecerá un plan de vigilancia anual alineado con la planificación estratégica de CSIRT-CV, en dos vertientes: interna y externa a la Generalitat Valenciana, según el tipo de fuentes analizadas. Estas dos vertientes del plan de vigilancia se plasmarán en sendos informes, uno interno para CSIRT-CV y otro para la Generalitat

A lo largo de 2023, CSIRT-CV ha elaborado varios informes, entre ellos destacan el de informe de Gestión de Incidentes y el informe de Tendencias de Malware. Además, se han publicado otros dos informes. Uno de ellos se corresponde con el Informe de Actividad de 2022[5], publicado en junio en el portal de CSIRT-CV, y otro informe relacionado con el Estudio de Ciberseguridad Industrial[6], cuya obtención es mediante solicitud a través del portal de concienciaT

Asimismo, desde CSIRT-CV se han enviado un total de 12 boletines mensuales de seguridad que recogen las noticias más relevantes acaecidas o relacionadas con el

(3) Vulnerabilidades reportadas por Red Team https://www.csirtcv.gva.es/csirt-cv-identifica-varias-vulnerabilidades-en-arconte-aurea-un-software-para-la-grabacion-de-vistas-judiciales/
(4) Vulnerabilidad QSige de IDM https://www.csirtcv.gva.es/el-red-team-del-csirt-cv-ocupa-la-primera-posicion-del-ranking-de-investigadores-de-problemas-de-seguridad-del-cna-de-incibe/
(5) Informe de Actividad de 2022 https://www.csirtcv.gva.es/informe-actividad-csirt-cv-2022/
(6) Estudio de Ciberseguridad Industrial https://concienciat.gva.es/estudio-de-ciberseguridad-industrial/

centro de seguridad y 291 boletines de alertas de vulnerabilidades a los usuarios suscritos a este servicio.

2.3 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. Los resultados se analizan y priorizan elaborando el correspondiente informe de auditoría, que se hará llegar a los receptores del servicio.

En 2023, se han realizado 162 auditorías de vulnerabilidades entre las habituales/rutinarias y otras ejecutadas bajo demanda. En estas auditorías se han auditado 39 organismos pertenecientes al ámbito de la Generalitat en el primer semestre del año, y 39 en el segundo.

La mayoría de las vulnerabilidades críticas se han detectado en software con funciones de servidor web y, en segundo lugar, en programas relacionados con dicho entorno web (Denegation of Service (DoS), Remote Code Execution, Buffer Overflow, Information Disclosure, XSS, Open Mail Relay, etc.), versiones de sistemas en servidores detectadas sin soporte y vulnerabilidades asociadas a certificados.

Posteriormente, también aparecen fallos de seguridad específicos en los sistemas Windows y Firewalls.

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.

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

Las conclusiones obtenidas deben servir para, de manera orientativa, dar una idea de cómo está el estado en cuanto a seguridad de las DMZ (Demilitarized Zone) desde la perspectiva interna de cada organismo y saber qué servicios son los que, predominantemente, están más expuestos a sufrir ataques de seguridad. Los resultados

detallados obtenidos para cada uno de los organismos se encuentran en nuestra plataforma CUSTODES a disposición de los correspondientes responsables.

2.4 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. Para ello, dado un objetivo que se pretenda auditar (persona, colectivo de personas, organismo/Conselleria) se buscará en Internet si se está haciendo un uso fraudulento o dañino usando información o el propio nombre del objetivo y se tomarán las medidas oportunas para mitigar estos riesgos.

Durante el año, no se han registrado peticiones de este servicio.

2.5 ANÁLISIS FORENSE

Tras un incidente de ciberseguridad, este servicio ofrece al solicitante 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 un análisis forense durante 2023, derivado de un incidente de compromiso de credenciales sin privilegios de dos usuarios de M365. En el forense, se analizó toda la traza dejada por el atacante con el objeto de determinar la actividad realizada y sus posibles pretensiones. Finalmente, se descartó que buscara alguna documentación concreta y se atribuyó a un ataque de phishing para seguir progresando a otros organismos.

Cabe señalar que la gestión de muchos incidentes de seguridad implícitamente contempla un análisis forense de distintos tipos de 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.

2.6 BASTIONADO DE ENTORNOS

Este servicio proporciona al solicitante 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 el año, se han registrado un total de siete solicitudes de bastionado. Entre las peticiones registradas se encuentran: evaluar alternativas o mejoras a las tecnologías de captchas, que utilizan varias aplicaciones web de GVA, realizar pruebas para crear una política VPN Host Checker en Linux, evaluar la viabilidad de accesos a dominios externos desde equipos de GVA o una consulta sobre requisitos y criterios necesarios a cumplir por el portal web de donantes para los accesos y sus registros, entre otras.

Además, tras varios ataques de ransomware a entidades locales y empresas, se ha solicitado a CSIRT-CV la redacción de un documento dirigido a los organismos del SPI en el que se recomienda el realizar un filtrado de los servicios expuestos a Internet de cada organismo.

Asimismo, hay que comentar las acciones llevadas a cabo por CSIRT-CV como preparativo del dispositivo de seguridad para las Elecciones de Mayo de 2023.

Por último, 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.

2.7 INTERCAMBIO DE INFORMACIÓN

El servicio consiste en que CSIRT-CV se transforme en el principal instrumento de intercambio de información relativa a ciberseguridad tanto en la Generalitat Valenciana como en empresas de la Comunitat, estableciendo canales de comunicación y alerta tanto internos en Generalitat como con organismos, grupos de interés en seguridad, autoridades, empresas… que permitan, con las restricciones necesarias para garantizar la legalidad vigente y la protección de información corporativa, un intercambio de información ágil, seguro y directo.

En el transcurso de 2023, teniendo más peso a finales de año, se han propuesto mejoras y cambios en el servicio de intercambio de información y detección de grupos APT (Advanced Persistent Threat) que se han materializado en varias iniciativas.

Una de ellas se basa en ampliar el abanico de detección de estos grupos avanzados a otras herramientas, además de CARMEN, como el EDR (Endpoint Detection and Response) o el Microsoft Defender.

Además, se empieza a clasificar y categorizar con mayor detalle este servicio en la herramienta eMAS. Con ello, hay que explicar que los eventos de intercambio de información pueden materializarse tras su análisis, en acciones en el equipo de Threat Hunting, que son los encargados de buscar intrusiones o actividad de esos actores avanzados. De estos análisis iniciales se derivan hipótesis de las cuales a su vez se pueden obtener reglas de detección y/o bloqueo para la actividad analizada.

Por otro lado, el intercambio de información, que puede provenir tanto de una fuente bastante viva como de un servicio de mensajería electrónica, de un informe de investigación online o de un incidente interno, se traduce en eventos de los cuales derivan acciones de bloqueo de indicadores de compromiso en las plataformas que así lo permiten.

Tras este resumen sobre los cambios en la operativa, hay que especificar que se han llevado a estudio 210 intercambios de información derivando en 17 hipótesis para los cuales se generaron 19 reglas de detección. Además, hay que comentar que gracias al análisis de la información entrante se ha procedido a crear alrededor de 50 eventos de bloqueo de indicadores en las distintas plataformas.

2.8 CUADRO DE MANDO DE SEGURIDAD

Este servicio consiste en informar en cada momento, y de forma gráfica y sencilla, del valor de una serie de indicadores importantes para el Centro de Seguridad. Los actuales indicadores han sido desarrollados de forma personalizada y se dividen en tres categorías (actividad, riesgo y calidad del servicio).

Los cuadros de mando se han seguido desarrollando con normalidad durante 2023. Concretamente, el proyecto de Business Intelligence (BI) ha seguido su desarrollo. Cabe

recordar que sus objetivos eran: disponer de una herramienta actual y con necesidad de menos mantenimiento para plasmar los indicadores de servicio, y servir como base para proporcionar unos informes al cliente que tengan la relación de incidentes y vulnerabilidades en sus organizaciones, entre otros, como el número de matriculaciones en los cursos online de ciberseguridad, el número de asistentes a las diferentes charlas formativas que realiza el Centro, etc.

A finales de 2023, se han comenzado a realizar sesiones formativas a los distintos usuarios del Servicio para que tomen contacto con la herramienta de BI COGNOS de IBM con la que se trabajará.

2.9 SERVICIO DE I+D+i

Este servicio permite a CSIRT-CV anticiparse a los problemas de seguridad y facilitar directrices para mitigar los riesgos más avanzados antes de que las amenazas asociadas se materialicen. El equipo de CSIRT-CV tiene la capacidad técnica suficiente para poder participar en proyectos de I+D internos o en colaboración con S2 Grupo y otras entidades nacionales o internacionales. S2Grupo hará uso de su experiencia en el ámbito de I+D europea para fomentar la participación del Centro de Seguridad en consorcios internacionales, con el objetivo de que el servicio alcance un grado de madurez que le permita definir y ejecutar una estrategia propia de investigación.

Durante 2023, el equipo del Centro de Seguridad TIC ha participado en diferentes proyectos internos de investigación con el objetivo de mejorar nuestros servicios. Se han evaluado productos, como Trellix EDR y CrowdStrike Falcon, así como mejoras en las capacidades de detección y respuesta automática de M365.

Como servicios externos, S2 Grupo solicitó, como en ocasiones anteriores, la colaboración de CSIRT-CV en proyectos europeos como SAURON o CyberSANE.

CyberSANE propone una solución para mejorar la detección y análisis de ciberataques a infraestructuras críticas y cuenta con la participación de 14 entidades europeas públicas y privadas. Por su parte, el objetivo principal de SAURON es proporcionar una plataforma de concienciación de la situación de seguridad en distintas dimensiones.

Debido al aumento de la demanda por parte de otros servicios del centro, no se ha

podido potenciar o dedicar más esfuerzos en otros proyectos de I+D+i que hubiera revertido en una mejora de los servicios que ofrece o en la forma de realizarlos.

2.10 LABORATORIO DE MALWARE

CSIRT-CV cuenta con un laboratorio de malware donde el equipo técnico analiza 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.

Está dispuesto en dos grandes bloques: el primer bloque comprende el análisis automatizado de muestras procedentes de fuentes externas, mientras que el segundo bloque está destinado al análisis manual por parte de los técnicos del CSIRT-CV de muestras detectadas en la propia organización.

Este servicio, tal y como estaba programado en el Plan Estratégico del centro ha visto incrementadas sus capacidades desde 2018 con el despliegue de un laboratorio físico y una Sandbox. Durante 2019, se continuó el trabajo de automatización y extracción de inteligencia y en 2020 alcanzó su estabilidad como servicio con una mayor capacidad de procesado y automatización de datos. Durante 2022 y 2023, se ha continuado mejorando y adaptando dichos sistemas a las nuevas técnicas y necesidades detectadas.

En cuanto al laboratorio no hay novedades, pero sí se ha hecho análisis de malware que puede consultarse a continuación.

2.11 TENDENCIAS Y ANÁLISIS DE MALWARE

El estudio de los resultados obtenidos por el laboratorio proporciona datos sobre las nuevas Tácticas, Técnicas y Procedimientos (TTP) empleadas por los delincuentes como son:

- Nuevas vulnerabilidades que están siendo aprovechadas.
- Nuevos formatos de fichero para la distribución de malware.

- Nuevos métodos de evasión de los sistemas de defensa que se estén

Durante el transcurso del año 2023 no se observa un cambio de tendencia con respecto al año anterior. Se sigue detectando el uso de ficheros ofimáticos que utilizan macros maliciosas, así como el uso de ficheros PDF con enlaces maliciosos incrustados para infectar a sus víctimas.

Debido a esto, los actores maliciosos han distribuido parte del esfuerzo en las primeras fases de infección en formatos diferentes de ficheros. Entre ellos se ha visto el repetitivo uso de correos phishing suplantando organismos nacionales (correos, bancos, organismos de la Generalitat, etc), tratando de engañar a los usuarios para robar sus credenciales en portales web falsos.

En 2023, CSIRT-CV ha gestionado 256 incidentes de tipo Código Dañino[7]. Algunos de los ejemplos más significativos de malware detectado en los incidentes gestionados han sido los siguientes: Emotet, ransomware Dharma, Agent Tesla, minero de Bitcoin, Raspberry Robin, gusano Brontok y Webshell.

