

eu 2010.es

tecniMAP 2010 Zaragoza
del 6 al 9 de abril

TITULO:

INTERCONEXIÓN DE REGISTROS A TRAVÉS DE CORREO ELECTRÓNICO SEGURO EN EL MINISTERIO DE DEFENSA

Coronel D. Fernando Armero Acebrón
Centro Corporativo de Obtención y Mantenimiento de Sistemas de Información (CCOMSI)
Subdirección General de Sistemas de Información y Telecomunicaciones (SDGSTT)
DIRECCION GENERAL DE INFRAESTRUCTURA (DIGENIN)
SECRETARIA DE ESTADO (SEDEF)
MINISTERIO DE DEFENSA (MINISDEF)

INTERCONEXIÓN DE REGISTROS A TRAVÉS DE CORREO ELECTRÓNICO SEGURO EN EL MINISTERIO DE DEFENSA

1. ANTECEDENTES.

Orden Ministerial 315/2002, de 14 de febrero, por el que se aprueba el Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de Defensa, donde se define la política CIS del Ministerio de Defensa.

Por medio del Real Decreto 1551/2004 de 25 de Junio por el que se desarrolla la estructura Orgánica del Ministerio de Defensa, se incluye dentro de la Secretaría de Estado, como nuevo organismo, la Inspección General del PDCIS (en adelante inspección General CIS ó IGEICIS).

El PDCIS, dentro del Plan de Obtención y Modernización de los Sistemas de Información (P3), se establecen los sistemas de información que necesita el departamento ministerial y una evolución desde la situación actual hasta la prevista.

El Sistema de Mensajería Oficial y Gestión Documental (P3.A7.S1) queda enmarcado en el Plan de Obtención y Modernización de los Sistemas de Información dentro del Área de Apoyo a la Organización.

Por Real Decreto 1126/2008 de 4 de julio por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, pasa a depender su obtención y mantenimiento de la Subdirección General de Servicios Técnicos y Telecomunicaciones (Dirección General de Infraestructura, Secretaría de Estado).

INTERCONEXIÓN DE REGISTROS A TRAVÉS DE CORREO ELECTRÓNICO SEGURO EN EL MINISTERIO DE DEFENSA

2. OBJETO DEL SISTEMA.

El Ministerio de Defensa dispone actualmente de un procedimiento para la interconexión de registros a través de correo electrónico seguro en el Ministerio de Defensa. Dicho procedimiento, en líneas generales, está basado en dos tipos de documento ("Oficio y Mensaje"), que contienen la información necesaria para hacer llegar el documento al destinatario e identificar al emisor de dicho documento. Todo ello sobre la base de una estructura de puntos de registro generales y auxiliares asociados a los organismos que registran la entrada y salida, y la encaminan hacia sus destinatarios finales, quienes archivan y custodian dicha correspondencia, cerrando así el ciclo de la tramitación.

Por un lado, surge la necesidad de reducir la demora de días o semanas en la distribución de comunicaciones oficiales entre sus departamentos a través de sus procedimientos habituales de registro y envío en valijas.

Por otro, los ciudadanos están cada vez más familiarizados con el correo electrónico personal como medio eficaz e inmediato para la comunicación. Sin embargo, este medio por sí mismo no es válido para la circulación de correspondencia oficial con carácter formal.

Ahora bien, para dotar de oficialidad, la normativa actual exige el cumplimiento de determinados requisitos. Entre estos requisitos cabe destacar la Firma Electrónica Avanzada del remitente, las garantías de integridad y no-repudio, el registro de entradas y salidas con sellado de tiempo y las políticas de conservación de esta correspondencia.

En definitiva deben implementarse todos aquellos mecanismos que permitan la consideración de los documentos en soporte electrónico como válidos a efectos legales.

El Ministerio de Defensa asumió este reto como una de las prioridades de su Plan Director de Sistemas de Información y Comunicaciones, llevando a cabo la construcción del Sistema de Mensajería Oficial y Gestión Documental (SIMENDEF).

