CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

INFORME DE ACTIVIDADES, CIBERAMENAZAS Y TENDENCIAS

2019

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

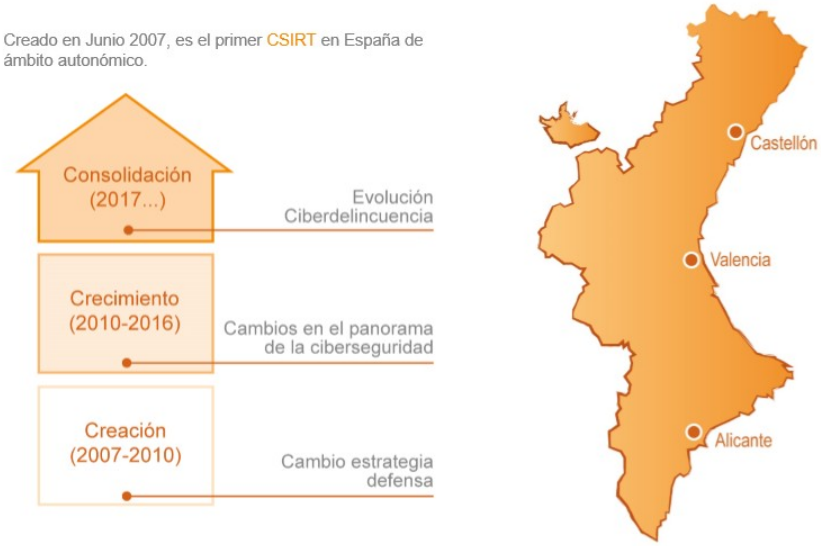
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa
UNIÓN EUROPEA

Índice

1 CSIRT-CV

CSIRT-CV es el Centro de Seguridad TIC de la Comunitat Valenciana.

Nace en junio del año 2007, como una apuesta de la Generalitat de la Comunitat Valenciana por la seguridad en la red.

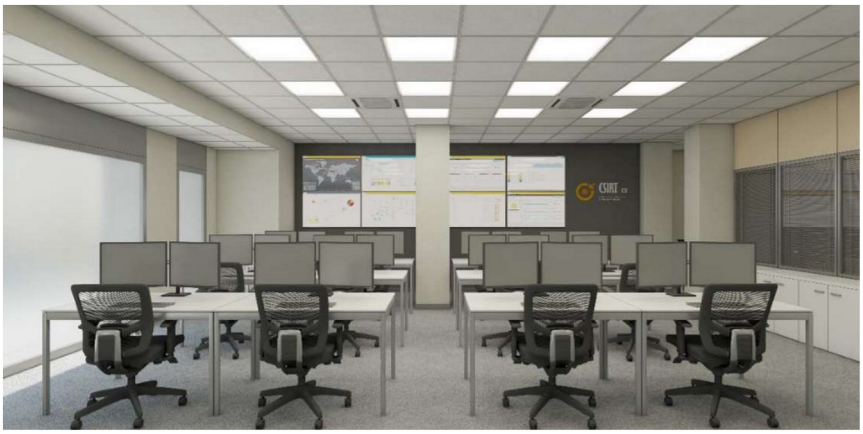


Se trata de una iniciativa pionera al ser el primer centro de estas características que se crea en España para un ámbito autonómico. Actualmente **CSIRT-CV** está adscrito a la Dirección General de Tecnologías de la Información y las Comunicaciones dentro de la Consellería de Hacienda y Modelo Económico.

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

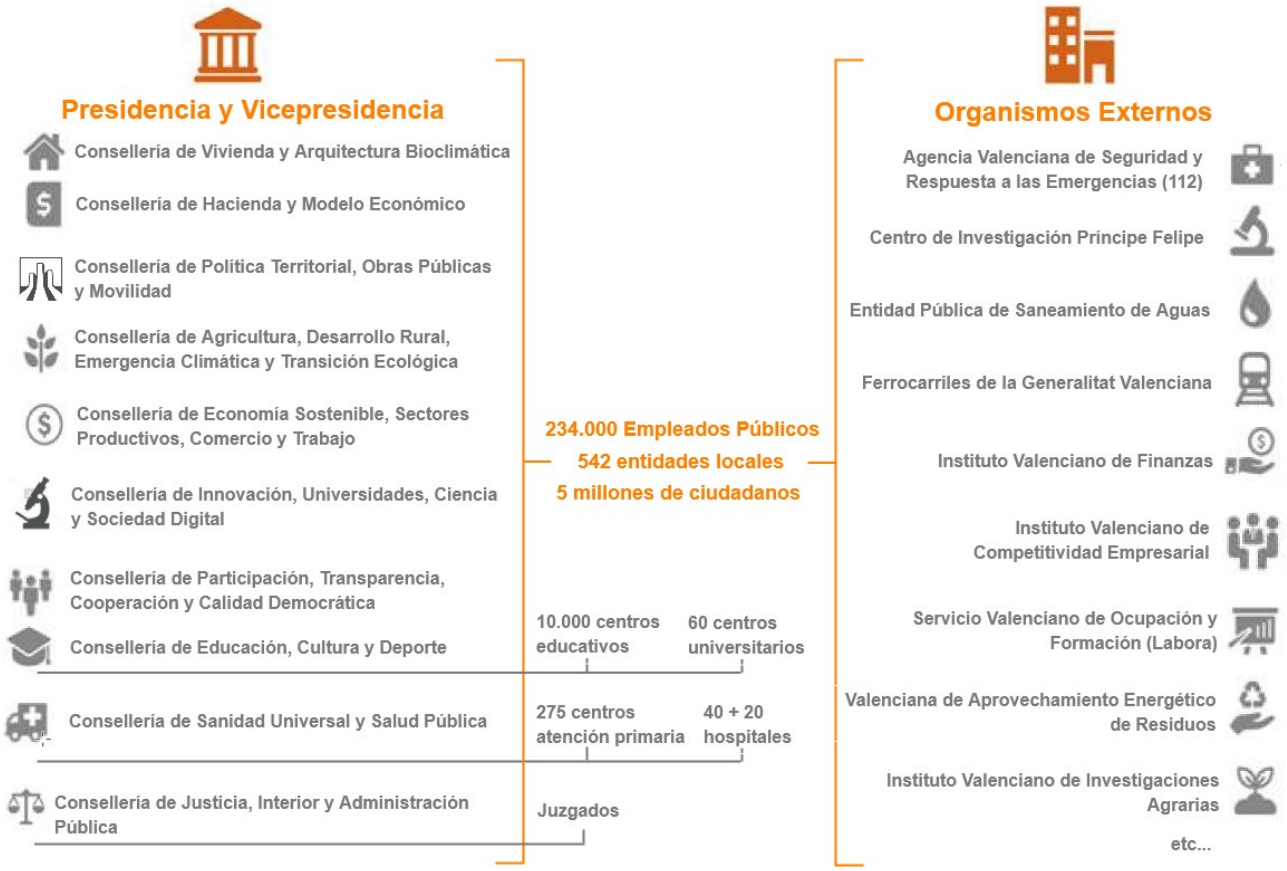
Los colectivos destinatarios de estos servicios son:

