CATASTRO Octubre 2007

Implantación y gestión operativa del entorno de seguridad perimetral en la Dirección General del Catastro

Ignacio Otero Romaní
Jefe de Sección de Sistemas Informáticos
Dirección General del Catastro

Para la Dirección General del Catastro la seguridad de la información constituye un valor fundamental fuertemente asociado al uso de las tecnologías de la información como instrumento para cumplir con las potestades encomendadas. El Catastro Inmobiliario, como registro administrativo dependiente del Ministerio de Economía y Hacienda en el que se describen los bienes inmuebles rústicos y urbanos, registra y gestiona un volumen importante de datos de carácter personal. La información contenida en las bases de datos catastrales, en particular aquella que comprende datos personales, está protegida por la Ley Orgánica 15/1999, de Protección de datos de carácter personal. Adicionalmente, tal como menciona el Real Decreto Legislativo 1/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley del Catastro Inmobiliario, se consideran datos protegidos el nombre, apellidos, razón social, código de identificación y domicilio de quienes figuren inscritos en el Catastro Inmobiliario como titulares. En consecuencia, el desarrollo de una adecuada política de protección de la información así como la implantación y desarrollo de infraestructuras y servicios específicos de seguridad cobra una especial relevancia en la Dirección General del Catastro.

La estrategia en materia de tecnologías de la información de la Dirección General del Catastro pasa por la mejora continua de la calidad de los distintos servicios de administración electrónica proporcionados, así como el desarrollo de nuevos servicios que atiendan a las demandas de los ciudadanos, empresas y Administraciones Públicas. Para ello, es de vital importancia contar con las infraestructuras y tecnologías que den soporte al crecimiento en volumen de usuarios, transacciones, procesos y aplicaciones de estos servicios, además de garantizar la entrega de los mismos, extremo a extremo, con un nivel adecuado de

seguridad. Estas infraestructuras permiten sustentar las distintas iniciativas innovadoras que la Dirección General del Catastro elabora para cumplir eficaz y eficientemente con su mandato de servicio público.

Dentro del marco de actuaciones estratégicas planteadas por la Subdirección General de Estudios y Sistemas de Información de la Dirección General del Catastro en 2005 se encontraba el análisis y estudio de viabilidad de la implantación de un entorno seguro de acceso a Internet y a redes externas para este Centro Directivo.

Como consecuencia del nuevo concurso de comunicaciones de voz, datos, telefonía móvil y acceso a Internet del Ministerio de Economía y Hacienda, vigente desde principios de 2006, la Dirección General del Catastro cuenta con un acceso a Internet propio repartido en 4 líneas redundantes con una capacidad agregada de 220 Mb/s, lo cual supone un incremento del 780% respecto de la capacidad anterior. Esta capacidad, muy por encima de la media de otras organizaciones públicas y privadas de similar o mayor tamaño, permite garantizar la escalabilidad de los servicios basados en Internet actuales y futuros. Por otro lado, el concurso también ha supuesto la mejora de los accesos de las Gerencias Territoriales con los Servicios Centrales y el resto de la red del Ministerio, pasando a disponer de líneas con capacidades por encima de los 5 Mb/s, presentando aumentos cercanos al 4.000%. En este momento, la Dirección General del Catastro cuenta con una de las redes de comunicación más punteras y modernas de España y Europa, que emplea las últimas tecnologías (IP, MPLS, VoIP, MetroEthernet, DWDM, etc.) disponibles en el mercado.

La provisión de una red de comunicaciones privada e independiente para la Dirección General del Catastro como la propuesta en el mencionado concurso requiere necesariamente de la definición e implantación de un entorno de seguridad perimetral y de red, de forma que puedan proporcionarse servicios basados en Internet y tecnología TCP/IP con las debidas garantías de seguridad, gestión y rendimiento, acordes con los objetivos estratégicos de la organización. De este modo se persigue la autonomía en la prestación de servicios de carácter telemático por parte de la Dirección General del Catastro y por tanto una mejora global de la calidad de servicio percibida por los usuarios.

Por todo lo anterior, la Dirección General del Catastro, tras una primera fase de análisis y diseño previo en la que se definió la arquitectura general, los requisitos de negocio y técnicos y las necesidades en materia de seguridad del futuro sistema, convocó un concurso público, en procedimiento, abierto para la *provisión e implantación de un entorno avanzado de seguridad perimetral que incluyera todos los elementos de seguridad y de gestión necesarios* para cumplir con todos los objetivos planteados.

La descripción de la experiencia práctica del equipo de gestión del proyecto durante las distintas fases: implantación y gestión operativa, es objeto del presente artículo.

La importancia de la seguridad de la información

La cuestión de la seguridad de la información y la protección de los datos de carácter personal cobra una especial importancia en un mundo digital y globalizado en la que la mayoría de los datos circulan por redes y sistemas de información automatizados. A la vez que se abren enormes posibilidades para el desarrollo de nuevos servicios y aplicaciones en Internet, también aumentan los posibles riesgos y amenazas sobre la identidad de las personas, sus libertades y derechos fundamentales.

En el caso de las Administraciones Públicas, la garantía de la privacidad y la protección de datos es un requisito de pri-

mera magnitud. Probablemente, las Administraciones Públicas poseen el mayor volumen de datos de carácter personal de ciudadanos y empresas. La divulgación o uso no autorizado de esta información puede provocar importantes perjuicios para las personas y organizaciones o incluso para las economías y mercados de los países. Por tanto, cualquier servicio o aplicación de Administración electrónica deberá diseñarse con las adecuadas medidas y garantías de protección de la información.

Asimismo, las distintas organizaciones tanto del sector público como del sector privado tienen una dependencia cada vez mayor respecto de la información que procesan en el desarrollo de sus actividades y potestades. Cualquier pérdida de *autenticidad, confidencialidad, integridad* o *disponibilidad* de la información y de los servicios que sobre ella se sustentan puede producir importantes impactos negativos. En consecuencia, resulta de vital importancia la adecuada protección de la información junto con una eficiente gestión de la seguridad de los sistemas basados en las tecnologías de la información, dado que la mayoría de organizaciones están actualmente conectadas a sistemas y servicios externos por medio de redes públicas potencialmente inseguras.

Tal como define la norma internacional ISO 27001 en materia de gestión de la seguridad de la información: "la información es un activo, que, como otros activos importantes del negocio, tiene valor para la organización y requiere una protección adecuada." Como base para una seguridad efectiva de las tecnologías de la información, la norma UNE 71501-1:2001 indica que "se deben formular los objetivos, estrategias y políticas generales de seguridad de la organización." Estas estrategias deben traducirse en la definición de distintos controles de seguridad que garanticen la protección en diversos dominios, entre los que se incluyen por ejemplo: la seguridad física y del entorno, la seguridad en el desarrollo de las aplicaciones y sistemas, el control de acceso, la gestión de incidentes, la continuidad de negocio o el cumplimiento de legislación específica de protección de datos. La norma ISO 17799:2005 "Código de buenas prácticas para la gestión de la seguridad de la información" incluye un catálogo exhaustivo de controles de seguridad definidos por expertos y organizaciones a lo largo de varios años de experiencia.

De forma específica, el control de acceso y la seguridad de las comunicaciones, las redes y el acceso a los sistemas y aplicaciones es el objeto del campo de la *seguridad perimetral,* que constituye uno de los ámbitos fundamentales para la protección de los activos de información.

¿Qué es la seguridad perimetral y de red?

La *seguridad perimetral o de red* es un término acuñado para hacer referencia a los controles, mecanismos, técnicas y estrategias utilizadas para controlar y proteger el acceso a recursos y servicios accesibles a través de una o varias redes informáticas externas.

Según Microsoft, el "el perímetro de red abarca cada punto donde la red interna de la organización se conecta a redes y sistemas que no son controlados por ella". En la política de seguridad perimetral de la Dirección General del Catastro se indica que "el perímetro de seguridad es la frontera lógica que delimita el conjunto de recursos y activos de la Dirección General del Catastro que deben ser objeto de protección. Adicionalmente, también establece el límite con los dominios, redes o zonas externas que no son confiables".

Es decir, el criterio fundamental utilizado para determinar donde se establece la frontera lógica de la red propia depende de los puntos donde existe una interconexión con redes no confiables. En este sentido, en

el caso concreto de la Dirección General del Catastro, el perímetro de seguridad de la red está delimitado por un lado, por la interconexión con Internet y por otro lado con el resto de redes de comunicaciones de los organismos externos con los que existe una conexión directa como puedan ser por ejemplo, el resto de Centros Directivos del Ministerio de Economía y Hacienda.