SIMENDEF se constituye como el único sistema para todo el Ministerio de Defensa que da soporte a los procedimientos actuales de tramitación de oficios y mensajes no clasificados de índole administrativa, articulando la comunicación entre sus Ámbitos Organizativos (registros).

3. SITUACIÓN ACTUAL

El sistema se encuentra construido e implantado en diferentes organismos, tanto del Órgano Central (SEDEF, DIGENIN, SMC, EMAD) como de los Ejércitos y Armada.

El resultado actual de implantación es:

	Total	O.C.	EMAD	Armada	Aire
Nº de Ámbitos Registrales	67	10	12	15	30
Nº de Autoridades	750	89	62	155	444
Nº de Usuarios	6.976	1.358	591	1.495	3.532
Nº Documentos Registrados	615.742	336.654	8.002	122.506	148.580
Nº Firmados	51.876	26.818	2.565	11.479	11.014
Nº Doc. Registrados Entrada	485.492	281.690	5.222	104.513	94.067
Nº Doc. Registrados Salida	130.250	54.964	2.780	17.993	54.513

Ilustración 1: Datos de implantación de SIMENDEF en el MINSDEF

4. DESCRIPCIÓN FUNCIONAL.

El Sistema proporciona un servicio de tramitación electrónica de correspondencia oficial no clasificada entre todos los ámbitos organizativos del Ministerio de Defensa que se encuentren conectados a su WAN de Propósito General¹.

El alcance funcional del Sistema abarca todo el ciclo del trámite oficial. Dicho trámite nace con la generación del documento dentro de un ámbito organizativo y continúa con la canalización del mismo a través del conducto reglamentario hasta que es firmado por la autoridad del ámbito y registrado de salida en su oficina de registro. Seguidamente se realiza el envío al ámbito organizativo de destino donde se registrará de entrada y se canalizará por el conducto reglamentario de dicho ámbito hasta que llegue al negociado encargado de tomar acción, archivo, custodia etc. El sistema proporciona siempre un acuse de recibo cuando entra la comunicación en el ámbito organizativo de destino.

¹ El Ministerio de Defensa dispone de dos redes de área extensa (WAN), físicamente aisladas, que dan soporte a todos los sistemas de información del Ministerio. Por una parte, una WAN para Mando y Control Militar (WAN-C2), y por otra parte, la WAN Corporativa de Propósito General (WAN-PG), que se extiende a la gran mayoría de los emplazamientos del Departamento.