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



Sala central de operaciones de CSIRT-CV

El principal objetivo de **CSIRT-CV** es contribuir a la mejora de la seguridad de los sistemas de información dentro de su ámbito, así como promover una cultura de seguridad y buenas prácticas en el uso de las nuevas tecnologías de forma que se minimicen los incidentes de seguridad y permita afrontar de forma activa las nuevas amenazas que pudieran surgir.



2 Servicios ofrecidos. Algunos datos

CSIRT-CV dispone de un amplio abanico de servicios ofrecidos en su ámbito que abarcan con amplitud todos los posibles escenarios dados dentro del ecosistema de la ciberseguridad:

Prevención	Detección	Respuesta
Auditorías de seguridad	Sistemas de decepción	Gestión de incidentes de seguridad
Test de intrusión	Securización de entornos	Grupo de intervención rápida
Informes y alertas. Observatorio de seguridad	Auditoría de seguridad semántica	Gabinete de crisis
Consultoría técnica y legal	Informe forense pericial	
Plan Valenciano de Capacitación	Detección de intrusos	
Intercambio de información	Detección de APT	
Cuadro de mando de seguridad	Test de intrusión	
I+D+i		
Laboratorio de malware		
Monitorización de servicios Web		
Normalización		
Auditoría ENS		
Validación de código		
Consultoría sobre las ISO 27001:2013		
Análisis de riesgos		
Auditoría RGPD		
Ciberseguridad industrial		
Planes de mejora de la seguridad		

Los servicios ofertados por CSIRT-CV pueden ser realizados de manera proactiva o bajo petición. La siguiente tabla se muestra algunos datos de los más relevantes.

Servicio ofrecidos	Total año 2019
Test de intrusión	56
Auditorías de seguridad	94
Consultoría técnica, organizativa y legal	168
Emisión notas de alerta temprana	19

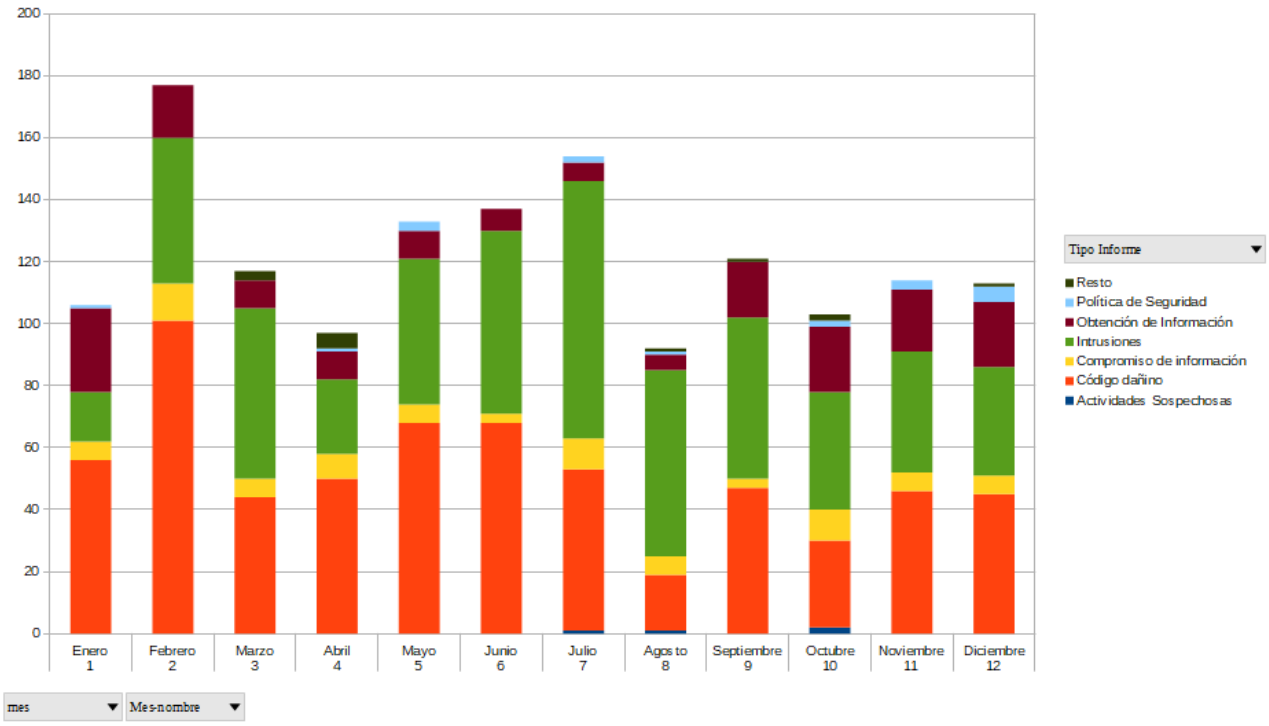
Entre las consultas externas atendidas predominan las relacionadas con dispositivos IoT, almacenamiento en la nube, mensajería segura, Office 365, correos fraudulentos, y consultas relacionadas con la implantación de controles del ENS entre otros.