2.13 MONITORIZACIÓN DE SERVICIOS WEB

Este servicio pretende ofrecer respuesta en tiempo real ante cualquier tipo de manipulación ilícita a los servicios web de la Generalitat. Se desplegará un sistema de monitorización de servicios web que detectará en un tiempo de respuesta mínimo cualquier modificación ilícita o la inclusión de código dañino sobre los mismos, además de su disponibilidad. La monitorización se apoyará en diversas herramientas automáticas y estará directamente ligada a los servicios de monitorización de presencia, seguridad semántica y sistemas de decepción, conformando en conjunto una maquinaria de vigilancia digital que permitirá detectar en tiempo real cualquier tipo de manipulación de los servicios web de Generalitat, reduciendo el impacto de un posible incidente de seguridad.

Para este servicio se dispone de un listado de sitios Web críticos en la Generalitat Valenciana a los cuales se les está realizando una monitorización más exhaustiva por parte de CSIRT-CV.

Este servicio se ha visto incrementado durante 2023 con la inclusión de nuevas páginas

(7) Clasificación establecida en la guía CCN-STIC 817, del Centro Criptológico Nacional.

web a este listado, gracias a la información proporcionada por los organismos del Sector Público Instrumental (SPI) en las reuniones de seguimiento del Plan de Mejora.

El proceso de monitorización consiste en detectar posibles modificaciones en las páginas web y avisar a los responsables de seguridad para que tomen las medidas oportunas. Normalmente, se trata de suplantaciones de identidad en las que los atacantes comprometen un servidor y les cambian la identidad.

2.14 NORMALIZACIÓN

Este servicio ofrece al solicitante la posibilidad de desarrollar o supervisar documentación basándonos en normas internacionales y en las mejores prácticas de ciberseguridad como los estándares ISO/IEC 27001 y 27002, NIST o las guías publicadas por CCN-CERT o ENISA asegurando una redacción clara y adecuada, según las directrices establecidas en la solicitud. Algunos ejemplos de documentación a solicitar pueden ser contratos de confidencialidad, procedimientos de seguridad o declaraciones de aplicabilidad.

Durante 2023, se ha seguido con la documentación en Confluence de aquellos procedimientos, o KBs (Knowledge Base), más utilizados en CSIRT-CV, abarcando todas las áreas operativas (Ataque, Defensa, GRC, Concienciación, Industrial, etc.), así como aspectos propios de la gestión interna del Centro.

En lo relativo al SOC de CSIRT-CV, a través de estos trabajos de normalización, se han actualizado y documentado múltiples procedimientos para cubrir las necesidades de los técnicos de Defensa, alcanzando un total de 66 instrucciones técnicas, con la singularidad del procedimiento de gestión de correo sospechoso, que fue elaborado conjuntamente por el equipo del proyecto de Entidades Locales (EELL), ya que se les trasladó la gestión de él.

Este procedimiento comprende tanto la recepción inicial y la solicitud para que la información sea completa, así como la gestión de todo el ciclo de vida del posible incidente, contando con actuaciones en la consola de M365 u otros elementos intermedios de ciberseguridad.

Además, a raíz de la actualización de GLORIA (la plataforma para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja

de eventos), las alertas de seguridad generadas cuentan con su propio procedimiento de análisis y contención, por lo que el número sería mayor.

También se han actualizado y ampliado los elementos que componen el cuerpo normativo en materia de ciberseguridad del Centro, permitiendo mejorar el grado de cumplimiento respecto al Esquema Nacional de Seguridad (ENS).

Para 2024, se espera aumentar las instrucciones para el tratamiento de las alertas en función del dispositivo que la genera, consiguiendo una gestión más uniforme y completa entre los técnicos.

2.15 AUDITORÍA ENS

El servicio de auditoría del ENS permite al solicitante obtener una valoración sobre su grado de cumplimiento del Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, identificando las posibles deficiencias y sugiriendo las medidas correctoras o complementarias necesarias dentro del alcance establecido en cada caso, según lo dispuesto en el artículo 34 del R.D.

Durante 2023, aunque no se ha realizado una auditoría como tal en materia del Esquema Nacional de Seguridad (ENS), se ha participado como personal de apoyo en auditorías realizadas a distintos organismos de la Generalitat Valenciana, entre ellas: la realizada a la Agencia Tributaria Valenciana (ATV), a la Agencia Valenciana Agraria (AVFGA), o a la Fundación de Investigación del hospital la Fe (IISLAFE).

Por otra parte, se han llevado a cabo mejoras en el Sistema de Gestión interno del Centro para incrementar el grado de cumplimiento de los requisitos del ENS.

2.16 AUDITORÍA RGPD

Este servicio se ofrece para dar cumplimiento a lo establecido por el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales, de acuerdo con el deber del responsable del tratamiento de aplicar medidas técnicas y organizativas apropiadas, y de poder demostrarlo (art. 24 RGPD). A este respecto, la auditoría RGPD evalúa el

nivel de seguridad existente en la gestión de datos de carácter personal. Como resultado del servicio, se entregará un informe de cumplimiento sobre los artículos auditados.

A pesar de no haber realizado ningún servicio como tal, se han realizado tareas internas relacionadas con la protección de datos, entre ellas: la actualización del curso Reglamento General de Protección de Datos (RGPD) o la revisión del apartado de Aviso Legal del cumplimiento web de los portales de csirtcv.gva.es y concienciat.gva.es.

2.17 CONSULTORÍA ISO 27001

Este servicio tiene como finalidad orientar al solicitante para planificar una estrategia de mejora de la seguridad en base a una norma de referencia como es la ISO 27001:2013, bien para su implantación, bien para su certificación o para cualquiera que sea el nivel que establezca como objetivo el solicitante. El alcance del servicio incluye la resolución de dudas, la revisión de documentación o el apoyo durante el proceso de adecuación/revisión del Sistema de Gestión de Seguridad de la Información (SGSI).

En el año 2023 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 SGSI.

En este ámbito cobra especial importancia el proyecto de transición a la nueva versión de la norma ISO 27001 (ISO 27001:2022). Con estos trabajos se está adaptando y ampliado el sistema de gestión existente para dar cobertura a los nuevos requisitos de la norma.

Para el 2024 se continuará con los trabajos de transición, con intención de renovar la certificación del SGSI con la nueva versión de la ISO 27001.

2.18 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. Estas revisiones permiten validar si el software desarrollado presenta vulnerabilidades que puedan poner en riesgo la seguridad de la información procesada o almacenada.

No se han registrado peticiones en este servicio en el año 2023, aunque es preciso matizar que, en la mayoría de los test de intrusión ejecutados, se realiza una fase de validación del código de la aplicación bajo análisis.

2.19 ANÁLISIS DE RIESGOS

Este servicio ofrece al solicitante la realización de un análisis de riesgos mediante la metodología MAGERIT, haciendo uso de la herramienta PILAR (si así lo requiere). Como resultado, se entregará un informe con los niveles de riesgo a los que está sujeta la organización, así como un plan de medidas correctoras para reducir el riesgo a unos niveles aceptables.

A lo largo de 2023, se han llevado a cabo varios análisis de riesgos:

- Análisis del sistema de información de la Agencia Valenciana de Fomento y Garantía Agraria (AVFGA).
- Análisis del sistema corporativo de autenticación, autorización, auditoría y SSO (Gvlogin).
- Análisis de riesgos sobre el sistema de expedientes de subvenciones tramitados electrónicamente (ESTER).

Por otro lado, también se han realizado dos análisis de riesgos relativos a interconexiones teniendo como base el ENS. Uno relacionado con el sistema de ticketing de la ACCV (interconexión Jira-Freshdesk), y otro relacionado con el sistema de grabación de vistas judiciales (interconexión Arconte-Aurea).

Por último, cabe destacar la revisión y actualización del análisis de riesgos de CSIRT-CV, desarrollado en el marco del SGSI e implementado a través de la herramienta PILAR.

2.20 FORMACIÓN Y CONCIENCIACIÓN

Este servicio ofrece acciones formativas y de concienciación en Ciberseguridad que puedan resultar de relevancia para la sociedad. Las acciones pueden ser cursos on-line o presenciales, jornadas, videotutoriales y guías específicas, entre otros contenidos.

La divulgación y concienciación es algo consustancial a la manera de entender la ciberseguridad en CSIRT-CV, por lo que el centro puso en marcha el Plan Valenciano de Capacitación (PVC) en Ciberseguridad, que sitúa a las personas en uno de sus principales ejes de actuación. El PVC aborda el servicio de Formación y Concienciación del CSIRT-CV para el cual se ha definido un calendario donde se han contemplado acciones concretas de formación y capacitación en materia de Ciberseguridad dirigidas a los diferentes colectivos identificados: ciudadanos, empleados públicos, empresas (PYME) y otras administraciones (Ayuntamientos, organizaciones, etc.)

Para realizar dichas acciones se han utilizado diferentes formatos y canales de comunicación: sesiones de concienciación en entes y organismos, jornadas sobre Ciberseguridad en centros educativos de Educación Secundaria, publicación de noticias en los portales de CSIRT-CV y concienciaT, así como en las redes sociales del centro de seguridad (Facebook[8], X[9] (antiguo Twitter), boletines informativos de seguridad de carácter mensual y alertas de seguridad para suscriptores, campañas de concienciación dirigidas a los ciudadanos, a las empresas y a los empleados públicos de la Generalitat Valenciana o cursos de formación online.

2.20.1 PLATAFORMA SAPS

Durante 2023, CSIRT-CV ha vuelto a ampliar su oferta formativa con cursos sobre seguridad online gratuitos, alcanzando la cifra de un total de 28. Los cursos formativos del CSIRT-CV están destinados, principalmente, a tres colectivos:

- Ciudadanos

(8) Perfil de Facebook https://www.facebook.com/CSIRTCV
(9) Perfil de X https://twitter.com/CSIRTCV

- Entidades Locales
- Empresas

Una de las principales novedades en el ámbito de la formación durante 2023, ha sido la publicación de tres nuevos cursos, destinados a las empresas y a sus plantillas, en la plataforma de aprendizaje eFormación[10] (SAPS) de la Generalitat Valenciana:

- Seguridad básica para técnicos informáticos[11].
- Curso básico para CEOS[12].
- Bastionado de WordPress[13].

Estos cursos han pasado de estar de la plataforma Moodle a la nueva plataforma eFormación, caracteriza por contar con un formato renovado e interactivo para estimular a los usuarios a cursar las diferentes formaciones.

A lo largo de 2024, está previsto que cambien de ubicación otros tres cursos dirigidos a empresas para completar este proceso de cambio de ubicación de las formaciones.

Además, también se han actualizado diversos contenidos de los cursos ya ofertados, como, por ejemplo, el perteneciente al curso de 'Reglamento General de Protección de Datos[14] (RGPD)'.

En este sentido, cabe resaltar que, durante 2023, los cursos de seguridad han formado a un total de 5.032 alumnas y alumnos, más de 61.000 personas desde 2009. El curso con más solicitudes en 2023, por segundo año consecutivo, ha vuelto a ser el de 'Reglamento General de Protección de Datos (RGPD)' con un total de 841 estudiantes matriculados.

La segunda formación más requerida ha sido 'Seguridad en el correo electrónico' (414), seguida de 'Introducción a la Seguridad Informática' con 341 matrículas en 2023.

En un futuro, está prevista la creación e incorporación de más cursos de formación con un formato más interactivo para el usuario, así como la actualización del temario de gran parte de la oferta formativa ofrecida por CSIRT-CV.

