

Integración de Servicios Geográficos en Plataformas de Gobierno Electrónico

Tesis de Maestría

Raquel Sosa

Agosto 2011

Orientador: Dr. Ing. Raúl Ruggia

Supervisor de Estudios: Dr. Ing. Franco Robledo

Resumen

El uso de información geográfica en los servicios públicos, resulta una realidad, y tiende a incrementarse así como a aumentar su complejidad. En este contexto, la información geográfica se presenta asociada a otros tipos de información según el área de aplicación. Como forma de responder, en forma sistemática y escalable, a las necesidades de información geográfica integrada a las operaciones del Estado, las administraciones se plantean la integración de servicios geográficos en las plataformas de gobierno electrónico.

Las Plataformas de Gobierno Electrónico se han desarrollado en forma muy importante en los últimos años para brindar servicios públicos a los ciudadanos a través de Internet. Dichas plataformas se basan en servicios, siguiendo arquitecturas de tipo SOA y utilizando middleware basado en SOAP, en particular de tipo Web Services y ESB.

En este marco, la integración de servicios de Información Geográfica con sistemas empresariales siempre ha planteado desafíos técnicos. A partir de la generalización de los Web Services y del desarrollo de plataformas de middleware, las tecnologías utilizadas por ambos tipos de sistemas comenzaron a avanzar, y a facilitarse la integración.

A pesar de los avances en las áreas mencionadas, la integración entre los mismos presenta algunas dificultades, derivadas del uso de diferentes formatos de información y de invocación de operaciones. En la actualidad, las plataformas de gobierno electrónico se basan fuertemente en Web Services y SOAP, con los que los GIS y sus servicios vía Internet no resultan totalmente compatibles. Se plantea la problemática de integración entre plataformas de gobierno electrónico y servicios de información geográfica, cuya resolución resulta clave para responder a necesidades importantes de las administraciones del Estado, en particular en Uruguay.

Esta tesis aborda dicha problemática, analizando los estándares de Web Services como mecanismo de integración, considerando los Web Services geográficos y su integración a una plataforma de gobierno electrónico. A los efectos de caracterizar las diferentes necesidades de integración entre ambos, se presentan cinco escenarios de uso de información geográfica en servicios del Estado. A partir de los escenarios de integración y de los diferentes protocolos de Web Services, esta tesis identifica en detalle los problemas de compatibilidad entre los mismos que resultan relevantes para la integración de Servicios Geográficos en plataformas de Gobierno Electrónico.

El encare de solución propuesto está basado en la inserción de *Componentes de Transformación de Protocolos* en los puntos de integración de la plataforma de Gobierno Electrónico con los sistemas servidores y clientes de información geográfica. Asimismo, entendemos importante destacar el aporte de la especificación formal de las transformaciones, que provee un marco para la demostración formal del cumplimiento de las propiedades de las transformaciones. Además del resultado obtenido en esta tesis, consistente en la especificación de transformaciones y demostraciones concretas realizadas, este encare permite avanzar en la aplicación de métodos formales para validar la correctitud de transformaciones y flujos que se especifiquen en este contexto de integración de sistemas.

Contenido

Contenido.....	5
Capítulo 1 – Introducción.....	7
Sección 1.1 - Contexto y Motivación	7
Sección 1.2 - Objetivos.....	8
Sección 1.3 - Solución Propuesta	9
Sección 1.4 - Aportes	10
Sección 1.5 - Organización de la Tesis.....	11
Capítulo 2 – Conocimiento Existente	13
Sección 2.1 – Plataformas de Gobierno Electrónico.....	13
2.1.1 Gobierno Electrónico	13
2.1.2 Plataformas de Gobierno Electrónico.....	14
2.1.3 Infraestructuras de Datos Espaciales	16
Sección 2.2 – Middleware de Gobierno Electrónico.....	18
2.2.1 Web Services SOAP	18
2.2.2 ESB.....	19
Sección 2.3 Tecnologías de Web Services Geográficos.....	24
2.3.1 Web Services Geográficos.....	24
2.3.2 Tecnologías de Web Services GIS y productos asociados	25
Sección 2.4 Conclusiones	27
Capítulo 3 – Análisis	29
Sección 3.1 - Presentación de Escenarios	29
3.1.1 Público general consultando información	29
3.1.2 Público especializado consultando información.....	30
3.1.3 Instituciones colaborando en la generación de información geográfica.....	30
3.1.4 Instituciones colaborando en trámites	31
3.1.5 Público generando Información Geográfica	32
Sección 3.2 – Análisis Técnico de Escenarios.....	33
3.2.1 Escenario I – Información Pública	33
3.2.2 Escenario II – Servicios para públicos específicos.....	37
3.2.3 Escenario III – Colaboración inter-institucional para la generación de Información Geográfica	41
3.2.4 Escenario IV – Colaboración para la realización de procesos	45
3.2.5 Escenario V – Generación Comunitaria de Datos (VGI)	49

Sección 3.3 - Resumen Análisis Escenarios	52
Capítulo 4 – Propuesta de Solución	57
Sección 4.1 - Visión General de la Solución	57
4.1.1 Introducción	57
4.1.2 Flujos y Transformaciones	59
4.1.3 Comparación de Protocolos de Web Services	63
Sección 4.2 Especificación de la solución.....	65
4.2.1 Definiciones previas	65
4.2.2 Transformaciones	67
4.2.3 Flujos	73
4.2.4 Demostraciones	76
Sección 4.3 - Alternativas de Implementación	80
4.3.1 Descripción General	80
4.3.2 Implementación de las Transformaciones de Protocolos.....	82
4.3.3 Implementación de Flujos.....	83
4.3.4 Relación Escenarios – Flujos	86
Capítulo 5 – Conclusiones y Trabajos Futuros	89
Sección 5.1 - Resumen y Contribuciones	89
Sección 5.2 - Trabajo en Curso y a Futuro	90
Referencias.....	92
Anexo - Caso de Estudio.....	96
Descripción.....	96
Datos y Servicios	97
Usuarios y Software Cliente	102
Referencias.....	102

Capítulo 1 – Introducción

Sección 1.1 - Contexto y Motivación

El uso de información geográfica en los servicios públicos, tanto para responder a funciones internas como para proveer servicios a los ciudadanos, resulta una realidad, y tiende a incrementarse así como a aumentar su sofisticación. En este contexto, la información geográfica se presenta asociada a otros tipos de información según el área de aplicación, destacándose la información ambiental y de recursos naturales, así como la socio-económica, de gestión territorial y de gestión de riesgos naturales. Un análisis del uso de información geográfica en servicios de seguridad social se puede encontrar en [5].

Como forma de responder, en forma sistemática y escalable, a las necesidades de información geográfica integrada a las operaciones del Estado, las administraciones se plantean la integración de servicios geográficos en las plataformas de gobierno electrónico.

Dentro de los ejemplos más destacados de este uso se encuentra la Agencia de Protección Ambiental (EPA) de Estados Unidos [6] que usa la información geográfica para la gestión ambiental y seguimiento de desastres. Sin embargo, todavía están lejos de generalizarse en el resto del mundo.

Por otra parte, las Plataformas de Gobierno Electrónico (PGE) [2] se han desarrollado en forma muy importante en los últimos años en todo el mundo para brindar servicios públicos a los ciudadanos a través de Internet. En Uruguay, la AGESIC (Agencia de Gobierno Electrónico y Sociedad de la Información) [1] es la encargada de llevar adelante y coordinar las actividades de Gobierno Electrónico. Los sistemas o plataformas de Gobierno Electrónico tienden a basarse en servicios, siguiendo arquitecturas de tipo SOA (Service Oriented Architecture) y utilizando middleware basado en SOAP, en particular de tipo Web Services y ESB (Enterprise Service Bus) [7]. En este sentido, la “Guía de Uso de la PGE del Estado uruguayo” [3] establece los mecanismos para la publicación y uso de servicios a través de la PGE de AGESIC.

En este marco, la integración de servicios de Información Geográfica con sistemas empresariales siempre ha planteado desafíos técnicos. Hasta hace unos 10 años, dicha integración requería el uso de tecnologías propietarias de los Sistemas de Información Geográficos (GIS) o implementaciones complejas. Asimismo, las plataformas de gobierno electrónico todavía eran muy incipientes.

Luego, a partir de la generalización de los Web Services y del desarrollo de plataformas de middleware, las tecnologías utilizadas por ambos tipos de sistemas comenzaron a converger, y a facilitarse la integración.

En nuestro país, se ha establecido un Consejo Asesor en temas de Información Geográfica y un Grupo de Trabajo IDE en el contexto de AGESIC, y se apunta a establecer una Infraestructura de Datos Espaciales uruguayo (IDEUy) [9]. Dicha Infraestructura se propone facilitar el acceso a la información geográfica generada por los organismos del Estado y permitir que se comparta entre los mismos.

A pesar de los avances en las áreas mencionadas, la integración entre los mismos presenta algunas dificultades, fundamentalmente derivadas del uso de diferentes formatos de información y de invocación de operaciones (o servicios remotos). En la actualidad, las plataformas de gobierno

electrónico se basan fuertemente en Web Services (WS) y SOAP, con los que los GIS y sus servicios vía Internet no resultan totalmente compatibles.

