CSIRT-CV, el nuevo Centro de Seguridad TIC de la Comunitat Valenciana

El pasado 1 de julio se adjudicó de forma definitiva el contrato para la prestación de Servicios de Telecomunicaciones y Soporte de Servicios TIC de la Generalitat Valenciana; dentro de dicho contrato, se reserva un lote a la Seguridad TIC de la Generalitat como función separada del resto, garantizando así la segregación de funciones necesaria a la hora de hablar de seguridad. En concreto, este lote tiene por objeto la implantación y coordinación de los planes de protección mediante el proyecto CSIRT-CV, y ha sido adjudicado a S2 Grupo. Este hito supone un punto de inflexión en la trayectoria actual del centro, hasta ahora focalizado en la respuesta a incidentes, que tiene como objetivo estratégico convertirse en el Centro de Referencia en Seguridad de la Generalitat de la Comunitat Valenciana.


Lourdes Herrero Gil / Antonio Villalón

El actual CSIRT-CV

Desde hace años, el Gobierno Valenciano viene impulsando diversas actuaciones reconocidas como punteras en el ámbito de la Administración Electrónica. Su visión, objetivos y planteamientos han ido más allá de la simple introducción del canal telemático y en especial de Internet, habiendo dado los pasos hacia una nueva administración orientada a la gestión del conocimiento y a la excelencia en la prestación de los servicios públicos. El uso de estas nuevas tecnologías supone un importante beneficio para el ciudadano –y por tanto debe ser impulsado por las Administraciones Públicas–, pero también introduce riesgos que deben ser convenientemente mitigados para poder abordar el principal reto al que nos enfrentamos a la hora de hablar de nuevas tecnologías: la **generación de confianza** suficiente, no sólo en la Administración Pública sino también en la sociedad en general.

En este sentido, la Generalitat tomó la decisión estratégica de impulsar el desarrollo del **Centro de Seguridad TIC de la Comunitat Valenciana** (CSIRT-CV), con vocación de ofrecer servicios de seguridad informática en el ámbito autonómico, ofreciendo una visión global de seguridad y proactividad en la gestión de incidentes y convirtiéndose así en un punto de referencia en la materia para las organizaciones que residen en su ámbito de acción. Este centro está operativo desde 2007, dentro del Plan Estratégico de Comunicaciones Avanzadas de la Generalitat (AVANTIC), y desde la creación del mismo su principal objetivo ha sido la prevención, detección, asesoramiento, seguimiento y coordinación necesarios para hacer frente a incidentes de seguridad informática.

CSIRT-CV cuenta desde sus orígenes con personal de S2 Grupo y, en estos tres años de vida, ha atendido 437 incidentes, emitido 80 boletines de seguridad y 25 de alertas, y publicado 1.997 noticias y 1.387 alertas. La web del centro (http://www.csirtcv.es/) ha servido más de un millón y medio de páginas y recibido más de 250.000 visitas; actualmente el número de suscriptores (boletines, recursos…) del centro supera los 600, y cuenta con 20 empresas o institutos tecnológicos asociados.

Con la puesta en marcha de CSIRT-CV, la Generalitat de la Comunitat Valenciana fue pionera en el ámbito de los centros de respuesta ante incidentes dentro de la administración pública; hasta el momento, el centro ha venido cubriendo su función de CSIRT –para la que fue diseñado–, pero en el marco de seguridad actual se hace necesaria una evolución desde la situación presente, que contemple una focalización global (cubriendo todos los ámbitos de la seguridad) y que amplíe los aspectos de prevención y colaboración. Y para evolucionar en este sentido es necesaria una nueva etapa del centro, en la que se renueve su modelo de gestión y se amplíe su catálogo de servicios, y mediante una adecuada transición se asuman tareas y funciones que puedan estar dispersas en la actualidad, convirtiendo así a CSIRT-CV en el centro de referencia en materia de seguridad de la Generalitat de la Comunitat Valenciana.

El marco de seguridad

¿Por qué era necesaria esa redefinición de CSIRT-CV que acaba de comenzar? En los últimos años el panorama global de la seguridad ha sufrido grandes cambios que afectan tanto a la percepción que la sociedad tiene de la seguridad, como a la forma en la que organizaciones de todo el mundo plantean sus estrategias de protección. Sin duda alguna, los lamentables atentados del 11-S contra el World Trade Center neoyorquino hicieron tambalear los principios básicos de seguridad –en todos los sentidos– que hasta entonces habían predominado en la materia; si hasta ese momento la seguridad estaba dividida en parcelas perfectamente delimitadas, sin ninguna relación necesaria *a priori* entre ellas, y cada una preocupada en luchar contra unas amenazas palpables y relativamente predecibles (accesos físicos, robos, seguridad perimetral, piratas...), a partir del once de septiembre de 2001 el panorama internacional de la seguridad dio un vuelco que, hoy en día, debido a factores como la globalización de la sociedad o la ubicuidad de las organizaciones, ya se considera irreversible.