En un mundo en el que las organizaciones realizan negocios, transacciones y relaciones a través de redes transnacionales de comunicaciones, la adecuada protección de los accesos constituye un requisito imprescindible. Hoy en día, existen múltiples y numerosas amenazas que puedan comprometer la disponibilidad, integridad y confidencialidad de los activos de información. La mayor parte de estas amenazas son generadas por terceras partes de forma intencionada, con el objeto de causar algún tipo de perjuicio u obtener un beneficio, generalmente económico, de los ataques producidos contra los sistemas de una organización a través de la red. Es fácil imaginar la motivación de determinados atacantes para comprometer la seguridad de los sistemas de información de las organizaciones públicas.

A continuación se analizan brevemente los tipos de amenazas más frecuentes a las que hace frente la seguridad perimetral y de red.

Entre el tipo de amenazas a las que hace frente la seguridad perimetral encontramos por ejemplo, la *modificación no autorizada de páginas y servicios webs* (conocido también por el término inglés "defacement") con objeto de dañar la reputación de una organización, introducir algún tipo de mensaje reivindicativo, interrumpir las operaciones o bien engañar a los usuarios para obtener algún tipo de beneficio.

Un tipo de ataque similar al anterior pero más dañino son los intentos de intrusión destinados al *robo de información protegida* o sensible. Estos ataques suelen ser muy sofisticados y tienen un objeto muy claro. Aprovechando posibles vulnerabilidades en los servicios, persiguen introducirse de forma no autorizada en bases de datos o servidores para obtener o modificar información protegida, obteniendo algún tipo de beneficio a cambio. Son numerosos los casos de robo de información de bases de datos con números de tarjetas de crédito de empresas que realizan transacciones de comercio electrónico. Una variante de este tipo de ataques es la *destrucción* de los datos de un servidor o servicio, provocando la indisponibilidad del mismo y la consiguiente pérdida de datos.

Otro tipo de amenazas frecuentes son los denominados *ataques de denegación de servicio,* cuyo objetivo es el de interrumpir el acceso a un determinado servicio informático por parte de los usuarios autorizados. Este tipo de ataques puede ser muy dañino ya que puede producir que una determinada página web o servicio no sea accesible durante un periodo de tiempo elevado. Un ejemplo reciente de este tipo de amenazas ocurrió en abril de 2007 cuando se produjo un ataque masivo de denegación de servicio contra las páginas y servicios web gubernamentales de Estonia. Durante varios días, la mayoría de los servicios de Administración electrónica de este país estuvieron inaccesibles para los ciudadanos. A fecha de hoy no se conoce con certeza la identidad de los atacantes, si bien se sospecha que fueron orquestados desde Rusia.

Una de las amenazas más comunes a las que la seguridad perimetral también hace frente son los *virus, gusanos y otro tipo de código malicioso.* De sobra es conocido el grado de impacto que produce este tipo de amenazas, tanto en equipos de usuario como en servidores. Asimismo, con la difusión de las redes e Internet, los ataques se han vuelto más sofisticados y los denominados "gusanos" son capaces de infectar, a través de Internet, millones de equipos en cuestión de horas. El impacto económico sobre la productividad de las organizaciones y el posterior coste de la limpieza del virus en cuestión puede ser muy elevado. Basta citar el

ejemplo relativamente reciente del virus "blaster" que causó importantes estragos en múltiples organizaciones a nivel mundial.

En relación con la amenaza anterior, la seguridad perimetral también actúa como elemento de filtrado de tráfico de datos procedente de redes externas. Un ejemplo especialmente importante es el uso del correo electrónico. Los sistemas utilizados en seguridad perimetral permiten establecer políticas específicas para el tratamiento y gestión del correo electrónico procedente o con destino a otras organizaciones y personas externas. En este sentido, se implementan mecanismos específicos para el control de código malicioso en ficheros adjuntos, tamaños de los correos, divulgación no autorizada de información protegida y control de correo no deseado (Spam). Como reseña, cabe mencionar que uno de los grandes problemas a los que hacen frente las organizaciones interconectadas de hoy en día es el problema del Spam. Como botón de muestra de la magnitud de este problema, la Dirección General del Catastro detecta y bloquea semanalmente más de 560.000 correos electrónicos no deseados, que además suponen aproximadamente el 90% de todos los correos recibidos en ese periodo. Este problema es difícilmente evitable en origen ya que las fuentes generadores de Spam se han vuelto tremendamente sofisticadas y la difusión (generalmente con remuneración económica) de direcciones de correo de destinatarios por parte de terceros está muy extendida. La seguridad perimetral ayuda a paliar este problema a través del bloqueo de este tipo de correos con el objeto de que el usuario no vea perturbada su productividad.

Otro tipo de ataque más específico que se produce a través del correo electrónico es el denominado *"phishing"* que consiste en el intento de suplantar la identidad de una organización externa (como por ejemplo un banco) a través de un correo electrónico falsificado que intenta provocar que el destinatario revele algún tipo de información personal o sensible (por ejemplo las claves de acceso a banca electrónica) a una tercera parte no autorizada.

También debemos mencionar otro tipo de amenazas típicas, como los programas *"spyware", "rootkits", troyanos,* etc. Este tipo de software se instala de forma sigilosa en equipos y servidores a través de Internet y proporciona información (por ejemplo contraseñas, claves de acceso, acceso a ficheros en los discos duros, etc.) de los usuarios a terceros que podrá ser utilizada para algún tipo de ataque posterior.

La seguridad perimetral también permite implementar de forma efectiva la *política de seguridad interna* de un determinado organismo. A través de distintos sistemas y tecnologías es posible limitar el acceso, por parte de los usuarios internos, a recursos no autorizados. Estas limitaciones van desde autorizaciones específicas de acceso a determinados servidores internos hasta restricciones en las páginas web que se pueden visitar, contenidos de Internet que se pueden descargar, uso de programas de descargas P2P, etc. Así, puede evitarse que determinados usuarios internos abusen de los recursos disponibles en detrimento de las necesidades reales del negocio. En este sentido, también debe destacarse que la seguridad perimetral debe evitar que se pueda utilizar la infraestructura de servidores y equipos de usuario de la organización como plataforma para lanzar ataques a terceras organizaciones. Los atacantes suelen utilizar equipos intermedios con el objeto de cubrir sus huellas y que sea más difícil rastrear las trazas de sus ataques.

Asimismo, debemos mencionar que las infraestructuras de seguridad perimetral permiten establecer mecanismos seguros para garantizar la seguridad de los *accesos remotos* de una organización. Actualmente, debido a las necesidades de flexibilidad y movilidad de las organizaciones es cada vez más frecuente que los empleados requieran el acceso a los recursos corporativos desde el exterior, mediante el uso de equipos portátiles, dispositivos móviles y accesos

públicos a Internet. Para permitir este tipo de accesos, se implementan redes privadas virtuales (VPN) que proporcionan un canal seguro y cifrado para el acceso remoto a través redes públicas no confiables como pueda ser Internet. La seguridad perimetral integra este tipo de tecnologías que extienden el perímetro de la red de la organización fuera de las fronteras físicas de sus propias oficinas e instalaciones.

Finalmente, entre los tipos de amenazas a las que la seguridad perimetral hace frente son todo tipo de ataques en red que puedan provenir desde el interior de la organización. Generalmente, los *ataques con mayor probabilidad de éxito son los que se originan en la propia organización,* bien porque algún empleado disponga de acceso a datos protegidos o bien porque al disponer de un equipo dentro de la red un atacante potencial tenga más fácil el acceso a datos y recursos protegidos. En el diseño del entorno de seguridad perimetral de la Dirección General del Catastro se ha realizado la separación de equipos cliente respecto de los servidores para añadir un control adicional, fundamentalmente motivado por el número de organismos públicos externos que se conectan a través de la red interna de comunicaciones.

Todas estas amenazas pueden materializarse en incidentes de seguridad cuyas *consecuencias* pueden ser realmente graves. Puede producirse una pérdida económica, un perjuicio a la imagen y reputación, un compromiso de la seguridad de los datos, la interrupción de procesos críticos de negocio, incumplimiento de mandatos legales (como legislación en protección de datos) y el deterioro en la relación con organizaciones colaboradoras, clientes o proveedores, entre otras.

Como veremos más adelante, las infraestructuras de seguridad perimetral y de red incluyen distintas elementos, sistemas y tecnologías para hacer frente a estas amenazas entre las que pueden destacarse los siguientes: cortafuegos, sondas de detección de intrusiones, antivirus perimetral, gestores de vulnerabilidades, equipos frontales, sistemas proxy de navegación web, soluciones de acceso remoto en red privada virtual (VPN), etc.