Se plantea, por lo tanto, la problemática de integración entre plataformas de gobierno electrónico y servicios de información geográfica, cuya resolución resulta clave para responder a necesidades importantes de las administraciones del Estado, en particular en Uruguay.

Las dificultades de integración tienen como consecuencias un costo importante en duplicación de trabajos a medida y en la subutilización de las plataformas de infraestructura ya desarrolladas. No pueden aplicarse en forma nativa mecanismos de procesamiento de datos provistos por herramientas de middleware (ruteo, transformación de mensajes, asincronismo, seguridad). Para poder hacerlo, deben implementarse específicamente, en las aplicaciones, mecanismos que los sustituyan, lo cual implica el desarrollo de soluciones a medida no estandarizadas y que llevan a la duplicación del trabajo y a una mayor complejidad de las aplicaciones.

Esta tesis aborda dicha problemática, analizando estándares de Web Services como mecanismo de integración, tanto los usados en plataformas de gobierno electrónico como en servicios de información geográficos, centrándose en los Web Services geográficos y su integración a una plataforma de gobierno electrónico. A los efectos de caracterizar las diferentes necesidades de integración entre ambos, se presentan cinco escenarios de uso de información geográfica en servicios del Estado.

Sección 1.2 - Objetivos

Dentro del contexto y problemáticas descritas antes, que resultan sumamente amplios, esta tesis se propone plantear soluciones al problema siguiente:

¿De qué forma, sistemática y basada en estándares, pueden integrarse los servicios de información geográfica en una plataforma de gobierno electrónico basada en SOA, e implementada utilizando Web Services así como middleware de tipo ESB?

Para encarar este problema se plantean los siguientes objetivos:

- Caracterizar el uso de servicios geográficos en un contexto de Gobierno Electrónico en diferentes escenarios, considerando distintos grados de complejidad en los servicios ofrecidos al usuario final.
- Identificar las situaciones de incompatibilidad entre los servicios de información geográfica y las plataformas de gobierno electrónico, teniendo en cuenta las tecnologías actualmente disponibles en productos de uso industrial/comercial.
- Proponer mecanismos, que sean sistemáticos y basados en estándares, para facilitar la integración de servicios de información geográfica en una plataforma de gobierno electrónico.

En este trabajo, se tomará como base la Plataforma de Gobierno Electrónico (PGE) del Uruguay, con el objetivo adicional de aportar encares de solución concretos al contexto uruguayo. Por otra parte, dadas las características de la PGE (basada en estándares y tecnologías de última generación), la discusión técnica y soluciones planteadas son igualmente válidas para otras plataformas y contextos de Gobierno Electrónico.

Sección 1.3 - Solución Propuesta

La solución planteada en esta tesis se basa en los siguientes elementos principales:

- Caracterización de escenarios de integración de Servicios Geográficos en un marco de Gobierno Electrónico, en particular tomando como referencia una arquitectura como la de Uruguay.
- Identificación de funcionalidades/operaciones que no pueden realizarse, o que resultan problemáticos, en la integración de servicios de información geográfica en una plataforma de gobierno electrónico. Se trata de identificar los tipos de casos que presentan mayores dificultades para ser resueltos en forma sistemática y en base a estándares.
- Especificación de transformaciones de datos que permitan el uso de los servicios de la Plataforma de Gobierno Electrónico en forma transparente, tanto para los clientes, como para los servidores de mapas. Este encare apunta a proveer un mecanismo sistemático para la integración de servicios y clientes que utilizan Web Services para GIS en una plataforma de Gobierno Electrónico que utiliza middleware (fundamentalmente Web Services y ESB) basados en SOAP (WS-SOAP).
- Especificación de flujos de operaciones, que usan las transformaciones mencionadas antes, para lograr llevar adelante las funcionalidades identificadas previamente, y que se insertan en los escenarios resultantes del análisis de contexto.

En la Figura 1 se muestra la arquitectura de la solución propuesta: tanto los clientes como el servidor de mapas trabajan con pedidos y respuestas de servicios de información geográfica, a la vez que también usan WS-SOAP cuando lo necesitan.

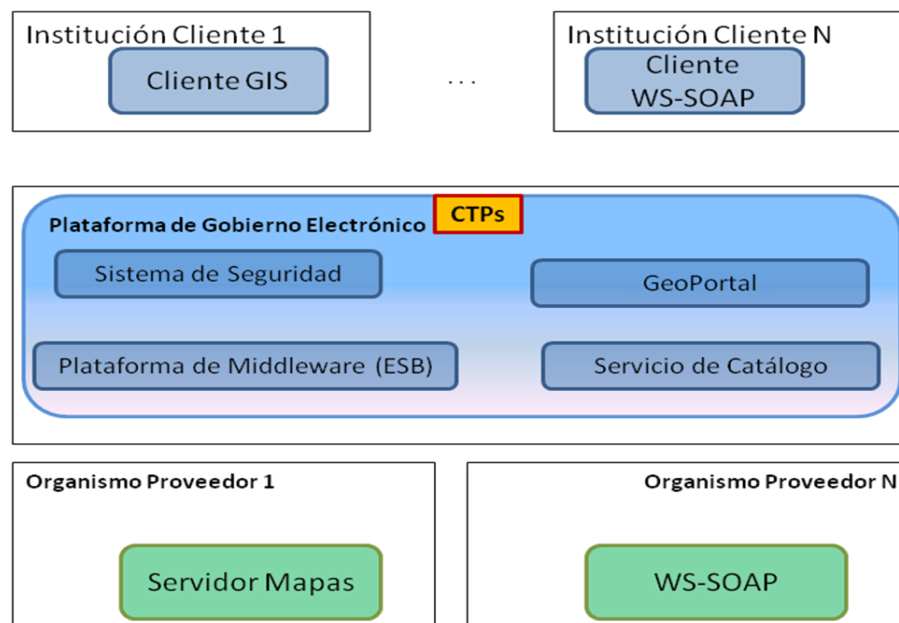


Figura 1 - Arquitectura Propuesta

La Plataforma de Gobierno Electrónico tiene sus componentes de servicios que permiten trabajar en forma eficiente con la seguridad y a través de la Plataforma de Middleware permite la integración de servicios entre organismos. El Servicio de catálogo gestiona la información de dominio que la plataforma requiere. El GeoPortal es una aplicación especializada en información geográfica.

El componente marcado como un punto de entrada a la plataforma (CTP Componente de Transformación de Protocolos) aplica las transformaciones propuestas. Esto permite que los pedidos y respuestas sean vistos dentro de la plataforma como cualquier otro pedido que la PGE maneja. En particular se podrán aplicar las políticas de seguridad y los mecanismos de ruteo que la plataforma ya tiene definidos

Es de destacar que esta propuesta de solución se basa en aprovechar al máximo los servicios que la plataforma ya brinda a los distintos organismos del Estado teniendo el menor de los impactos posible en las aplicaciones de clientes y proveedores.

Sección 1.4 - Aportes

Esta tesis presenta una aproximación al problema de integración de servicios de información geográfica en plataformas de gobierno electrónico, poniendo énfasis en el uso de tecnologías y plataformas actualmente utilizadas en servicios geográficos y de Gobierno Electrónico en general. Dicha aproximación comienza a alto nivel proponiendo y analizando escenarios funcionales de uso integrado de información geográfica entre diferentes instituciones. Luego de este análisis, se realiza una síntesis de las incompatibilidades técnicas más importantes para lograr dicha integración. Finalmente se propone una propuesta de solución enfocada en el uso más eficiente posible de las tecnologías ya disponibles y centrando la solución en el ámbito de trabajo de la Plataforma de Gobierno Electrónico.

Las principales contribuciones de este trabajo son las siguientes:

- Identificación y descripción de escenarios de integración de servicios geográficos en una plataforma de gobierno electrónico, basándose diferentes tipos de servicios ofrecidos y de clientes consumidores, así como en características de los procesos que pueden realizar organismos participantes de la plataforma de gobierno electrónico.
- Análisis sobre la compatibilidad de Web Services Geográficos y Plataformas de Gobierno Electrónico, tomando como base los escenarios identificados. Este análisis identifica en detalle los elementos de incompatibilidad entre los protocolos involucrados, sentando las bases para definir una propuesta de solución a este problema.
- Propuesta de solución para mejorar la compatibilidad entre las plataformas de gobierno electrónico y los servicios de información geográfica, a través de mecanismos basados en transformaciones de paquetes de datos. Esta propuesta de solución trata de aprovechar al máximo los sistemas y plataformas existentes, teniendo en cuenta que se trata de infraestructura ya establecida y que funciona adecuadamente en sus propios contextos de uso.

Asimismo, en esta tesis se presentan encares de implementación de la solución propuesta utilizando tecnologías y productos utilizados en Servicios Geográficos y Plataformas de Gobierno Electrónico.

Sección 1.5 - Organización de la Tesis

Esta tesis presenta en el capítulo 2 una revisión del conocimiento existente. En el capítulo 3 se muestra un análisis de la problemática en base a escenarios de integración. En el capítulo 4 se presenta un enfoque de solución. Finalmente en el capítulo 5 se presentan las conclusiones del presente trabajo y las líneas futuras a seguir.