(10) Plataforma de aprendizaje eFormación https://saps.gva.es/es/inicio

(11) Apartado de cursos de la web de concienciaT https://concienciat.gva.es/cursos/introduccion-a-la-seguridad-informatica/

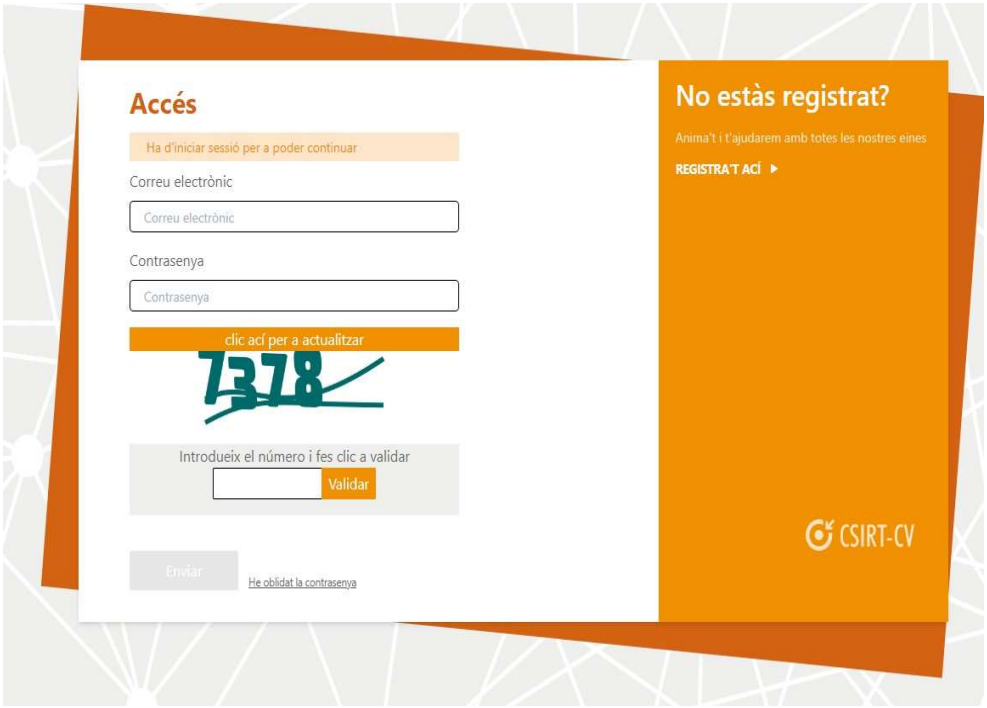
(12) Estudio de Ciberseguridad Industrial https://concienciat.gva.es/estudio-de-ciberseguridad-industrial/

(13) Apartado de Entidades Locales de concienciaT https://concienciat.gva.es/entidades-locales/

(14) Curso RGPD https://concienciat.gva.es/cursos/**reglamento**-general-de-proteccion-de-datos/

2.20.2 HERRAMIENTA AVALUAT

CSIRT-CV, dentro de su 'Plan de Capacitación en Ciberseguridad para Empresas[15]', ha seguido ofreciendo, en su portal de Concienciación, la posibilidad de que las empresas, organizaciones o entes se registren, de manera gratuita, para evaluar su nivel de madurez en ciberseguridad en los diferentes aspectos que engloban a una organización a través de la herramienta AvaluaT[16].



Acceso a AvaluaT

Mediante esta herramienta, 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 para llevar a cabo y así alcanzar los objetivos recomendados.

Durante 2023, CSIRT-CV ha llevado a cabo una mejora de la aplicación, que incluía tanto correcciones menores como nuevas funcionalidades para ofrecer un mejor servicio al tejido empresarial de la Comunitat Valenciana. Al cierre del ejercicio, se encontraba disponible al público la versión 2.0.0 y la línea de trabajo es seguir trabajando en esta

(15) Sección de Empresas de concienciaT https://concienciat.gva.es/empresas/

(16) Plataforma AvaluaT https://avaluat.concienciat.gva.es/

plataforma para mejorar el servicio. Hasta la fecha, más de un centenar de empresas han hecho uso de AvaluaT desde que viera la luz en 2020.

2.20.3 CAMPAÑAS DE CONCIENCIACIÓN

En CSIRT-CV, definimos campaña de concienciación como una acción puntual de educación o refuerzo cuyo objetivo es lograr un cambio de hábitos en los usuarios finales mediante la divulgación de mensajes relacionados con la ciberseguridad a través de diferentes contenidos como pueden ser artículos, infografías, newsletters, vídeos, etc.

A lo largo de 2023, se han lanzado un total de seis campañas de concienciación, dirigidas a los ciudadanos de la Comunitat Valenciana, por medio de las redes sociales en las que está presente CSIRT-CV (Facebook y X), así como del portal de concienciaT, además de otra campaña de concienciación de carácter interno dirigida al personal de la Generalitat Valenciana.

A continuación, se presenta una descripción de cada una de ellas.

2.20.3.1 ‘ Fortaleciendo la Ciberseguridad Industrial en la Comunitat Valenciana[17’]

Esta campaña surge a raíz del estudio realizado por CSIRT-CV para medir el nivel de madurez de las empresas de la Comunitat Valenciana en ciberseguridad industrial, cuyo resultado se presentó en Valencia, en el mes de febrero del pasado año, durante la celebración de la I Jornada de Ciberseguridad Industrial.

El estudio proporcionó un retrato robot sobre el estado en ciberseguridad de las empresas ubicadas a lo largo y ancho de las tres provincias valencianas y de él nació la necesidad de establecer una estrategia a seguir público-privada en este campo.

Actualmente, la ciberseguridad es vital en cualquier empresa, independientemente del sector al que se dedique o del tamaño que posea. Si una organización puede ver afectado su proceso productivo por un incidente de seguridad es primordial estar preparado y prevenido, por lo que desde CSIRT-CV se ofrecieron varios consejos mediante material diverso para concienciar a las pyme sobre la necesidad de contar con una Política de Ciberseguridad activa; establecer un Plan de Formación y Concienciación para sus plantillas con el fin de evitar y minimizar los riesgos relacionados con la ciberseguridad; contar con herramientas capaces de detectar actividades sospechosas y establecer buenas prácticas en las empresas para prevenir incidentes de ciberseguridad.

Imagen de la campaña de Concienciación ‘Fortaleciendo la Ciberseguridad Industrial en la Comunitat Valenciana’

(17) Campaña concienciaT https://concienciat.gva.es/tips_de_seguridad/campana-fortaleciendo-la-ciberseguridad-industrial-en-la-comunitat-valenciana/

2.20.3.2 ‘10 Consejos sobre Ciberseguridad para disfrutar sin sobresaltos en Semana Santa[18]’

Con motivo de la Semana Santa y Pascua en la que miles de ciudadanos se toman unos días de desconexión y ocio, CSIRT-CV relanzó esta campaña de concienciación con 10 recomendaciones básicas de seguridad para ponerlos en práctica antes de salir de casa.

Como bien es sabido, la época vacacional es uno de los períodos más críticos para la ciberseguridad de los usuarios puesto que al tener que planificar y contratar diferentes servicios como vuelos, hoteles, reservas en restaurantes, excursiones…en muchas ocasiones de forma online, se baja la guardia en cuanto a la seguridad. Una circunstancia que es aprovechada por los ciberdelincuentes para robar datos e información de los usuarios, de ahí la insistencia del CSIRT-CV para concienciar en este tipo de situaciones.

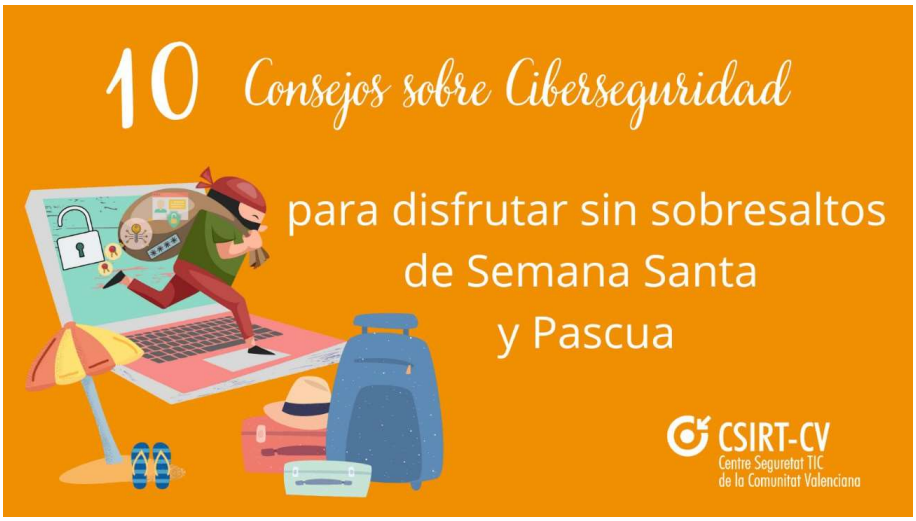


Imagen de la campaña de Concienciación ‘10 consejos sobre Ciberseguridad para disfrutar sin sobresaltos en Semana Santa y Pascua’

(17) Campaña concienciaT https://concienciat.gva.es/tips_de_seguridad/disfruta-de-unos-dias-de-descanso-sin-sobresaltos-en-semana-santa-con-estos-10-consejos-sobre-ciberseguridad/

2.20.3.3 ‘Inteligencia Artificial: ¿amiga o enemiga?’[19]

El sector de la IA ha crecido exponencialmente en los últimos años, y aunque la tecnología ya empieza a calar en algunos ámbitos de la vida en general, todavía la sociedad no se ha adaptado a este nuevo paradigma.

En muchas ocasiones se hace uso de la inteligencia artificial sin ser conscientes de ello. Esta tecnología está presente, por ejemplo, en asistentes virtuales, casas inteligentes, chatbots o redes sociales y en la mayoría de los ámbitos: sanitario, educativo, empresarial, económico, cultural, turístico, publicitario y generación de contenido, entre otros.

En este sentido, desde CSIRT-CV consideró de vital importancia llevar a cabo una campaña de concienciación para explicar a los ciudadanos las ventajas que aporta la IA a la sociedad, así como los riesgos que conlleva y algunas recomendaciones para un uso correcto y seguro.

Además, se completó esta campaña con uno de los casos de uso que más dio que hablar durante 2023: ChatGPT. Toda la información de esta campaña se puede encontrar publicada en el apartado de Consejos y Campañas de la web conciencia T[20].

Imagen de la campaña de Concienciación ‘Inteligencia Artificial: ¿amiga o enemiga?’

(19) Campaña conciencia T https://concienciat.gva.es/tips_de_seguridad/inteligencia-artificial-amiga-o-enemiga/
(20) Campaña conciencia T https://concienciat.gva.es/tips_de_seguridad/

2.20.3.4 ‘Diez recomendaciones de ciberseguridad para las vacaciones’[21]

Una vez más, la época estacional se impuso en la programación del centro de seguridad autonómico y se republicaron una serie de consejos para mantenerse a salvo de las ciberamenazas durante el descanso estival. El objetivo de esta campaña era lanzar una serie de recomendaciones, a través de los perfiles de las redes sociales del CSIRT-CV, para recordar qué hacer antes y durante las vacaciones para no caer en las trampas de los atacantes, quienes son conscientes de que, en los meses de verano, se baja la guardia en ciberseguridad, mientras que ellos incrementan su actividad delictiva.

Redes WiFi, contraseñas, redes sociales, correo electrónico, juegos online y copias de seguridad, entre otros, fueron los temas tratados en esta acción.

Imagen de la campaña de Concienciación ‘Diez recomendaciones de ciberseguridad para las vacaciones’

(21) Campaña concienciaT https://concienciat.gva.es/tips_de_seguridad/diez-recomendaciones-de-ciberseguridad-para-las-vacaciones/

2.20.3.5 ‘Para. Piensa. Conecta. Sé más inteligente que un hacker’[22]

Coincidiendo con el Mes Europeo de la Ciberseguridad, un año más CSIRT-CV se sumó a la iniciativa anual de ENISA (Agencia de la Unión Europea para la Ciberseguridad) en materia de concienciación, al poner en marcha esta campaña centrada en cuatro escenarios: redes sociales, correos electrónicos, identidad digital y ciberestafas.

Escenarios presentes en el día a día de los ciudadanos y que provocan que miles de usuarios de todo el mundo caigan en las redes de los ciberdelincuentes. El objetivo de esta acción era insistir en la necesidad de analizar cada situación mediante tres acciones: Para. Piensa. Conecta.