En último lugar, también debemos mencionar que las infraestructuras de seguridad perimetral están indisolublemente unidades a la infraestructura de red sobre las que se implementan. Por tanto, el rendimiento y la disponibilidad de los servicios de red e interconexión dependerán en gran medida de la infraestructura de seguridad. Esto implica que el diseño deberá tener en cuenta los criterios de alta disponibilidad y capacidad que se estén solicitando a los servicios de red y telecomunicaciones. Ello podrá requerir de sistemas redundantes y de la adquisición de equipos con capacidad suficiente para absorber y analizar el tráfico de la organización.

Proyecto de seguridad perimetral en la Dirección General del Catastro

El proyecto de implantación de un entorno de seguridad perimetral en la Dirección General del Catastro nace de la necesidad de prestar un mayor número de servicios, basados en Internet, tanto para usuarios externos como para los propios usuarios internos. La resolución del nuevo Concurso de comunicaciones del Ministerio de Economía y Hacienda ha permitido que la Dirección General del Catastro disponga de un acceso a Internet propio y una red WAN privada virtual que interconecta la sede central con las Gerencias Territoriales y la sede central con el resto de Centros Directivos del Ministerio.

Un requisito previo a la utilización de esta nueva infraestructura de comunicaciones es la implantación de un entorno de seguridad perimetral que garantice la seguridad y disponibilidad de los servicios, activos e información.

El equipo de proyecto asignado por la Subdirección General de Estudios y Sistemas de Información identificó dos grandes subproyectos en la adopción de una infraestructura de seguridad perimetral:

1. *Subproyecto de implantación del entorno de seguridad perimetral:* abarca el diseño, construcción, configuración y puesta en marcha del entorno de seguridad perimetral y la gestión asociada en el marco de los sistemas y la infraestructura de comunicaciones de la Dirección General del Catastro.
   El proyecto de implantación presenta la complejidad añadida de abordar la migración desde una situación inicial muy distinta a la prevista finalmente, requiriendo la coordinación de múltiples recursos, sistemas y servicios con responsables distintos.
2. *Subproyecto de gestión operativa:* finalizada la implantación del entorno y una vez estuviera éste plenamente operativo, comienza la gestión y operación del mismo para garantizar el cumplimiento de los objetivos planteados.
   Para la gestión de estos proyectos se ha utilizado la metodología de gestión de proyectos del PMI (Project Management Institute).

Durante la planificación inicial del proyecto, se identificaron los siguientes *objetivos fundamentales:*

- Implantación de un entorno de seguridad perimetral sobre la nueva infraestructura de comunicaciones de la Dirección General del Catastro, plenamente funcional y con una garantía de nivel de seguridad y calidad de servicio igual o superior a la proporcionada en su momento por la infraestructura de seguridad compartida de la Subsecretaría del Ministerio de Economía y Hacienda.
- Dotar a la Dirección General del Catastro con un sistema y modelo de gestión del entorno que, incluyendo los recursos humanos expertos permita operar y gestionar dicho entorno de forma coordinada y normalizada y según las necesidades de seguridad, evolución futura, crecimiento y rendimiento de los sistemas y servicios informáticos propios.
- La implantación del entorno y la puesta en marcha del sistema de gestión debería realizarse durante el año 2006.

Los objetivos anteriores, se enmarcan dentro del *objetivo estratégico* de la Dirección General del Catastro consistente en la apuesta decidida por el crecimiento y consolidación de los servicios, basados en Internet, prestados tanto a usuarios externos como internos, para los que se requiere un alto nivel de seguridad de la información.

Teniendo presentes los objetivos planteados, los *factores que determinaban el éxito* del proyecto a la finalización del mismo son:

- El entorno implantado debe permitir a la Dirección General del Catastro la *prestación de servicios* (actuales y futuros) basados en Internet con las suficientes garantías de seguridad, disponibilidad y rendimiento.
- El *nivel de seguridad perimetral,* proporcionado por el entorno implantado, debe ser equiparable (como mínimo) al existente antes de la implantación, en términos de número de incidentes, gravedad y erradicación de los mismos, activos afectados, etc.
- El proyecto debía posibilitar que, *para finales de 2006,* todos los sistemas de la Dirección General del Catastro, actualmente ubicados en la Subsecretaría del Ministerio de Economía y Hacienda, estuvieran instalados y operativos en la Dirección General del Catastro, adecuadamente integrados en el entorno de seguridad perimetral.

- La Dirección General del Catastro debe disponer de un *sistema de gestión de la seguridad perimetral* que esté perfectamente definido y operativo, que permita realizar los cambios y configuraciones requeridos según la política de seguridad adoptada, proporcione la información de estado y estadística necesaria para la toma de decisiones y también la detección y actuación rápida frente a posibles incidentes de seguridad.
- La Dirección General del Catastro debe contar con un *equipo de RRHH dedicados a la gestión* del entorno de seguridad perimetral que tengan habilidades y experiencia contrastada, además de un conocimiento profundo del entorno y de los sistemas de esta organización.
- Resulta necesaria la existencia de *documentación* amplia, extensa, actualizada y detallada sobre la configuración, funcionamiento, procesos y procedimientos de gestión, estado y datos estadísticos del entorno de seguridad perimetral.
- Implantación de una *cultura de seguridad* en el ámbito de los sistemas y redes de la Dirección General del Catastro y el personal que tiene responsabilidad sobre los mismos.

Diseño de la seguridad perimetral

El diseño de la infraestructura de seguridad perimetral de la Dirección General del Catastro se ha realizado siguiendo principios de diseño ampliamente utilizados y probados en el mercado. El concepto básico que subyace al diseño particular es de *"defensa en profundidad"*. Según este principio, cualquier componente o elemento de seguridad es insuficiente por sí sólo y el mejor grado de seguridad sólo podrá proporcionarse a través de una adecuada combinación de elementos dispuestos en capas superpuestas que proporcionen una protección global. Aún así, este principio asume que la seguridad absoluta no existe y que siempre existe un grado de vulnerabilidad que deberá ser asumido, de modo que la adaptación y mejora continua son aspectos clave. Por otro lado, la evolución vertiginosa de la tecnología y los productos implica que el grado de exposición a vulnerabilidades esté variando constantemente, a medida que se descubren nuevas formas para realizar un ataque o explotar una debilidad en los sistemas.

Según la filosofía de la "defensa en profundidad", el grado de seguridad óptimo se obtiene en base al uso combinado de distintos componentes y controles de seguridad (organizativos, legales y técnicos), tal como se muestra en la Figura 1.

Por otro lado, la adecuada selección de controles y tecnologías de seguridad es importante para determinar el coste global de la solución diseñada. Según la metodología propuesta en la norma ISO 270001 anteriormente propuesta, la selección de los controles debe obedecer a tres fuentes, tal como se muestra en la Figura 2.

Por un lado, los controles deben alinearse en todo momento con los principios, visión, misión y objetivos estratégicos de la organización. Por otro lado, la selección de controles debe obedecer a una cuestión de necesidad. A través de un análisis de riesgos de los sistemas de información es posible determinar qué amenazas y vulnerabilidades son más críticas y por tanto justificar la selección de un control que ayude a mitigarlas. Finalmente, todo organismo está sujeto a una serie de regulaciones y legislación general o específica en relación con la protección de la información y los datos personales. En general, este tipo de regulaciones incluye la obligatoriedad de implementar una serie de controles que podrán ser auditados por terceras partes independientes, como puede ser el caso de la Agencia de Protección de Datos.

