CT CATASTRO Abril 2009

Arquitectura del nuevo Centro de Proceso de Datos de la Dirección General del Catastro

Jorge Moreno del Val
Coordinador de Área de Sistemas y Explotación
Subdirección General de Estudios y Sistemas de Información
Dirección General del Catastro
María del Carmen Zarcero García-Risco
Jefa de Área de Seguridad Informática
Subdirección General de Estudios y Sistemas de Información
Dirección General del Catastro

La Dirección General del Catastro (DGC) ha consolidado recientemente sus sistemas de servicios centrales en un único Centro de Proceso de Datos (CPD) en modalidad de "housing". El presente artículo pretende describir la arquitectura de la solución adoptada, tanto a nivel físico, como lógico.

La migración a este nuevo CPD se enmarca en el contexto del proceso de centralización de los sistemas de la DGC, consiguiendo eliminar los dos centros de datos de que se disponía en Madrid (Paseo de la Castellana y Alcalá).

Este CPD da soporte a los siguientes servicios:

- **Oficina Virtual del Catastro (ovc)**: Sistema basado en Internet orientado a permitir la interacción con el catastro de ciudadanos y agentes externos (Notarios, registradores, ayuntamientos, poder judicial).
- **Escritorio de Aplicaciones de Gestión Catastral (EAGC)**: Sistema basado en Internet, que da acceso a las aplicaciones catastrales mediante tecnología Citrix para usuarios externos que requieren funcionalidades avanzadas.
- **Base de Datos Nacional de Catastro (BDNC)**: Sistema que consolida los datos distribuidos en las bases de datos de las 52 gerencias del Catastro, permitiendo una visión integral del territorio gestionado por la DGC.
- **Base de datos de Patrones de Bienes Inmuebles (BDP)**: Sistema que con-

solida los padrones emitidos por las gerencias del catastro para los ayuntamientos
- Aplicaciones de entorno Intranet: Aplicaciones que dan soporte a procedimientos internos del Catastro.
- Futuros SIGECA (1) y SIGC (2) centralizados: Actualmente las aplicaciones corporativas, SIGECA y SIGCA se ejecutan en cada una de las 52 gerencias del catastro, estando las bases de datos separadas. Se centralizarán próximamente en una única base de datos consolidada.
- Servicios horizontales:
  – Seguridad Perimetral
  – Comunicaciones LAN/WAN (3)
  – Servicios de autenticación de usuarios
  – Servicio de acceso a Internet
  – Correo electrónico corporativo
  – Servicios de almacenamiento y réplica de datos (SAN (4))
  – Servicios de copia de seguridad
- Entornos de desarrollo y preproducción para todo lo anterior

Al diseñar este CPD, desde la DGC nos enfrentábamos a muchos retos, el primero de todos, un traslado con garantías, con un mínimo impacto en los usuarios.

Por otra parte y por vez primera, la DGC asumiría de manera independiente la gestión de la infraestructura de la OVC, que hasta ahora dependía de la SGTIC (5), de la Subsecretaria del Ministerio de Economía y Hacienda (MEH) a nivel de red, Seguridad Perimetral, acceso a Internet, y alojamiento de los equipos.

Este CPD asumirá, en 2010, la nueva base de datos centralizada de Catastro, que sustituirá a las 52 bases de datos provinciales distribuidas por las gerencias. Esto supone un reto muy importante, con estimaciones de varios miles de usuarios y un ancho de banda agregado de acceso a base de datos de más de 1gbps.

Para asumir con garantías todos estos riesgos, se decidió, que de manera previa al traslado, se realizara la adquisición y puesta a punto de una nueva infraestructura de red y seguridad perimetral, que, por un lado aportara un mejor rendimiento, y por otro permitiera "preconfigurarla" para cada uno de los equipos conectados de manera que el traslado fuera "Plug & Play-enchufar y listo", reduciendo los riegos del mismo.

Los anteriores CPD de la DGC habían crecido muy rápidamente, por lo que no se pudo planificar su diseño, ni su crecimiento posterior, por lo que la migración a un nuevo CPD suponía, además de un gran reto, una oportunidad para no repetir errores anteriores, y buscar la optimización del diseño de cara al ahorro de espacio, de energía y a la eficiencia en el cableado y mantenimiento posterior.

Diseño del CPD

Principios de diseño

A continuación citamos las principales ideas que han inspirado el diseño del nuevo CPD principal de la DGC.

Escalabilidad:

La DGC se encuentra inmersa en el proceso de consolidación de sus 52 bases de datos provinciales en una única base de datos nacional, los volúmenes de usuarios y tráfico previstos son enormes.

Además el nuevo CPD acoge los servicios de la Oficina Virtual del Catastro. Con

(1) SIstema de GEstión CAtastral. Datos alfanuméricos.

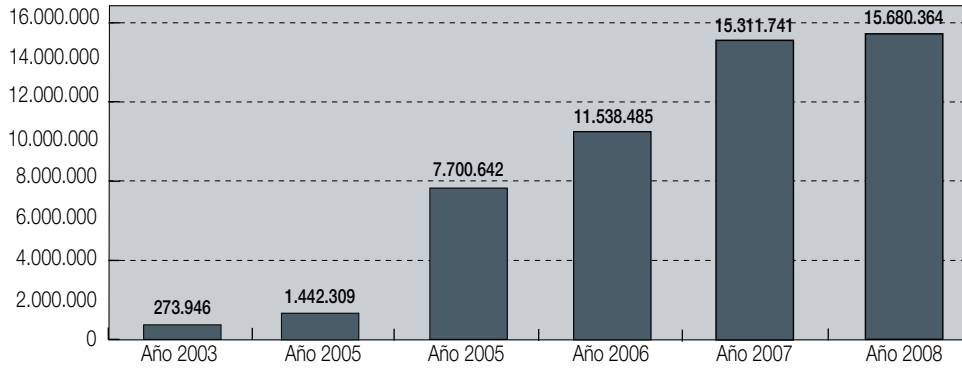
(2) Sistema de Información Geográfica CAtastral. Datos cartográficos.

(3) Local Area Network/Wide Area Network.

(4) Storage Area Network.

(5) Subdirección General de Tecnologías de Información y Comunicaciones.