2.1 Gestión de incidentes de seguridad

La actividad principal de CSIRT-CV se centra, como todo CSIRT, en la **gestión de incidentes de seguridad**. Para ello se proporciona una solución integral a cualquier compromiso relacionado con seguridad de la información que se pueda producir, incluyendo entre otros: 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.

Durante el 2019 el equipo de analistas del centro han gestionado un total de 1742 incidentes de seguridad y se ha tenido que movilizar al Grupo de Intervención Rápida en una ocasión.

A continuación se muestra una gráfica con la distribución de la tipología y evolución temporal:



Podemos deducir que los incidentes de tipo "Intrusiones" (intentos de acceso no autorizados o intrusiones) y los de tipo "Código dañino", son los que más se han dado por volumen. Se observa también que en el segundo semestre se ha vuelto a alcanzar la cantidad de incidentes de tipo "Obtención de Información" (relacionados a correos maliciosos) de principio de año que se habían visto reducidos entre los meses de mayo y agosto.

3 Ciberamenazas y tendencias

Durante el 2019 las dos principales ciberamenazas a las que hacer mención son los ataques de **Denegación de Servicio,** que se fueron detectados durante la primera mitad de año en nuestro ámbito, y el inicio de varias **campañas de distribución del malware Emotet**, que dieron comienzo en las últimas semanas del 2019.

Al margen de dichos ataques, se ha detectado que los principales objetivos a explotar han sido **servidores Web**, fundamentalmente a través del intento de subida de ficheros que permitan tomar el control del sitio, o a través del intento de explotación de vulnerabilidades de inyección SQL, con el objetivo de manipular las bases de datos del servicio.

Además, se ha puesto de manifiesto de nuevo (como es habitual cada año) un incremento de intentos de acceso a través de **servicios directos** a los equipos como SSH, VNC o escritorios remotos.

Los **gestores de contenido** más atacados en nuestro ámbito han sido Drupal -de una forma muy agresiva- seguidos de Joomla y Wordpress. En el caso de Drupal, este incremento de ataques está motivado por la reciente publicación de una vulnerabilidad crítica, que se suma a las publicadas en 2018 (Drupalgeddon), y que permiten provocar fallos en la disponibilidad, confidencialidad e integridad de los sistemas.

Tal y como sucedía el pasado año, se ha detectado un aumento significativo de ataques hacia routers y otros elementos de **electrónica de red**, confirmando la tendencia en alza de usar estos dispositivos como punto de entrada a las organizaciones. En este contexto, es destacable que nuevas botnets, como Echobot, utilizan vulnerabilidades en estos dispositivos para propagarse, como ha quedado patente en nuestras fuentes de información.

Por otro lado, las reiteradas vulnerabilidades críticas en plataformas como Oracle Weblogic provocan que los delincuentes se fijen más en ellas como objetivo para introducir malware en los servidores, tal y como se ha visto en nuestros sistemas de detección de intrusos.

En cuanto a **países** de los que proceden los ciberataques, el top 5 ha sido USA, China, Alemania, Gran Bretaña y Francia. Recordar que la geolocalización del ataque no siempre corresponde a la del origen del atacante, y que en este top 5 influye también el hecho de que en esos países se concentre un mayor volumen de equipos y servicios, siendo más probable un ataque desde ellos.

Remarcar por último que entre los sectores más atacados encontramos el educativo y las administraciones locales (ayuntamientos).

A continuación se detallan algunos de los puntos más interesantes a destacar en este aspecto.

3.1 Vulnerabilidad en el plugin Calmar Webmedia Total Donations (CVE-2019-6703)

Los **gestores de contenido (CMS) son un gran blanco para los atacantes** ya que su uso está muy extendido. Los CMS además, cuentan habitualmente con una gran variedad de módulos y/o extensiones que amplían sus funcionalidades pero que, en ocasiones, no están lo suficientemente protegidos ni mantenidos, y se convierten en una potencial puerta de entrada de un atacante.

En enero de 2019 se publicó una vulnerabilidad de criticidad alta que afectaba al plugin "Calmar Webmedia Total Donations" para Wordpress. Esta vulnerabilidad permitía tomar el control total de los sitios sin necesidad de estar autenticado. Los delincuentes no tardaron en aprovechar esta vulnerabilidad para infectar de forma masiva sitios Wordpress.

Desde CSIRT-CV, durante este año, se ha detectado un gran volumen de intentos de explotación de este fallo en las infraestructuras de Generalitat.

3.2 Vulnerabilidad en el componente Oracle WebLogic Server de Oracle Fusion Middleware (CVE-2019-2725)

Durante 2018 se detectó el intento de explotación masivo de una vulnerabilidad que afecta al componente Oracle WebLogic Server de Oracle Fusion Middleware, **CVE-2017-10271**[1] y que los atacantes utilizaban principalmente para distribuir CryptoMiners[2].

Siguiendo con el mismo patrón, en abril se publicó una nueva vulnerabilidad de criticidad alta que afecta de nuevo a WebLogic, en concreto en el componente Oracle WebLogic Server de Oracle Fusion Middleware (subcomponente: Web Services) que, de una manera sencilla permitía que un atacante no autenticado con acceso a la red a través de HTTP, ponga en peligro la integridad, confidencialidad y disponibilidad de los servidores Oracle WebLogic.

1 https://nvd.nist.gov/vuln/detail/CVE-2017-10271
2 https://www.fireeye.com/blog/threat-research/2018/02/cve-2017-10271-used-to-deliver-cryptominers.html

3.3 ThinkPHP RCE (CVE-2018-20062)

ThinkPHP es un conocido framework open-source de desarrollo Web. A finales de 2018 se publicó una vulnerabilidad de criticidad alta por la que se podía ejecutar código remotamente. No tardó en publicarse un exploit que los delincuentes utilizaron para, de forma masiva, comprometer miles de sitios.

Los sistemas de detección de CSIRT-CV registraron cientos de intentos de explotación de esta vulnerabilidad contra la infraestructura de Generalitat.