Ante la llegada de cualquier tipo de mensaje, es preciso examinarlo para después pasar a la acción. Incorporando buenas prácticas de seguridad en el entorno laboral y personal, se consigue navegar por Internet de forma segura y con confianza, convertirse paulatinamente en ‘Human Firewall’, además de ponérselo difícil a los ciberatacantes.

Ilustración 7: Imagen de la campaña de Concienciación ‘Para. Piensa. Conecta. Sé más inteligente que un hacker’

(22) Campaña concienciaT https://concienciat.gva.es/tips_de_seguridad/para-piensa-conecta-se-mas-inteligente-que-un-hacker/

2.20.3.6 ‘Dispositivos conectados sí, pero sin riesgos’[23]

2023 se despidió con una campaña centrada en los dispositivos conectados a Internet. La Navidad y las Rebajas son épocas propicias para regalar juguetes interactivos, relojes inteligentes, auriculares, gadgets tecnológicos, dispositivos inteligentes para la casa como aspiradoras robóticas, asistentes virtuales, sistemas de seguridad con alarmas y cámaras, termostatos inteligentes…

Un sinfín de regalos apreciados por su capacidad para hacer la vida cotidiana más fácil y eficiente, pero cuyos riesgos son desconocidos por una gran mayoría. Al ser dispositivos conectados a la red son susceptibles de ser atacados por ciberdelincuentes, de ahí la importancia de concienciar a la población sobre el uso seguro y responsable de las nuevas tecnologías, así como el conocimiento de las medidas de seguridad de estos aparatos para garantizar la seguridad de la información que almacenan.

Para esta acción, desde CSIRT-CV se proporcionaron una serie de consejos, se enumeraron algunos riesgos y se especificaron los ámbitos en los que se encuentran dispositivos conectados y que son de uso más común entre la población. Hogares inteligentes o casas domóticas (Smart home), juguetes interactivos (Smart toys), Internet de las Cosas (IoT) y dispositivos electrónicos inteligentes que se incorporan en alguna parte de nuestro cuerpo (Wearables) fueron las temáticas escogidas para esta campaña cuya información, al igual que las del resto de iniciativas, puede encontrarse en el apartado de Consejos y Campañas de la web concienciaT.

Imagen de la campaña de Concienciación ‘Dispositivos conectados sí, pero sin riesgos

(23) Campaña concienciaT https://concienciat.gva.es/tips_de_seguridad/nueva-campana-dispositivos-conectados-si-pero-sin-riesgos/

2.20.3.7 Campaña de Concienciación dirigida al personal de la Generalitat Valenciana

A lo largo de 2023, CSIRT-CV también ha puesto en marcha una campaña de concienciación en Ciberseguridad dirigida al personal de la Generalitat Valenciana, que se seguirá desarrollando durante 2024, tras un análisis de las necesidades de seguridad en las que se evaluó el panorama de las amenazas que afecta a este sector para decidir la estrategia a implantar.

Con el objetivo de reducir y mitigar las ciberamenazas centradas en el ser humano, se ha optado por el envío de correos electrónicos e infografías de forma periódica con temas que la organización experimenta o experimentará en el ámbito de la ciberseguridad y en los que es crucial el papel del usuario para garantizar la seguridad de la información empresarial. La temática, adaptada al nivel corporativo, ha sido variada y ha abarcado el uso de la Inteligencia Artificial, la compartición segura de archivos, seguridad en el móvil y estafas por correo electrónico, entre otras materias. El material gráfico puede se ha publicado en el portal corporativo de Funciona[24] para que cualquier usuario pueda acceder a él en cualquier momento.

Infografía 'Cómo compartir archivos de forma segura' perteneciente a la campaña corporativa de GVA

(24) Portal Funciona https://funciona.gva.es/va/inici?p_p_id=58&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&saveLastPath=0&_58_struts_action=%2Flogin%2Flogin

2.20.4 JORNADAS DE CIBERSEGURIDAD EN CENTROS DE SECUNDARIA

El Plan Valenciano de Capacitación identifica a los adolescentes como uno de los colectivos más vulnerables ante las amenazas digitales, por lo que durante 2023 se han continuado con las Jornadas de Concienciación sobre Ciberseguridad[25] en los centros educativos. Su objetivo desde 2017 es, instaurar y reforzar una Cultura de Ciberseguridad y buenas prácticas en el uso de las nuevas tecnologías, principalmente, entre los adolescentes.

El alcance de esta iniciativa abarca todos los institutos públicos, concertados y privados de la Comunidad Valenciana, centrándose en los alumnos de 1º de la ESO y su entorno más cercano, madres, padres, tutores y profesores, para que puedan encontrar en las personas adultas respuestas en sus dudas del día a día relacionadas con los medios tecnológicos.

Durante 2023, se han realizado las Jornadas de Concienciación sobre Ciberseguridad en 56 centros de educativos de la Comunitat Valenciana. Concretamente, se han formado a más de 6.300 personas durante esos doce meses de los cuales, 4.694 fueron menores, 817 familiares y 808 docentes. Desde el inicio del proyecto, se han celebrado un total de 410 sesiones y concienciado a más de 38.000 personas.

Este proyecto seguirá celebrándose a lo largo 2024 en aras a concienciar a la comunidad educativa sobre las prácticas seguras en Internet, los peligros potenciales y la protección de la información personal.

Estudiantes durante una sesión del CSIRT-CV

(25) Jornadas de Ciberseguridad en centros educativos del Portal Funciona https://concienciat.gva.es/jornadas-de-ciberseguridad-en-centros-de-secundaria/

2.20.5 JORNADAS DE CONCIENCIACIÓN EN OTROS CENTROS

A lo largo de 2023, se han realizado otras tres jornadas de concienciación por parte de CSIRT- CV en otros centros con la finalidad de mejorar el nivel de ciberseguridad de los usuarios. La Fundación Acción contra el Hambre, el IES Camp de Morvedre, el personal técnico de la Administración Pública. Además, se han impartido sesiones en diferentes organismos del SPI (Sector Público Instrumental).

Además, junto con el Institut Valencià d'Administració Pública (IVAP), CSIRT-CV ha organizado un curso sobre 'Desarrollo seguro de aplicaciones'[26], que ha sido impartido por personal del centro de seguridad al igual que en años anteriores

2.20.6 PLAN DE CAPACITACIÓN TÉCNICA

Este apartado recoge la formación que ha recibido, en general, el equipo de CSIRT-CV y la DGTIC.

Durante el año, el personal de CSIRT-CV y compañeros de la Subdirección de Ciberseguridad de la DGTIC ha recibido formación en metodología OWASP Top Ten (Open Web Application Security Project). OWASP es una metodología de seguridad de auditoría web, abierta y colaborativa, orientada al análisis de seguridad de aplicaciones Web, y usada como referente en auditorías de seguridad.

Asimismo, la plantilla de CSIRT-CV también ha recibido formaciones en Metodologías Agile y de BI para una mejor eficiencia de sus competencias laborales en el día a día.

Además, todos los miércoles del año (exceptuando verano y festivos) de 9 a 9:30 horas, se han celebrado las Paper Session, impartidas por el personal de CSIRT-CV y dirigidas tanto a los técnicos del centro de seguridad como al personal de la DGTIC.

La temática de las más de 30 sesiones que se han celebrado en 2023 ha sido variada y se han tratado temas relacionados con los entornos médicos, la Comunicación de CSIRT-CV, Confluence, Proyectos de mejora de la capacidad de detección, Análisis de Riesgos o casos concretos como Flipper Zero o Grupo RansomHouse, entre otras exposiciones.

(26) Curso en el IVAP https://concienciat.gva.es/sabias_que/sabias-que-el-csirt-cv-imparte-un-curso-sobre-desarrollo-seguro-de-aplicaciones-en-el-ivap/

3 Servicios de Detección

3.1 DETECCIÓN APT - THREAT HUNTING

Es un servicio es la definición de la metodología a seguir para prestar el servicio de Detección de Amenazas Persistentes Avanzadas (APT) de CSIRT-CV. Este servicio está basado en la herramienta CARMEN, que proporciona la capacidad para la identificación de amenazas persistentes avanzadas mediante la adquisición, procesamiento y análisis de tráfico de red saliente e interno de la organización, y en el trabajo de analistas especialistas en APT encargados de buscar patrones anómalos y analiza si éstos se deben a actividades de malware dirigido.

Durante 2023, se ha continuado con el servicio orientado a la detección de Amenazas Persistentes Avanzadas (APT). El servicio se ha enfocado con el objetivo del análisis de los flujos de red/endpoint para identificar compromisos por parte de malware, en especial el asociado a APT.

En el primer semestre de 2023, CARMEN era la única herramienta de Threat Hunting que se utilizaba en el servicio, pero en el segundo semestre se han incorporado nuevas herramientas como Microsoft Defender o Trellix EDR para cubrir técnicas que únicamente con CARMEN no se pueden monitorizar. Ello permite que los analistas dispongan de más utilidades para la detección de amenazas.

Al haber adoptado un modelo de servicio más abstracto y disponer de diversas herramientas, se ha adaptado la creación de hipótesis y reglas para detectar comportamientos muy concretos y así evitar ruido innecesario. Esto ha generado que haya menos alertas para revisar, y, por tanto, menos incidentes relacionados con grupos APT o con el servicio de Threat Hunting[27].

(27) Curso en e Hasta el mes de septiembre el servicio estaba sin definir a nivel de hipótesis/reglas/alertas, por lo que no se encuentran dichos indicadores antes de este mes

3.3 PLANES DE MEJORA Y GRUPOS DE TRABAJO

Este servicio pretende la mejora de la seguridad de organismos y por ende de la Generalitat Valenciana. Ante una solicitud recibida y evaluada en CSIRT-CV se realizarán evaluaciones de seguridad, tanto técnicas como organizativas, que permitan a un organismo identificar su grado actual de cumplimiento con respecto a unas buenas prácticas reconocidas y le faciliten adicionalmente las iniciativas y proyectos a acometer para mejorar aquellos puntos más débiles, de manera priorizada en el tiempo y contando siempre con el equipo del Centro.

En 2023, se ha continuado con diferentes Planes de Mejora, iniciados con anterioridad, así como otros nuevos que han ido surgiendo:

- Plan de Mejora para la Agencia Valenciana de Emergencias
- Auditorías de Piloto Portal Tenable de Gestión de Vulnerabilidades
- Mejora de las capacidades de monitorización en la red corporativa de GVA
- Incorporación del SPI
- Proyecto Piloto de Alcoi
- Proyecto Piloto de Sagunto
- Proyecto Piloto de Castellón
- Proyecto piloto del sistema centralizado de detección de vulnerabilidades
- Estudio de implantación de una red de monitorización

Algunos de los proyectos de mejora abordados comenzaron con algunos estudios en fase de piloto para valorar la viabilidad con la intención de continuar con dichos proyectos en los casos en los que su viabilidad fuera validada por el equipo de CSIRT-CV.

Entre esos proyectos se encuentran: el Portal de Tenable.io para la gestión de vulnerabilidades, las pruebas de crear una red paralela de monitorización en la red corporativa de GVA y el piloto para la integración del GLORIA distribuido en el Ayuntamiento de Alcoy.

A continuación, se amplían algunos de estos planes.

3.4 INCORPORACIÓN DEL SPI

A lo largo de 2023, hemos seguido con los trabajos del Plan de Mejora del Sector Público Instrumental (SPI). Durante este año, se han integrado un total de 15 entes y organismos del SPI en CSIRT- CV.

Los organismos integrados son:

- La Agència Valenciana Antifrau (AVAF)
- La Agencia Valenciana de Seguridad y Respuesta a Emergencias (112 Comunitat Valenciana)
- La Sociedad Valenciana de Gestión Integral de los Servicios de Emergencias (SGISE)
- El Institut Valencià de Cultura (IVC)
- El Instituto Valenciano de la Competitividad Empresarial (IVACE)
- La Sociedad Valenciana de Aprovechamiento Energético de Residuos S.A. (VAERSA)
- Turisme Comunitat Valenciana
- El Consell Jurídic Consultiu de la Comunitat Valenciana (CJCCV)
- La Entitat Valenciana d'Habitatge i Sòl (EVHA)
- La Ciudad de las Artes y de las Ciencias S.A (CAC)
- El Institut Valencià de Conservació, Restauració i Investigació (IVCR+i)
- El Instituto Valenciano Atención Social-Sanitaria (IVASS)
- La Entidad Pública de Saneamiento de Aguas Residuales de la Comunidad Valenciana (EPSAR)
- Sindicatura de Comptes

Uno de los objetivos de este proyecto es dar a conocer el papel y las funciones del Centro de Seguridad TIC, así como el catálogo de servicios que presta a los diferentes organismos, y por otra parte el de ayudar a mejorar la seguridad de la información en la red.