Figura 1
Visitas a la OVC



más de 15 millones de visitas anuales, un crecimiento de su uso que se ha visto incrementado en los últimos años tal como se muestra en la Figura 1 y una disponibilidad 24x7x365, asumir el servicio de OVC planteaba un reto para la infraestructura de comunicaciones y seguridad perimetral de la DGC.

Por todo ello, se diseñó el CPD para que pudiera crecer con facilidad, tanto físicamente (con un nuevo pasillo y prolongación de los existentes) como lógicamente. Los equipos y armarios de comunicaciones ya contemplan esta posibilidad.

Además se adquirieron equipos que soportan anchos de banda muy superiores a los actuales de cara al proyecto de centralización.

Seguridad

Dado que se dispone de datos protegidos por la LOPD, la seguridad de los sistemas es algo importante para la DGC. Esto se ha tenido en cuenta tanto desde el punto de vista físico, a la hora de diseñar las políticas de acceso, como, sobre todo, desde el punto de vista lógico, utilizando equipos Firewall, IDS, IPS, Sniffer, etc.

Al mismo tiempo que se instaló el CPD, se inició un proyecto para dotarlo de una infraestructura de backup común a todos los equipos y susceptible de ser operada en remoto.

Por otra parte, los datos más críticos para la organización son replicados de manera síncrona en la sede de Paseo de la Castellana, vía un réplica de cabinas mediante un enlace DWDM.

Flexibilidad:

El cambio es un factor cada día mas presente en el mundo de las infraestructuras, por lo que a la hora de diseñar el CPD, era necesario asumir que no iba a ser inmutable, y prepararlo para acoger nuevos servicios con la mayor sencillez y rapidez posibles.

La implantación del proceso de gestión de la configuración, así como de una serie de procesos estándares para las actividades mas frecuentes, permite el despliegue de nuevos equipos en tiempo record.

Asimismo, la infraestructura de comunicaciones y cableado permiten ser reconfiguradas en cuestión de minutos, sin necesidad de mover una baldosa.

Robustez:

La importancia de los servicios que presta este CPD obliga a que su funcionamiento

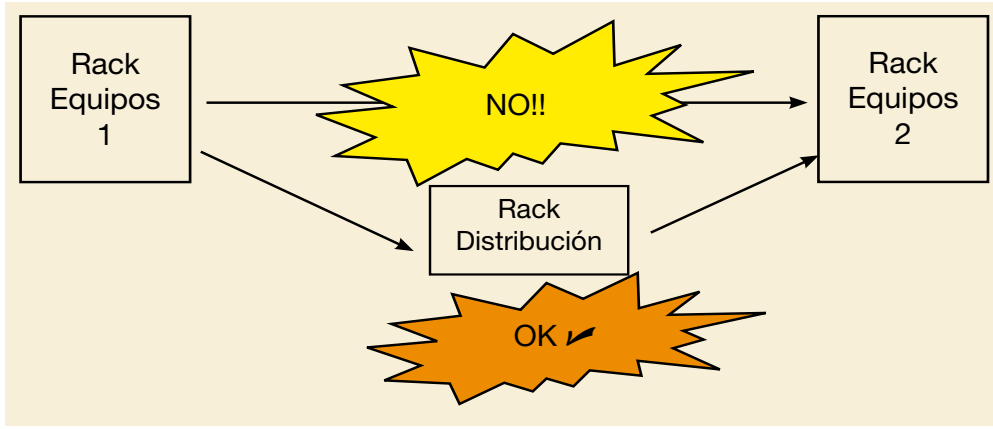


Figura 2.

no presente lagunas, habiéndose cuidado la redundancia en todos los aspectos para todos los sistemas.

Se ha fomentado la operación en caliente de todos los dispositivos que lo permiten, para minimizar el tiempo de parada en caso de incidencia.

Como parte del diseño se añadieron varias medidas con el fin de evitar desconexiones accidentales de componentes:

- El etiquetado de todos los componentes y cables
- Documentado de estas conexiones

Para evitar la rotura de cables y latiguillos de fibra óptica se instalaron pasahilos para ayudar a guiarlos. La política de cableado obliga a cablear de manera ordenada, respetando estas normas.

Se llegaron a evaluar latiguillos ethernet que no podían desconectarse sin una herramienta especial, pero se prefirió confiar la protección del servicio a la documentación y los procedimientos.

Mantenibilidad:

Se buscó que el CPD no fuera un gran proyecto inicial, que poco a poco fuera deteriorándose hasta una nueva mudanza, sino que junto con su base de datos de configuración fuera evolucionando, y permitiera que las operaciones de mantenimiento sobre el mismo se realizaran de manera fácil, sencilla y con el mínimo coste posible.

Diseño físico

Como hemos visto, este proyecto permitió hacer un diseño nuevo de todo el CPD teniendo en cuenta las necesidades actuales y a medio plazo de la DGC.

A continuación se enumeran los distintos apartados del diseño físico del CPD y los cambios que se introdujeron.

Cableado:

En los CPD anteriores, se utilizó un diseño de cableado punto – a – punto, en el que los cables se tendían según se necesitaban, haciendo difíciles y costosas las ampliaciones, por esto mismo, en algunos casos, se empleaban conmutadores locales en los armarios de equipos, lo que producía un rendimiento medio-bajo de la red.

