Autoritat de Certificació de la Comunitat Valenciana: acciones en el área de seguridad 2006 – 2008

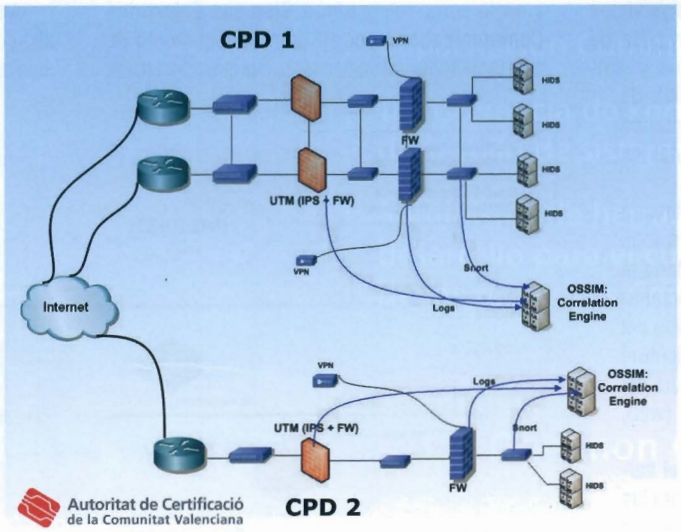
A lo largo del periodo 2006-2008 la Autoritat de Certificació de la Comunitat Valenciana ha llevado a cabo diversas estrategias y proyectos para mejorar, modernizar y ampliar los servicios que presta y las infraestructuras utilizadas para ello. La ACCV, que es el prestador de servicios de certificación público valenciano, inició su andadura en el año 2000 y, desde la fecha, ha expedido certificados digitales a casi 140.000 usuarios, a través de una extensa red de más de 350 Puntos de Registro de Usuario, que suponen una cobertura del 80% de la población de la Comunitat Valenciana. Entre los usuarios de los servicios de la ACCV se encuentran la Generalitat, más de 130 ayuntamientos con los que ha suscrito convenio, diversos organismos de la Administración General del Estado, colegios profesionales y algunas empresas y entidades financieras.


Ángel Alonso Parrizas / Joaquín Galeano Senabre

Dado que uno de las activos más importantes de la ACCV es la confianza que los usuarios depositan en sus servicios, es preciso llevar a cabo permanentemente un trabajo de revisión y mejora de la seguridad, los procedimientos, procesos y productos de la ACCV. Desde ese punto de vista, uno de los objetivos que se marcó para el periodo 2006-2008, que sirvió como punto de referencia para mejorar la infraestructura de seguridad, políticas y procedimientos de seguridad, fue la obtención del sello WebTrust para Autoridades de Certificación, que emite el AICPA (**American Institute of Certified Public Accountants**), con la participación de las empresas **SSI Consultores** y **Ernst & Young**.

Certification Authorities WebTrust

Por otra parte, tras un análisis del impacto en los procesos de negocio y en los servicios críticos (BIA), y como respuesta y desarrollo del correspondiente Plan de Continuidad de Negocio (BCP), se puso en funcionamiento un segundo Centro de Proceso de Datos donde la mayoría de servicios críticos están en activo-activo y donde algunos servicios no tan críticos, como la emisión de certificados, se podrían llevar a cabo en el CPD de respaldo a modo de *hot-site*.



Despligue de servicios

Todo este despliegue de servicios redundados en *mirroring* ha obligado a la actualización de los sistemas hardware y elementos de red, que en su mayoría han sido sustituidos por plataformas más modernas con nuevas funcionalidades, como es el caso de instalación de sistemas de prevención de intrusos y dos niveles de cortafuegos que operan sobre diversas arquitecturas hardware y software.

Uno de los puntos claves que ha permitido una mejora en el acceso a los servicios de emisión de certificados y un mayor alcance geográfico a los distintos puntos de registro, desplegados a lo largo de toda la Comunidad Valenciana, es la utilización de concentradores VPN con autenticación de cliente mediante certificados digitales de la propia ACCV, donde se ha optado por la migración de concentradores VPN con protocolo IPSec de Cisco y por concentradores VPN con SSL de **Juniper**.

Análisis de riesgo

Para tener un control sobre el nivel de riesgo de la organización y la adecuación de las contramedidas implantadas, se desarrolló un Análisis de Riesgo siguiendo la metodología MAGERIT en su versión 2, con la ayuda de la herramienta PILAR. Como resultado de este análisis de riesgo se lleva a cabo una gestión del riesgo sistemática y, entre otras medidas, se ha aumentado el número de auditorías de seguridad perimetrales y de test de intrusión donde han participado el Área de Seguridad del **CTSI** (**Centro de Telecomunicaciones y Sistemas de Información de la Generalitat Valenciana**) y empresas consultoras como Ernst & Young.

Detección de intrusos y gestión de *logs*

En cuanto a la modernización de los controles de detección, se decidió implementar una arquitectura distribuida de sistemas de detección de intrusos y correlación de *logs* basada en software libre, con **Snort**, **Osiris**, **Snare** y **OSSIM**. La información de este proyecto ya fue difundida en enero de 2007 en el boletín electrónico ACCV-Informa (disponible en htttp://www.accv.es/noticias/noticia98_c.htm).

Por último, y con la migración de las oficinas principales de la ACCV, los controles de acceso para tareas de administración y mantenimiento para el personal de la ACCV se han incrementado. Así, ahora los usuarios de la ACCV necesitan autenticarse con certificados digitales de sesión *logon* en el controlador de dominio para poder administrar y operar con los sistemas. ■

Como respuesta y desarrollo del correspondiente Plan de Continuidad de Negocio (BCP), se ha puesto en funcionamiento un segundo Centro de Proceso de Datos donde la mayoría de servicios críticos están en activo-activo.

Ángel Alonso Parrizas
CISSP, CISA, CISM, GCIH, GCIA, GCFW
Área de Seguridad

Joaquín Galeano Senabre
Coordinador

ACCV