3.5 PROYECTO PILOTO DE ALCOY

El Ayuntamiento de Alcoy ha sido escogido para ser uno de los proyecto piloto del Plan de Choque de Ciberseguridad para las Entidades locales de la Comunitat Valenciana de más de 50.000 habitantes, por lo que se ha incluido en la Red Nacional de Centros de Operaciones de Ciberseguridad, a través del CSIRT-CV, y el consistorio ha sido

beneficiario de sus servicios.

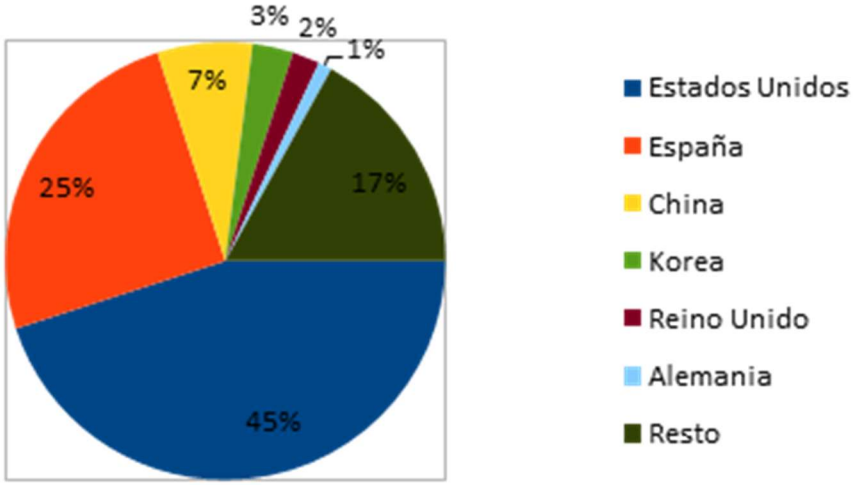
Tras el despliegue de la solución de Gloria del CCN, como herramienta SIEM en las instalaciones del Ayuntamiento e integrar en GLORIA el Firewall como única fuente de datos, desde CSIRT-CV se ha realizado la gestión de los eventos generados en la consola de GLORIA, notificando de los riesgos y proponiendo iniciativas de seguridad para cada uno de los riesgos identificados.

3.6 DETECCIÓN Y PROTECCIÓN ANTE INTRUSOS

Durante 2023, el equipo del CSIRT-CV ha realizado un importante trabajo de ajuste sobre las sondas NIDS que administra, aplicando 34 cambios en reglas ad hoc. De igual forma, se han aplicado más de 107 nuevas reglas de correlación sobre la plataforma Tritón.

Los sistemas de detección de intrusos del CSIRT-CV han generado al menos 340 millones de alertas provocadas por ciberataques. Mientras que, en 2022, destacaron las alertas relacionadas con herramientas de control remoto de los sistemas como MyWebExPC o Teamviewer, en 2023 han predominado los escaneos de criticidad baja de diferentes tipos; desde los escaneos SSH a escaneos a puertos de base de datos (como el puerto 3306/TCP de MySQL).

A continuación, se muestra un gráfico con los ciberataques recibidos según el país de origen:



Ciberataques recibidos según el país de origen.

Estados Unidos es el origen desde el que se reciben más ataques, seguido de España, y el resto de los países en menor medida. Cabe destacar que los atacantes utilizan con frecuencia VPNs, botnets y diferentes técnicas para ocultar su origen, por lo que no implica que todos los ataques procedan realmente de estos orígenes.

En el IPS que gestiona CSIRT-CV se ha llevado a cabo un trabajo intenso en el bloqueo preventivo de nuevas técnicas de ataque, realizando hasta 581 cambios en la configuración, detección y bloqueo del dispositivo.

4 Servicios de Respuesta

4.1 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.

Teniendo en cuenta la clasificación de ciberincidentes, publicada por el CCN-CERT en su guía CCN-STIC 817, el número de ciberataques gestionados por CSIRT-CV durante 2023 asciende a 1.788 incidentes, un 56% más respecto a 2022, ya que se gestionaron un total de 1.144 incidentes.

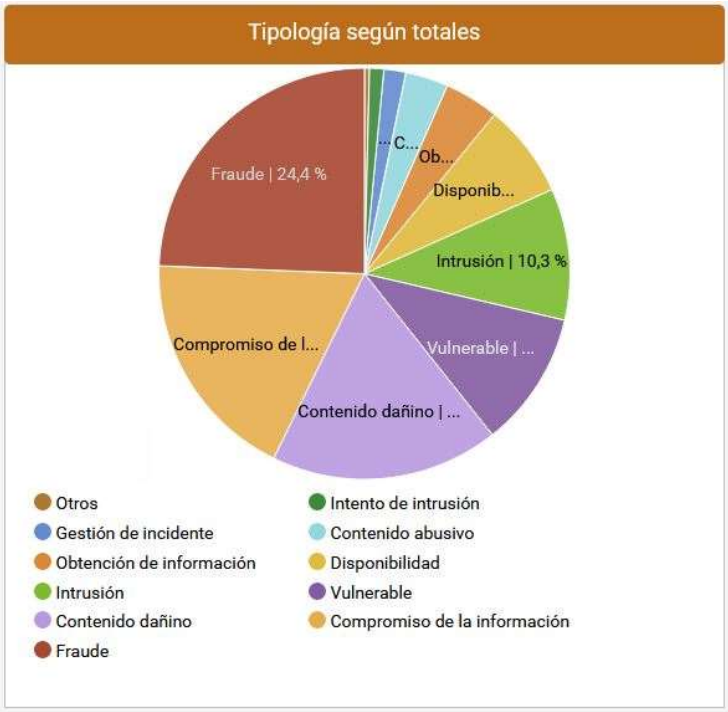
Los meses con mayor número de incidentes gestionados a lo largo de 2023 fueron marzo (238), diciembre (198) y enero (194) como puede comprobarse en la siguiente tabla de la evolución de incidentes por mes.

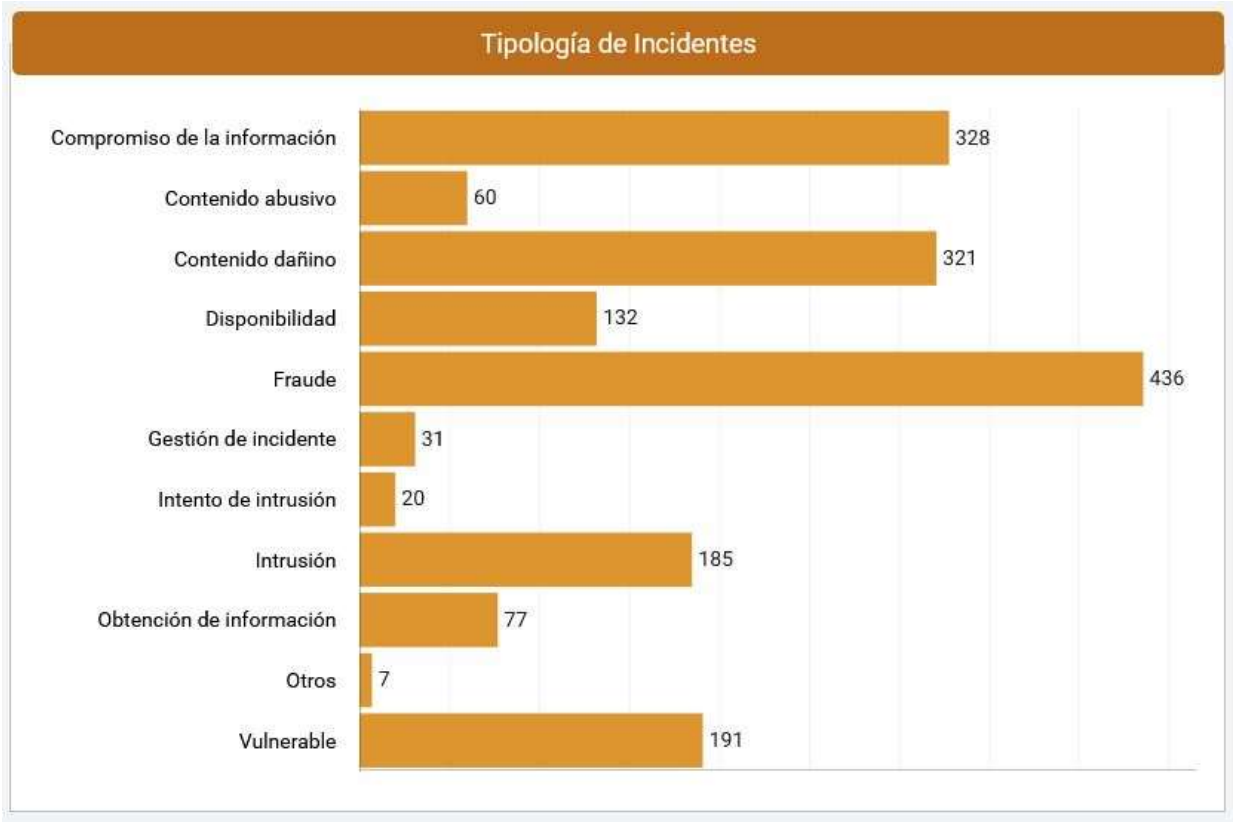
Evolución incidentes

Total	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Resumen
2023	194	134	238	95	110	106	147	112	142	148	164	198	1.788
Resumen	194	134	238	95	110	106	147	112	142	148	164	198	1.788

Del total de los incidentes gestionados en 2023, la cifra más destacada se corresponde con la categoría de ‘Fraude’ al gestionarse 436 incidentes (entre los que destacan los casos de phishing y de suplantación de identidad). Le siguen, por orden de mayor a menor número de incidentes gestionados, 328 casos de ‘Compromiso de la Información’; 321 ocasiones relacionadas con ‘Contenido dañino’, 191 sucesos catalogados como ‘Vulnerable’ o 185 incidentes relacionados con ‘Intrusión’.

A continuación, se muestra una gráfica de los incidentes gestionados por tipología.





En la información que muestra el gráfico anterior se puede observar que la mayoría de los incidentes fueron de tipo 'Fraude', ya que se reciben innumerables campañas de phishing, al ser el correo electrónico el punto de entrada con mayor probabilidad de éxito de los atacantes.

Además, destacan otras categorías: 'Contenido dañino', que consiste en la detección de comportamientos que señalan a un posible compromiso de un equipo; 'Vulnerable' supone que un servicio mal configurado o desactualizado puede permitir el acceso a un atacante, y tanto 'Compromiso de información' como 'Intrusión' consisten en cuentas de correo comprometidas.

4.2 GIR Y GESTIÓN DE CRISIS

CSIRT-CV cuenta con un Grupo de Intervención Rápida (GIR) ante incidentes de seguridad especialmente relevantes, prestando apoyo técnico y organizativo a Conselleries u otros organismos para, ante cualquier problema, recuperar el servicio interno y para los ciudadanos en el menor tiempo posible; las actuaciones del GIR se gestionarán y dirigirán desde el servicio de Gestión de Incidentes, pudiendo realizar el personal del GIR desplazamientos locales de forma puntual.

En este servicio también se contempla la Gestión de Crisis. Una crisis es un tipo especial de incidente que requiere, además del proceso de gestión de incidentes, la reunión de un comité de crisis para la toma rápida y efectiva de decisiones que permitan superar dicha crisis. CSIRT-CV ofrece un soporte en la gestión de crisis de seguridad, prestando apoyo técnico y legal e incluso facilitando ubicaciones propiedad de terceros adscritos al centro, con los que previamente se hayan firmado los correspondientes acuerdos de confidencialidad, para las reuniones del gabinete de crisis en la ciudad de Valencia.