3.4 Vulnerabilidad en Drupal (CVE-2019-6340)

El pasado 2018, los análisis de CSIRT-CV concluyeron que Drupal, con diferencia, había sido el CMS más atacado en nuestro ámbito. En concreto, se habían intentado explotar de forma masiva dos vulnerabilidades, **CVE-2018-7600**[3] **y CVE-2018-7602**. La primera de ellas (**Drupalgeddon2**) corresponde a una vulnerabilidad crítica en el núcleo de Drupal que permitiría ejecución remota de código (RCE) y que fue publicada y parcheada en marzo de 2018, afectando a miles de sitios web[4]. La segunda vulnerabilidad se publicó en abril siendo también de tipo RCE crítico.

Actualmente se siguen explotando activamente estas vulnerabilidades sumándose una nueva vulnerabilidad para Drupal, CVE-2019-6340, que fue publicada el pasado febrero. Una validación incorrecta de datos de entrada provocaría fallos en el sistema atacado.

Desde CSIRT-CV se han detectado numerosos registros de este tipo de intentos de ataque.

3.5 Botnet Echobot

Echobot es una botnet en auge diseñada para atacar gran cantidad de equipos cliente y de red como VMware, Oracle y hasta routers con DD-WRT, entre otras decenas de modelos.

Esta botnet lleva tiempo funcionando utilizando la botnet Mirai como red de ataque. Esta había tiene por objetivo routers (ASUS y NETGEAR, principalmente), además de equipos Belkin, chips Realtek, equipos DELL y hasta sistemas de virtualización VMware y servidores Oracle con el fin de tomar el control de ellos, infectarlos con malware y utilizarlos en ataques de mayor escala.

En CSIRT-CV se ha detectado un incremento de intentos de compromiso por esta botnet.

3 https://www.certsi.es/alerta-temprana/vulnerabilidades/cve-2018-7600
4 https://badpackets.net/over-100000-drupal-websites-vulnerable-to-drupalgeddon-2-cve-2018-7600/

3.6 Crawlers

Durante este año se han detectado numerosos escaneos con herramientas automáticas, como viene siendo habitual en los últimos años. En particular se ha detectado **un aumento del uso de herramientas de tipo crawler como BLEXBot**.

3.7 Malware

El análisis de las tendencias empleadas por los atacantes en este año indica que el phishing sigue siendo la principal vía de entrada a las organizaciones para la distribución de código dañino. Del mismo modo, los formatos y extensiones de los documentos analizados suelen ser en su mayoría **ficheros ofimáticos**. Estos archivos maliciosos adjuntos al correo suelen ser empleados para explotar vulnerabilidades conocidas de Microsoft Office con exploits públicos, y principalmente son vulnerabilidades existentes de años anteriores (2017 y 2018) según el análisis.

Cabe destacar una nueva variante observada en ataques de phishing empleando ficheros comprimidos con formato poco habitual como es "ACE", cuyo contenido es un fichero ejecutable malicioso.

Gran parte del malware analizado es de tipo "Downloader", cuya función principal es la de descargar otro código dañino más avanzado que amplíe las capacidades del original, incorporando funciones dañinas adicionales.

La tipología del código dañino detectado es variada, desde malware simple pero con alto impacto, como Orbix, una antigua amenaza que afecta a la disponibilidad del equipo afectado, hasta DarkGate, una nueva amenaza compleja y sigilosa que dispone de capacidades de robo de contraseñas, ransomware o minería de criptomonedas.

A continuación se indican las diversas técnicas empleadas contra nuestro ámbito en el año 2019:

- Explotación de vulnerabilidades de Microsoft Office mediante el uso de ficheros ofimáticos (Rich y Composite Document File).
- Ficheros ofimáticos (Microsoft Word 2007 y Microsoft Excel) con macros.
- Ficheros PDF con enlaces malicioso incrustados en su contenido.
- Ficheros comprimidos con formato"ACE".
- Uso de ficheros comprimidos "RAR", "ZIP" con contenido malicioso.

3.8 Campañas masivas de distribución de malware emotet

A finales de agosto de 2019 se observó, tras la publicación de diversas noticias de seguridad, que los servidores de C&C del grupo detrás de **Emotet,** se reactivaban tras un parón de inactividad en los meses de junio y julio. Menos de un mes después de esta reactivación, dio comienzo una campaña de envío de correos maliciosos a países de todo el mundo.

Los primeros correos con la firma Emotet observados el 16 de septiembre iban dirigidos principalmente a personas, empresas y entidades gubernamentales de Alemania, Reino Unido, Polonia, Italia y USA. El 17 de septiembre organismos públicos en España comenzaron a detectar actividad de esta Campaña, incluido CSIRT-CV.

Para infectar una organización con Emotet, los actores maliciosos envían oleadas de correos con documentos ofimáticos adjuntos capaces de descargar el malware de internet y ejecutarlo, permitiendo a este **robar credenciales, analizar el entorno, moverse por la organización, etc.**

En la Comunitat Valenciana se han detectado varias organizaciones que han sufrido este tipo de incidentes.

3.9 Incidentes derivados de ingeniería social

A lo largo de 2019 se ha detectado un notable aumento de intento de compromisos o fraude usando técnicas de ingeniería social, principalmente a través de los siguientes métodos:

- Oleadas de llamadas de **falsos técnicos de Microsoft** que intentan hacerse con el control del equipo de la víctima
- **Fraude al CEO**
- Correos **phishing** dirigidos basados en información pública o robada sobre las víctimas

Con este tipo de incidentes, las medidas técnicas a aplicar para evitar casos de infección son necesarias para minimizar el impacto, sin embargo no son suficientes, siendo imprescindible una labor de **concienciación** a los usuarios.

3.10 Elecciones 2019

Cualquier proceso electoral es complejo y tiene una infraestructura, tanto física como tecnológica, críticas para su buen funcionamiento y la fiabilidad de los resultados que se deriven de su desarrollo.