Figura 1. Diseño de la seguridad perimetral: defensa en profundidad

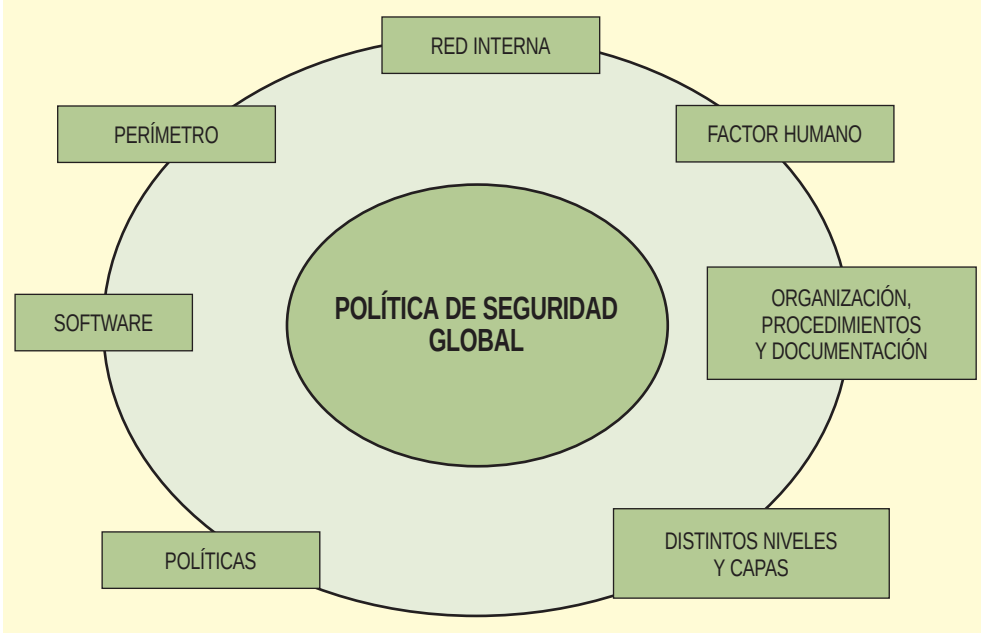
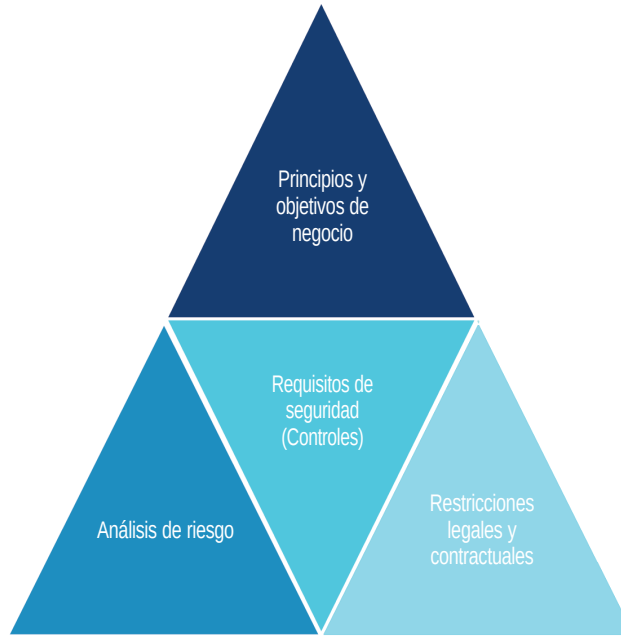


Figura 2. Selección de controles para seguridad de la información



Ejemplos de tipos de controles específicos para seguridad perimetral son: políticas, normas y procedimientos, la organización de la gestión, controles de tipo legal y medidas técnicas y tecnológicas. En el caso de la seguridad perimetral existen numerosos controles de tipo técnico que se apoyan sobre distintas tecnologías y productos de múltiples fabricantes, lo cual puede añadir cierta complejidad a la solución finalmente adoptada.

La organización internacional SANS (www.sans.org), que realiza estudios, análisis, formación y difusión en cuestiones de seguridad de la información clasifica los distintos controles técnicos de la seguridad perimetral en capas, siguiendo la arquitectura de "defensa en profundidad". En concreto, distingue entre los siguientes niveles o capas:

– *Nivel 1: Bloqueo de ataques en nivel de RED*

A pesar de que las amenazas internas suelen producir el mayor impacto, el tráfico externo produce más del 99.99% de los ataques registrados. La seguridad efectiva empieza por la tecnología que dificulte a los atacantes externos el acceso a la red interna.

– *Nivel 2: Bloqueo de ataques en el HOST*

Cuando un ataque supera las defensas de red, los distintos equipos (PCs, servidores, etc.) deberán estar preparados para detenerlo o minimizar el daño. También es importante para redes encriptadas y entornos de virtualización, donde el nivel de red no es visible.

– *Nivel 3: Eliminación de vulnerabilidades*

Todos los sistemas y aplicaciones son susceptibles de configuraciones incorrectas. El proceso de mitigación de vulnerabilidades debe ser continuo.

– *Nivel 4: Soporte seguro para usuarios autorizados*

La seguridad no puede ser tan restrictiva como para impedir a los usuarios autorizados realizar su trabajo. Debe conjugarse el bloqueo de usuarios no autorizados con el acceso con un adecuado nivel de servicio al usuario autorizado.

– *Nivel 5: Minimización de daños y maximización de eficiencia*

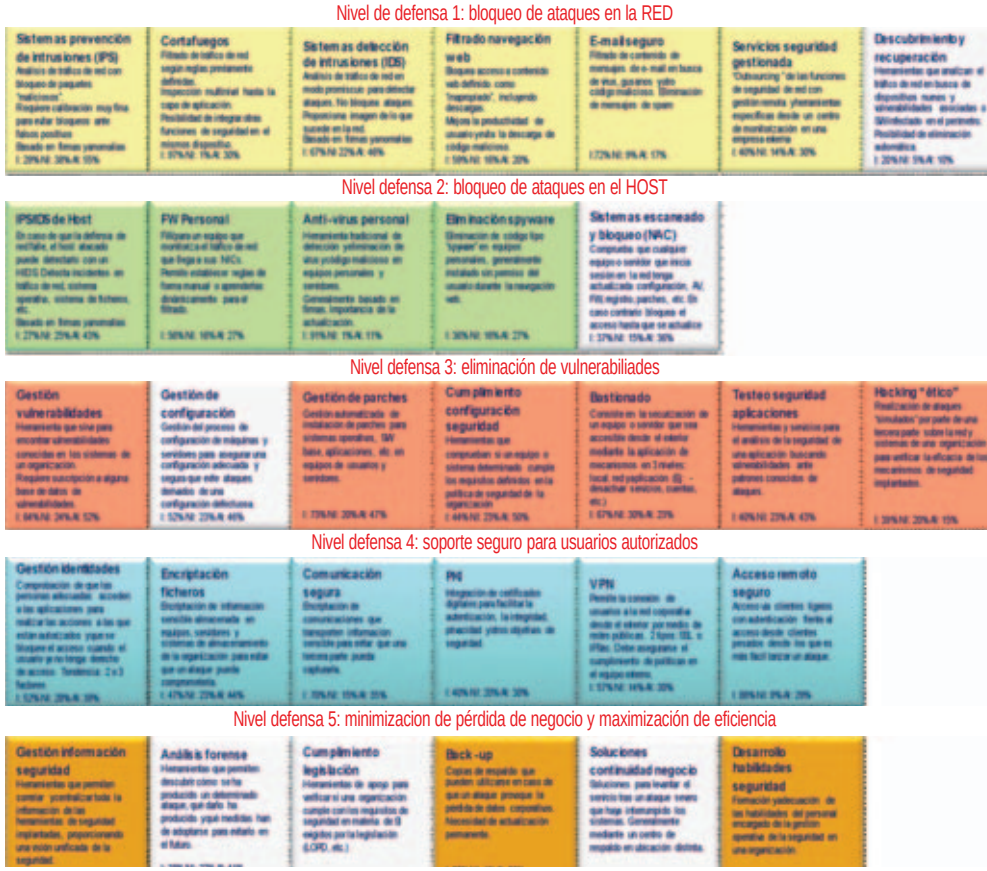
La seguridad es un proceso de mejora y aprendizaje continuos. Hay que prever la posibilidad de un ataque con éxito, minimizar el daño del mismo y realizar un aprendizaje para evitarlo en el futuro.

Sin entrar en un análisis exhaustivo de cada una de las tecnologías y tipos de productos existentes en cada uno de estos niveles, en la siguiente Figura 3 se muestran las más habituales, clasificadas por los distintos niveles identificados. Todas las que aparecen sombreadas, han sido seleccionadas (o ya existían previamente) para formar parte del diseño de seguridad perimetral de la Dirección General del Catastro.

Finalmente, en relación con el diseño de la seguridad perimetral, además de una adecuada selección de controles y la definición preliminar de la arquitectura técnica concreta que se vaya a utilizar hay que tener en cuenta múltiples consideraciones adicionales, entre las que podemos mencionar: la identificación de los activos de información a proteger, la arquitectura de separación de recursos y control de acceso, sistemas de monitorización, el rendimiento y capacidad requerido de la infraestructura, cuestiones de alta disponibilidad y redundancia, soluciones de continuidad de negocio, integración con las redes de área local y extensa subyacentes, integración con redes inalámbricas, usuarios remotos, existencia de Intranets y Extranets, etc.

Todos estos requisitos, junto con los controles finalmente elegidos, deberán conjugarse con el coste del proyecto. En definitiva, deberá alcanzarse un compromiso entre el coste de la arquitectura, el nivel de riesgo residual que se va a asumir y los requisitos de capacidad y alta disponibilidad exigidos por el negocio.