Para el nuevo CPD se pensó que sería mejor rediseñar el sistema de cableado en vez de simplemente pedir al adjudicatario que replicara el sistema anterior en la nueva ubicación. Ver figura 2

Por tanto, se decidió emplear un sistema de cableado estructurado, tal como lo

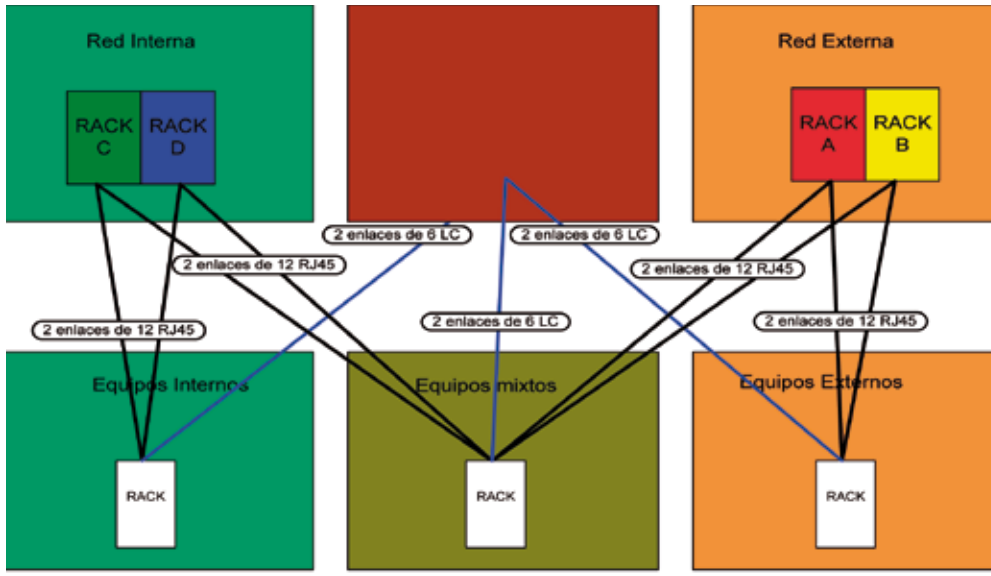


Figura 3.

dictan normas como TIA-942, en el que se tienden de antemano grupos de conexiones entre los armarios de equipos y de infraestructura, aunque solo vaya a utilizarse una de ellas.

Al contrario que en los anteriores CPD, se decidió ubicar los equipos de comunicaciones y Seguridad Perimetral en 4 armarios de infraestructura diferentes, de manera que no hubiera dos equipos con la misma función en el mismo armario. Estos 4 armarios de infraestructura (A, B, C, D) fueron distinguidos con colores para seguir mejor el destino de los cables. Los equipos correspondientes a la zona externa fueron ubicados en los armarios A y B y los de la zona interna en los armarios C y D.

La electrónica de red SAN se colocó en un único armario (E) por problemas de espacio, si bien está configurado como si fueran dos, al ser redundantes los equipos y los enlaces. Ver figura 3

De este modo, los diferentes armarios de equipos se encuentran distribuidos en estrella, siendo su centro los armarios de infraestructura, base para la arquitectura de red y seguridad perimetral del CPD.

Como hemos dicho, en un sistema de cableado estructurado, se tienden de antemano grupos de conexiones entre los armarios de equipos y de infraestructura, estos grupos de conexiones se denominan "enlaces".

La unidad mínima para el cableado de cobre serían enlaces de 12 conectores RJ45, y para el de fibra serían enlaces de 6 conectores LC. Además, para cada enlace a un armario de infraestructura se tiende otro de las mismas características al armario gemelo.

Los enlaces llevan asociado un código único de 3 cifras, consistente en la letra del armario de infraestructura destino y dos cifras. Por ejemplo, A12, luego se añade el número de puerto con un guión: A12-07

En la figura 4 se muestra la parte trasera de un armario de equipos, en la que se pueden ver los paneles de parcheo que conectan a los 4 armarios de infraestructura.

Este sistema plantea muchas ventajas:

- No es necesario abrir el suelo para tender nuevos cables
- Los cables pueden seguirse con facilidad, gracias a la numeración de los enlaces.

Figura 4.

Pero tiene un claro inconveniente, su coste, dado que se tienden muchos enlaces, que si bien en principio no se usan, aportan flexibilidad, garantizando el retorno de la inversión cuando haya que cambiar la configuración del armario de equipos.

Las diferentes interfaces de todos los equipos se encuentran etiquetadas, de manera que son identificables de manera unívoca. Ver figura 5.

Todas las interconexiones entre equipos, enlaces y conmutadores se encuentran recogidas en una base de datos de configuración (CMDB (6)), que permite una gestión sencilla del cableado, pese a no encontrarse delante de el.

De este modo, pueden desplegarse nuevos equipos conociendo de antemano como serán conectados, pudiendo generarse un plan de intervención con antelación. Ver figura 6.

El cableado discurre por el falso suelo, que cuenta con un metro de altura. Bajo el se distribuyen, de manera diferenciada las bandejas del cableado horizontal tanto eléctrico como de cobre y fibra óptica. El suelo está formado por baldosas ignifugas, con capacidad suficiente para soportar el peso de los diferentes armarios de equipos. Todos los materiales utilizados son ignífugos, con una protección contra-incendios A1 según norma UNE-13501.

Figura 5.

Disposición física

El espacio destinado al CPD de la DGC cuenta con una superficie de 60 m^2 ampliable con otros 20 m^2 adyacentes, en la forma de un nuevo pasillo.

A la hora de planificar la disposición de los armarios, se tuvieron en cuenta:

- Redundancia: Dentro de un límite, se ubicaron los armarios con la misma funcionalidad lo más lejos posible, sobre todo para los que dan servicios comunes.
- Disipación de calor: La distribución de los sistemas se ha realizado en base a tres pasillos, siguiendo la filosofía de pasillo frío-caliente para una mejor refrigeración de la sala. Se ha tenido en cuenta la ubicación de los equipos de frío y la disipación de los equipos al ubicarlos.
- Cercanía: Para aquellos armarios que necesitaran interconexiones no so-

(6) Configuración Management Data Base.

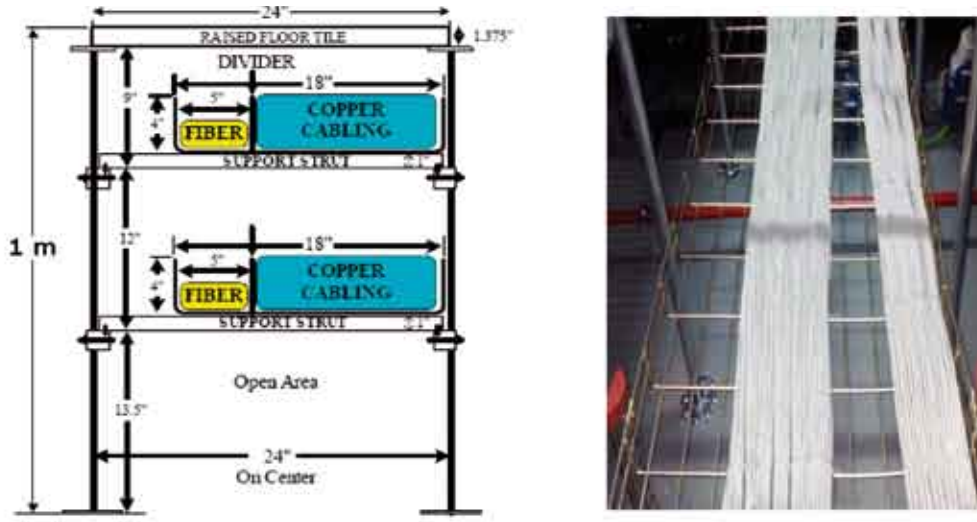


Figura 6.