Durante 2023, el Grupo de Intervención Rápida (GIR) de CSIRT-CV se ha activado en cinco ocasiones debido a incidentes de seguridad. Concretamente, dos ayuntamientos de la Comunitat Valenciana sufrieron un ataque de ransomware, otros dos incidentes afectaron a una Conselleria de la Generalitat Valenciana por una ataque de DDoS y temas de infraestructura y/o configuración. Por último, varias cuentas de correo de la Generalitat se vieron comprometidas al recibir un phishing, por lo que también se activó el GIR.

4.3 VULNERABILIDADES RELEVANTES GESTIONADAS

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

Durante 2023, se han detectado decenas de vulnerabilidades de impacto moderado y alto tanto en el ámbito TIC de la Generalitat Valenciana como en el sector industrial para las que se llevaron a cabo algunas medidas como, por ejemplo, enviar el aviso para notificar la vulnerabilidad en la que se recomienda actualizar a la última versión o tomar las medidas preventivas temporales hasta que llega la actualización para mitigar los posibles riesgos que pueda generar esa brecha de seguridad.

4.4 CONSULTAS GENÉRICAS

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

Durante el año, se han atendido 168 consultas de diferente índole relacionadas con la ciberseguridad. La mayoría de las consultas están relacionadas con los informes diarios que se emiten a las Consellerias, 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

El 80% de las consultas proceden del proyecto ciudadanos y CSIRT-CV las recibe a través de JIRA o correo electrónico.

5 Servicios bajo demanda y proyectos especiales

Este apartado recoge proyectos, estudios y actividades puntuales que responden a solicitudes concretas para dar respuesta a actuaciones relacionadas con el ámbito del contrato y que están fuera de la planificación del centro. Al ser servicios definidos en el catálogo, pero cuya dimensión, muy variable, no se puede concretar hasta el momento de la solicitud.

Dichos servicios bajo demanda y proyectos especiales están englobados, entre otras en las siguientes categorías:

- Procedimientos de actuación ante nuevos ataques
- Auditorías extraordinarias
- Ciberataques de gran complejidad o impacto
- Formación ante nuevos riesgos
- Test de intrusión
- Jornadas de Ciberseguridad en centros educativos de Educación Secundaria
- Ciberseguridad Industrial

En este punto podemos comentar que los proyectos realizados durante este año 2023 engloban las auditorías extraordinarias internas semestrales.

A continuación, se expone Ciberseguridad Industrial más ampliamente.

5.1 CIBERSEGURIDAD INDUSTRIAL

Este servicio pretende mejorar el nivel de ciberseguridad industrial de los sistemas SCADA gestionados por organismos de la Generalitat Valenciana y las infraestructuras críticas de la Comunitat Valenciana. Es posible realizar acciones en las líneas que se indican a continuación: Evaluaciones de ciberseguridad industrial, monitorización de la ciberseguridad industrial, concienciación especializada y proyectos de I+D+i.

Durante 2023 se ha continuado con la realización de proyectos que se comenzaron en el año 2022 y se han iniciado nuevos. Estos proyectos ayudan a mejorar la ciberseguridad industrial dentro del CSIRTCV. Con este fin, se van a describir ocho

proyectos, tres de ellos principalmente enfocados en la concienciación y promoción de los proyectos desarrollados en el CSIRT-CV y otros cinco con el objetivo de desarrollar capacidades dentro del CSIRT-CV y en su establecimiento como referente en materia de ciberseguridad industrial.

Los proyectos son:

1. I Jornada de Ciberseguridad Industrial
2. Formación entornos industriales
3. Publicación Vulnerabilidades OT
4. Finalización y mejora del proyecto SmartCity
5. Desarrollo de ataques simulados a la SmartCity
6. Desarrollo de ataques simulados al Entorno médico
7. Correlación de IOCs de la Honeynet con otras plataformas
8. Despliegue de sonda SAT-ICS

El primero de los proyectos, la I Jornada de Ciberseguridad Industrial[28] fue celebrada en la Ciudad de las Artes y las Ciencias en Valencia. Durante el evento se presentó el Estudio de Ciberseguridad Industrial de la Comunitat Valenciana[29].

El segundo proyecto, Formación entornos industriales, ha consistido en la realización de una formación de ciberseguridad industrial para el personal de la Subdirección General de Ciberseguridad. Durante la formación se han utilizado los entornos del Laboratorio de Ciberseguridad Industrial.

La Publicación de Vulnerabilidades OT es un proyecto con continuación del servicio que se comenzó a ofrecer durante el año 2021. Las vulnerabilidades críticas que afectan a los entornos industriales son publicadas en el espacio web del CSIRT-CV[30]. Además, estas vulnerabilidades se envían a los usuarios suscritos a este tipo de alertas.

El cuarto proyecto ha consistido en la finalización del entorno SmartCity y además se ha mejorado su desarrollo incluyendo una visualización 3D de la ciudad de Valencia.

El quinto y sexto proyecto han consistido en la elaboración de ataques a los entornos de SmartCity y Entorno médico. Simulando un ataque real en estos entornos y

(28) I Jornada de Ciberseguridad Industrial https://www.csirtcv.gva.es/csirtcv-i-jornada-ciberseguridad-industrial/
(29) Estudio sobre Ciberseguridad Industrial https://concienciat.gva.es/estudio-de-ciberseguridad-industrial/
(30) Apartado de Actualidad de la web del CSIRT-CV https://www.csirtcv.gva.es/actualidad/

observando las consecuencias de un ciberataque.

El séptimo proyecto ha comenzado en 2023 y se estima que finalice en 2024. Se trata de la obtención de los indicadores de compromiso (IOCs) generados en la Honeynet y la correlación de estos con otras plataformas y/o organizaciones.

Finalmente, el último proyecto y que está en activo, es el despliegue de una sonda SAT-ICS en un entorno de GVA para monitorizar el tráfico de carácter industrial y así proteger la red.

6 Servicios internos

6.1 CERTIFICACIÓN ISO 27001

Este servicio consiste en llevar a cabo todas las tareas necesarias para el mantenimiento de la certificación ISO 27001 del Sistema de Gestión de la Seguridad de la Información (SGSI) implantado en el CSIRT-CV, dando cobertura en su alcance a todos los servicios prestados por el mismo. Estas tareas incluyen, desde el prisma de la mejora continua, el mantenimiento del sistema documental del SGSI, del análisis de riesgos, el SOA (declaración de aplicabilidad), auditorías internas y soporte a las auditorías externas de revisión/certificación, indicadores, resolución de no conformidades, etc.

Durante todo el año 2023 se han realizado tareas asociadas al mantenimiento del SGSI y, por tanto, de la certificación ISO 27001. Para ello, se planifican las tareas a abordar durante el año, monitorizando su estado y ejecución por parte de los responsables asignados.

En relación con la certificación, se está llevando a cabo un Plan de adecuación a la nueva norma ISO 27001. En este sentido, se está ejecutando la revisión de la documentación SGSI y su operativa para adaptarla a los nuevos requerimientos y controles de seguridad.

En términos generales, los resultados del SGSI se consideran favorables, destacando las siguientes medidas:

- Plan de choque del área de Sistemas. Destinado a optimizar tareas y aliviar la carga de trabajo a la que está sometida el área de Sistemas.

- Plan de Gestión de Vulnerabilidades. Destinado a mejorar la identificación y corrección de vulnerabilidades, así como lograr una distribución más eficiente de responsabilidades.

- Plan de adecuación a la nueva norma ISO 27001. Las tareas de adecuación avanzan satisfactoriamente según lo planificado. El objetivo es llegar a la auditoría externa habiendo realizado la adecuación.

6.2 PROMOCIÓN DEL CENTRO Y PLAN DE COMUNICACIÓN

Servicio enfocado a la comunicación y conocimiento de la actividad de CSIRT-CV a la sociedad en general y a los diferentes colectivos más vulnerables detectados de la Comunitat Valenciana con el objetivo de fomentar un cambio de hábito general en la población en pro de una mejora de la ciberseguridad global de la ciudadanía.

Este servicio se ha desarrollado en 2023 a través de diferentes acciones, que se enumeran a continuación en los siguientes apartados: Portales web; Material gráfico; Redes sociales; Eventos y jornadas y Presencia en medios de comunicación.

6.2.1 PORTALES WEB

CSIRT-CV cuenta con dos portales: CSIRT-CV[31] y concienciaT[32] que han recibido cerca de 39.500 visitas durante 2023, lo que supone un incremento del 13% respecto al mismo período de 2022.

Por su parte, el portal de CSIRT-CV (www.csirtcv.gva.es) ha tenido 18.280 visitas el pasado año. Al igual que en ejercicios anteriores, se ha continuado con la publicación de las principales noticias acaecidas en el entorno de CSIRT-CV, la divulgación de más de 290 alertas de seguridad y la publicación de 12 boletines de actividad de carácter informativo y periodicidad mensual. En este sentido, cabe resaltar que el número de suscriptores a las alertas de seguridad asciende a 1.550 mientras que los suscriptores de los informes de actividad mensuales se sitúan en los 2.046 inscritos.

Por otra parte, el portal enfocado a la concienciación en Ciberseguridad (https://concienciat.gva.es/) ha recibido más de 21.200 visitas en 2023. Se trata del portal más representativo del Centro de Seguridad actualmente y, por tanto, cuenta con un gran número de lectores. La publicación de contenido relacionado con la ciberseguridad se ha ampliado con nuevas campañas de concienciación (ya enumeradas en el apartado anterior), nuevas infografías, cursos, guías, vídeos y noticias relacionadas con el centro de seguridad y la ciberseguridad.

(31) Web del CSIRT-CV https://www.csirtcv.gva.es/

(32) Web de concienciaT https://concienciat.gva.es/

Las descargas es uno de los indicadores más destacados de este portal. En 2023, se han registrado un total de 3.490 descargas. La guía 'Nmap6 - Listado de Comandos' encabeza el ranking de documentos más demandados con 1.281 solicitudes, seguida por la guía 'Gestores de Contraseñas' (452). El tercer puesto lo ostentan las infografías en castellano con 285 descargas en 2023.

Portal de CSIRT-CV

6.2.2 MATERIAL GRÁFICO

El material gráfico en la Concienciación juega un papel crucial al hacer que la información publicada sea más atractiva, comprensible y recordable por el usuario. Por ello, desde CSIRT- CV se ha incrementado este tipo de contenido elaborando e incorporando infografías en las cuatro campañas de concienciación de nueva creación que se han publicado en el portal de concienciaT.

También se han creado nuevas infografías[33] con motivo de días señalados relacionados con la Ciberseguridad como puede ser el 'Día de los Gamers[34]' o 'Día de los Abuelos[35]' o republicando otras infografías como 'Protección de datos[36]' o 'Internet Segura[37]' para

(33) Apartado de Infografías de la Web de concienciaT https://concienciat.gva.es/infografias/
(34) Infografía Día de los Gamers https://concienciat.gva.es/infografias/10-consejos-de-ciberseguridad-para-gamers/
(35) Infografía Día de los Abuelos https://concienciat.gva.es/infografias/sabias-que-hoy-es-el-dia-de-los-abuelos/
(36) Infografía Protección de Datos https://concienciat.gva.es/infografias/infografia-dia-proteccion-datos/
(37) Infografía Día de Internet Segura https://concienciat.gva.es/infografias/dia-de-internet-segura-pdf-interactivo/

sumarse a la causa específica con consejos relacionados con la seguridad de la información. Se han contabilizado un total de 285 descargas de infografías en castellano y 132 en valenciano durante 2023 en concienciaT, mientras que en el portal de CSIRT-CV las descargan han sumado 230 peticiones.

Asimismo, se ha generado un nuevo tipo de material gráfico: los vídeo-cartoons, que incluyen consejos básicos de seguridad. En 2023, se han abarcado dos temáticas: compras online[38] (con motivo del Black Friday, Cyber Monday, Navidad y rebajas) y smishing[39] (ante la recepción de SMS y mensajes que se suelen recibir en el teléfono móvil con el final y comienzo de un año). La estrategia es seguir generando este tipo de contenido durante 2024 al contar con buena aceptación entre el público objetivo.