Como consecuencia de los acontecimientos de la última década relacionados con la seguridad, que abarcan tanto los atentados terroristas como los grandes desastres naturales, la evolución de los ciberdelitos y las mafias organizadas que operan en la red, emerge con fuerza una corriente que nace, como era previsible, en los Estados Unidos de América. Esta corriente tiene como núcleo central la **convergencia** de las seguridades y la **colaboración** en materia de seguridad, aspectos incuestionables de las nuevas estrategias en este ámbito, además de la consideración de la **infraestructura crítica nacional**: aquellos sectores básicos para el funcionamiento de una nación –administración pública, energía, alimentación, finanzas...– han comenzado a considerarse *de facto* objetivo común de nuevas amenazas, y por tanto a protegerse de forma conjunta mediante un concepto clave que destaca por encima de los demás: la colaboración a través del intercambio de información (***information sharing***).

La misión del CSIRT-CV es contribuir a la seguridad de la Generalitat, y por extensión a la de sus ciudadanos y organizaciones, para prevenir, detectar y responder a las amenazas, vulnerabilidades e incidentes que les afecten o puedan afectar, independientemente del origen de los mismos; y servir como canal principal de comunicaciones para la Administración Pública en materia de seguridad.

El nuevo CSIRT-CV

Los principios básicos de convergencia y colaboración anteriormente expuestos, sobre los que tanto se está trabajando en el mundo de la seguridad a nivel internacional en los últimos años, determinan las bases –y la necesidad– del nuevo enfoque planteado para CSIRT-CV.

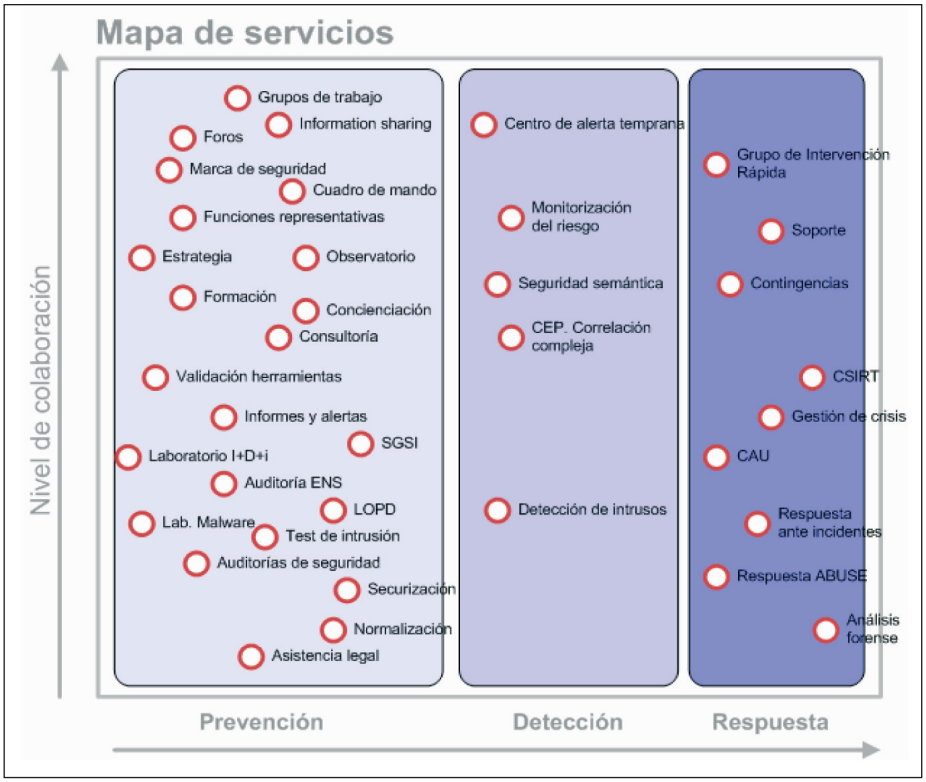
Estos dos principios se han venido fortaleciendo con la actividad que a nivel europeo e internacional se está desarrollando en materia de seguridad, y en particular en lo referente a la protección de las infraestructuras críticas (PIC) como continuación de la corriente iniciada en Estados Unidos tras la PDD 63 (*Presidential Decision Directives 63*), por

la que se crearon los ISAC (*Information Sharing & Analysis Center*), centros cuyo modelo es seguido, al menos parcialmente, en CSIRT-CV.

Pero no sólo a la hora de hablar de centros de seguridad se ha avanzado considerablemente durante los últimos años; en paralelo a la protección de infraestructuras críticas, a la convergencia, y a los múltiples avances técnicos que implican modificaciones en los niveles de riesgo de cualquier organización –por supuesto, incluyendo la administración pública–, los aspectos regulatorios y normativos también apuntan en la misma dirección. Familias de normativas como ISO 27000 o ISO 28000, y regulaciones como el Esquema Nacional de Seguridad o el Reglamento de Desarrollo de la LOPD, demuestran el interés en la normalización y regulación de la seguridad, que deja de percibirse como algo estrictamente técnico y pasa a gestionarse y, en ocasiones, incluso a legislarse; es decir, que hay un tránsito del universo de las buenas prácticas o recomendaciones a, en muchos casos, la obligación.