Capítulo 2 – Conocimiento Existente

En este capítulo se presenta el conocimiento existente que resulta relevante para el análisis de los problemas abordados en esta tesis así como para las propuestas de solución. En primer lugar, se describen las Plataformas de Gobierno Electrónico, que corresponden al contexto de ejecución de los servicios de Gobierno Electrónico en el cual interesa integrar los Servicios de Información Geográficos. Luego, la Sección 2.2 presenta las tecnologías de middleware utilizadas en las Plataformas de Gobierno Electrónico, las cuales constituyen la base técnica para la integración. Por otra parte, la Sección 2.3 presenta las tecnologías de Servicios Geográficos, poniendo foco en los mecanismos de Web Services Geográficos, que son los que se utilizarán para la integración a una Plataforma de Gobierno Electrónico. Finalmente, en la Sección 2.4 se presentan conclusiones sobre las características de las tecnologías existentes y su aplicación en el encare de los objetivos de esta tesis.

Sección 2.1 – Plataformas de Gobierno Electrónico

En esta sección presentaremos algunos conceptos de Gobierno Electrónico para entender el rol que juegan las Plataformas de Gobierno Electrónico. En paralelo se han desarrollado iniciativas específicas para la gestión eficiente de la Información Geográfica a nivel Estatal a través de las Infraestructuras de Datos Espaciales.

2.1.1 Gobierno Electrónico

El Gobierno Electrónico son las actividades del gobierno realizadas a través del uso de las Tecnologías de Información y Comunicación (TIC). Esto se realiza para optimizar la gestión del Estado y brindar sus servicios en forma más efectiva a los ciudadanos.

“Promover la aplicación y uso de tecnología en los organismos del Estado, con el fin de mejorar el acceso a la información, trámites y servicios ofrecidos a los ciudadanos; aumentar la eficiencia y eficacia de la gestión pública e incrementar sustantivamente la transparencia y participación de la ciudadanía, son los principales conceptos asociados al Gobierno Electrónico” – AGESIC

Las iniciativas de Gobierno Electrónico se han creado en los últimos 10 años, dados los avances que han tenido las TICs. Sin embargo, lograr que efectivamente se brinden los servicios públicos a través de Internet y en forma completamente digital depende de varios factores: tecnológicos, organizacionales, legales y políticos. Se requiere el desarrollo de una plataforma tecnológica que brinde soporte a los procesos de gestión gubernamental, pero también se requiere la coordinación institucional para llevar adelante dichos procesos y el soporte legal para darle validez a los procesos.

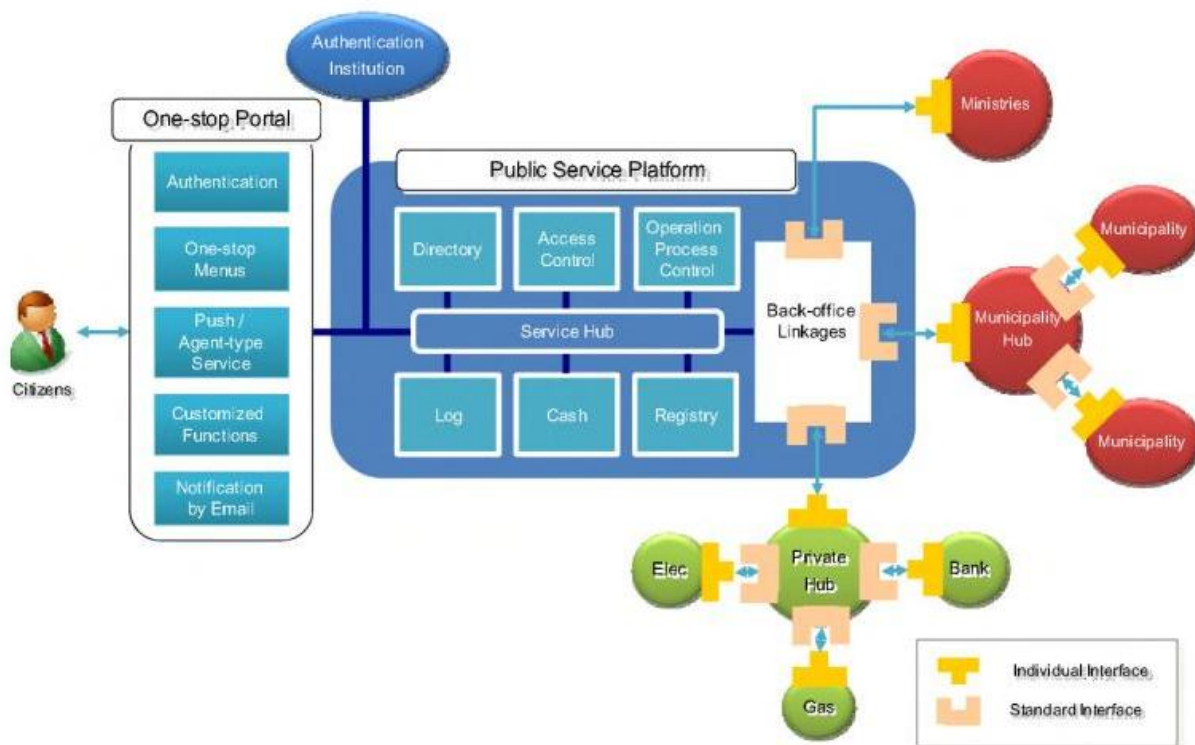
En “Information Systems for eGovernment a Quality-of-Service Perspective” [8], los autores presentan las diferentes dimensiones de las iniciativas de Gobierno Electrónico desde un marco teórico de Calidad de Servicios. En la sección 4 del libro se presentan como caso de estudio las experiencias de Gobierno Electrónico de Italia y la planificación de nuevos servicios e integración de sistemas de información del Ministerio de Agricultura de Túnez.

A nivel regional, en el año 2007, se firmó la “Carta Iberoamericana de Gobierno Electrónico” en la XVII Cumbre Iberoamericana de Ministros de Administración Pública y Reforma del Estado realizada en Chile. Dicho documento presenta los acuerdos políticos que los países impulsarán a nivel nacional y para lograr también la integración regional. Siguiendo estos lineamientos a nivel iberoamericano, en la Cumbre de 2010 se aprobó el documento “Bases para una Estrategia Iberoamericano de Interoperabilidad” [10]. Dicho documento profundiza en cada aspecto de gobierno electrónico proponiendo lineamientos que permitan la interoperabilidad.

2.1.2 Plataformas de Gobierno Electrónico

Las Plataformas de Gobierno Electrónico son el soporte tecnológico para los servicios de Gobierno Electrónico. Incluyen desde el hardware y las conexiones de red hasta los productos de software que permiten la interconexión de sistemas a nivel interinstitucional. Estas plataformas son las que permiten brindar los servicios a los ciudadanos y tienen características avanzadas de disponibilidad, confiabilidad y seguridad.

En [7] se presenta la Plataforma de Gobierno Electrónico de Japón y se profundiza en los desafíos de integración entre instituciones para brindar servicios administrativos integrados en un portal a los ciudadanos.



Next-generation One-stop Portal for Japan's e-Gov

Figura 2 - Arquitectura de la Plataforma Japonesa de eGov y su Portal

Como se ve en la Figura 2 la plataforma de servicios públicos brinda servicios centrales (Control de Acceso, Log, Control de Proceso, Directorios, Registros) para permitir la integración de diferentes

sistemas de distintos organismos a través de interfaces estándar. El portal brinda los servicios a los ciudadanos invocando a los diferentes organismos de acuerdo al servicio solicitado por el ciudadano.

Plataforma de Gobierno Electrónico del Estado Uruguayo PGE_Uy

En Uruguay la AGESIC [1] es la agencia responsable de la Plataforma de Gobierno Electrónico [2]. Dicha Plataforma tiene un componente de conectividad llamado REDUy, que es una red de alta velocidad que interconecta los diferentes organismos. A través de dicha red se logra la interconexión física de los organismos públicos con alta velocidad y disponibilidad de las conexiones. Sobre esta red, en AGESIC opera la Plataforma de Middleware que brinda servicios centrales a través de sus componentes base y algunas aplicaciones y accediendo a servicios de diferentes organismos. Esto no sustituye los portales de los organismos, pero permite brindar al público un único punto de acceso a servicios distribuidos.

En la Figura 3 se muestra la arquitectura de la Plataforma de Gobierno Electrónico uruguayo y sus conexiones a través de la REDUy con los diferentes organismos del Estado.