Figura 3. Tecnologías para el diseño de la seguridad perimetral



Implantación del entorno de seguridad perimetral

El proyecto de implantación del entorno de seguridad perimetral de la Dirección General del Catastro fue dividido en tres fases claramente diferenciadas, tal como se muestra a continuación, de forma esquemática:

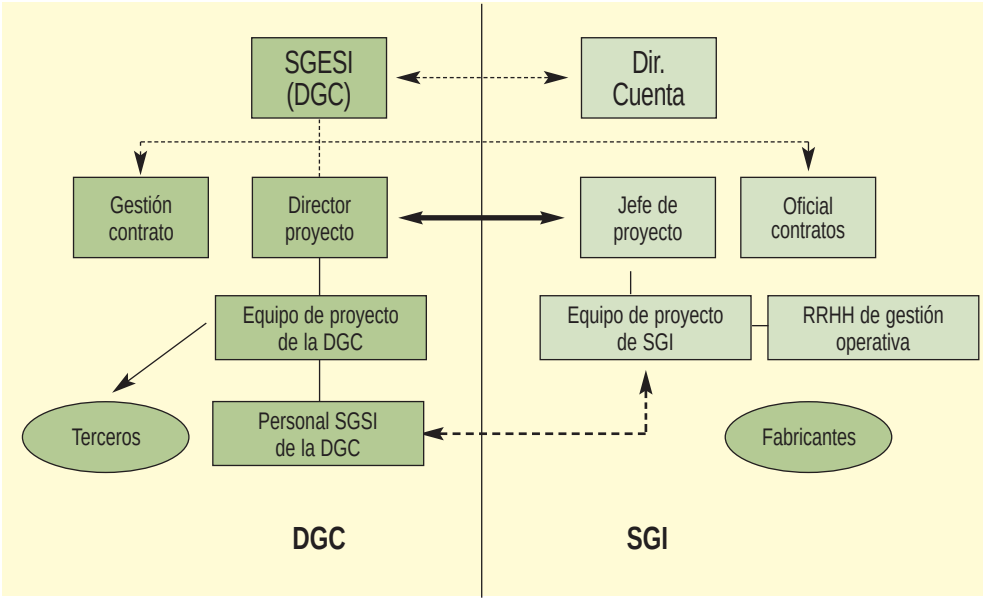
Especificación y contratación de sistemas y consultoría

- Definición de requisitos del servicio y análisis de riesgos en la infraestructura de red de la Dirección General del Catastro.
- Elaboración del Pliego de Prescripciones Técnicas y Cláusulas Administrativas del concurso público para el suministro de los productos y tecnologías así como la asistencia técnica y recursos humanos necesarios para la gestión operativa.
- Evaluación de las ofertas recibidas y seguimiento del concurso y la contratación.

Migración de servicios horizontales

- Diseño global de la arquitectura de seguridad perimetral.
- Implantación inicial del entorno de seguridad perimetral.

Figura 4. Estructura de organización del equipo de proyecto



- Migración de los servicios horizontales para utilizar las nuevas líneas de acceso a Internet (sin interrupción de servicio):
  - Acceso a Internet para usuarios internos
  - E-mail y servicios de mensajería
  - DNS para resolución de usuarios internos
  - Interconexión con la red de comunicaciones de área extensa (WAN)
  - Prestación de servicios web al exterior: página web del Catastro y Escritorio de Aplicaciones de Gestión Catastral (Citrix).
  - Establecimiento de los sistemas de acceso remoto: VPN y movilidad.

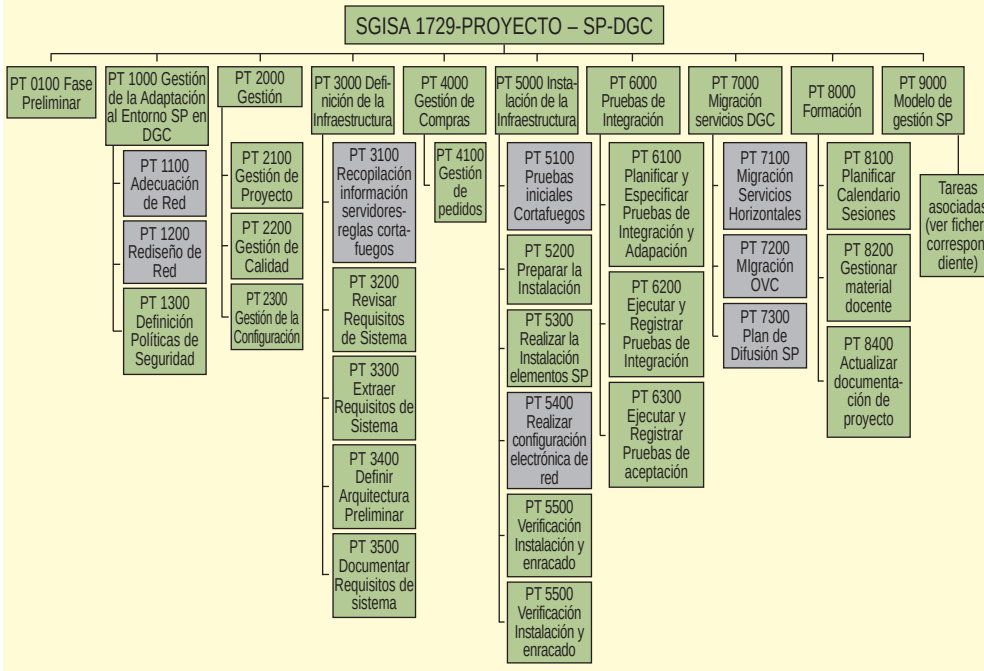
Integración de la oficina virtual del Catastro

- Incluye la preparación previa del entorno para "recibir" a la plataforma de sistemas de la Oficina Virtual del Catastro.
- No obstante la gestión operativa comenzará al final de la migración de servicios horizontales.

Por motivos no imputables al proyecto, no se ha podido llevar a cabo la tercera fase y por tanto, la infraestructura de sistemas de la Oficina Virtual del Catastro continúa en las dependencias de la Subsecretaría del Ministerio de Economía y Hacienda. La segunda fase del proyecto comenzó en abril de 2006 y finalizó a finales de junio de 2006. Desde el 1 de julio de 2006, dio comienzo el subproyecto de gestión operativa.

Uno de los factores claves en el desarrollo de la implantación fue la formación de un equipo mixto de trabajo, de alta integración y perfiles complementarios tanto por parte de la empresa adjudicataria del concurso (GMV-SGI), como por parte de la Dirección General del Catastro que involucró a los diferentes departamentos relacionados con la nueva infraestructura. En la Figura 4 se muestra la estructura adoptada.

Figura 5. Estructura de descomposición del trabajo



Este equipo de proyecto tuvo como objetivo prioritario realizar una migración transparente de los servicios para los usuarios de la organización. Dicha migración, realizada en distintas subfases, siguió al pie de la letra las directrices marcadas por la metodología y experiencia del equipo de proyecto y de las necesidades de la Dirección General del Catastro.

Tampoco hay que olvidar que de forma sincronizada con la implantación del nuevo entorno de seguridad perimetral, se realizó la implantación de procedimientos de gestión y seguridad para el mantenimiento y operación de la nueva infraestructura y la organización correspondiente de los recursos humanos.

El equipo conjunto se responsabilizó del diseño, implantación y gestión operativa de una arquitectura de seguridad perimetral completa para la Dirección General del Catastro. Esto ha supuesto el suministro, instalación y configuración de un exhaustivo conjunto de elementos de seguridad, incluyendo cortafuegos, sondas de detección de intrusión (de red y de servidor), gestores de ancho de banda, gestores de vulnerabilidades, solución antivirus de navegación web y correo electrónico, solución de control de destinos web, solución securizada de DNS, solución de acceso remoto seguro, herramienta de gestión de información de seguridad y equipos, consolas y software de gestión de los distintos elementos de seguridad. Adicionalmente se realizó un profundo rediseño de la electrónica de nivel 2 de la red interna así como la integración y migración de las nuevas infraestructuras de comunicaciones del Ministerio. El alcance detallado se resume en los puntos siguientes y en la estructura de descomposición del trabajo de la Figura 5:

- Diseño, construcción e implantación de una *arquitectura de seguridad perimetral* completa para la red de comu-

nicaciones de la Dirección General del Catastro.
- Suministro, instalación y configuración de los *elementos de seguridad* que conforman el entorno de seguridad perimetral según la arquitectura definida, la política de seguridad y el pliego de prescripciones técnicas del concurso.
- Suministro, instalación y configuración de los *servidores adicionales* para servicios de correo electrónico y DNS debidamente securizados y configurados.
- Suministro, instalación y configuración de los *elementos físicos adicionales* para construir la infraestructura.
- Implantación de una *plataforma de gestión operativa* y especificación, documentación y puesta en marcha de un *modelo de gestión* de la seguridad perimetral y de sistemas.
- Elaboración de toda la *documentación* asociada al proyecto.
- *Provisión de los recursos humanos* necesarios para la gestión operativa del entorno.
- *Formación y traspaso de conocimiento* del entorno al personal especializado y la Subdirección General de Estudios y Sistemas de Información.
- *Integración de la red de comunicaciones* y los sistemas de la Dirección General del Catastro en el entorno de seguridad perimetral. *Migración desde la situación previa.*