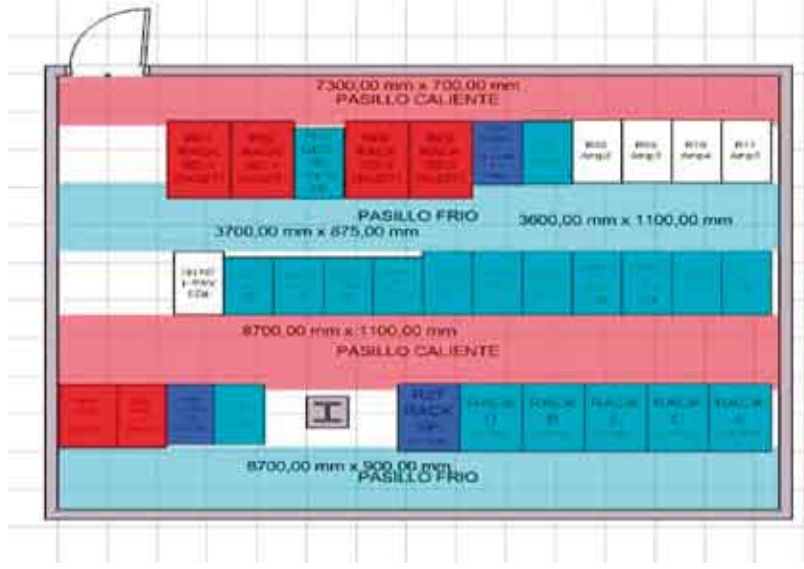


Figura 7.

portadas por el sistema de cableado estructurado ha sido necesario tratar su ubicación de manera especial.

- Soporte: Dado que muchos equipos tienen unos requerimientos de servicio 24x7, y además disponen de componentes que pueden ser intercambiados en caliente, era necesario disponer de pasillos con una anchura suficiente, que permitiera dar servicio a las máquinas sin apagarlas. Ver figura 7.

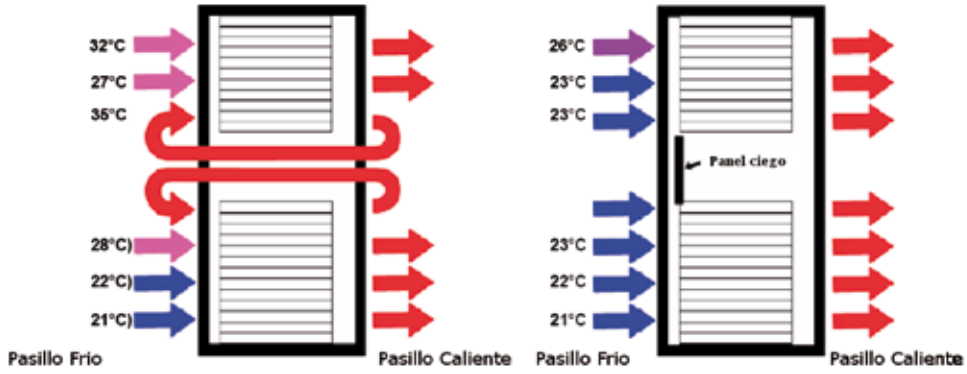


Figura 8.

Refrigeración

En un CPD de Housing, la refrigeración es responsabilidad del proveedor de servicios, que garantiza el mantenimiento de unas condiciones apropiadas de humedad y temperatura, reflejadas en Acuerdos de Nivel de Servicio (ANS o SLA).

Aun así, la DGC aprovechó la ocasión para mejorar la disposición de los equipos, y la circulación del aire en sus armarios, mediante la adición de paneles ciegos o "blanking panels" en los espacios vacíos de los armarios orientados hacia los pasillos fríos, optimizando los flujos de circulación del aire.

En la figura 8 puede verse como el uso de estos paneles evita el retorno del aire caliente a los equipos, evitando el sobreesfuerzo de sus ventiladores, y el gasto innecesario en refrigeración.

Por otro lado, los equipos se dispusieron de manera que los focos de mayor calor se situaran cerca de los equipos de refrigeración, para que el calor generado fuera absorbido lo más rápido posible, sin que por ello la refrigeración de la salas dejara de ser redundante.

Alimentación

Además de mantener las especificaciones de los equipos, se añadió alimentación redundante para aquellos equipos que no la tenían, o cuando no existía esta opción, se conectaron los equipos que daban un mismo servicio a distinta fase eléctrica.

En todos los armarios nuevos se instalaron dos PDU (7) de tipo barra, por su sencillez de gestión y cableado.

En este punto es necesario decir, que el proveedor de housing provee a todos los armarios de dos circuitos de alimentación redundante, disponiendo estos de SAI (8) y generador, ambos redundantes. Por otro lado, el edificio cuenta con doble acometida de corriente redundante, conectada a dos subestaciones eléctricas diferentes.

Seguridad Física de los equipos:

El edificio se estructura por plantas dedicadas al alojamiento de sistemas y permite dividir el espacio en nodos donde se ubicarán:

- Sala de operadores de telecomunicación
- Las "jaulas" de los clientes
- Centro de operación

(7) Power Distribution Unit, unidad de distribución de corriente.

(8) Sistema de Alimentación Ininterrumpida.

Figura 9.

El acceso físico al edificio se realiza a través de un control de seguridad a la entrada, siendo obligatorio el uso de tarjetas de identificación para el acceso a las diferentes dependencias. Estas tarjetas se asignan tras un riguroso registro de los nombres y horas de entrada y salida de todas las personas que acceden a los locales. El control de acceso viene regulado por unos protocolos de actuación definidos por la empresa, que entrega a la DGC informes de gestión relativos a los accesos.