6.2.3 REDES SOCIALES

CSIRT-CV está presente en las redes sociales de Facebook y X (antiguo Twitter), canales de comunicación que utiliza para crear una Cultura de Ciberseguridad entre sus seguidores a través de la emisión diarias de noticias diarias, recomendaciones, alertas y consejos sobre ciberseguridad.

Respecto a las redes sociales, los perfiles de CSIRT-CV en Facebook y X han experimentado un aumento de seguidores respecto a 2022 al pasar de los 2.287 a los 2.425 seguidores en Facebook (incremento del 6%) y de los 6.481 seguidores de 2022 a los 7.039 de 2023 en X (incremento del 8%).

Cifras positivas que instan al centro de seguridad a seguir trabajando en la misma línea, pudiendo incorporar nuevas acciones y contenidos, con el fin de atraer y retener cada vez a más usuarios a través de la concienciación en Ciberseguridad.

6.2.4 EVENTOS Y JORNADAS

Durante el año 2023, CSIRT-CV ha participado en los siguientes eventos y jornadas:

- XVII Jornadas STIC CCN-CERT y V Jornadas de Ciberdefensa[40]: ESPDEF-CERT, organizadas por el Centro Criptológico Nacional (CCN), bajo el lema ‘Compartir

(38) Vídeo-cartoon Compras Seguras https://concienciat.gva.es/sabias_que/compras-seguras-online-en-el-black-friday-cyber-monday-navidad-y-rebajas/
(39) Vídeo-cartoon Smishing https://concienciat.gva.es/sabias_que/descifrando-el-smishing-lo-que-debes-saber-para-mantenerte-a-salvo/
(40) XVII Jornadas STIC CCN-CERT https://concienciat.gva.es/sabias_que/csirt-cv-participa-en-las-xvii-jornadas-stic-ccn-cert-y-v-jornadas-de-ciberdefensa-espdef-cert/

para ganar' en Madrid. Marina Galiano, integrante de CSIRT-CV, participó con la ponencia titulada 'El Amperio contra Carga: atacando a un cargador eléctrico en una SmartCity'. Durante su intervención, explicó las consecuencias que sufre un cargador eléctrico al recibir ataques de ciberdelincuentes y cuáles podrían ser las consecuencias a nivel social (noviembre 2023).

- Congreso IARIA 2023[41] sobre Fronteras en Ciencia, Tecnología, Servicios y Aplicaciones (Annual Congress on Frontiers in Science, Technology, Services, and Applications), un evento que cuenta con la presencia de científicos, especialistas y tomadores de decisiones de todas las entidades económicas, educativas y gubernamentales en sistemas socia- les, software, análisis de ciencia de datos, comunicaciones, tecnología y servicios en red. Marina Galiano presentó dos de los proyectos en los que está trabajando e investigando CSIRT-CV en el área de la Ciberseguridad Industrial: el funcionamiento real de una Unidad de Imagen Médica y una SmartCity (noviembre, 2023).

- II Foro de responsables Autonómicos en Materia de Digitalización[42]. El director general de Tecnologías de la Información y las Comunicaciones, José Manuel García Duarte, participó en este foro en Murcia (octubre, 2023).

- El Congreso de Ciberseguridad en el sector salud 5.0[43], organizado por Red Seguridad, contó con la presencia de la subdirectora de Ciberseguridad de la Conselleria de Hacienda, Economía y Administración Pública, Carmen Serrano. (septiembre, 2023).

- La I Jornada de Ciberseguridad en el Territorio Rural[44], organizada por Diputación de León, con la participación del Centro Criptológico Nacional CCN CERT, la Federación Española de Municipios y Provincias la Oficina de Seguridad del Internauta - INCIBE contó con la participación de Lourdes Herrero, jefa del servicio de Confianza Digital de la Generalitat Valenciana (marzo, 2023).

- Mes Europeo de la Ciberseguridad[45]. Con carácter anual, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) organiza el mes dedicado a la ciberseguridad y un año más CSIRT-CV se sumó a esta iniciativa (octubre, 2023).

(41) Congreso IARIA https://concienciat.gva.es/sabias_que/csirt-cv-participa-en-el-congreso-iaria-para-exponer-dos-proyectos-relacionados-con-la-seguridad-industrial/

(42) II Foro de responsables Autonómicos en Materia de Digitalización https://comunica.gva.es/es/detalle?id=375612010&site=373422916&fbclid=IwAR3lmEnQHNR3cIKHUVBUSELwTfUCWh0bKxrjPWjfDfWvQnnzN7EqSU-MOPY

(43) Congreso de Ciberseguridad en el sector salud 5.0 https://www.redseguridad.com/canal-redseguridad/eventos/congreso-de-ciberseguridad-sector-salud-5-0-3_20230926.html

(44) I Jornada de Ciberseguridad en el Territorio Rural https://jornadasciber.dipuleon.es/

(45) Mes Europeo de la Ciberseguridad https://cybersecuritymonth.eu/countries/spain/campana-de-concienciacion-en-ciberseguridad https://cybersecuritymonth.eu/activities?containsDate=&endDate=&perPage=10&reqPage=2&searchText=&sortOrder=descending&startDate=February%202%2C%202024 https://cybersecuritymonth.eu/

- I Jornada de Ciberseguridad Industrial[46]. CSIRT-CV organizó esta jornada en la que se presentaron los resultados del primer estudio sobre el 'Estado de la Ciberseguridad Industrial de las Empresas de la Comunitat Valenciana[47]'. El conseller de Hacienda y Modelo Económico, Arcadi España, inauguró esta jornada (febrero, 2023).

- CSIRT-CV participó el dispositivo especial de vigilancia digital de las Elecciones Autonómicas del 28 de mayo[48] mediante la monitorización del proceso electoral desde el punto de vista de la ciberseguridad para prevenir, detectar, evitar y mitigar, en el caso de que fuera necesario, la intrusión de terceros o posibles ciberataques que alteraran el transcurso de la jornada electoral.

- El IES de Camp de Morvedre celebró la Semana de Internet e invitó al CSIRT-CV a participar con una charla de concienciación en Ciberseguridad a los estudiantes de Bachillerato y 4º de la ESO de este centro.

- UNDP/ UNICC/FIRST Technical Colloquium. El 25 y 26 de septiembre de 2023, CSIRT-CV participó en estas jornadas, que se celebraron en las instalaciones de Naciones Unidad en Quart de Poblet, en la que se presentaron avances en la gestión de la ciberseguridad, así como exponer la investigación de ciberincidentes relevantes.

- XVII Jornadas STIC CCN-CERT y V Jornadas de Ciberdefensa: ESPDEF-CERT, organizadas por el Centro Criptológico Nacional (CCN), bajo el lema "Compartir para ganar" en Madrid. Marina Galiano, integrante de CSIRT-CV, participó con la ponencia titulada 'El Amperio contra Carga: atacando a un cargador eléctrico en una SmartCity'. Durante su in- tervención, explicó las consecuencias que sufre un cargador eléctrico al recibir ataques de ciberdelincuentes y cuáles podrían ser las consecuencias a nivel social (noviembre 2023).

- Congreso IARIA 2023 sobre Fronteras en Ciencia, Tecnología, Servicios y Aplica- ciones (Annual Congress on Frontiers in Science, Technology, Services, and Applications), un evento que cuenta con la presencia de científicos, especialistas y tomadores de decisio- nes de todas las entidades económicas, educativas y gubernamentales en sistemas socia- les, software, análisis de ciencia de datos, comunicaciones, tecnología y servicios en red. Marina Galiano presentó dos de los proyectos en los que está trabajando e investigando CSIRT-CV en el área de la Ciberseguridad Industrial: el funcionamiento real de una Unidad de Imagen Médica y una SmartCity (noviembre, 2023).

(46) Nota de prensa de la I Jornada de Ciberseguridad Industrial https://comunica.gva.es/es/detalle?id=369846892&site=174859746

(47) Estudio sobre el 'Estado de la Ciberseguridad Industrial de las Empresas de la CV https://concienciat.gva.es/sabias_que/i-jornada-de-ciberseguridad-industrial-en-valencia-inscribete-antes-del-8-de-febrero/

(48) Elecciones Autonómicas del 28 de mayo https://concienciat.gva.es/sabias_que/sabias-que-csirt-cv-monitorizara-las-elecciones-del-28m-para-prevenir-detectar-y-evitar-posibles-ciberataques/

- La Generalitat Valenciana recibe el premio CIO 100 Awards 2023[49] al mejor proyecto de Seguridad y Resiliencia. José Manuel García Duarte, fue el encargado de recoger el galardón. Este premio reconoce el esfuerzo de la institución, y en particular, de la Dirección General de Tecnologías de la Información y las Comunicaciones (DGTIC), a través del Centro de Ciberseguridad de la Comunidad Valenciana (CSIRT-CV), en el diseño y ejecución del Plan de Ciberseguridad dirigido a un total de 584 entidades locales de la región.

Nota de prensa del premio CIO 100 Awards Spain 2023

- II Foro de responsables Autonómicos en Materia de Digitalización. El director general de Tecnologías de la Información y las Comunicaciones, José Manuel García Duarte, participó en este foro en Murcia (octubre, 2023).

- El Congreso de Ciberseguridad en el sector salud 5.0, organizado por Red Seguridad, contó con la presencia de la subdirectora de Ciberseguridad de la Conselleria de Hacienda, Economía y Administración Pública, Carmen Serrano. (septiembre, 2023).

- La I Jornada de Ciberseguridad en el Territorio Rural, organizada por Diputación de León, con la participación del Centro Criptológico Nacional CCN CERT, la Federación Española de Municipios y Provincias la Oficina de Seguridad del Internauta - INCIBE contó con la participación de Lourdes Herrero, jefa del servicio de Confianza Digital de la Generalitat Valenciana (marzo, 2023).

- Mes Europeo de la Ciberseguridad. Con carácter anual, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) organiza el mes dedicado a la

(49) Premio CIO 100 Awards 2023 https://dgtic.gva.es/va/-/la-generalitat-recibe-el-premio-cio-100-awards-spain-2023-al-proyecto-del-a%C3%B1o-de-innovaci%C3%B3n-tecnol%C3%B3gica-en-ciberseguridad

ciberseguridad y un año más CSIRT-CV se sumó a esta iniciativa (octubre, 2023).

- I Jornada de Ciberseguridad Industrial. CSIRT-CV organizó esta jornada en la que se presentaron los resultados del primer estudio sobre el 'Estado de la Ciberseguridad Industrial de las Empresas de la Comunitat Valenciana'. El conseller de Hacienda y Modelo Económico, Arcadi España, inauguró esta jornada (febrero, 2023).

- CSIRT-CV participó el dispositivo especial de vigilancia digital de las Elecciones Autonómicas del 28 de mayo mediante la monitorización del proceso electoral desde el punto de vista de la ciberseguridad para prevenir, detectar, evitar y mitigar, en el caso de que fuera necesario, la intrusión de terceros o posibles ciberataques que alteraran el transcurso de la jornada electoral.

- El IES de Camp de Morvedre celebró la Semana de Internet e invitó al CSIRT-CV a participar con una charla de concienciación en Ciberseguridad a los estudiantes de Bachillerato y 4º de la ESO de este centro.

- UNDP/ UNICC/FIRST Technical Colloquium. El 25 y 26 de septiembre de 2023, CSIRT-CV participó en estas jornadas, que se celebraron en las instalaciones de Naciones Unidad en Quart de Poblet, en la que se presentaron avances en la gestión de la ciberseguridad, así como exponer la investigación de ciberincidentes relevantes.