En los últimos años, dichos comicios electorales han sido especialmente objetivo de distintos tipos de ciberataques con diferentes objetivos, desde campañas de desinformación, intentos de manipulación de la información que se expone al público, denegación de servicio a las infraestructuras tecnológicas involucradas en él, etc.

Con motivo de las elecciones que se llevaron a cabo el pasado abril, mayo y noviembre, CSIRT-CV puso en marcha un operativo especial que contemplaba varias vertientes de actuación para evitar que el desarrollo de las elecciones pudiese verse perjudicado a través de ataques informáticos:

- Vigilancia digital en fuentes abiertas (Social Intelligence)
- Monitorización de sistemas y redes
- Auditorías de seguridad
- Bastionado de entornos

Con un equipo multidisciplinar formado por casi todo el equipo de CSIRT-CV se inició una campaña de preparación para este operativo a finales de enero y que duró hasta finales de junio.

4 Plan Valenciano de Capacitación

Conseguir una gestión eficaz de la ciberseguridad no depende sólo de la implantación de medidas técnicas o de la definición de procedimientos: es fundamental la implicación de las personas. Esta circunstancia queda claramente reflejada en la Agenda Digital de la Comunidad Valenciana, estableciendo líneas de trabajo destinadas a mejorar la cultura en ciberseguridad de ciudadanos y empresas. De la misma forma se incluyen en la estrategia nacional y europea de ciberseguridad.

La divulgación y concienciación es algo consustancial a la manera de entender la ciberseguridad en CSIRT-CV, por lo que el centro ha puesto en marcha el Plan Valenciano de Capacitación que sitúa a las personas en uno de sus principales ejes de actuación.

Para abordar este plan de la mejor forma posible, se ha definido un calendario donde se contemplan acciones concretas dirigidas a los colectivos identificados: ciudadanos, Generalitat, PYMES y otras administraciones públicas. Entre estas acciones podemos destacar jornadas familiares de seguridad, conferencias, guías y estudios.

Durante el año 2019 se ha continuado con la realización de algunas de las iniciativas del plan que se iniciaron durante el 2018, siendo el ejemplo más claro de ello las jornadas de concienciación en los centros educativos. Lo que comenzó en 2018 como un proyecto piloto cuyo alcance eran 14 centros, se ha convertido en un gran proyecto en el que se ha conseguido llegar hasta ahora, a más de 150 centros de la Comunidad Valenciana.

Otras de las iniciativas que se ha consolidado durante este año han sido las jornadas de concienciación a empleados de la Generalitat Valenciana, destacando las que se han realizado en diversos hospitales de la Comunidad Valenciana las cuales, dada su buena acogida, necesitaron de ediciones adicionales.

El año 2019 finaliza con el planteamiento y desarrollo de iniciativas, dentro del **Plan Valenciano de Capacitación**, dirigidas a la empresas de la Comunidad Valenciana. Entre estas iniciativas destaca la creación de una herramienta que permitirá que las empresas puedan realizar un autodiagnóstico en materia de ciberseguridad. También se ha puesto en macha una plataforma de formación on-line con diversos cursos y vídeos interactivos destinados a mejorar la formación en ciberseguridad del personal técnico y CEOs de las empresas.

A modo de resumen, este año destacan las siguientes acciones llevadas a cabo:

- Ampliación de contenidos del portal concienciación en ciberseguridad https://concienciat.gva.es/**,** incluyendo nuevos apartados:

  - **¿Sabías que…?**: sección centrada en consejos cortos o noticias de actualidad.

•**Jornadas de ciberseguridad** para los centros de secundaria de la Comunitat Valenciana.

•**Empresas** creación de un apartado dentro de la web de concienciaT destinado a la formación y concienciación de las empresas de la Comunidad Valenciana.

- Gran difusión en los medios de comunicación del Plan Valenciano de Capacitación, haciendo especial hincapié en las jornadas de ciberseguridad en centros educativos.
- Pruebas de Humsec a diferentes colectivos de nuestro ámbito.
- Campañas de concienciación online en redes sociales:
  - "Consejos para dispositivos IoT"[5]
  - "Contra la desinformación en el ciberespacio: ¡Stop Fake News!"[6]
  - "No cierres los ojos a la ciberseguridad, descubre concienciaT"[7]
  - "Historias Virtuales para no dormir", destacar la gran repercusión en medios que tuvo esta campaña. La campaña constaba de 8 pequeños relatos relacionados con la ciberseguridad ambientados en una estética de terror que se lanzaron a mediados de octubre y concluyeron en Halloween.[8]
- Publicación de informes de carácter público:
  - Informe actividades del centro del año 2018[9]
  - Informe EMOTET, interesante informe publicado en septiembre de 2019 a raíz de la reactivación de la famosa botnet.[10]
  - Informe de actividades del centro primer semestre de 2019[11]

5 https://concienciat.gva.es/tips_de_seguridad/consejos-para-dispositivos-iot/
6 https://concienciat.gva.es/tips_de_seguridad/contra-la-desinformacion-en-el-ciberespacio-stop-fake-news/
7 https://concienciat.gva.es/tips_de_seguridad/no-cierres-los-ojos-a-la-ciberseguridad-descubre-concienciat/
8 https://concienciat.gva.es/tips_de_seguridad/historias-virtuales-para-no-dormir/
9 https://www.csirtcv.gva.es/es/descargas/informe-actividades-csirt-cv-2018.html
10 http://www.csirtcv.gva.es/es/descargas/emotet-campa%C3%B1a-septiembre-2019.html
11 http://www.csirtcv.gva.es/es/descargas/informe-actividad-csirt-cv-s12019.html

Imagen de la Campaña de Historias Virtuales para no dormir

- Publicación de infografías:
  - Infografía sobre dispositivos IoT
  - Infografía sobre seguridad en el puesto de trabajo
  - Infografía de Ciberseguridad en entornos sanitarios
  - Infografía en Halloween "Que estas ciberpesadillas no te quiten el sueño"

Durante el año 2019 se ha continuado con la republicación de infografias ya elaboradas en fechas destacadas. Así mismo durante el mes de diciembre se publicó en el portal concienciaT y RRSS nuestra tradicional tarjeta navideña. Además durante ese mismo mes y dado que se aproximaban las numerosas compras navideñas, como vídeo de la noticia del mes se publicó un vídeo con consejos de seguridad en compras on-line además de un gif animado.