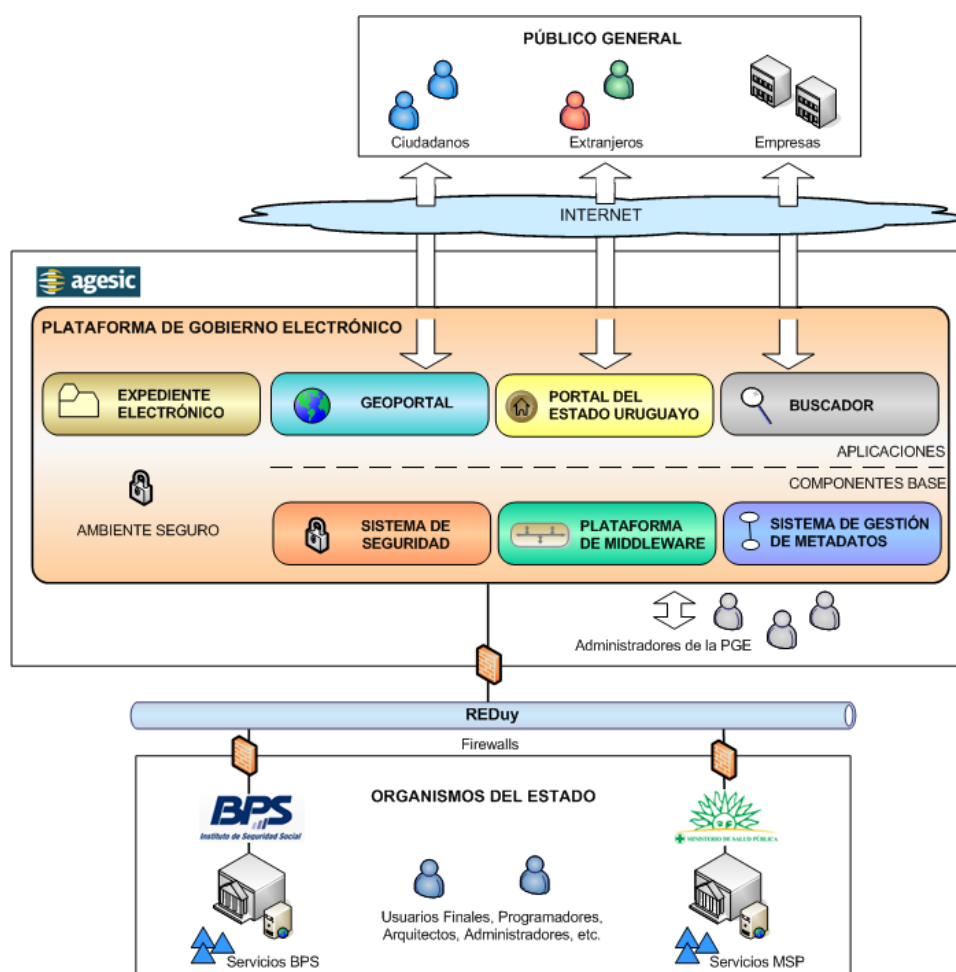


Figura 3 - Arquitectura de la PGE_Uy¹

¹ Tomada de la “Guía de Uso de la Plataforma de GE del Estado Uruguayo” [3]

Dentro de la plataforma se destacan los Componentes Base: el Sistema de Seguridad, la Plataforma de Middleware y el Sistema de Gestión de Metadatos. La plataforma permite interconectar sistemas de distintos organismos usando sus Componentes Base y a su vez brinda Aplicaciones para usuarios finales. Las aplicaciones actuales son: el Sistema de Expediente Electrónico, el Portal del Estado Uruguayo, el Buscador y el GeoPortal.

La Plataforma de Middleware se basa en Tecnologías de Integración de Servicios y además brinda Entornos de Ejecución para Aplicaciones y Servicios. En la Figura 4 se ven estos componentes dónde se destaca el Enterprise Service Bus.



Figura 4 - Plataforma de Middleware de la PGEUy

En las siguientes secciones entraremos en detalles en las características de los ESB.

2.1.3 Infraestructuras de Datos Espaciales

Las Infraestructuras de Datos Espaciales (IDE) son la plataforma tecnológica en conjunto con las políticas y los acuerdos organizacionales que permiten la disponibilidad y el acceso a los datos espaciales (o Información Geográfica) [19]. Además del software y los datos espaciales, son de gran importancia las políticas de uso de los datos espaciales y la forma de acceso a los mismos.

Las Infraestructuras de Datos Espaciales surgen a nivel estatal como una forma de no duplicar esfuerzos y lograr mayor eficiencia en la gestión de los datos espaciales. Dentro del Estado, si un organismo genera un juego de datos espaciales, puede ponerlo a disposición de otros organismos para que no tengan que volver a generarse.

Como casos destacados de IDE podemos citar los de la Unión Europea (INSPIRE) [36] y la IDE de España (IDEE) [37]. En Uruguay, la AGESIC ha tomado la coordinación de la iniciativa de creación de una IDE, existiendo el Grupo de Trabajo IDEUy [9]. Este grupo ya ha propuesto la adopción como estándar de representación de datos geográficos el Sistema de Referencias UTM Zona 21 S.

Para compartir datos espaciales se propone una arquitectura federada de servidores de mapas que brindan servicios web geográficos. En este esquema los organismos públicos generadores de la información la publican para el uso de los demás organismos públicos. Para lograr el descubrimiento de la información hay un Nodo Central que se conecta a los diferentes organismos para brindar la información a los usuarios como se muestra en la Figura 5.

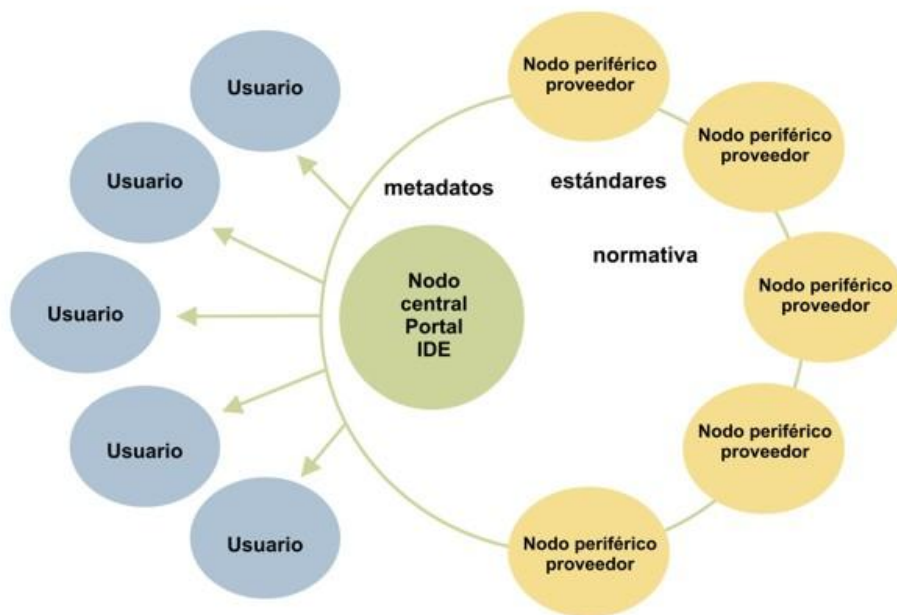


Figura 5 - Arquitectura IDEUy

El Nodo Central de la IDEUy se aloja en la Plataforma de Gobierno electrónico como la aplicación “GeoPortal”. La comunicación del Nodo Central con los nodos Periféricos se basa en los estándares de Web Services Geográficos. Se apunta a que los servicios de la IDEUy se integren a través de la Plataforma de Gobierno Electrónico del Uruguay. Distintos organismos tienen diferente grado de avance en el desarrollo de servicios geográficos para la IDE. Algunos de dichos trabajos se presentaron en el Primer Congreso Uruguay IDE – 2010 [52].

Sección 2.2 – Middleware de Gobierno Electrónico

Las plataformas de Gobierno Electrónico tienden a basarse en Arquitecturas Orientadas a Servicios, e implementan la comunicación entre sistemas a través de Web Services y de Enterprise Service Bus

2.2.1 Web Services SOAP

Los Web Services SOAP son un mecanismo estándar de comunicación que permite intercambiar información estructurada en ambientes distribuidos y descentralizados [12]. El protocolo SOAP define que las comunicaciones se realizan enviando mensajes de ida y vuelta entre un cliente y el proveedor del servicio, pudiendo pasar en el camino por otros nodos SOAP. Los mensajes SOAP tienen formato XML y siguen una estructura básica de documento: una sección de cabecales y una sección de cuerpo del mensaje. Esta forma de comunicación es independiente de la plataforma de implementación que se use en el cliente y el servidor.

Los Web Services SOAP son independientes de las plataformas de implementación y se basan en estándares de la web. Se definen los roles de cliente (o consumidor) y proveedor de servicios y un conjunto de mecanismos básicos para lograr la comunicación. En la Figura 6 se muestra la arquitectura básica de Web Services. Los Proveedores de Web Services publican en el Service Broker los contratos de servicio (en lenguaje WSDL). Los Consumidores se conectan al Service Broker para descubrir (find) qué servicios hay disponibles y luego de conocer la especificación del servicio se conectan al mismo (bind) realizando la invocación. En estándar para definir las funciones de los Service Brokers es UDDI (Universal Description, Discovery and Integration) [11].