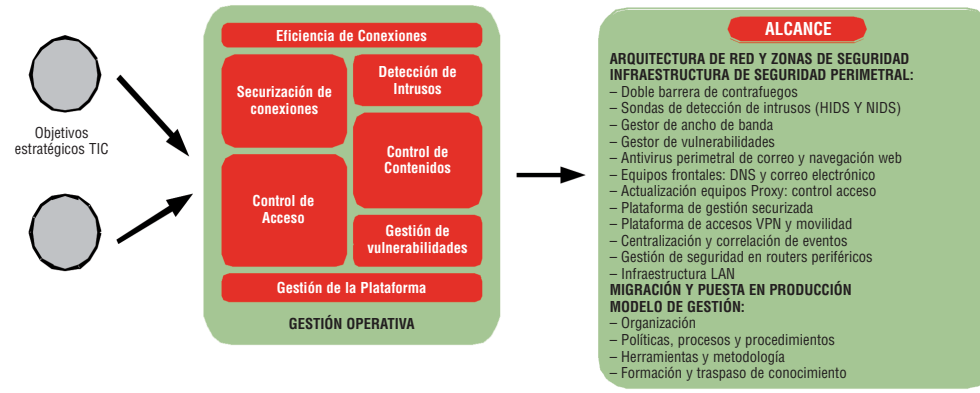
El equipo de proyecto planteó una arquitectura de seguridad que perseguía la consecución de los siguientes objetivos:

- Seguridad de la infraestructura implantada.
- Infraestructura tolerante a fallos.
- Escalabilidad en servicios, rendimiento y funcionalidades.
- Eficiencia.

Estos objetivos de alto nivel se tradujeron en la utilización de determinadas técnicas de diseño. La primera de ellas es el empleo de una arquitectura multi-zona de seguridad que permitiera asumir sólo los riesgos imprescindibles para cada una de las funcionalidades, teniendo también en cuenta aspectos de seguridad interna. Se tuvo en cuenta también el concepto de alta disponibilidad a dos niveles, tanto mediante la utilización de técnicas de *clustering* que permitieran recuperarse ante situaciones de fallo a los elementos que proporcionan los servicios, como a nivel de conmutación de los elementos de electrónica de red. También se hizo uso del reparto de carga garantizando la capacidad de asumir mayores cargas de servicio (escalado) y la redundancia ante fallos. Finalmente, se creó una red dedicada de gestión para todos los elementos de la infraestructura. Esta red aumenta el grado de seguridad ya que al estar aislada de la red de servicio, impide que un atacante potencial pueda acceder de forma sencilla a las consolas de gestión y modificar la política de seguridad. Estas características se resumen en la Figura 6.

Además, se prestó especial interés a la hora de diseñar una infraestructura que fuera fácilmente administrable y gestionable. Dos razones conducen a este punto: la primera de ellas es un razonamiento en torno al concepto de eficiencia. Un sistema difícil de administrar normalmente proporciona una menor prestación de servicio, pues parte del esfuerzo debe concentrase en el propio sistema en vez del objetivo para el cual ha sido implantado. La segunda razón hace referencia a un axioma básico de seguridad: reducción de complejidad. Una plataforma de administración y gestión bien diseñada debe ser capaz de aislar la complejidad intrínseca de la infraestructura y proporcionar la información justa y necesaria, aumentando la eficiencia del sistema y mejorando la seguridad del mismo.

Figura 6. Esquema de diseño específico de la arquitectura de seguridad perimetral de la Dirección General del Catastro



En la Figura 7 se muestra un diagrama esquemático simplificado de la arquitectura actual de seguridad perimetral de la Dirección General del Catastro:

Figura 7. Esquema simplificado de la arquitectura de seguridad perimetral actual de la Dirección General del Catastro

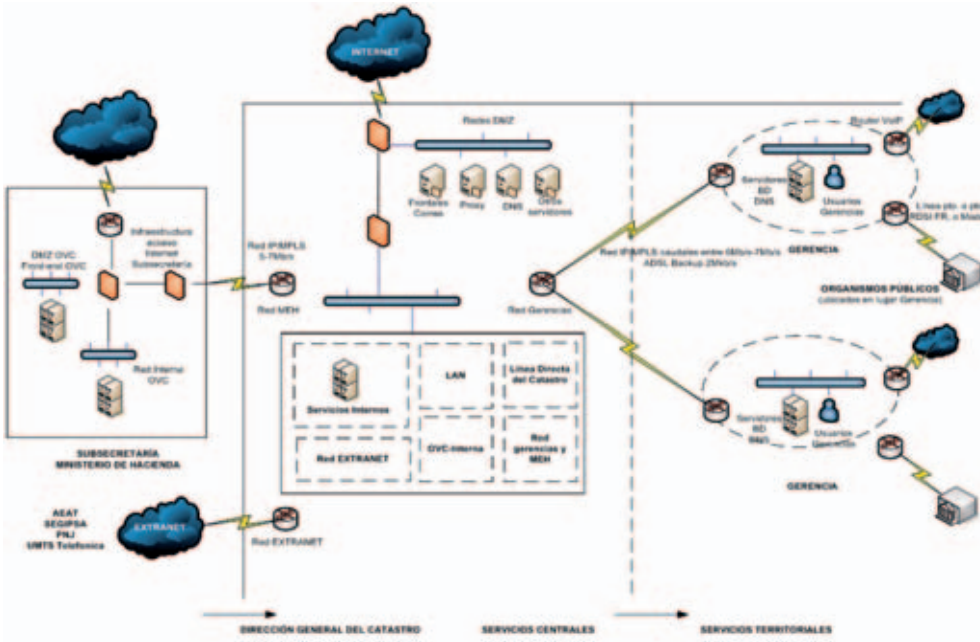
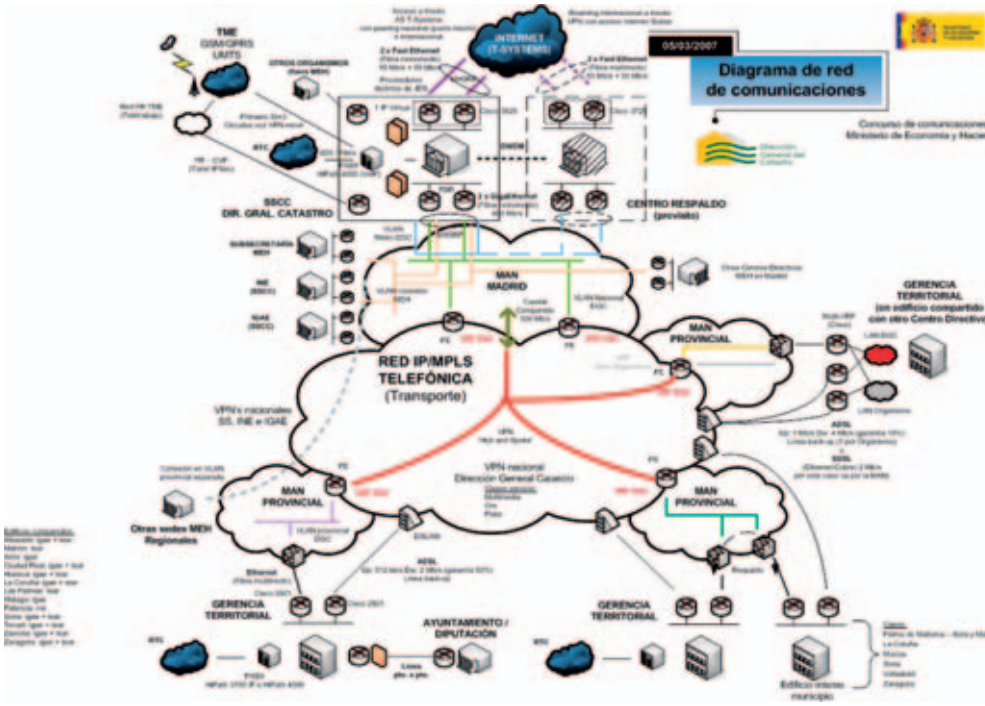


Figura 8
Integración de la seguridad perimetral y la red de comunicaciones de la Dirección General del Catastro



Con la infraestructura de seguridad perimetral implantada, el esquema de la arquitectura de comunicaciones de la Dirección General del Catastro a mediados de 2006 quedó como se muestra en la Figura 8.