Otra de las iniciativas destacables acontecidas durante el 2019 fue la invitación a los empleados públicos de la Generalitat y sus familias a participar en la **Jornada Familiar de Ciberseguridad en el Hogar y a visitar la primera falla cibersegura de la historia**. Durante el transcurso de la jornada los adultos asistieron a una conferencia titulada "La identidad digital de nuestra casa: cómo protegerla ante los riesgos del Internet de las Cosas", mientras que los más pequeños pudieron participar en talleres interactivos para prevenir el ciberacoso**.** Además, durante la jornada, se pudo visitar el monumento fallero dedicado a la ciberseguridad en los hogares conectados y donde quedaron unidas la

tradición de la fiesta centenaria de las fallas con la tecnología del siglo XXI.

Imagen de la Primera falla Cibersegura

4.1 Cursos online y formación presencial

El centro sigue potenciando su oferta formativa para ciudadanos con cursos y microcursos online que se imparten a través de la plataforma SAPs?[12] y de los que periódicamente se van abriendo nuevas ediciones para poder incrementar el número de alumnos formados. El material está elaborado íntegramente por el equipo de analistas propio.

Durante el año 2019 se han formado cerca de **2974 alumnos**.

Cursos online ofertados por CSIRT-CV
Uso seguro en iOS
Uso seguro de Android
Introducción a la GSI
Herramienta Nmap

MicroCursos online ofertados por CSIRT-CV
Seguridad informática
Introducción al malware
Seguridad en redes sociales
Seguridad en redes inalámbricas

12 http://www.saps.gva.es/

Seguridad en Internet para menores
Seguridad en redes P2P
Navegación segura
Seguridad en dispositivos portátiles
Seguridad en juegos online
Seguridad en el correo electrónico
Seguridad en móviles, PDAs y smartphones
Delitos tecnológicos
Compras online seguras

De igual forma, se han organizado diferentes charlas divulgativas destinadas a concienciación para familias, en centros educativos (se profundizará sobre ésto en puntos posteriores), en determinados colectivos desprotegidos, dirigidas al sector sanitario y a altos cargos, entre otros.

4.2 Concienciación en centros educativos

El Plan Valenciano de Capacitación identifica a los adolescentes como uno de los colectivos más vulnerables, por lo que durante todo el año 2019 se ha continuado con las jornadas de ciberseguridad en los centros educativos

El alcance de la propuesta abarca todos los institutos públicos, concertados y privados de la Comunidad Valenciana, centrándose en los alumnos de 2º de la E.S.O. y su entorno más cercano, madres, padres y profesores, para que puedan encontrar en las personas adultas respuestas en sus dudas del día a día.

Durante el año 2019 se han formado 10.500 alumnos, cerca de 2.000 profesores y 1.700 madres y padres de 123 centros educativos diferentes.

4.3 Portales principales. Material publicado

El portal www.csirtcv.gva.es donde se publican diariamente noticias de seguridad y se alerta sobre las vulnerabilidades más importantes, es la imagen principal del centro de cara al exterior. Durante el año 2019, el portal ha recibido cerca de 600.000 visitas y se han publicado más de 500 publicaciones.

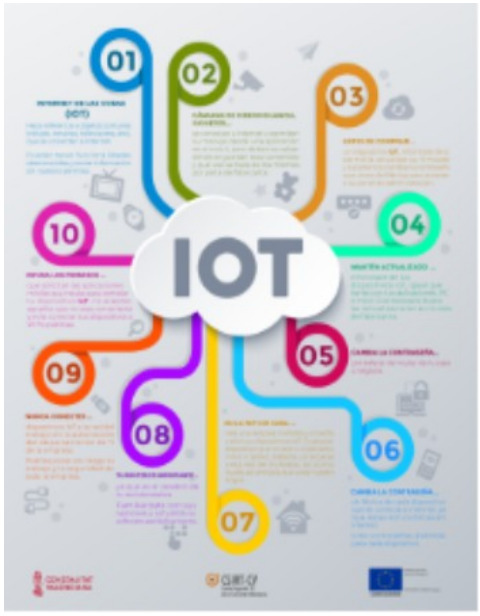
En relación al portal de concienciación **concienciaT** https://concienciat.gva.es/, destaca el aumento de las visitas respecto al período anterior, sumando casi 120.000. En dicho portal se pueden consultar, entre otros, vídeos formativos y promocionales, infografías o información sobre nuestros cursos en SAPS.

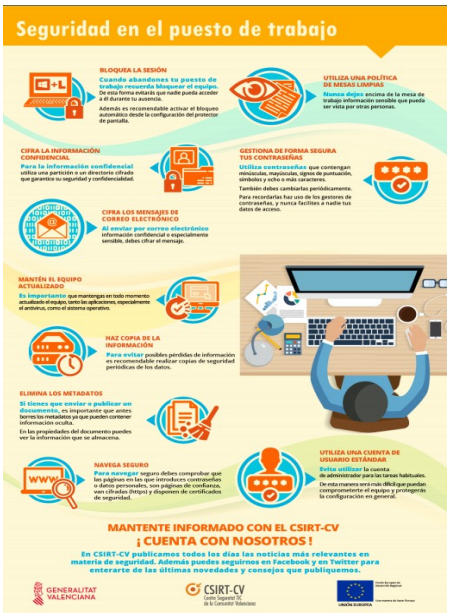
Estos portales disponen además de una serie de guías e informes así como otro tipo de

material sobre ciberseguridad. Durante el 2019 este contenido ha tenido más de 120.000 descargas.