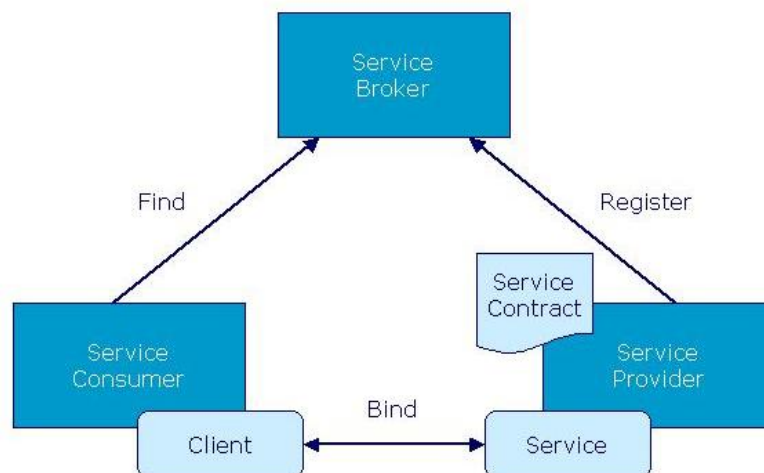


Figura 6 - Arquitectura Web Services²

Además se define un rol de “Registro” o “Service Broker” que es un repositorio de descripciones de servicios. Esto permite que los clientes puedan descubrir dinámicamente nuevos servicios.

Los Web Services son la base para lograr interoperabilidad entre distintas plataformas de desarrollo ya que son independientes de ellas. Permiten publicar funciones de aplicaciones en la web y realizar

² Tomado de <http://lists.w3.org/Archives/Public/www-ws-arch/2002Sep/att-0180/SOA.jpg>

invocaciones. Al estar basados en estándares de la Web, también pueden ser usados para comunicación de aplicaciones entre distintas organizaciones a través de Internet.

La especificación de Web Services es lo suficientemente simple y genérica como para que se puedan implementar en diferentes plataformas. Como limitación tiene que en la especificación básica no se poseen características avanzadas que requieren las aplicaciones empresariales, como por ejemplo seguridad y transaccionalidad.

Extensiones de Web Services SOAP: WS-*

Los estándares de Web Services SOAP [12] resuelven el problema de la comunicación entre diferentes plataformas de desarrollo, logrando un primer nivel de interoperabilidad. Sin embargo, a la hora de integrar aplicaciones de negocio se requiere asegurar determinadas propiedades de las comunicaciones que no están comprendidas en los estándares básicos de Web Services. Por esto, diferentes organizaciones han generado propuestas de estándares que extienden las especificaciones de Web Services para asegurar dichas propiedades. A estas extensiones se las conoce como WS-* [14] y se enfocan en diferentes aspectos de la comunicación: la seguridad, confidencialidad, comunicaciones seguras, transaccionalidad. Estas especificaciones establecen como extender el protocolo SOAP (y sus mensajes) para intercambiar información adicional o asegurar la información que se envía (por ejemplo encriptando los datos sensibles).

WS-Security – es una extensión del protocolo SOAP para lograr intercambios seguros de mensajes SOAP. Establece un framework general que permite trabajar con diferentes protocolos de seguridad sin definir uno en particular. La especificación provee tres grandes mecanismos: inclusión de información de seguridad (tokens), integridad del mensaje y confidencialidad del mensaje. Combinando estos tres mecanismos con otros estándares se pueden implementar diferentes mecanismos de seguridad de acuerdo a las necesidades.

WS-Trust – extensión de WS-Security que permite establecer relaciones de confianza entre dos partes, brindando mecanismos para trabajar con credenciales de seguridad.

La especificación completa de los WS-* se puede encontrar en [13].

2.2.2 ESB

De acuerdo a [17], el Enterprise Service Bus (ESB) es *“una plataforma de integración basada en estándares que combina mensajería, Web Services, transformación de datos y ruteo inteligente para conectar y coordinar, de forma confiable, la interacción de un gran número de aplicaciones diversas a través de empresas extendidas y con integridad transaccional”*.

A lo largo su historia, los diferentes tipos de Middleware fueron surgiendo para resolver limitaciones de sus predecesores. Los ESB apuntan a cubrir carencias de los Servidores de Aplicaciones, en particular para la implementación de aplicaciones siguiendo arquitecturas de tipo SOA.

En la siguiente figura se muestra en el centro las vías de intercomunicación que brinda un ESB y los conectores a distintos tipos de aplicaciones de diferentes plataformas que soporta (Web Services, aplicaciones JEE, aplicaciones .NET, aplicaciones legadas).

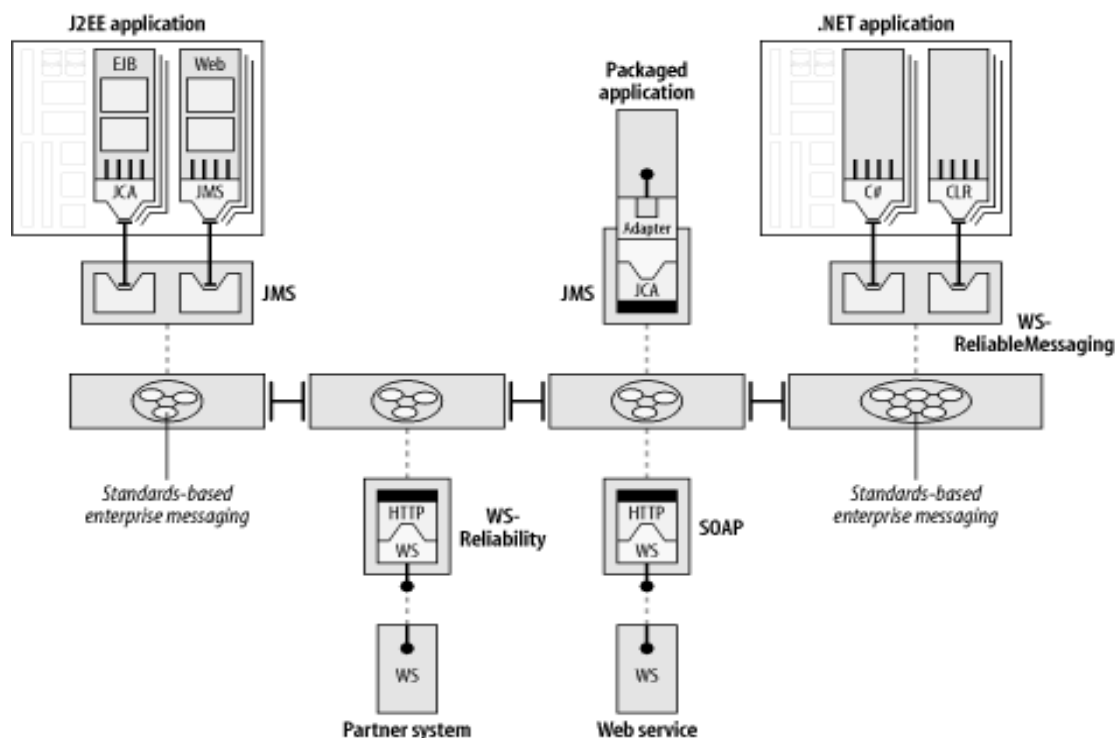


Figura 7 - Arquitectura de un ESB³

El ESB es una plataforma de base para la implementación de una SOA ya que provee interoperabilidad entre aplicaciones usando adaptadores e interfaces basados en estándares.

Los ESB brindan a las aplicaciones funcionalidades de conectividad, transformación de mensajes, ruteo inteligente, mensajería asíncrona. Además de esto tienen funcionalidades propias de monitoreo de su funcionamiento y administración.

Conectividad

Un ESB incluye adaptadores para brindar conectividad, que le permiten interactuar a través de protocolos de comunicación y transporte como HTTP, FTP, POP3/SMTP y el sistema de archivos. Se configuran a través de archivos de configuración, típicamente XML, o interfaces gráficas. Los adaptadores permiten satisfacer un requerimiento de integración común conocido como conversión de protocolo (*protocol switch*).

Transformación de Mensajes

Los ESBs incluyen funcionalidades de transformación de mensajes, que facilitan la interacción entre aplicaciones que utilizan distintos formatos o modelos de datos. Permiten especificar y ejecutar transformaciones XSLT, y además incluyen herramientas para realizar transformaciones desde otros formatos.

³ Tomada de [17]

Ruteo Intermediario

El ruteo intermediario es la funcionalidad del ESB para definir, en tiempo de ejecución, el destino de un mensaje de acuerdo a distintos elementos: basado en contenido, ruteo para balanceo de carga, ruteo basado en contexto y ruteo basado en itinerario.

El ruteo basado en contenido es el tipo de ruteo más común en productos ESB. Se determina el destino del mensaje en base a su contenido. En el caso de SOAP, la lógica de ruteo se puede basar en el contenido del cuerpo o de los encabezados del mensaje. Para evaluar el contenido de mensajes XML, se utiliza XPath y/o XQuery. Además, también es común el uso de motores de reglas.

El ruteo para el balanceo de carga determina el destino del mensaje en base a una estrategia de balanceo de carga como *Round-Robin*, *Random* y *LeastLoad*. Es usado para evitar sobrecargar los servicios que brindan las aplicaciones.

Ruteo basado en contexto: determina el destino del mensaje en base a propiedades del contexto de ejecución: día-hora, o la carga actual del sistema.

En el ruteo basado en itinerario se determina el destino del mensaje en base a un itinerario, que se incluye en el propio mensaje y especifica al ESB el camino que debe seguir el mismo.

Mensajería Asincrónica

Los ESBs generalmente incluyen sistemas de mensajería que permiten proveer funcionalidades de mensajería (colas de mensajes), con diferentes propiedades (con garantía de entrega, persistencia, etc).