Con esta situación como telón de fondo, el nuevo CSIRT-CV que desde el 1 de julio está en marcha nace con el objetivo de convertirse en el centro de referencia en seguridad para toda la Generalitat, mediante un planteamiento holístico y colaborativo. Para ello, el diseño del nuevo CSIRT-CV se basa en **cinco grandes pilares;** el primero de ellos es el **modelo de transición**, que como su nombre indica define la transición del actual centro al nuevo CSIRT-CV, necesaria para lograr los objetivos planteados para el organismo y que consta de dos grandes líneas maestras: la ampliación del ámbito de actuación de CSIRT-CV y el incremento de sus niveles de colaboración. Mediante esta transición se pretende ubicar a CSIRT-CV como un centro avanzado basado en la sociedad del conocimiento compartido, con un alto grado de colaboración y con el enfoque global de la seguridad necesario para aportar valor añadido a las organizaciones a las que presta servicio; como modelos de centros de similares características encontramos los ISAC estadounidenses, los WARP británicos o el SIZ alemán.

El segundo gran pilar del nuevo CSIRT-CV es el **modelo de transformación de servicios**, que mediante el diseño de la matriz de servicios –y por tanto, del catálogo de servicios– del centro detalla el camino a seguir por CSIRT-CV durante los próximos años, definiendo así el detalle de tipo de centro a conseguir; este pilar, junto al modelo de transición, conforma el plan evolutivo de CSIRT-CV. En este sentido, se clasifican los servicios del centro en tres grandes familias: los servicios de **prevención** (aquellos que evitan los incidentes), los servicios de **detección** (los que los detectan una vez materializados) y los servicios de **respuesta** (los que permiten responder de forma adecuada a los incidentes que se producen en las organizaciones); adicionalmente, se establece la dimensión de la **colaboración**, aspecto que, como se ha indicado, es vital para el éxito de cualquier centro de seguridad en la actualidad.



Los servicios que se van a ofrecer desde CSIRT-CV abarcan no sólo la respuesta propia de cualquier CSIRT. Como se puede ver en la matriz anterior, existe una amplia focalización en los aspectos preventivos y, en especial, en los niveles de colaboración de los servicios del centro (*information sharing*, funciones representativas, Centro de Alerta Temprana…). Estos servicios son el núcleo del centro hacia el exterior –colaboradores, clientes, administraciones públicas, FFCCSE…–, y, por tanto, constituyen un excelente resumen de qué es lo que pretende aportar CSIRT-CV durante los próximos años, por supuesto teniendo en cuenta que se trata de un catálogo de servicios altamente dinámico, por las características propias del centro y de la seguridad en general.

Para completar el diseño del nuevo CSIRT-CV, es necesario también un tercer pilar relativo al **modelo de gestión del centro**, del que se deriva el mapa de procesos de CSIRT-CV, y que marca el diseño conceptual y la orientación propuesta para el centro. Se trata de un modelo de gestión certificable y alineado con los principales referenciales y códigos de buenas prácticas internacionales, orientado al proceso –no a las funciones– y con una gran carga de servicios de información y en general de prevención, respetando totalmente las distintas funciones de seguridad internas a cada organismo o *conselleria* pero intentando fomentar, desde los servicios diseñados para el centro, las colaboraciones y agrupaciones en todos los sentidos con un objetivo común, el definido en la **misión** de CSIRT-CV.

Como últimos pilares de CSIRT-CV, pero no por ello menos importantes, se considera la **plataforma de gestión del centro**, que permitirá a CSIRT-CV funcionar tal y como se ha planteado, controlando satisfactoriamente sus servicios y sus procesos; dicha plataforma de gestión se sustenta en una plataforma tecnológica que cubre desde los aspectos más técnicos hasta los aspectos de gestión y estrategia corporativas, para lo que CSIRT-CV utilizará una *suite* de herramientas *ad hoc*, basada en tecnología y productos nacionales. Y, por supuesto, para poner en funcionamiento un centro como el planteado, se encuentra finalmente el quinto gran pilar de CSIRT-CV: su **equipo humano**, responsable en última instancia del éxito del Centro. En este caso, éste cuenta con un equipo multidisciplinar, altamente cualificado y con un elevado nivel de conocimiento y experiencia acumulados, capaz de proporcionar a CSIRT-CV un valor añadido inmejorable para la consecución de sus objetivos como centro de seguridad.

En definitiva, el nuevo CSIRT-CV nace con la vocación de convertirse en un centro de referencia no sólo para la Generalitat de la Comunitat Valenciana o en el ámbito autonómico, sino también en el nacional, mediante una visión global de la seguridad –no centrada exclusivamente en el ámbito TIC– y mediante unos niveles de colaboración acordes con los requisitos y recomendaciones marcados internacionalmente en este sentido. ■

Lourdes Herrero Gil
Directora
CSIRT-CV
Dirección General de Modernización
GENERALITAT VALENCIANA
herrero_lou@gva.es

Antonio Villalón
Director de Seguridad
S2 GRUPO
avillalon@s2grupo.es