centradores VPN con SSL de Juniper. VPM con protocolo IPSec de Cisco y por conha optado por la migración de concentradores tificados digitales de la propia ACCV, donde se

## Análisis de riesgo

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

Angel Alonso Parrizas / Joaquín Galeano Senabre

## CPD 1

VPN con autenticación de cliente mediante cer-

Valenciana, es la utilización de concentradores

niveles de cortafuegos que operan sobre diver-

de sistemas de prevención de intrusos y dos

cionalidades, como es el caso de instalación

plataformas más modernas con nuevas fun-

que en su mayoría han sido sustituidos por

de los sistemas hardware y elementos de red,

CPD 2

donde la mayoría de servicios críticos están en activo-activo.

(BCP), se ha puesto en funcionamiento un segundo Centro de Proceso de Datos

Como respuesta y desarrollo del correspondiente Plan de Continuidad de Negocio

## y gestión de logs

Detección de intrusos

noticias/noticia98\_c.htm). ponible en htttp://www.accv.es/ electrónico ACCV-Informa (disen enero de 2007 en el boletín de este proyecto ya fue difundida Snare y OSSIM. La información software libre, con Snort, Osiris, y correlación de logs basada en temas de detección de intrusos arquitectura distribuida de sisse decidió implementar una de los controles de detección, En cuanto a la modernización

para tareas de administración y ACCV, los controles de acceso de las oficinas principales de la Por último, y con la migración

los sistemas. dominio para poder administrar y operar con digitales de sesión logon en el controlador de la ACCV necesitan autenticarse con certificados se han incrementado. Así, ahora los usuarios de VODA al el personal de la ACCV

Area de Seguridad CISSP, CISA, GISM, GCIH, GCIA, GCFW ANGEL ALONSO PARRIZAS

Coordinador **Јордији Сагерио Ѕенавре** 

## 8002 – 8002 babirugəs əb səri lə Comunitat Valenciana: acciones en Autoritat de Certificació de la

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

algunas empresas y entidades financieras.

que se marcó para el punto de vista, uno de los objetivos y productos de la ACCV. Desde ese dad, los procedimientos, procesos de revisión y mejora de la seguricabo permanentemente un trabajo en sus servicios, es preciso llevar a confianza que los usuarios depositan más importantes de la ACCV es la Dado que uno de las activos

seguridad, políticas infraestructura de para mejorar punto de referencia que sirvió como periodo 2006-2008,

la obtención del sello WebTrust para y procedimientos de seguridad, fue

Por otra parte, tras un análisis del Consultores y Ernst & Young. la participación de las empresas SSI of Certified Public Accountants), con emite el AICPA (American Institute Autoridades de Certificación, que

enlos servicios críticos (BIA), y como impacto en los procesos de negocio y

de respaldo a modo de hot-site. certificados, se podrían llevar a cabo en el CPD servicios no tan críticos, como la emisión de cos están en activo-activo y donde algunos de Datos donde la mayoría de servicios crítifuncionamiento un segundo Centro de Proceso de Continuidad de Negocio (BCP), se puso en respuesta y desarrollo del correspondiente Plan

Despligue de servicios

dos en mirroring ha obligado a la actualización Todo este despliegue de servicios redunda-

desplegados a lo largo de toda la Comunidad geográfico a los distintos puntos de registro, emisión de certificados y un mayor alcance una mejora en el acceso a los servicios de Uno de los puntos claves que ha permitido sas arquitecturas hardware y software.

òissifitad de Certificació eneisnalev tetinumo al ab

SIC / No.19 / ABRIL 2008