En base a estos sistemas de mensajería el ESB puede realizar mapeos entre estilos de interacción y controlar/balancear la carga de mensajes. Manejar en forma asincrónica las interacciones para soportar cargas de pedidos mayores a las procesables.

Monitoreo

Los ESB proveen nativamente distinta información de monitoreo. Por ejemplo, tiempos de respuesta o cantidad de mensajes procesados. Esto permite saber en todo momento cómo está funcionando y realizar una administración más eficiente del mismo.

En un ESB todo objeto es considerado un servicio o mensaje, y la forma de interacción entre servicios es a través de mensajes. Uno de los aportes del ESB es la separación entre la lógica asociada a la comunicación e integración de aplicaciones y la lógica de negocio. Toda lógica asociada al paradigma “find-bind-invoke” es responsabilidad del ESB, y los principales componentes encargados de esta tarea son los mecanismos de mensajería, XML, los servicios, un direccionamiento inteligente de mensajes y los mecanismos de mediación.

Los ESB implican el uso intenso de mensajería, servicios, bajo acoplamiento, transformaciones, protocolos y direccionamiento inteligente. El nombre “Bus” proviene de la idea de “transportador” de mensajes.

Los servicios son considerados entidades abstractas (abstract endpoints) las cuales se conectan al ESB para proveer una funcionalidad a todo el sistema. Estas funcionalidades pueden ser tan variadas como uno desee: puede ser una funcionalidad de infraestructura, como lo puede ser una transformación XSLT o una funcionalidad asociada a un proceso de negocio concreto, como el cálculo de un impuesto.

La filosofía que siguen los ESBs es que los servicios sean independientes entre sí y cada servicio se conecte al bus en la medida que este sea requerido por el sistema global. Importante: Los servicios ESBs no necesariamente tienen que ser servicios Web.

Desde su concepción, los ESBs separan la lógica de la aplicación o negocio, de la lógica asociada a la comunicación e integración. Estos quitan el direccionamiento del endpoint, de mensajes y tareas referentes a las orquestaciones. Las comunicaciones son “soft” y pueden ser modificadas en tiempo de deployment o ejecución, en lugar de ser “hard” y sólo poder ser modificadas en tiempo de compilación.

Existen tres grandes conceptos asociados a la forma de direccionamiento de los ESBs:

- Abstracción de servicios. Los ESBs realizan el enlace entre el cliente y el servicio en tiempo de ejecución. El cliente no necesita saber la URI del servicio, ya que el ESB se maneja con alias. De esta forma es sencillo sustituir en tiempo de deployment/ejecución un servicio por otro.
- Orquestación y procesos de negocio. En la mayoría de los ESBs es posible definir procesos de negocio como simples secuencias de pasos, así como también mediante una sofisticada orquestación, tal cual puede ser especificada utilizando lenguajes como WS-BPEL.
- Direccionamiento basado en reglas. Los ESB pueden contar con la posibilidad de proveer servicios especializados en ruteo y brindar un direccionamiento inteligente de mensajes basándose en su contenido. Este tipo de direccionamiento se basa en reglas, las cuales pueden ser descritas en Javascript, XPath, WS-BPEL o cualquier otro lenguaje de tercera generación. WS-BPEL permite manejar escenarios más complejos que los que pueden ser definidos con los itinerarios y requieren de servicios de orquestación especializados.

El lenguaje nativo en los ESB para representación de datos es el XML, que es considerado por la industria el vehículo ideal para el intercambio de datos estructurados entre aplicaciones.

Una SOA provee una abstracción que evita detalles referentes a la infraestructura necesaria en su implementación. Los servicios no necesitan saber de protocolos, ni de direccionamiento de mensajes y sólo se dedican a recibirlos (como eventos generados por el ESB) y procesarlos. El ESB es el encargado de proporcionar esta infraestructura y realizar el correcto direccionamiento de los mensajes.

La Figura 8 muestra un ejemplo de arquitectura de integración entre sistemas de una organización en base a un ESB. En medio se ve que diferentes tipos de aplicaciones se conectan al Bus de Servicios a través de diferentes adaptadores que usan distintos protocolos. Dentro del ESB la comunicación es transparente porque cada adaptador convierte el protocolo específico de la aplicación al protocolo común del ESB.

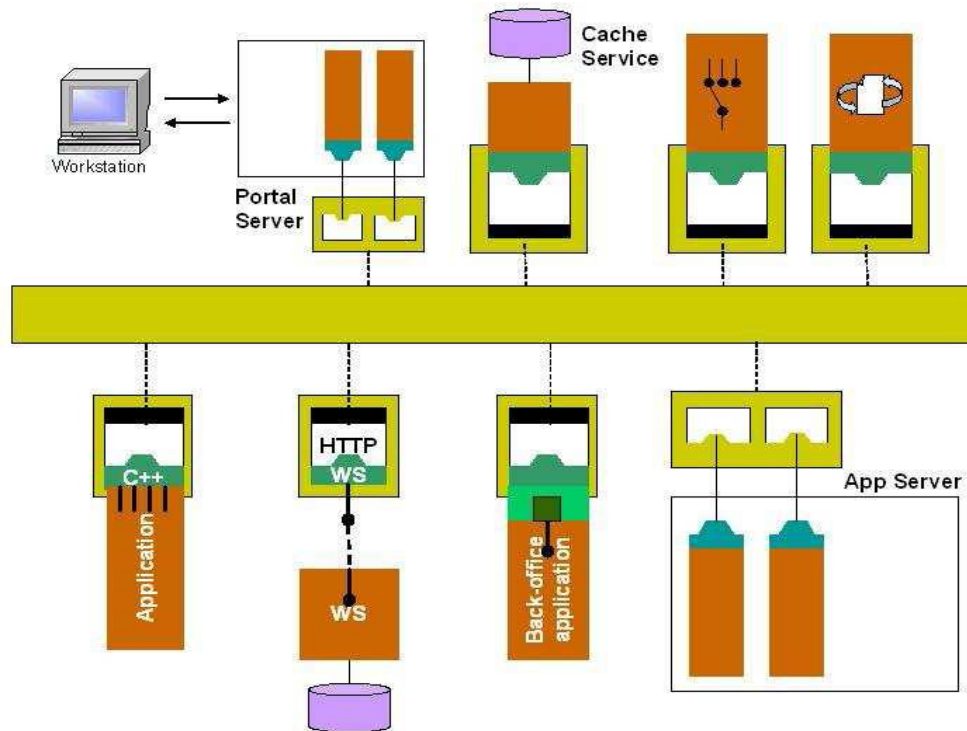


Figura 8 - Integración de sistemas de una organización utilizando un ESB

En [17] y [18] se puede encontrar más información sobre los ESB, sus funcionalidades y su uso para integrar sistemas.

Sección 2.3 Tecnologías de Web Services Geográficos

En esta sección se presentan los estándares de Web Services Geográficos, entrando en detalle en los más usados: Web Map Service (WMS)[23] y Web Feature Service (WFS)[24]. También se introduce el rol del Servidor de Mapas, un nuevo componente especializado que aparece en las arquitecturas de sistemas.

2.3.1 Web Services Geográficos

El Open Geospatial Consortium [15] es la organización que propone estándares de tecnología sobre datos espaciales. Hay estándares para la representación, almacenamiento e intercambio de información geográfica (modelos de datos), así como una Arquitectura de Referencia y múltiples estándares de diferentes tipos de servicios. Los servicios web que trabajan con datos espaciales son en su mayoría “Data Services”: tienen interfaces estandarizadas y bien conocidas y lo que cambia es el conjunto de datos que brindan.

A nivel de tecnologías, los Web Services GIS, más conocidos como OGC Web Services [16], están especificados en función de los estándares más simples de la web: el protocolo HTTP y el formato XML. Usando los métodos del protocolo HTTP (GET y POST) se realizan invocaciones a métodos fijos para enviar y recibir datos. Las descripciones de estos servicios describen principalmente la estructura de los datos que el Web Service ofrece, ya que los métodos son conocidos.

Para ofrecer información geográfica se puede usar tanto el estándar **WMS - Web Map Service** [23] como el estándar **WFS - Web Feature Service** [24]. Para descubrir las características de un servicio de información geográfica (particularmente las características de la información que provee) se usa el protocolo **CSW - Catalog Service for the Web** [25].

El protocolo estándar WMS [23] está pensado para generar vistas de los datos geográficos para el usuario final y ofrece tres métodos para publicar datos geográficos:

- **getCapabilities** – devuelve la descripción de los datos disponibles en el servicio.
- **getMap** – devuelve una imagen resultado de superponer las capas solicitadas, para el área solicitada de acuerdo a los parámetros de entrada.
- **getFeatureInfo** – devuelve los datos de las capas elegidas asociados a un par de coordenadas (con cierta tolerancia, que puede ser un radio). De acuerdo a la especificación del estándar este método es opcional.

El protocolo estándar WFS [24] está pensado para ofrecer acceso a datos geográficos a otras aplicaciones, ya que toda la información que recibe y envía es en formato XML. Este estándar solamente aplica a información geográfica vectorial. Este estándar define los siguientes métodos que tienen diferentes niveles de obligatoriedad:

1. **getCapabilities** – devuelve las características del servicio.
2. **describeFeatureType** – describe un tipo de información vectorial (como un XML Schema).