El acceso a la "jaula" de la DGC se encuentra protegida a través de puertas de acceso:

- Al centro de datos
- A la planta
- Al nodo
- A la "jaula"

Además, la sala de sistemas puede ser considerada "limpia" ya que cuenta con presión positiva en el aire y medidas para controlar el polvo y minimizar la exposición de los equipos a la electricidad electroestática.

Por otro lado, en cuanto a la detección y extinción de incendios la sala cuenta con detectores de incendios, con sistema VESDA (9), sistemas de alarma para la protección del personal, extintores y un sistema automatizado y redundante de extinción de incendios. Además cuenta con protocolos de actuación aplicables durante y después de cualquier incidente.

1.1. Diseño lógico

El enfoque adoptado para el diseño lógico de toda la infraestructura ha seguido las pautas marcadas por el concepto de ***defensa en profundidad***, de forma que se apliquen contramedidas y controles de seguridad en cada capa de la infraestructura de información de la organización comenzando por la infraestructura de red y seguridad perimetral. Ver figura 9.

Este modelo contempla varias capas, aunque aquí nos centraremos en las relativas a la arquitectura de red y seguridad perimetral.

No obstante, toda organización que intente salvaguardar sus activos, deberá implantar adicionalmente controles y salvaguardas a todos los niveles organizativos, ya sea a través de políticas y procedimientos de seguridad, mediante mecanismos de seguridad físicos de los centros y medidas de seguridad aplicables a cada uno de los activos informáticos, las aplicaciones y los datos, que no serán objetos de este artículo.

Zonas de seguridad y defensas perimetrales

Toda arquitectura de seguridad tiene como objetivo la defensa del perímetro de

(9) Very Eartly Detection Apparatus, dispositivo de detección muy temprana de humo, que funciona aspirando el aire mediante redes de tuberías distribuidas por la sala, y buscando partículas en el.

red. El perímetro es el punto o puntos de separación de la red interna confiable para la organización que se encuentra en contacto con otras redes no fiables, no sólo considerada ésta como la red de Internet, sino de otras redes de usuarios o extranets relacionadas con la organización con los que se tenga conexión.

El perímetro se delimita a través del uso de *líneas de cortafuegos* que actúan a modo de barrera separando de forma lógica las diferentes zonas de seguridad.

La red del CPD se encuentra dividida en 3 zonas de seguridad claramente diferenciadas:

- Externa: Engloba todos aquellos servicios y redes que realizan un uso intensivo de Internet y que por tanto se caracterizan por un alto nivel de exposición frente a ataques o incidentes de seguridad.
- Interna: Formada por los sistemas que dan soporte al backoffice de la DGC, e interconexiones con la red WAN que conecta con las gerencias, la Intranet Administrativa, el resto del Ministerio de Economía y Hacienda y otros organismos colaboradores.
- Gestión: Es una tercera zona de seguridad, separada de las dos anteriores que engloba la parte de gestión de todos los activos informáticos y elementos de seguridad de la infraestructura. Esta zona de seguridad no es accesible desde fuera del perímetro de seguridad y a efectos del resto de redes es transparente. Las redes de gestión juegan un papel muy importante, dadas las características del CPD. Los sistemas deberán ser gestionados en remoto con la mínima intervención humana, permitiendo que sólo en casos de averías graves o nuevas implantaciones de sistemas sea necesario trasladarse al centro de proceso de datos.

Estas zonas deben ser salvaguardadas frente a la interconexión con otras redes ajenas a la organización o incluso diferentes segmentos lógicos cuyos niveles de seguridad no tienen por qué ser acordes con las políticas de Seguridad de la DGC.

Defensa en red

Pese a que tradicionalmente, se hacen grandes esfuerzos en la protección del perímetro externo, no debe descuidarse la protección frente a los ataques recibidos desde dentro de la propia organización, que según Gartner suponen más del 70 % de los recibidos anualmente.

Para ello, se introducen conceptos de segmentación de redes a nivel de infraestructura de red para evitar la visibilidad directa entre las mismas, y se usan sistemas de detección y/o prevención de intrusiones para la monitorización y actuación frente a posibles ataques o comportamientos maliciosos.

Las redes más expuestas a ataques externos se encuentran monitorizadas a través de sistemas de prevención de intrusiones, IPS (10) Este tipo de sistemas se encargan de analizar todo el tráfico que pasa través de ellos en busca de patrones de posibles ataques. Su comportamiento puede ser simplemente informativo a través del envío de alertas o proactivo mediante la terminación de los distintos ataques detectados.

Arquitectura técnica

Como ya hemos visto, el diseño de la red del CPD se basa en el concepto de "Zona de seguridad", esto se plasma en que cada zona cuenta con una pareja de cortafuegos en alta disponibilidad que realizan el enrutamiento y una serie de switches que la segmentan en VLANS, asignados de manera única a esa zona.

(10) Intrusion Prevention System, Sistema de detección de intrusiones capaz de reaccionar frente a los ataques y abortarlos.