Además de lo mencionado anteriormente, en concienciaT periódicamente se publican infografías donde se presentan de forma didáctica y visual diferentes consejos de seguridad. Concretamente durante el año 2019 se han publicado cuatro infografías que ha tenido una gran aceptación entre nuestros visitantes:

- Infografía sobre dispositivos IoT[13]
- Infografía sobre seguridad en el puesto de trabajo[14]
- Infografía de Ciberseguridad en entornos sanitarios[15]
- Infografía en "Halloween que estas ciberpesadillas no te quiten el sueño"[16]





13 https://concienciat.gva.es/infografias/infografia-con-consejos-de-seguridad-sobre-dispositivos-iot/
14 https://concienciat.gva.es/infografias/infografia-con-consejos-sobre-seguridad-en-el-puesto-de-trabajo/
15 https://concienciat.gva.es/infografias/infografia-consejos-ciberseguridad-entornos-sanitarios/
16 https://concienciat.gva.es/infografias/infografia-de-halloween/

5 Observatorio de ciberseguridad

En el ecosistema de la tecnología en el que nos encontramos actualmente se están viviendo actualmente ciertas circunstancias externas que aumentan exponencialmente el riesgo al que las corporaciones se exponen.

Como resultado del análisis del 2019, se puede indicar que tanto los dispositivos médicos como los IoT continúan siendo objetivo claro para los ciberdelincuentes. Esta situación viene marcada por una circunstancia común al mundo IoT: la falta de regulación en dispositivos, sumado a la falta de medidas de seguridad algunas implementaciones de fábrica.

El análisis externo pone de manifiesto el auge de las amenazas híbridas, el ciberespionaje, y el uso de la nube para perpetrar ataques, entre otros. A estas amenazas hay que sumar las que se arrastran de los últimos años, como son el incremento del uso de IA contra los sistemas de defensa, la sofisticación en los correos phishing, o el ransomware y criptojacking como tendencias en malware. De este análisis también se puede destacar que surgen nuevos eventos relevantes que podrían afectar a nuestro ámbito y que se detallan a continuación.

5.1 Amenazas híbridas

Las denominadas "amenazas híbridas", tal y como se recoge en la Estrategia de Seguridad Nacional de 2017, "*son acciones combinadas que pueden incluir, junto al uso de métodos militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica o campañas de influencia en redes sociales, que se han manifestado especialmente en procesos electorales. La finalidad última que se persigue es la desestabilización, el fomento de movimientos subversivos y la polarización de la opinión pública*".

La desinformación representa, por su parte, una de las armas que configuran este tipo de amenazas.

Desde McAfee[17] predicen un crecimiento de la colaboración clandestina de los cibercriminales. Esto impulsará el volumen y la sofisticación de este tipo de amenazas.

"*La tendencia a externalizar los ataques llevará al uso de inteligencia artificial en tácticas de ataque mucho más elaboradas", explica el fabricante, señalando que "durante el próximo año, los ciberdelincuentes utilizarán bots para extorsionar a las marcas con campañas de desprestigio en redes sociales, plataformas que continuarán siendo objetivo de ataques populares*".

5.2 Ciberespionaje

Tal y como señala ENISA[18], varios informes de organizaciones de investigación de seguridad global revelaron que el ciberespionaje se está convirtiendo en una práctica habitual de ciertos estados y grupos de cibercriminales. Estos se dirigen habitualmente contra entidades gubernamentales, ferrocarriles, hospitales, etc. con el objetivo de obtener beneficios geopolíticos, secretos de estado o comerciales, propiedad intelectual o industrial, así como datos en informaciones de sectores estratégicos.
Según se indica en el informe de Amenazas y Tendencias de 2019 publicado por el CCN-CERT, las redes de tecnología operacional (OT) de las industrias son un campo de acción idóneo para los actores de las ciberamenazas. Estos agentes utilizan herramientas de administración remota (RAT) que ya están instaladas en los sistemas de control industrial (ICS).

17 https://bitlifemedia.com/2018/12/las-19-tendencias-y-predicciones-de-ciberseguridad-para-2019/
18 Fuente: ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends. FINAL VERSION. 1.0. ETL

5.3 Ataques a la nube. CloudHopper

Las empresas que alojan datos de otras compañías en sus servidores, o administran los sistemas de información de sus clientes de forma remota, se convierten en objetivos muy tentadores para los delincuentes ya que atacando estos sistemas, es posible acceder a los de los clientes. Si bien es cierto que las grandes empresas de la nube como Amazon y Google pueden permitirse invertir mucho en ciberseguridad eso no los hace inmunes a una filtración.

Esto ya está pasando. El Gobierno de EE.UU., recientemente acusó a unos ciberdelincuentes chinos de infiltrarse en los sistemas de una compañía que administraba[19] las tecnologías de información de otras empresas. Mediante este acceso, los atacantes supuestamente pudieron acceder a los ordenadores de 45 compañías de todo el mundo, en distintas industrias desde la aviación hasta la exploración de petróleo y gas.

Apodado "Cloudhopper" por los expertos en seguridad, se prevé que este tipo de ataque se sofistique en los próximos meses. Chenxi Wang, fundador de la empresa especializada en ciberseguridad Rain Capital, afirma que "*veremos a delincuentes que pasan de centrarse en el malware de escritorio al malware de los centros de datos*" ya que ofrece importantes economías de escala.

5.4 Marco estratégico y legal

En España, en 2019, se han publicado los siguientes textos asociados a la seguridad de la información que pueden afectar a la Generalitat Valenciana y otras administraciones públicas que deberían tomarse en consideración:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (diciembre de 2018).
- CCN-STIC-882 Guía de Análisis de Riesgos para Entidades Locales.
- CCN-STIC 883 Guía de implantación del ENS para Entidades Locales.
- CCN-STIC-801 Responsabilidades y Funciones en el ENS (actualización).
- Estrategia Nacional de Ciberseguridad 2019 (26 de abril).
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

19 https://www.technologyreview.com/f/612655/chinese-hackers-allegedly-stole-data-of-more-than-100000-us-navy-personnel/

5.5 Ingeniería social

Como hemos visto en el puntos más interesantes del año, la ingeniería social ha sido durante este año una técnica para de robo de información sensible y de infección de sistemas muy utilizada por los actores maliciosos. Se ha visto el uso de información pública para generar correos de *spear phishing,* o ataques dirigidos, en los que se da confianza al usuario de la legitimidad del correo añadiendo información de su entorno en el correo. También se ha visto que cada vez, los correos utilizados por (en este caso) Emotet, son más difíciles de diferenciar de un correo legítimo debido a que se utilizan noticias de actualidad para darle veracidad e interés al contenido de los mensajes.