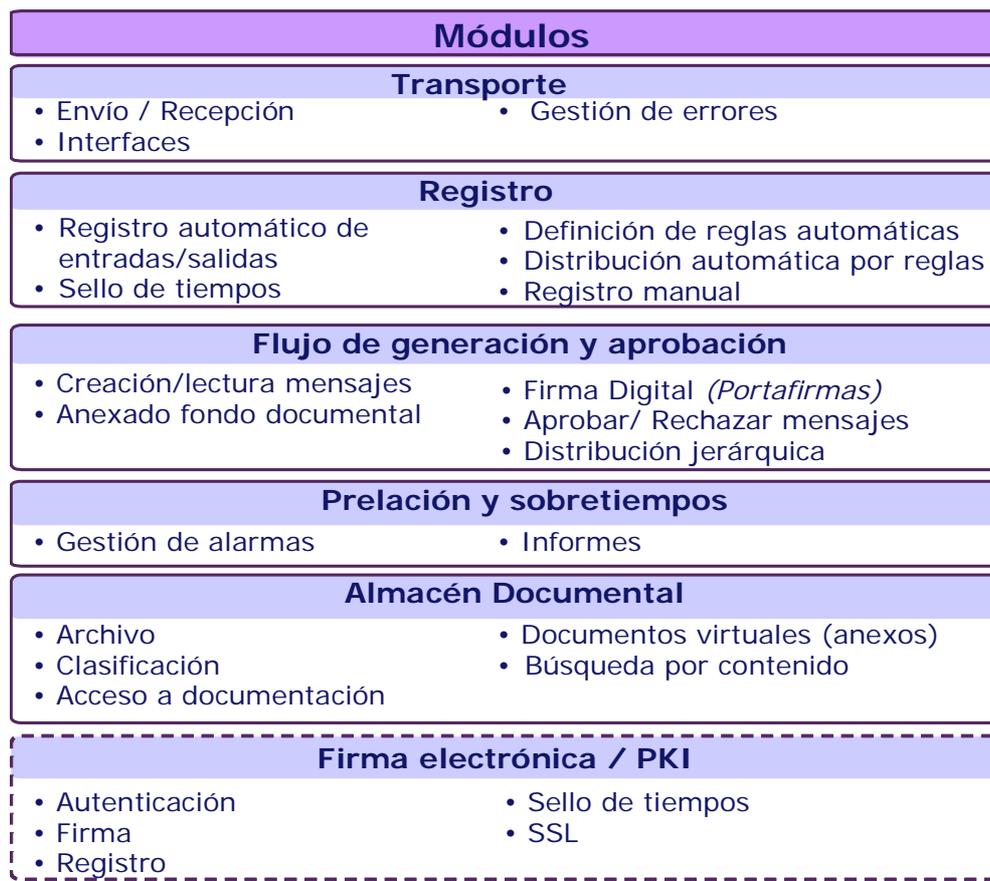


Ilustración 2: Composición funcional del sistema

El sistema ofrece una solución de alcance corporativo a las necesidades de Transporte, Registro, Circulación por Conducto Reglamentario y Gestión Documental de la información, y en base a estas necesidades se estructuran sus módulos y unidades funcionales.

4.1 Ciclo de comunicaciones oficiales

Todo miembro del Ministerio de Defensa es un usuario potencial de SIMENDEF, ya que puede generar un oficio, que deberá firmar su autoridad, o puede recibir en su bandeja de entrada un oficio.

El sistema da soporte al proceso de generación, circulación, aprobación y firma del oficio de una forma ágil, rápida y auditable: el proceso básico comienza cuando un usuario genera un oficio en la herramienta y lo envía a su nivel jerárquico superior para su validación. El validador lo recibe y puede modificarlo, devolverlo o enviarlo a su vez a otro nivel jerárquico que repetirá el proceso. Dependiendo del ámbito organizativo la cadena de validación será más o menos larga y estas acciones pueden ejercerse hasta el mismo momento de la firma. Finalmente el oficio llega al órgano auxiliar del mando quien lo subirá al portafirmas digital de la autoridad. La autoridad firmará el oficio que se registrará automáticamente de salida y se enviará a su destino o destinos.

En el ámbito organizativo de **destino** se registrará automáticamente de entrada y caerá de forma automática en la bandeja de algún miembro del ámbito organizativo. Desde ahí podrá distribuirse hacia otras unidades de la organización hasta que se requiera.

La distribución de oficios y mensajes entrantes, además, dispone un sistema de reglas que permite automatizar la entrega a los destinatarios finales.