Gestión operativa

Más importante que la propia implantación del entorno de seguridad perimetral ha sido el diseño y puesta en producción del modelo de gestión operativa del servicio, de forma que se garantice que el grado de seguridad proporcionado se alinee en todo momento con los objetivos estratégicos de la Dirección General del Catastro.

En este sentido, durante la implantación del proyecto, se trabajó en la definición de un modelo de gestión orientado a servicio, basados en procesos, procedimientos, indicadores clave de rendimiento y que integrara todo el ciclo de vida completo de gestión de una infraestructura de seguridad compleja como la implantada en la Dirección General del Catastro. Como elemento de referencia se ha tomado el conjunto de buenas prácticas en gestión de servicios de tecnologías de la información: ITIL (Information Technology Infrastructure Library). Utilizando varias de sus orientaciones, se ha confeccionado un modelo propio ajustado a las necesidades y recursos de la Subdirección General de Estudios y Sistemas de Información.

Adicionalmente a lo anterior, la gestión operativa de la seguridad perimetral en la Dirección General del Catastro implica de forma directa a un equipo (mixto de funcionarios y personal externo) de cuatro personas que cubre un horario presencial de lunes a viernes de 8h a 20h. Asimismo, se ha incluido un servicio de soporte remoto en 24x7 para los intervalos de tiempo fuera de este horario. Este servicio cuenta con un equipo de soporte remoto que interviene en caso de que algún elemento crítico de la infraestructura esté indisponible.

El modelo de gestión definido se ha planteado con los siguientes objetivos:

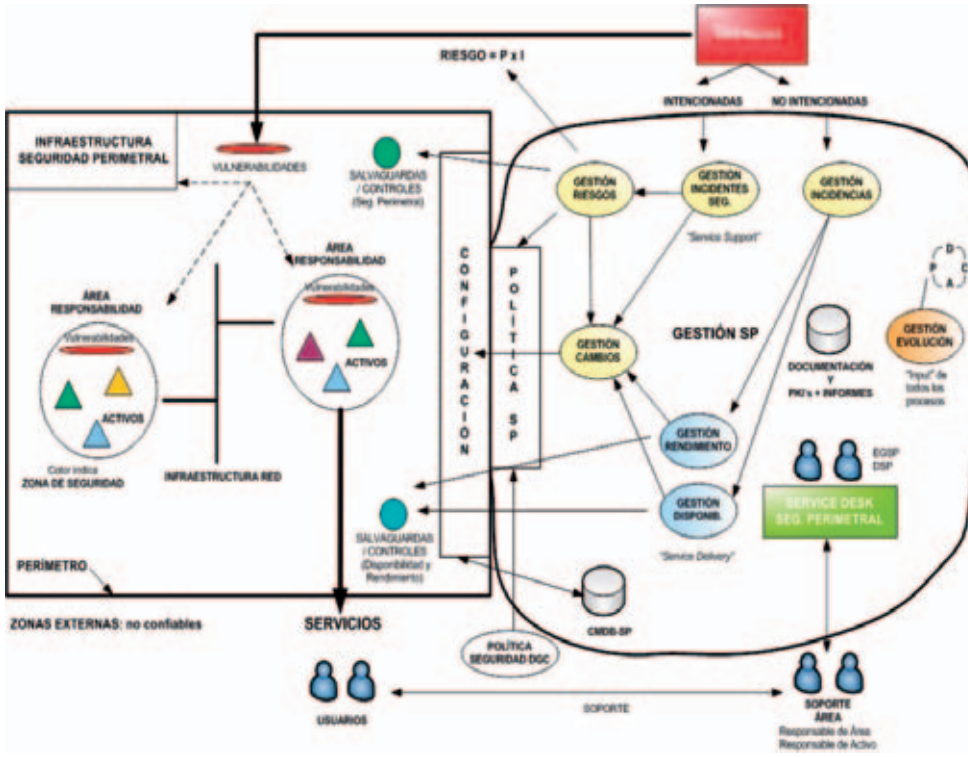
- Garantizar la *seguridad* de los activos protegidos por la infraestructura de seguridad perimetral frente a amenazas externas al perímetro, bien mediante la prevención y gestión de los riesgos o mediante la respuesta rápida ante incidentes y eventos de seguridad.
- Permitir la realización de *cambios* y modificaciones sobre la configuración de la infraestructura de seguridad con objeto de adaptarla de forma continua a las necesidades de los servicios y de la política de seguridad de la organización, además de garantizar la escalabilidad y crecimiento en servicios y funcionalidades.
- Garantizar la *disponibilidad y rendimiento* de la infraestructura de seguridad perimetral y de los servicios que sobre ella se presten, contribuyendo a su adecuada calidad de los servicios de Administración electrónica.
- Dotar a la Subdirección General de Estudios y Sistemas de Información de una *visión actualizada y detallada del funcionamiento* de la infraestructura de seguridad perimetral y de su gestión.

Para la elaboración del modelo de gestión se identificaron los distintos subservicios que se prestan en relación con la seguridad perimetral:

- Servicio de seguridad perimetral y de red.
- Servicio DNS (resolución de nombres) externo.
- Servicio de pasarela de correo electrónico.
- Servicio de acceso a Internet y navegación web.
- Servicio NTP de sincronización de tiempos.
- Servicio de acceso remoto VPN y autenticación RADIUS para usuarios con dispositivos móviles.
- Servicios de gestión del ancho de banda y prioridad de tráfico.
- Servicio de gestión de vulnerabilidades de servidores.

En base a esta clasificación se construyó un modelo de procesos de gestión orientados a la gestión proactiva de la seguridad, tal como se muestra en la Figura 9. Concretamente, se han definido procesos para la gestión de cambios, incidencias, incidentes de seguridad, riesgos, rendimiento y disponibilidad. Adicionalmente, se ha introducido un proceso de mejora continua de la calidad del servicio a través de la conocida rueda de Deming. Por otro lado, se ha elaborado un marco de relaciones entre los distintos componentes físicos y lógicos del modelo así como un "service-desk" de atención a los usuarios. En este sentido, se tomo la decisión de aprovisionar un servicio de nivel 2, sin atención directa a usuario final y los "clientes" del mismo son el resto de personal de operación y soporte de la Subdirección General de Estudios y Sistemas de Información. Finalmente, también se ha generado un repositorio de configuración de los sistemas de la infraestructura, denominado CMDB-SP y que sigue la filosofía y terminología de ITIL.

Figura 9
Modelo de gestión adoptado en la gestión operativa de la seguridad perimetral en la Dirección General del Catastro



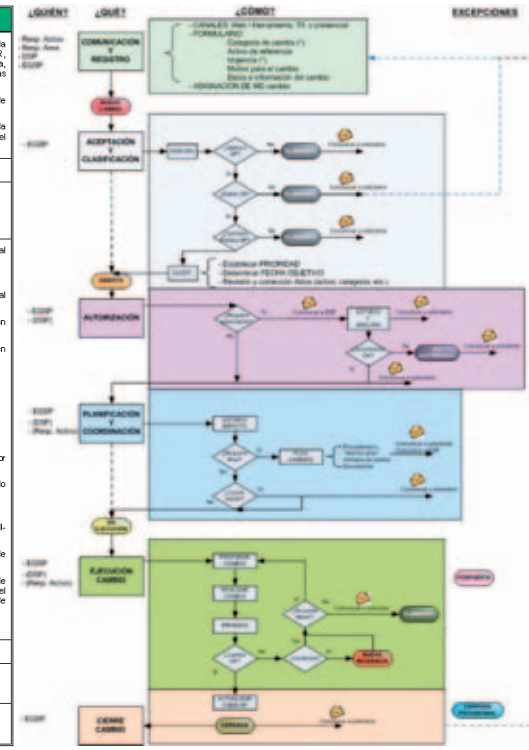
En la figura 10 se muestra un ejemplo de diseño de uno de los procesos y el procedimiento asociado. Para todo el modelo de gestión se ha creado un repositorio de documentación, de forma que todos los procesos y procedimientos están documentados.

Adicionalmente a lo anterior, se ha incorporado una herramienta específica para la gestión operativa que integra la relación con los usuarios del servicio, el registro y seguimiento de peticiones de servicio e incidencias y la generación de informes y un cuadro de mando con los indicadores clave del servicio. De esta forma el personal directivo de la Dirección General del Catastro puede comprobar el adecuado funcionamiento del servicio. Con este fin, se ha definido un sencillo acuerdo de nivel de servicio con los compromisos de respuesta y objetivos para el Área de seguridad perimetral.