3. **getFeature** – solicitud de datos geográficos de acuerdo a los parámetros. Tiene similitud a un **SELECT** de **SQL**, ya que se puede elegir las capas a solicitar, qué atributos de estas se desea obtener y se pueden aplicar filtros.
4. **getGmlObject** – permite obtener cualquier elemento **GML** a partir de un identificador. Usando dicho identificador, el servidor **WFS** puede reenviar la solicitud a otros servidores si él no posee la información solicitada.
5. **Transaction** – permite modificar los datos ya que tiene varias formas de funcionamiento: **Insert**, **Delete** y **Update** (se pasa por parámetro la función a usar).
6. **LockFeature** – bloquea una entidad para realizar transacciones. Es un método opcional.

Si un servicio **WFS** ofrece los primeros tres métodos se dice que es un servicio **WFS básico** (ya que solamente permite consulta de datos). Si además ofrece el método **getGmlObject** es un **WFS** con **XLink**, esto significa que el servidor puede solicitar datos adicionales a otros servidores. Cuando un **WFS** básico ofrece el método **Transaction** se vuelve un **WFS Transaccional** (sigue siendo opcional el método **LockFeature**) ya que permite modificar los datos. Finalmente se considera **WFS-Transaccional** con **XLink** al servidor que ofrece los métodos del 1 al 5, este servidor puede hacer actualizaciones de datos y además solicitarlas a otros servidores.

El estándar CSW [25] define un servicio base de catálogos de información geográfica. Este estándar es extendido para soportar diferentes estándares de metadatos de información geográfica e incluso se ofrecen diferentes métodos de consulta para distintos estándares de metadatos. El catálogo permite a los proveedores de servicios de datos publicar sus características para ser localizados y describe detalladamente los datos que ofrece. Estas descripciones pueden ser hechas siguiendo distintos estándares de metadatos geográficos: **ISO 19115** o **FGDC** por ejemplo. El estándar de servicios de catálogos define métodos para publicar metadatos y para consultarlos. Además define una funcionalidad especial llamada “**Harvesting**” para recolectar metadatos alojados en otros servidores de catálogos, lo que permite que las consultas realizadas por usuarios puedan ser distribuidas.

Es de destacar que los estándares **WMS** y **WFS** prevén un conjunto de parámetros obligatorios y algunos opcionales, pero todos son funcionales. Es decir, estos protocolos no tienen incorporado ningún tipo de seguridad.

El **OGC** ha propuesto el estándar **GeoXACML** [27] como un estándar de seguridad para brindar Control de Acceso a los Servicios **WMS** y **WFS**. Este estándar define en detalle cómo describir y luego aplicar políticas de control de acceso extendiendo el estándar **XACML** [28]. Como es un estándar reciente aún no hay implementaciones del mismo en productos comerciales. En [49] se puede encontrar un análisis sobre el mismo y el diseño de un prototipo de servidor de seguridad.

2.3.2 Tecnologías de Web Services GIS y productos asociados

El software que provee los **OGC web Services** es conocido genéricamente como Servidor de Mapas [26] y puede correr tanto sobre un servidor Web como sobre un Servidor de Aplicaciones (dependiendo del producto).

Hay distintos productos de software que pueden ser clientes de un Servidor de Mapas. Si el cliente es web se lo llama Visualizador de Mapas (o simplemente Visualizador Web [26]) ya que las funciones que ofrecen son generalmente de consulta (al estilo Google Maps [29]). Los sistemas **GIS** desktop [26] tradicionales (centrados en producción y análisis de información geográfica) también han incorporado

funcionalidades para conectarse con Servidores de Mapas usando los protocolos estándares (WMS y WFS).

Como se ve en la Figura 9 el Servidor de Mapas atiende pedidos de la web que son enviados usando HTTP y se especializa en el acceso a diferentes tipos de fuentes de Información Geográfica.

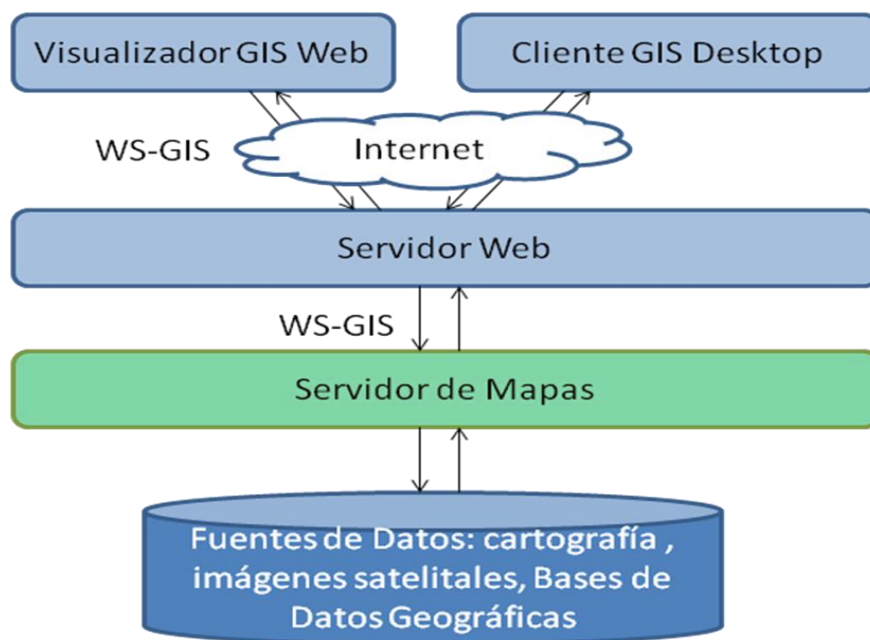


Figura 9 - Rol del Servidor de Mapas

El Servidor de Mapas expone la Información Geográfica que obtiene de distintos tipos de fuentes a través de los distintos tipos de Web Services Geográficos: WMS y WFS (en la figura los notamos como WS-GIS). Internamente el Servidor de Mapas se especializa en acceder a distintos tipos de fuentes de datos geográficos: imágenes satelitales, archivos shape y bases de datos geográficas. También tienen la posibilidad de conectarse a otros Servidores de Mapas a través de los Web Services Geográficos. De acuerdo al protocolo que se usan para publicar la información es el tipo de información que devuelven: desde XML y GML hasta imágenes PNG, JPG, GeoTiff y GIF.

Aunque hay diversos productos de Servidores de Mapas, al ofrecer servicios estándares pueden ser accedidos por cualquier software cliente que entienda los protocolos usados.

En el mercado hay una gran cantidad de productos Servidores de Mapas, tanto open source como propietarios que implementan los estándares de Web Services Geográficos. En [29] se presenta un relevamiento de los servidores de mapas actuales (publicado en Revista GeoFocus año 2010). Los más conocidos son MapServer [33] y GeoServer [34] en el mundo open source y ArcGIS Server[35] de ESRI. De la misma manera hay distintos productos de visualización web, desde componentes livianos en javascript como OpenLayers [31], hasta productos con características avanzadas para geoprocetamiento como i3geo[32]. A nivel de clientes Desktop algunos de los más usados son: gvSIG[39], QuantumGIS[40] y ArcGIS[35], que implementan clientes de web services geográficos.

Sección 2.4 Conclusiones

En este capítulo se presentaron los conceptos fundamentales sobre Plataformas de Gobierno Electrónico y las tecnologías en las que se apoyan. Dentro de dichas tecnologías se destaca el ESB como la Plataforma de Middleware para la integración de servicios, principalmente basados en WS-SOAP. Asimismo el ESB brinda soporte para las tecnologías avanzadas de Web Services SOAP: sus extensiones WS-* y en particular WS-Security.

A nivel de Información Geográfica, el mecanismo estándar para compartirla son los Web Services Geográficos: WMS y WFS.

La Gestión de la Información Geográfica a nivel estatal se plantea a través de una Infraestructura de Datos Espaciales que se apoya en estándares de Información Geográfica para compartir los datos, en particular en los de Web Services Geográficos. Al contar con una IDE es deseable integrar los servicios de Información Geográfica en las aplicaciones de negocio de Gobierno Electrónico. Algunas aplicaciones interesantes van desde servicios de seguridad social [5], aplicaciones meteorológicas [52] hasta planificación estratégica [50].

En la Figura 10 se muestra la Arquitectura planteada para la integración de Tecnologías de Información Geográfica a través de una Plataforma de Gobierno Electrónico. Ya existen por separado los Clientes GIS y los Servidores de Mapas, pero sus pedidos no pueden ser manejados por los Componentes de las Plataformas de Gobierno Electrónico: el Sistema de Seguridad y la Plataforma de Middleware. El GeoPortal es el único componente en la PGE especializado en Información Geográfica, pero sus tecnologías son de Interacción con usuarios finales. El GeoPortal funciona como otro cliente GIS alojado en la Plataforma de Gobierno Electrónico.