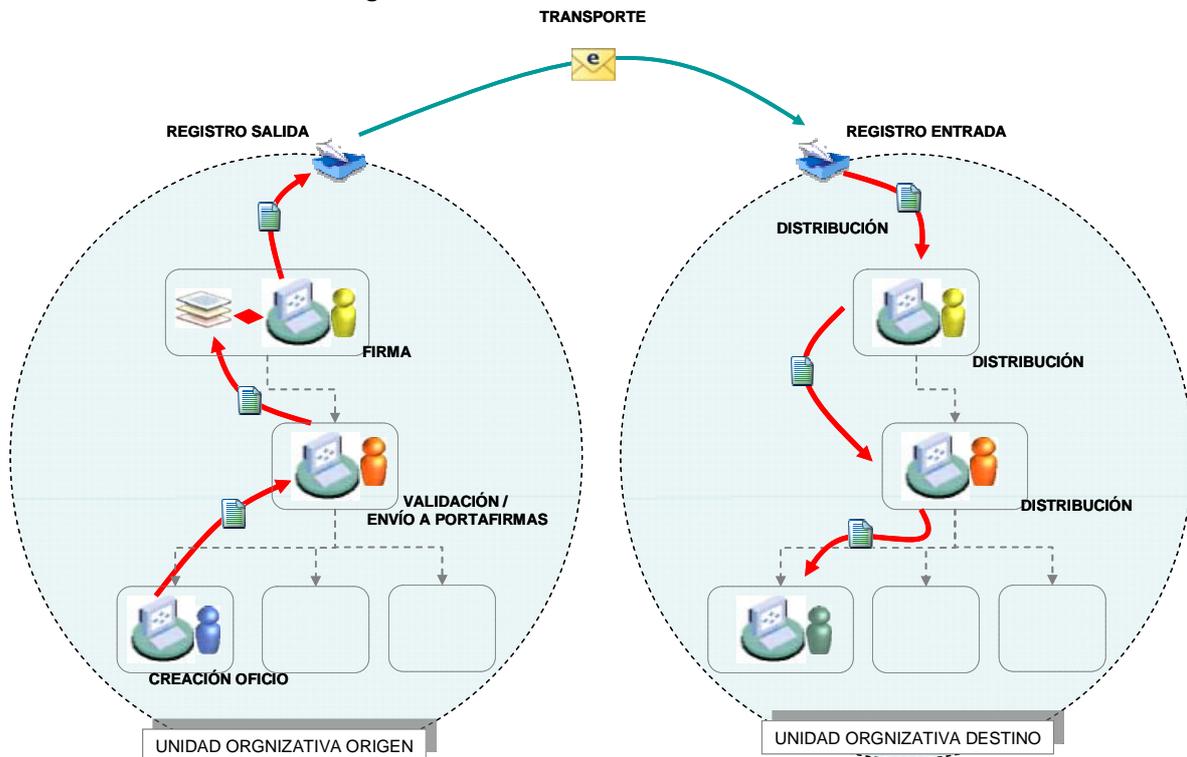


Ilustración 3: Ciclo de comunicaciones oficiales

El sistema gestiona automáticamente la trazabilidad del oficio y mensaje, quedando registrada la vida del mensaje, no sólo en cuanto a los sellos oficiales de entrada y salida, sino también en cuanto a los movimientos y accesos dentro del propio ámbito.

El sistema dispone también, en su módulo funcional de registro, de las capacidades de registro manual. De esta forma, este sistema atiende a todas las necesidades de registro (electrónico y manual) de todo el Ministerio.

4.2 El oficio y la firma electrónica

A través de SIMENDEF se envían oficios y mensajes electrónicos con la estructura e identidad del tipo "Oficio" y "Mensaje", normalizado en la Administración General del Estado.

Este oficio recibe la firma electrónica de la Autoridad remitente y los sellos electrónicos de salida y entrada. Adicionalmente, puede disponer de documentos adjuntos los cuales a su vez pueden estar firmados electrónicamente.

Cada sello de entrada y salida incorpora un "sellado de tiempos" que garantiza la fecha y hora en la que se produjo el registro del documento (ROA y dentro de la infraestructura de PKI).

La firma electrónica es la que proporciona validez legal al documento electrónico, ya que ofrece garantías de **inalterabilidad** y **no repudio**.

Además se genera un "código de validación", para que cualquier organismo dentro de la organización que no disponga de SIMENDEF, al recibir el documento en papel, pueda validar y verificar que es una impresión de un documento electrónico firmado y registrado por la autoridad y registro que aparecen en el oficio o mensaje y que se encuentra en el Gestor Documental de dicho organismo emisor.