Sin lugar a dudas, la ingeniería social es una técnica muy utilizada a la hora de hacer ataques de phishing, difícil de contrarrestar usando sólo medidas técnicas, sino que es necesaria la formación de los usuarios para prevenir ataques exitosos de ingeniería social.

6 Relaciones y acuerdos institucionales

El servicio de Intercambio de información que presta CSIRT-CV tiene como objetivo que el centro se transforme en el principal instrumento de intercambio de información relativa a ciberseguridad, tanto en la Generalitat como en empresas de la Comunitat Valenciana, estableciendo canales de comunicación y alerta tanto de forma interna como con organismos externos, grupos de interés de seguridad, autoridades, empresas, etc. Esto permitirá, con las restricciones necesarias para garantizar la legalidad vigente y la protección de información corporativa, un intercambio de información ágil, seguro y directo.

Entre los organismos con los que más información se intercambia está el CCN-CERT, con quien, a través de la herramienta LUCIA, se comparte información sobre incidentes de seguridad. También de forma periódica con otros CERTS, se ponen en común IOC y analizadores para la herramienta CARMEN. Además este año se ha incrementado la comunicación con el foro CSIRT.es sobre todo a través de aplicaciones seguras de mensajería desplegadas por el CCN-CERT o la lista de correo del propio foro.

Así mismo durante este año se han iniciado los trabajos de colaboración entre CSIRT-CV y el CCN-CERT para la implantación de las herramientas CLARA y ANA en CSIRT-CV.

Destacar también la estrecha colaboración existente con las FCSE y CCN-CERT en el transcurso de varios incidentes que han tenido lugar durante el primer semestre del 2019.

Además durante el primer semestre de 2019 se produjo la adhesión de CSIRT-CV como miembro del **Club Singular**, cuyo objetivo es la concienciación de la sociedad en materia

de ciberseguridad, poniendo el foco de atención en colectivos especialmente vulnerables como los niños o víctimas de violencia de género. Desde esta perspectiva, una de sus primeras acciones fue colaborar con la jornada de la Falla Cibersegura que se ha mencionado anteriormente.

Otro de los eventos destacados que se han llevado a cabo durante este año y que ha servido para incrementar las relaciones entre CSIRT-CV y otras instituciones internacionales, fue la visita de una delegación de directores de seguridad de la información de diferentes agencias de la ONU, durante la visita los miembros de la comitiva pudieron conocer de primera mano tanto las instalaciones del CSIRT-CV como las tareas que se realizan en materia de ciberseguridad, las herramientas y los procedimientos que se utilizan a nivel más técnico.

7 Cultura de ciberseguridad

CSIRT-CV está presente en las redes sociales de Facebook y Twitter, canales de comunicación que utiliza - junto a otros – para crear una cultura de ciberseguridad entre sus seguidores a través de la emisión diarias de noticias diarias, recomendaciones, alertas y consejos sobre ciberseguridad.

En la misma línea, el servicio de comunicación persigue convertir al centro en el referente de la Comunidad Valenciana en materia ciberseguridad y fomentar una sociedad segura e informada.

Durante este curso y con motivo del día de Internet Segura, el 5 de febrero la Directora de CSIRT-CV participó en un programa sobre el ciberacoso en la televisión autonómica valenciana À Punt. Así mismo, durante la jornada diversos medios de comunicación se hicieron eco de las jornadas de ciberseguridad que se estaban llevando a a cabo en los centros educativos de la Comunidad Valenciana.

Otras asistencias destacadas a diferentes eventos y jornadas públicas han sido:

- Congreso 56th TF-CSIRT & FIRST Regional Symposium que tuvo lugar en Tallin, Estonia, del 21 al 23 de enero de 2019.
- Jornada en Universidad de Valencia en la que se impartió la charla "*Incidentes de seguridad en el mundo real*".
- Congreso organizado por la Universidad Internacional de Valencia para fomentar la participación de la mujer en la tecnología. La Directora de CSIRT-CV participó en un debate en dicho evento.
- Jornada en la Universidad Politécnica de Valencia, en la que se impartió una ponencia dirigida a un grupo de trabajo formado por docentes que desarrollarán un programa de concienciación en el uso seguro de tecnologías para colectivos

desfavorecidos.

- Congreso Securmática. CSIRT-CV, junto con la Jefa del Servicio de Seguridad de la Generalitat, impartieron una ponencia acerca de la integración segura de dispositivos IoT y médicos en Generalitat Valenciana.
- Ponencia de la Dra. del centro sobre el Plan Valenciano de Capacitación en Ciberseguridad impartida en las JORNADES PROTECCIÓ DE DADES EN CENTRES EDUCATIUS que tuvo lugar en Gandía el pasado 4 de Mayo.
- Ponencia en las Jornadas CCN-STIC titulada: vSOC para las EELL Valencianas: Proyecto piloto entre CSIRT-CV y la Diputación Provincial de Valencia para la mejora de la seguridad en la Administración Local, impartida por la Dra. del Centro.
- Ponencia "Vigilancia Digital de procesos electorales" impartida en las Jornadas CCN-STIC y en FIRST de Bilbao
- Taller "Forense en Windows" impartido en las Jornadas CCN-STIC
- Participación de la directora del centro en Cybercamp impartiendo la ponencia "Plan Valenciano de Capacitación en Ciberseguridad de CSIRT-CV: Una estrategia centrada en las personas"
- Taller en CyberCamp titulado "Análisis forense digital"

Como asistentes, CSIRT-CV ha estado representado en las siguientes jornadas:

- Jornada SAT organizada por el CCN-CERT en Madrid.
- Reunión CSIRT.es en Madrid.
- Congreso ISMS-Forum en Madrid.