Finalmente, también debemos mencionar la importancia de la política de seguridad en el modelo de gestión. La política de seguridad perimetral es el conjunto de objetivos, normas, reglas y restricciones de seguridad en base a las cuales se configura cada elemento de la infraestructura con objeto de proteger de forma adecuada los distintos activos y datos e información contenida en los mismos, así como implantar y controlar la aplicación de la política de seguridad general de la Dirección General del Catastro.

Figura 10
Ejemplo de proceso y procedimiento de gestión operativa

PROCESO:	GESTIÓN DE CAMBIOS
OBJETIVOS:	1. Establecer un procedimiento formal para la solicitud de cambios en la configuración de la infraestructura de seguridad perimetral por parte de las AR, el EGSP y de la DSP que permita realizarlos de forma eficiente y controlada, evitando posibles errores o vulnerabilidades que afecten a los sistemas (derivados del cambio) y reduciendo el impacto de dichos cambios. 2. Realización de los cambios necesarios y requeridos como consecuencia de alguno de los demás procesos de gestión de la seguridad perimetral. 3. Fomentar la planificación adecuada de los cambios requeridos sobre la seguridad perimetral y asignar de forma eficiente los recursos disponibles del EGSP a la gestión de los mismos.
ENTRADAS:	Petición de cambio / servicio
SALIDAS:	Registro de cambio Modificación de configuración de sistema Actualización de CMDB-SP (si es necesario)
ACTIVIDADES Y REQUISITOS:	Se requiere la definición y documentación del procedimiento que soporte al proceso. El procedimiento debe considerar lo siguiente: • Definición de los mecanismos y canales para la solicitud de cambios. • Normalización de formatos de solicitud de cambios por parte de las AR al EGSP. • Automatización y soporte de las actividades del procedimiento con herramienta técnica. • Deberá realizarse una categorización de cambios indicando cuáles requieren aprobación de la DSP • Idealmente, todo cambio solicitado al EGSP deberá: o Quedar registrado o Ser aceptado o Ser clasificado: según nivel de prioridad y nivel de impacto o Estudiado y evaluado su impacto y consecuencias o Planificado (estimación) y aprobado (si es requerida aprobación por parte del DSP). Comunicado con antelación a las partes afectadas. o Evaluado a posteriori para garantizar su efectividad (incluyendo pruebas) o Concluir en una actualización de los repositorios de configuración o En la medida de lo posible incluir un mecanismo planificado de "roll-back" o marcha atrás. • Se requiere que el procedimiento sea conocido por las distintas Áreas de Responsabilidad y personal de explotación de sistemas de la DOC. • Se requiere que el procedimiento sea ágil y elimine en la medida de lo posible la "burocracia" asociada (si el cambio es menor podrá suprimirse el procedimiento), permitiendo el establecimiento de vías directas de comunicación entre las AR y el EGSP. • Se requiere que el procedimiento sea aprobado y apoyado por la SGESI.
PROCEDIMIENTO:	SP-PROC-003 – Procedimiento de gestión de cambios
PROCESOS RELACIONADOS:	Proceso de gestión de incidencias (de entrada y de salida) Proceso de gestión de incidentes de seguridad (de entrada)
CONTROL DEL PROCESO:	A través de las métricas siguientes: • Tiempo de ejecución de cambio



Resultados

El éxito del proyecto se ha centrado en la plena satisfacción de varios objetivos. En primer lugar, el entorno implantado permite a la Dirección General del Catastro la prestación de servicios (actuales y futuros) basados en Internet con las suficientes garantías de seguridad, disponibilidad y rendimiento.

Por otro lado, el nivel de seguridad perimetral que proporciona el nuevo entorno es adecuado a la necesidad, utilizando nuevas tecnologías y mejorando la seguridad interna, en términos de número de incidentes, gravedad y erradicación de los mismos, activos afectados, etc. Otro objetivo fundamental es la consolidación de los servicios prestados por la Dirección General del Catastro, posibilitando que próximamente todos los sistemas actualmente ubicados en otros organismos del Ministerio, estén instalados y operativos en las instalaciones de la organización, adecuadamente integrados en el entorno de seguridad perimetral (como por ejemplo, la Oficina Virtual del Catastro).

Tras la ejecución del proyecto de implantación, la Dirección General del Catastro dispone ya de un sistema de gestión de la seguridad perimetral que está perfectamente definido y operativo, que permite realizar los cambios y configuraciones requeridos según la política de seguridad adoptada, proporcionando la información de estado y estadística necesaria para la toma de decisiones y también la detección y actuación rápida frente a posibles incidentes de seguridad. Este hecho ha

permitido la mejora en la implantación de una cultura de seguridad en el ámbito de los sistemas y redes de la Subdirección General de Estudios y Sistemas de Información y el personal que tiene responsabilidad sobre los mismos.

Por otro lado, respecto al desarrollo de la ejecución del proyecto hay que destacar el escaso impacto para los usuarios durante el proceso de migración, gracias a su planificación en fases y a la meticulosidad en las medidas de seguridad que afectan a los usuarios. En este aspecto también ha sido importante el cumplimiento estricto de plazos, adecuándose a los períodos críticos para los distintos servicios. De hecho, se produjo la migración de todos los servicios horizontales con un mes de adelanto sobre la previsión inicial del proyecto.

Tras la puesta en producción, se ha apreciado un considerable aumento del caudal de comunicaciones para usuarios y aplicaciones así como una respuesta rápida en la resolución de incidencias, debido al proceso de centralización llevado a cabo en los Servicios Centrales. Asimismo se ha constatado un notable incremento de la confianza de los usuarios y los departamentos involucrados en la Dirección General del Catastro en los servicios relacionados con Internet, gracias a un planificado proceso de comunicación y explicación de procedimientos y procesos.

Respecto de los resultados de la gestión operativa del entorno, se puede resumir en las siguientes cifras e indicadores clave de rendimiento, desde el 1 de julio de 2006:

Se han realizado 650 peticiones de servicio sobre la infraestructura.

- Se han realizado 357 peticiones de cambio sobre la infraestructura.
- Se han gestionado 110 incidencias (de las cuales 94% tenían prioridad baja).
- No se ha materializado ningún incidente de seguridad perimetral a pesar de haber detectado varios intentos.

En relación con el cumplimiento de los acuerdos de nivel de servicio establecidos, desde el 1 de julio de 2006:

- Las peticiones de servicio con prioridad *crítica* se han resuelto, en promedio, en 0.7 horas (el objetivo es inferior a 1 hora).
- Las peticiones de servicio con prioridad *alta* se han resuelto, en promedio, en 7.2 horas (el objetivo es inferior a 8 horas).
- Las peticiones de servicio con prioridad *media* se han resuelto, en promedio, en 21 horas (el objetivo es inferior a 2 días).
- Las peticiones de servicio con prioridad *bajan* se han resuelto, en promedio, en 108 horas (el objetivo es inferior a 1 semana laboral).
- El tiempo medio de repuesta a peticiones de servicio es de 5 minutos.
- La disponibilidad promedio global de la infraestructura (excluyendo paradas planificadas de la red o del CPD) ha sido del 99.99%.

Conclusión

Varias han sido las conclusiones derivadas de la puesta en marcha y ejecución de un proyecto de esta índole. Una de ellas es la necesidad del establecimiento de adecuadas medidas de planificación en todas las fases del proyecto, resultando clave establecer efectivos canales de comunicación con todos los actores involucrados. Es evidente que estos proyectos requieren dar la importancia necesaria, no sólo a los aspectos tecnológicos, sino también los aspectos organizativos y específicamente al cumplimiento en todo momento de los requisitos del negocio.

Asimismo, la planificación de las fases del proyecto, el tiempo dedicado al análisis y diseño previo así como la definición del modelo de gestión con antelación a la puesta en servicio de la infraestructura han sido

elementos clave para la garantía del éxito. También debe mencionarse la orientación de servicio que se ha dado a la infraestructura así como el establecimiento de la cultura de la seguridad durante toda la implantación del proyecto.

Finalmente cabe destacar el alineamiento de la empresa adjudicataria del concurso con los objetivos de servicio público de la Dirección General del Catastro, desarrollándose durante el proyecto una situación de mutuo enriquecimiento provocado por la aportación de la experiencia técnica en materia de seguridad de la información de la empresa y el conocimiento del funcionamiento de las administraciones publicas y de los servicios por parte del personal de la Dirección General del Catastro.

Teniendo en cuenta la importancia que la Dirección General del Catastro dedica a la seguridad de la información y a la protección de datos de carácter personal como elementos clave de gestión pública, el actual entorno de seguridad perimetral cumple plenamente con los objetivos establecidos proporcionado un adecuado nivel de seguridad en la protección de los activos de información y servicios electrónicos de la Dirección General del Catastro y del Ministerio de Economía y Hacienda. ■