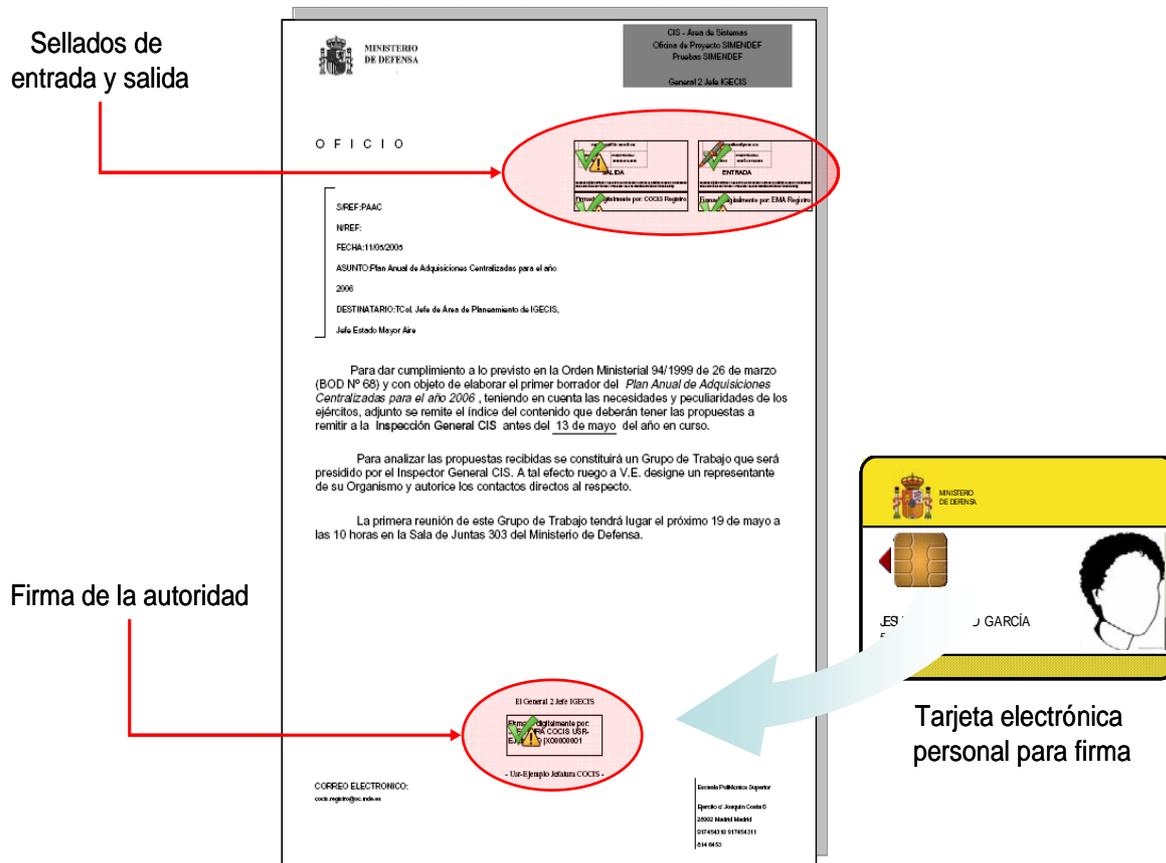


Ilustración 4: Ejemplo de Oficio con la firma y sellos electrónicos

En el proceso de creación, validación y firma de los mensajes, aparece el concepto de "Portafirmas de Salida Digital", que permite a las Autoridades revisar y firmar mensajes para su envío y paralelamente el "Portafirmas de Entrada Digital" para informar a la Autoridad de la entrada en ese ámbito organizativo. Todo esto en base al procedimiento que se articule para el despacho de las Autoridades con sus órganos auxiliares. Para ello, se han implementado utilidades que agilizan el proceso, hasta ahora costoso, relacionado con la firma digital. Así, se dispone de facilidades para la firma múltiple de mensajes con introducción de un único PIN por sesión, la posibilidad de deshacer firmas, bloqueo/deshbloqueo del portafirmas digital, etc.

4.3 La gestión documental

Los documentos registrados quedan automáticamente archivados en un almacén documental, junto con sus documentos adjuntos. El gestor documental es único para todo el Ministerio, aunque cada ámbito sólo podrá acceder a su documentación, lo que proporciona ventajas inmediatas en cuanto a su acceso, estructura y custodia de los documentos.