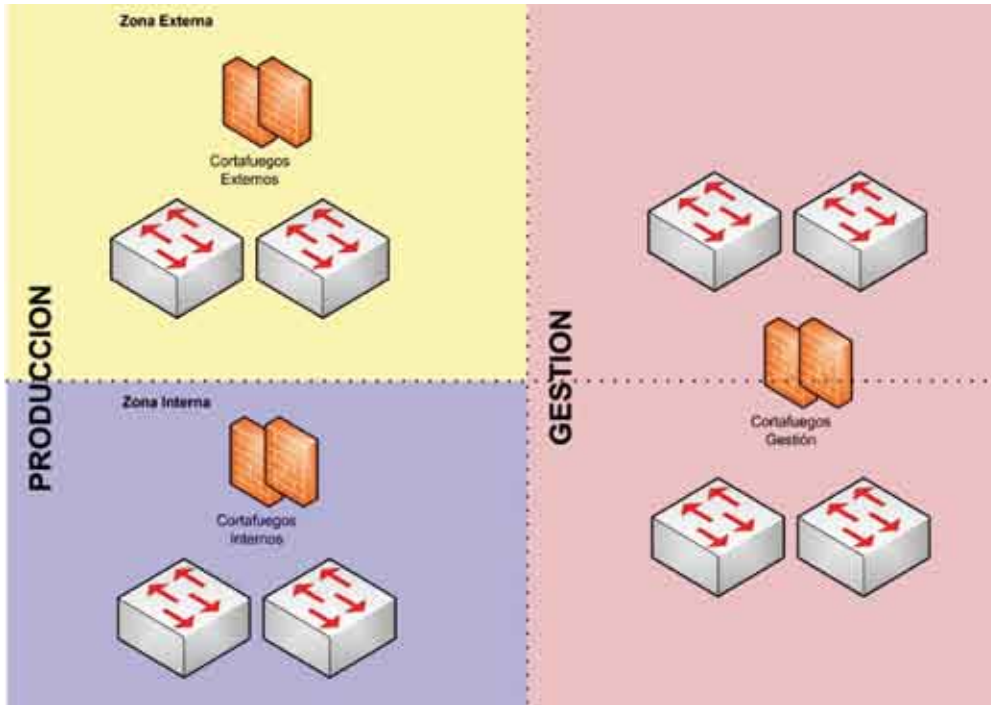


Figura 10.

De esta manera, el único contacto posible entre dos zonas de seguridad es a través de los cortafuegos, lo que impide cualquier tipo de ataque a nivel 2.

Las zonas de seguridad existentes son 3, Zona Externa, Zona Interna y Zona de Gestión. Ver figura 10.

Como ya se ha comentado, todas estas zonas de seguridad se encuentran segmentadas lógicamente en redes aisladas a través del concepto de redes locales virtuales o VLAN (11). Se trata de un concepto de seguridad aplicable a nivel de redes de área local en las que un único dominio de difusión se divide a varios dominios disjuntos a través de la configuración de la electrónica de red. De esta forma, aplicando la famosa regla del *divide y vencerás* se reduce el nivel de exposición frente ataques entre las redes, siendo éstas controladas por los sistemas cortafuegos.

Cada sistema cortafuegos presenta una interfaz de red redundada en todas las redes tanto Externas como Internas, realizando el enrutamiento entre las diferentes redes de acuerdo a unas reglas predefinidas que intentan garantizar la máxima seguridad y permitiendo un mínimo de privilegios.

El uso de reglas de filtrado tiene que llegar a un compromiso entre funcionalidad y seguridad. El abrir demasiado el tráfico permitido incrementa los niveles de funcionalidad alcanzables entre las diversas redes para con los distintos servicios pero puede implicar problemas de rendimiento y agujeros de seguridad que deben ser evitados. Hay que llegar a un compromiso entre ambos criterios.

(11) Virtual Local Area Network.

Descripción de las infraestructuras implantadas

La centralización de todos los sistemas de la DGC en un único CPD y el traslado de todos los sistemas que dan servicio a la Oficina Virtual del Catastro, anteriormente alojados en el CPD de la SGTIC de la Subsecretaría del Ministerio de Economía y Hacienda, obligó a la DGC a valorar la necesidad de cambiar y mejorar la arquitectura de red anteriormente implantada, de forma que permitiera ofrecer sus servicios con la mayor robustez, rendimiento y seguridad y con los niveles de disponibilidad y redundancia necesarios. Por todo ello, se decidió rediseñar la red y renovar la infraestructura de Seguridad Perimetral de manera previa al traslado.

Diseño de la red

A la hora de diseñar la nueva red, la DGC se planteó los siguientes requisitos:

- Rendimiento: La electrónica de red debía de ser capaz de conmutar un muy alto volumen de tráfico, dado que con la próxima centralización del catastro se iban a instalar más de 20 máquinas con interfaces 10 Gigabit Ethernet.
- Aislamiento: Desde el primer proyecto de seguridad perimetral, se tenía muy claro que las redes que daban servicios al exterior debían de estar separadas físicamente de las redes internas. El mismo criterio aplicaba para las redes de gestión.
- Soporte de filtrado multicast: Entre los diferentes sistemas que emplea la DGC se utiliza el multicast a nivel 2 para conseguir la alta disponibilidad. La electrónica de red debía permitir que el uso de este protocolo no degenerase en "tormentas" que disminuyeran el rendimiento de la red.
- Enrutamiento en los cortafuegos: Pese a que todos los fabricantes de electrónica de red integran en sus productos enrutadores, se decidió que todo el tráfico de cada zona pasara por sus cortafuegos, aportando un alto nivel de control de la red.

Redes de producción

Finalmente, y tras analizar diferentes alternativas presentes en el mercado, se tomó la decisión de utilizar los productos de CISCO para los entornos productivos.

La red está diseñada siguiendo el modelo de "Campus Network" propugnado por CISCO, con la salvedad de que se sustituye la conmutación de nivel 3 en los switches por enrutamiento en los firewalls, excepto en la parte de CORE.

Pese a contar con los protocolos propietarios de CISCO, todos los elementos de la red han sido configurados con estándares, como IEEE 802.1q (para agregar interfaces) o IEEE 802.1s (Múltiples Instancias de Spanning Tree). Ver figura 11.

En la Zona Interna, el CORE de la red está formado por 2 Catalyst 6509-E, a los que se conecta una capa de acceso formada por los switches de los equipos blade, mientras que el resto de máquinas, fundamentalmente UNIX, se conecta directamente al CORE.

En esta zona, el routing se realiza por los cortafuegos, para todas aquellas VLANS con equipos conectados, mientras que el switch enruta aquellas que son de transporte, como la interconexión con Castellana, mediante OSPF.

La red de Castellana está conectada con el CPD mediante dos enlaces Gigabit Ethernet, que podrían haber permitido una interconexión a nivel 2, lo que se conoce como "LAN extendida". Pese a que habría sido más sencillo de implantar, se optó por utilizar enrutamiento, ya que aísla completamente la red del CPD de un fallo de nivel 2 en Castellana.