6.2.5 VISITAS A CSIRT-CV

A lo largo de 2023, CSIRT-CV ha recibido las siguientes visitas:

- CIPFP Misericordia (Centro Integrado Público de Formación Profesional).
- Universitat de València.
- Ayuntamiento de Alcoi.
- Ayuntamiento de Castellón.
- Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

6.2.6 ENTREVISTAS REALIZADAS AL EQUIPO DE CSIRT-CV

- Autelsi Insights[50] entrevista al director general de Tecnologías de la Información y las Comunicaciones (DGTIC) de la Conselleria de Hacienda, Economía y Administración Pública, José Manuel García Duarte (12/12/2023).
- Radio Valencia Cadena Ser[51] entrevista a la subdirectora de Ciberseguridad de la Conselleria de Hacienda, Economía y Administración Pública, Carmen Serrano, para hablar del balance de actividad de 2022 de CSIRT-CV (05/07/2023).

6.2.7 PRESENCIA EN MEDIOS

Este apartado recoge algunas de las noticias de los medios de comunicación en las que ha aparecido CSIRT-CV.

CSIRT-CV ha estado presente en varios medios de comunicación a lo largo de 2023. A continuación, puede verse un ejemplo de ello:

I Jornada Ciberseguridad Industrial

(50) Entrevista al DG de la DGTIC https://autelsinsights.es/jose-manuel-garcia-duarte-director-general-de-tecnologias-de-la-informacion-y-las-comunicaciones-de-la-generalitat-valenciana/

(51) Entrevista a la subdirectora de Ciberseguridad: https://cadenaser.com/comunitat-valenciana/2023/07/05/la-generalitat-gestiono-1144-ciberataques-el-ano-pasado-radio-valencia/

- Nota prensa GVA: Arcadi España: “El estudio de la ciberseguridad industrial en las em- presas valencianas nos permitirá definir la estrategia más segura para el sector” https://comunica.gva.es/es/detalle?id=369846892&site=17485974 (15/02/2023).

- ConcienciaT: https://concienciat.gva.es/sabias_que/i-jornada-de-ciberseguridad-industrial-en-valencia-inscribete-antes-del-8-de-febrero/ (15/02/2023).

- CSIRT-CV: https://www.csirtcv.gva.es/csirtcv-i-jornada-ciberseguridad-industrial/ (15/02/2023).

- INCIBE: https://www.incibe.es/agenda/i-jornada-ciberseguridad-industrial-comunidad-valenciana (15/02/2023).

- UNION PROFESIONAL DE VALENCIA: https://www.unionprofesionalvalencia.com/agenda/i-jornada-de-ciberseguridad-industrial-de-la-comunidad-valenciana/ (15/02/2023).

- COL.LEGI OFICIAL DE PSICOLOGÍA: https://www.cop-cv.org/noticia/15524-i-jornada-de-ciberseguridad-industrial-de-la-comunidad-valenciana#.Y_NmGXbMI2w (15/02/2023).

- El periodic.com: Arcadi España: “El estudio de la ciberseguridad industrial en las empresas nos permitirá definir la estrategia más segura para el sector” https://www.elperiodic.com/arcadi-espana-estudio-ciberseguridad-industrial-empresas-permitira-definir-estrategia-segura-para-sector_882930 (15/02/2023).

- Valencia Plaza: El ITE analiza potenciales puntos débiles para proteger a la industria valenciana de ciberataques https://valenciaplaza.com/ite-analiza-potenciales-puntos-debiles-proteger-industria-valenciana-ciberataques (nombran al CSIRT-CV y el Estudio de Ciberseguridad) (25/05/2023).

Ransomware Ayuntamiento de Requena

- Levante EMV: Requena aún arrastra dos meses después problemas informáticos tras el ataque https://www.levante-emv.com/comunitat-valenciana/requena-utiel/2023/02/17/requena-problemas-ciberataque-hackeo-83101509.htm (17/02/2023).

CSIRT en España

- Los CSIRT con sede en España en los foros de referencia Los CSIRT con sede en España en los foros de referencia https://revistasic.es/agora-sic/los-csirts-espanoles-en-los-foros-de-referencia/ (03/03/2023).

Campaña de concienciación Inteligencia Artificial: ¿amiga o enemiga?

- GVA nota de prensa: El Centro de Seguridad TIC lanza una campaña para concienciar a la ciudadanía sobre el buen uso de la inteligencia artificial y ChatGPT https://comunica.gva.es/va/detalle?id=372813854&site=174859746 (16/06/2023).
- Valencia News: El Centro de Seguridad TIC lanza una campaña para concienciar a la ciudadanía sobre el buen uso de la Inteligencia Artificial y ChatGPT https://valencianews.es/economia/el-centro-de-seguridad-tic-lanza-una-campana-para-concienciar-a-la-ciudadania-sobre-el-buen-uso-de-la-inteligencia-artificial-y-chatgpt/ (16/06/2023).
- Noticias CV El Centro de Seguridad TIC lanza una campaña para concienciar sobre el buen uso de la inteligencia artificial y ChatGPT https://www.noticiascv.com/el-centro-de-seguridad-tic-lanza-una-campana-para-concienciar-sobre-el-buen-uso-de-la-inteligencia-artificial-y-chatgpt/ (20/06/2023).

Balance Actividad CSIRT-CV 2022

- Nota de prensa sobre balance actividad 2022 a través de GVA https://comunica.gva.es/va/detalle?id=372957322&site=174859746 (27/06/2023).
- La Vanguardia: La Generalitat gestionó 1.144 ciberataques en 2022, un 57 % de ellos intentos de fraude https://www.lavanguardia.com/vida/20230628/9073519/generalitat-gestiono-1-144-ciberataques-2022-57-intentos-fraude.html (28/06/2023).
- Valencia Plaza: El Centro de Ciberseguridad de la Comunitat Valenciana gestiona 1.144 incidentes en 2022 https://valenciaplaza.com/centro-ciberseguridad-comunitat-valenciana-gestiona-1144-incidentes-2022 (28/06/2023).
- El Economista: Los ciberataques a la Administración valenciana aumentaron un 24% el año pasado https://www.eleconomista.es/tecnologia/noticias/12345982/06/23/los-ciberataques-a-la-administracion-valenciana-aumentaron-un-24-el-ano-pasado.html (29/06/2023).
- CiberSecurityNews: El Informe anual de CSIRT-CV revela aumento de ciberamenazas y tendencias preocupantes en 2022 https://cybersecuritynews.es/el-informe-anual-de-CSIRT-CV-revela-aumento-de-ciberamenazas-y-tendencias-preocupantes-en-2022/ (29/06/2023).

Convenio para impulsar la ciberseguridad

- Cuadernos de Seguridad: Nuevo convenio en la Comunidad Valenciana para impulsar la digitalización y ciberseguridad https://cuadernosdeseguridad.com/2023/07/convenio-comunidad-valenciana-ciberseguridad/ (05/07/2023).

Correos engañosos

- Levante: Los correos engañosos son ya más de la mitad de los ataques en la red https://www.levante-emv.com/comunitat-valenciana/2023/07/18/correos-engano- sos-son-mitad-ataques-90007164.html (18/047/2023).

Jornadas Concienciación en centros educativos

- Nota de prensa Conselleria Hacienda: La Generalitat organiza nuevos talleres prácticos para formar al alumnado de la ESO, a sus familiares y a docentes frente a los ciberdelitos y el ciberacoso https://comunica.gva.es/es/detalle?id=374398223&site=373422916 (11/09/2023).
- La Vanguardia: La Generalitat formará en Ciberseguridad al alumnado de ESO, familias y profesores https://www.lavanguardia.com/vida/20230911/9218861/generalitat-formara-ciberseguridad-alumnado-familias-profesores.html
- El Periòdic: Nuevos talleres prácticos para formar al alumnado de la ESO, a sus familiares y a docentes frente a los ciberdelitos y el ciberacoso https://www.elperiodic.com/nuevos-talleres-practicos-para-formar-alumnado-familiares-docentes-frente-ciberdelitos-ciberacoso_921528 (11/09/2023)

Campaña 'Para. Piensa. Conecta. Sé más inteligente que un hacker

- Presidencia lanza la nota de prensa de la campaña del mes de la Ciberseguridad: La Generalitat lanza la campaña de concienciación 'Para. Piensa. Conecta' con motivo del Mes Europeo de la Ciberseguridad https://comunica.gva.es/va/detalle?id=374899286&site=373422916 (01/10/2023).
- Terreta Radio: La Generalitat lanza la campaña de concienciación 'Para. Piensa. Conecta' con motivo del Mes Europeo de la Ciberseguridad https://terretaradio.es/la-generalitat-lanza-la-campana-de-concienciacion-para-piensa-conecta-con-motivo-del-mes-europeo-de-la-ciberseguridad/ (01/10/2023).
- Gob clipping: La Generalitat lanza la campaña de concienciación Para. Piensa. Conecta con motivo del Mes Europeo de la Ciberseguridad

https://govclipping.com/es/valencia/press_release/2023-10-01/19505-generalitat-lanza-campana-concienciacion-para-piensa-conecta-motivo-mes-europeo-ciberseguridad (01/10/2023).

Campaña Dispositivos Conectados

- Nota de prensa campaña Dispositivos Conectados: La Generalitat lanza recomendaciones de seguridad sobre juguetes y dispositivos conectados a Internet ante la campaña navideña https://comunica.gva.es/va/detalle?id=377260536&site=373422916 (11/12/2023).

- El Español: Dispositivos conectados pero sin riesgos: la Generalitat recomienda aumentar la seguridad en los IoT https://www.elespanol.com/alicante/20231211/dispositivos-conectados-sin-riesgos-generalitat-recomienda-aumentar-seguridad-iot/816418574_0.html (11/12/2023).

- Crónica Local: Recomendaciones de seguridad sobre juguetes y dispositivos conectados a Internet https://www.cronicalocal.es/noticia/5367/noticias-regionales/recomendaciones-de-seguridad-sobre-juguetes-y-dispositivos-conectados-a-internet.html (11/12/2023).

- Castellón Diario: El riesgo en juguetes y dispositivos conectados a Internet https://castellondiario.com/el-riesgo-en-juguetes-y-dispositivos-conectados-a-internet/ (11/12/2023).

- Esdiario: Generalitat lanza una campaña para prever ciberataques en los regalos navideños https://www.esdiario.com/valencia/776495607/generalitat-ciberataques-regalos-juguetes-dispositivos.html (11/12/2023).

Centro de Innovación y Competencia en Ciberseguridad

- El Consell autoriza el convenio de colaboración para impulsar el Centro de Innovación y Compe- tencia en Ciberseguridad https://www.csirtcv.gva.es/el-consell-autoriza-el-convenio-de-colaboracion-para-impulsar-el-centro-de-innovacion-y-competencia-en-ciberseguridad/ (15/12/2023).

Premio CIO 100 Awards Spain

- Nota de prensa de GVA: La Generalitat recibe el premio CIO 100 Awards Spain 2023 al proyecto del año de innovación tecnológica en ciberseguridad https://dgtic.gva.es/va/-/la-generalitat-recibe-el-premio-cio-100-awards-spain-2023-al-proyecto-del-a%C3%B1o-de-innovaci%C3%B3n-tecnol%C3%B3gica-en-ciberseguridad (15/12/2023).

- Computer World: Los ‘CIO 100 Awards Spain 2023’ distinguen los proyectos de

innovación tecnológica del año https://www.computerworld.es/tendencias/los-cio-100-awards-spain-2023-distinguen-los-proyectos-de-innovacion-tecnologica-del-ano (14/12/2023).

- Valencia Plaza: La Generalitat, premio CIO 100 Awards Spain al proyecto del año de innovación en ciberseguridad https://valenciaplaza.com/generalitat-premio-cio-100-awards-spain-proyecto-ano-innovacion-ciberseguridad (15/12/2023).

- Es radio: La Generalitat recibe el premio CIO 100 Awards Spain 2023 https://www.esdiario.com/valencia/845247702/la-generalitat-recibe-el-premio-cio-100-awards-spain-2023.html (15/12/2023).

- CIO España: La Generalitat Valenciana, galardonada con el premio 'CIO 100 Awards' al mejor proyecto de Seguridad y Resiliencia https://www.ciospain.es/administraciones-publicas/la-generalitat-valenciana-galardonada-con-el-premio-cio-100-awards-al-mejor-proyecto-de-seguridad-y-resiliencia (19/12/2023).

CSIRT-CV

Centre Seguretat TIC
de la Comunitat Valenciana