4.4 Funciones avanzadas: prelación y sobretiempos

Fruto de las aportaciones de los usuarios, se desarrolló una función adicional que permite la denominada "prelación y control de sobretiempos". Esta nueva función consiste en que:

- El sistema asegura **la entrega** en destino del mensaje.
- El sistema garantiza además **la apertura** del documento dentro de los tiempos definidos.

Cuando por motivos técnicos o de otro tipo el mensaje no ha podido ser enviado o cuando el receptor no lo ha abierto dentro del tiempo estipulado, el sistema genera alarmas para que el CECOM que corresponda pueda actuar rápidamente y efectuar la entrega por otros medios (reenvío, envío por fax o por mensajero) o asegurar que el documento sea leído (aviso al destinatario mediante llamada telefónica u otros medios).

4.5 Canales alternativos: correo electrónico, fax, cliente web

SIMENDEF permite canales alternativos de comunicación cuando el receptor o emisor del mensaje no dispone del sistema. SIMENDEF puede recibir del exterior directamente en su buzón de entrada de registro correos electrónicos e incluso faxes. Del mismo modo puede enviar los oficios directamente a una cuenta de correo o un número de fax cuando el receptor disponga de alguno de estos medios.

Asimismo, para facilitar el acceso al sistema desde cualquier terminal conectado a la WAN de propósito general, SIMENDEF dispone de un acceso web con toda la funcionalidad del cliente pesado.

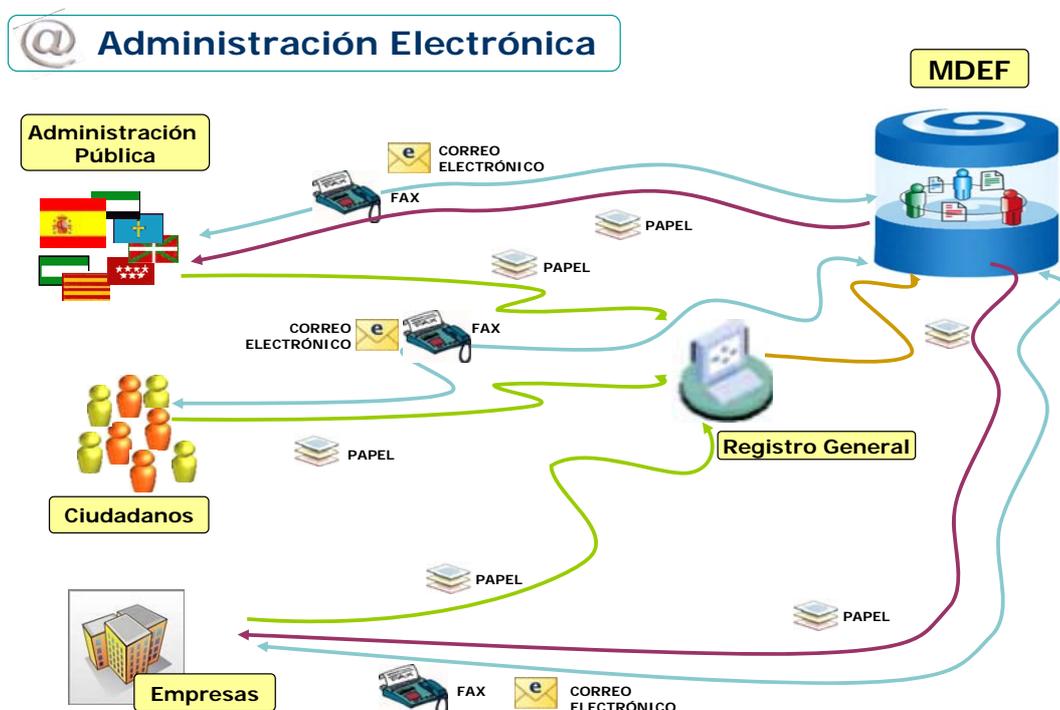


Ilustración 5: Distintos canales de comunicación

4.6 Integración con otros sistemas

Adicionalmente a los canales alternativos de comunicación descritos en el punto anterior, SIMENDEF dispone de mecanismos que permiten su integración con otros sistemas mediante intercambio de ficheros en formato XML o siguiendo estándares SICRES.