En la Zona Externa, existen otros 2 Catalyst 6509-E, que concentran los equipos de las diferentes DMZ y los equipos que dan acceso a Internet, así como los dispositivos

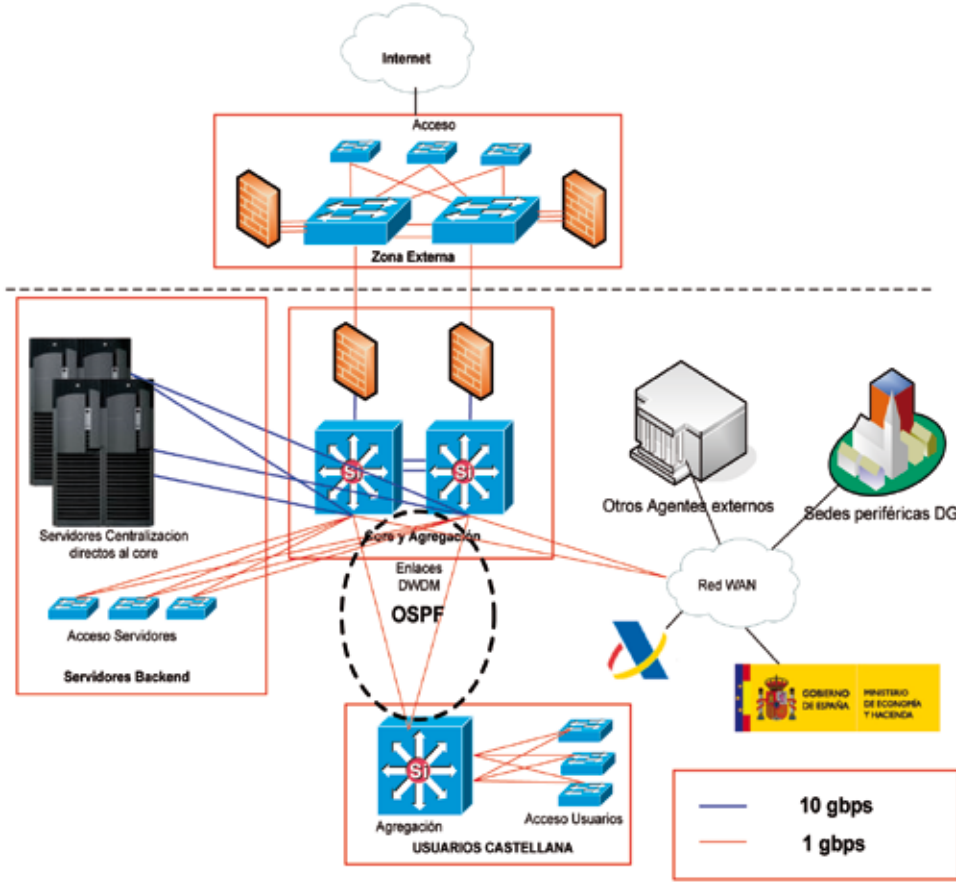


Figura 11.

de Seguridad Perimetral. En esta zona, el routing es realizado por los cortafuegos, al estar mas expuesta a ataques.

Dentro de la gama de Cisco Catalyst, se optó por la serie 6500 para el Core de la red y para la zona externa, con dos equipos Catalyst 6509 con supervisora 720 en cada una de ellas. Esta elección está justificada por el elevado rendimiento que estos equipos proporcionan, su alto grado de fiabilidad, liderazgo del sector y por ofrecer con garantías los requisitos necesarios para los nuevos retos que se avecinan en cuanto a capacidad, robustez y funcionalidad.

Estos equipos, catalogados como carrier-class (12), son sistemas modulares y redundantes, tanto en fuentes de alimentación como en capacidad de proceso, al permitir el uso de dobles supervisoras que garanticen la continuidad del servicio, son capaces de soportar cotas de tráfico superiores a 720 Gbps y disponen de tarjetas modulares que proveen conectividad

(12) Término que indica que son equipos capaces de aportar los requisitos que necesita un proveedor e servicios de comunicaciones (carrier), a saber, funcionamiento 24x7x365

de hasta 48 puertos Gigabit Ethernet, ó 8 puertos 10 Gigabit Ethernet por módulo. Ver figura 12.

A la hora de configurar los equipos, no solo se ha valorado la velocidad del chasis o las supervisoras, sino que se han elegido tarjetas modulares capaces de funcionar a "velocidad del cable", o wire speed, es decir, que no tienen penalización o sobresuscripción, sino que cada puerto ethernet dispone de su propio ancho de banda hacia el bus del switch.

Especialmente importante es la posibilidad de absorber grandes cantidades de tráfico y el uso de interfaces 10 Gigabit Ethernet, debido al proceso de centralización de las bases de datos catastrales, que se hará sobre dos equipos HP Superdome 64, con 128 núcleos Itanium Montvale, y 1 TB de RAM (13) cada uno, que demandarán un muy elevado rendimiento de la red. Estos equipos, son superiores en rendimiento a muchos mainframes, y son utilizados en entornos de computación científica, pudiendo poner a prueba cualquier infraestructura de red.

Además de los Catalyst 6500, se han utilizado, tanto en el CPD como en Castellana, equipos de la serie 3750, por su versatilidad y alto rendimiento, dado que permiten interconectarse entre si a velocidades de 32 gbps.

Red de gestión

Las redes de gestión están implementadas con electrónica de red HP ProCurve, de la serie 28XX. Están formadas por 4 switches para cada zona de seguridad (externa e interna) y se interconectan a las redes en producción a través de la línea de cortafuegos de gestión.

Estas redes, al igual que las de producción, están segmentadas en VLANs, que son enrutadas por los cortafuegos de gestión.

Figura 12.

La infraestructura de Seguridad Perimetral

La arquitectura de Seguridad perimetral de la DGC separa lógicamente las diferentes subredes a través de las tres líneas de cortafuegos implantadas. De esta forma se corresponderán zonas de seguridad con líneas de cortafuegos externa, interna y de gestión.