Esta capacidad de integración es fácilmente extensible en caso necesario para adaptarse a los requisitos de intercambio que puedan surgir de convenios con otras administraciones.

Asimismo, con objeto de facilitar el despliegue y no interrumpir el normal funcionamiento de aquellos organismos que utilicen otros sistemas de registro, SIMENDEF ha implementado un mecanismo de **compatibilidad** que le permite recibir e interpretar correctamente, así como enviar en el formato adecuado, correspondencia de y hacia otros sistemas de registro (como el SIR). De esta manera se facilita el despliegue en organizaciones de grandes dimensiones, permitiendo que sea progresivo y sin interrumpir las comunicaciones entre entornos migrados y no migrados.

En la actualidad está integrado con el Sistema de Infraestructura de Defensa (SINFRADEF) en el Módulo de Gestión Patrimonial, quedando en los expedientes abiertos/cerrados en este sistema, vinculados a comunicaciones oficiales (oficios y/o mensajes) que se realicen tanto de entrada como de salida desde el propio sistema (WEB_Services).

4.7. Seguridad y Auditoría de la Información.

El sistema cuenta con varios mecanismos para asegurar la validez, disponibilidad y continuidad de los datos del sistema:

A) Mecanismos que aseguran la validez e integridad de la información:

- 1) Firma electrónica avanzada ya mencionada, que asegura la integridad y no repudio de la información contenida en los oficios y mensajes.
- 2) Un módulo de auditoría que permite el control de todas las acciones ejercidas en el sistema a dos niveles:
 - a. A nivel de usuario, quedando registrada las acciones realizadas, las fechas y los participantes en el proceso de elaboración de los oficios y mensajes.
 - b. A nivel de administración, identificando todas las acciones realizadas a nivel de registro por el administrador o administradores, quedando registrado el momento, el autor, el tipo de acción realizada así como el valor cambiado.

B) Mecanismos que asegura la recuperación de los datos y tolerancia a fallos

- 1) Redundancia de los datos que facilitan su recuperación en caso de catástrofe: Caché de los datos contenidos entre elementos distintos de la arquitectura (Notes y Documentum) que facilita la recuperación de los datos que por cualquier motivo no estuvieran ya en backup.
- 2) Redundancia de los elementos de la arquitectura con sincronización de datos, para alta disponibilidad y continuidad del servicio (ante caídas del elemento principal permiten la continuidad del servicio al entrar en funcionamiento la arquitectura de respaldo).

5. ARQUITECTURA HARDWARE SIMENDEF.

En la arquitectura hardware de SIMENDEF que da servicio a uno o varios ámbitos registrales, cabe destacar lo siguiente:

- Los entornos Windows están **virtualizados**, por lo que el esquema representa máquinas virtuales y no físicas.
- El entorno HP-UX (Documentum) es único pero existen más servidores Domino y BEA en el entorno Windows para dar servicio al resto de ámbitos registrales. El esquema hardware es el mismo para todos ellos
- Según las pruebas de carga y rendimiento que se realizaron en su momento, cada servidor Domino podría dar servicio a unos 2000 usuarios potenciales y un servidor BEA puede dar servicio hasta tres servidores Domino. El número total de servidores finales dependerá en cada momento del grado de despliegue alcanzado y de los recursos físicos asignados a cada máquina Windows virtualizada.
- La firma de documentos **se realiza en cliente** mediante la MMAR TEMD y el KeyOne DeskTop. Esta infraestructura de firma en cliente ha sido desarrollada por terceros y para SIMENDEF (como para cualquier otro sistema que deba realizar firma) es un servicio del que hace uso.

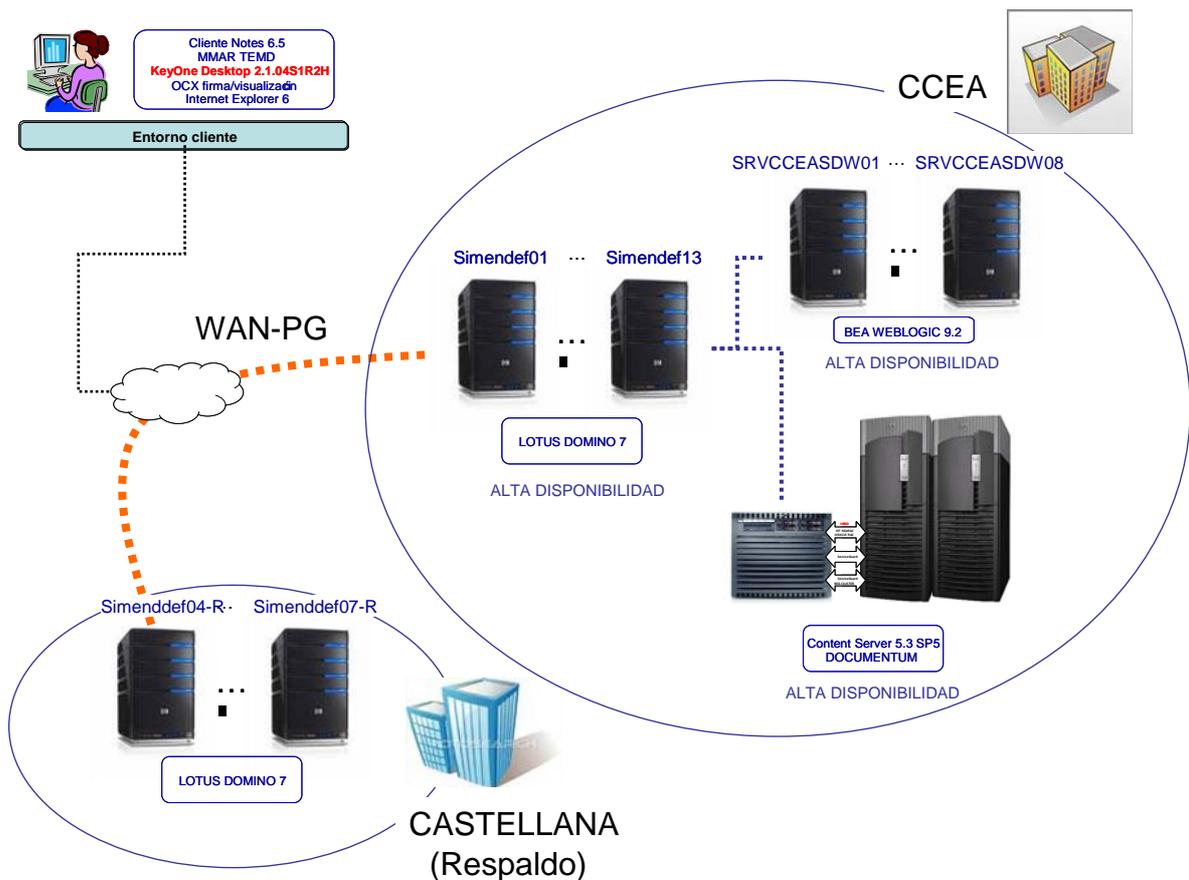


Ilustración 6: Arquitectura del sistema.

Como puede apreciarse el usuario sólo interactúa con la capa Notes de SIMENDEF. Internamente el servidor de Domino puede interactuar con otro servidor Domino o con un BEA (que, a su vez, puede interactuar con Documentum).

NO existe una interacción directa con BBDD Oracle, por lo que no se muestra en el esquema. El Oracle existente es el que da servicio a Documentum.

Es posible que el KeyOne Desktop (infraestructura de firma en local) conecte con servicios de la WAN-PG.