Esto nos permite no sólo alcanzar altos niveles de seguridad para aquellos sistemas expuestos a Internet, sino que también realiza una separación interna cliente/servidor garantizando la seguridad tanto en el acceso a las aplicaciones de los usuarios internos, como en las relaciones con los agentes ex-

(13) Random Access Memory

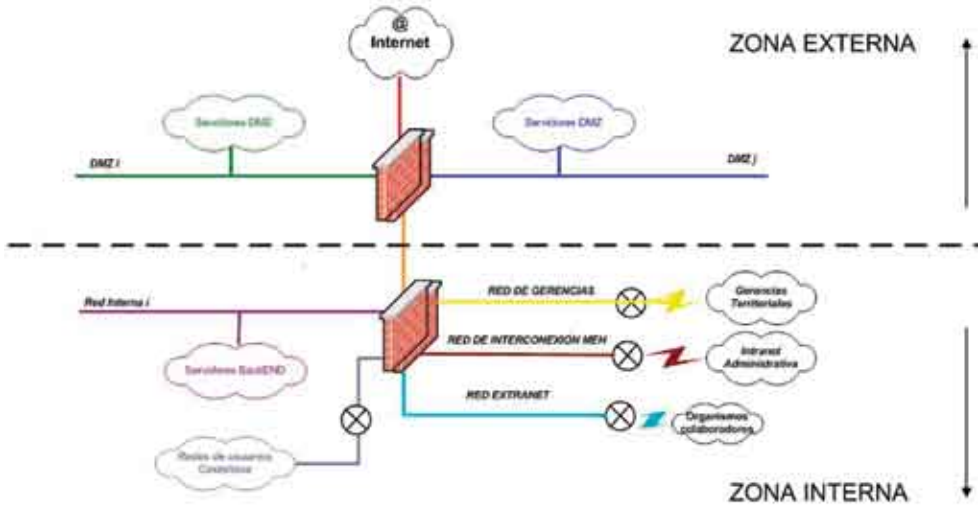


Figura 13. Arquitectura de red

ternos – colaboradores, EELL, ministerios…. Ver figura 13.

Sistemas cortafuegos

Estas barreras de cortafuegos pertenecen a fabricantes distintos, CheckPoint y StoneGate, formados por nodos redundados y balanceados en modo activo-activo. Para un mayor aprovechamiento de la capacidad de proceso y eficiencia de los sistemas cortafuegos se optó por la modalidad de alta disponibilidad activo-activo multicast, de forma que todos los nodos reciben todo el tráfico y se alcanzan unos niveles de rendimiento muy elevados.

Los cortafuegos fueron dimensionados a nivel hardware con una gran capacidad de proceso soportando flujos de tráfico superiores a 3 Gbps, con interfaces 1/10 Gigabit Ethernet dedicadas a los distintos segmentos de red, y permitiendo una capacidad de filtrado acorde a los nuevos retos de centralización e integración.

Las redes de producción se encuentran separadas de las de gestión a través de una línea de cortafuegos que segmenta las redes pertenecientes a gestión. En este caso, por no requerirse niveles de rendimiento tan altos como los relativos a las redes en producción se optó por la configuración de 2 nodos redundados en alta disponibilidad con un modo activo-pasivo. Este tipo de balanceo implica que uno de los nodos actúa como pivote, controlando el trabajo de ambos cortafuegos.

Sistemas de detección de intrusiones

Las redes DMZ, o desmilitarizadas se encuentran reforzadas a través de sondas de prevención de intrusiones (IPS) que revisan todo el tráfico que pasa a través de ella en busca de comportamientos anormales de red y posibles ataques. Está formado por nodos dimensionados con alta capacidad de proceso y flujos de tráfico superiores a 4 Gbps y hacen uso de tarjetas de red tolerantes a fallos o *bypass* que permiten que ante la caída de las mismas pueda seguirse ofreciendo servicio.

Adicionalmente, en todas las subredes se han configurado interfaces espejo o port-

mirror que van dirigidas a sistemas sniffer, que permitan la monitorización y análisis de problemas de red y flujos de tráfico.

Conclusiones

El diseño del CPD se ha visto englobado dentro del complejo traslado de todos los sistemas informáticos de las DGC en la modalidad de alojamiento externo. Esto ha constituido un gran reto para la DGC. Por una parte, implicaba grandes riesgos al no contar con el respaldo necesario de todos sus sistemas y por otra parte, debería realizarse en un tiempo relativamente corto para evitar la falta de servicio e inoperatividad de sus servicios ofrecidos, englobados principalmente por la Oficina Virtual y la Base de Datos Nacional del Catastro.

Por todo ello, se ha profundizado en el correcto diseño físico y lógico de las infraestructuras base del CPD: diseño del espacio físico, diseño estructurado del cableado y distribución de los activos informáticos y de las infraestructuras de red y seguridad perimetral.

La arquitectura de red ha sido diseñada buscando la seguridad, la disponibilidad, y el rendimiento, por ese orden. Es primordial conseguir unos altos niveles de seguridad para la protección del perímetro, manteniendo altos niveles de disponibilidad de forma que ante la caída de algún elemento se mantenga el servicio, y por último, es necesario un elevado rendimiento de la red, tanto en velocidad como en latencia.

La implementación rápida y efectiva de la nueva infraestructura de red y seguridad perimetral y la correcta gestión de la configuración de la información relativa al traslado (sistemas informáticos, conexiones, parcheos, cableado y alimentación eléctrica) ha resultado crítica para la correcta realización del traslado al tratarse de la base sobre la que se asientan todos los sistemas de la DGC.

Pero, cabe decir que mientras la ingente cantidad de datos recopilados y los procedimientos desarrollados se mantengan actualizados y operativos, este CPD seguirá prestando sus servicios sin alteración. Es igual o más importante la operación día a día de los sistemas que su diseño inicial por lo que deberán cuidarse su explotación futura.

Para realización del diseño e implantación de esta parte de proyecto del CPD, ha resultado imprescindible el apoyo de COLT, empresa proveedora del servicio de housing, de HP, integrador en la parte de infraestructura de red y GMV-SGI en el entorno de Seguridad Perimetral.

La DGC cuenta, por tanto, con un CPD puntero en cuanto a infraestructuras y dimensionamiento que puede ser tomado como ejemplo de buenas prácticas en cuanto a arquitectura y configuración y que ha supuesto una mejora de los servicios ofrecidos tanto a los ciudadanos como a su personal interno. Y que mantiene una filosofía de mejora continua en aras de la obtención de niveles cada vez mayores de calidad y servicio. ■