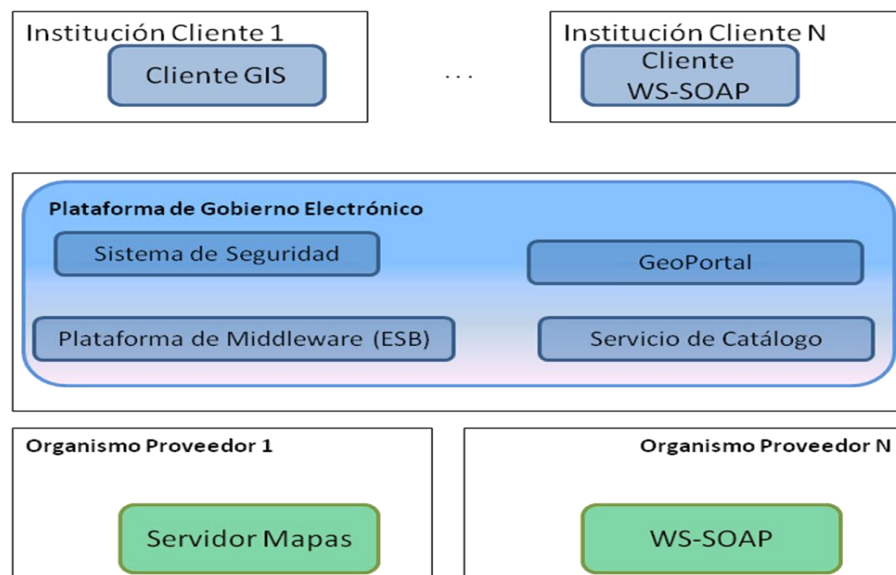


Figura 10 Arquitectura Planteada

Por un lado la Plataforma de eGov ya provee mecanismos de seguridad y una plataforma de middleware para interconectar aplicaciones entre organismos. Por otro lado dichos organismos pueden aprovechar

la Información Geográfica en sus procesos de negocio, es decir los servicios que brindan a los ciudadanos. Como hay un conjunto importante de productos que ya implementan los estándares de WS GIS y estos no son directamente compatibles con los estándares que usan las Plataformas de Gobierno Electrónico se plantean desafíos teóricos y prácticos interesantes para lograr esta integración.

Capítulo 3 – Análisis

En este capítulo se presentan escenarios relevantes de integración de servicios de información geográfica en una plataforma de gobierno electrónico. Si bien este es un análisis general se toma como plataforma de referencia la Plataforma de Gobierno Electrónico (PGE) de AGESIC Uruguay [2], tanto por interés en avanzar hacia la aplicación práctica de estas técnicas a nivel nacional, así como debido a las características avanzadas de la PGE que la convierten también en una plataforma modelo. Una primera versión de este análisis fue publicada en [51].

En primer lugar, la Sección 3.1 presenta los escenarios desde un punto de vista de las motivaciones y forma de uso. Luego, en la Sección 3.2, se presentan las características técnicas de los escenarios, estableciendo las componentes de software y protocolos que se utilizarían en cada uno. El objetivo es caracterizar técnicamente los escenarios, para analizar las situaciones de incompatibilidad entre protocolos GIS y SOAP. Finalmente, en la Sección 3.3 se realiza un análisis de los escenarios, resumiendo las características técnicas de cada uno, y analizando las principales diferencias entre los protocolos así como las consecuencias prácticas de las mismas, y finalmente detallando los principales problemas de compatibilidad que se detectan en el análisis realizado.

Sección 3.1 - Presentación de Escenarios

En esta sección se presentan los escenarios desde un punto de vista de uso y explicando las motivaciones prácticas para su existencia.

3.1.1 Público general consultando información

En la actualidad numerosos organismos generan información de interés público, que puede ser utilizada tanto por otros organismos como por los ciudadanos o público en general. Este tipo de información es la básica sobre el territorio y debe tenerse publicada la última versión oficial. Como ejemplo podemos considerar el mapa político con los límites oficiales, la orografía, mapas topográficos, etc. En Uruguay el organismo que genera la cartografía oficial es el Servicio Geográfico Militar del Ministerio de Defensa [22]. Esta información es considerada básica y puede tener cambios en largos períodos de tiempo, sobre todo cuando hay avances tecnológicos que permiten generar una nueva versión del conjunto de datos con mayor exactitud.

Asimismo, cabe tener en cuenta la información catastral y de infraestructura vial (caminería), que es provista tanto por organismos centrales como municipales, y que resulta de gran interés de consulta por el público en general.

En este escenario, que llamaremos “Consulta de información pública”, se prevé que la información publicada sea solamente de consulta ya que es de interés general. Por esto no se requieren controles estrictos de seguridad en el acceso a la información; sin embargo, es posible que se necesiten mecanismos de control para asegurar la disponibilidad. A nivel de protocolos esta información se puede brindar a través de servicios OGC [16] tanto WMS como WFS de sólo lectura.

Este escenario está pensado para ofrecer información básica general, de los tipos descriptos antes, al público. Si bien esta información estará disponible para el público en general, pero también puede ser de utilidad para funcionarios de diferentes organismos del estado. La información puede ser accedida

desde visualizadores web o desde aplicaciones SIG de escritorio para realizar cruzamiento con información propia del usuario. Esto nos permite tener una única fuente referencia de información básica oficial, confiable y catalogada con sus metadatos.

Este escenario requiere el uso de mecanismos de auditoría para monitorear el uso del servicio y asegurar la disponibilidad del servicio. A medida que vaya creciendo la demanda sobre el servicio se deberá prever que la plataforma pueda soportarlo.

3.1.2 Público especializado consultando información

Algunos organismos pueden generar información de particular interés para otros organismos. Esto evitaría que el cliente tenga que asumir la tarea de generarlos, cuando ya hay un organismo experto en la generación de dicha información. Este caso puede ser el de la información meteorológica, que la genera la Dirección Nacional de Meteorología del Ministerio de Defensa [38]. La información meteorológica (tanto histórica como los pronósticos) es de especial utilidad para estudios medioambientales y para establecer acciones ante emergencias climáticas. Aunque la información meteorológica se publica a los ciudadanos por diferentes medios, allí se brinda resumida y para cortos períodos de tiempo.

En este escenario, que llamaremos “Servicios para públicos específicos”, un organismo especializado en determinado tipo de información geográfica brinda servicios específicos para otro organismo de acuerdo a los requerimientos del organismo cliente. Dicha información se puede publicar tanto por WMS como WFS de sólo lectura ya que será accedida solamente para consulta. Se deberán proveer mecanismos de seguridad para control de acceso para asegurar que quienes acceden a estos servicios sean de los organismos para quienes fueron desarrollados. Esto es particularmente importante con datos que deben ser protegidos.

Este escenario permite que un organismo cliente pueda tener un acceso seguro a la información geográfica que necesita según los acuerdos que realice con el organismo proveedor de dicha información. Esto permite optimizar la generación de la información y que no se tengan que duplicar tareas generando la información en la organización cliente.

La limitación principal de este escenario es que el organismo cliente puede no cumplir sus funciones si no tiene acceso a la información provista por el organismo proveedor. Se debe asegurar la disponibilidad del servicio para que el organismo cliente pueda usar la información en sus tareas.

3.1.3 Instituciones colaborando en la generación de información geográfica

Muy frecuentemente, un organismo es responsable de un conjunto de datos pero no tiene la posibilidad de mantenerlo adecuadamente actualizado. Esto puede pasar con organismos que tienen jurisdicción sobre grandes áreas del territorio. En algunos casos se tiene la posibilidad de trabajar en conjunto con organismos locales que conocen el territorio más de cerca. Esto motiva que con la colaboración de organismos locales, se pueda actualizar el conjunto de datos global con mayor frecuencia y a menor costo.

Este escenario, que llamaremos “Colaboración para la generación de información geográfica”, se basa en que el organismo central tiene acuerdos con los organismos locales para colaborar en la actualización de determinada información. Para esto el organismo central brinda un servicio que permita a los

organismos colaboradores actualizar la información. Esto se puede hacer a través de un servicio WFS transaccional y requiere seguridad adicional para validar que quiénes actualizan la información son los habilitados para hacerlo. A nivel del organismo central se deberá ir validando la actualización de la información y consolidándola en nuevas versiones del conjunto de datos.

Como ejemplo podemos considerar que el Ministerio de Transporte y Obras Públicas (MTOP)[46] es responsable de las rutas nacionales, pero podría contar con la colaboración de las Intendencias para mantener la información sobre su estado actualizada.

Este escenario tiene como limitación el requerir un fuerte control de seguridad para asegurar que quién actualiza la información es realmente un funcionario de un organismo colaborador. A su vez, es recomendable que el organismo central tenga un conjunto de datos oficial y otro conjunto de datos “en edición” hasta validar la información que recibe de sus colaboradores.

3.1.4 Instituciones colaborando en trámites

Es muy común que uno o varios organismos que tienen participación en un mismo trámite público, deben compartir datos para lograr brindar un servicio a los ciudadanos. Tradicionalmente el ciudadano consultaba información (en un formulario) en un organismo y lo llevaba a otro para realizar un trámite. Esto se puede hacer más eficientemente si el segundo organismo consulta online dicha información, ahorrándole tiempo y costos al ciudadano. Esto ocurre por ejemplo con la información catastral al realizar modificaciones sobre los padrones o la propiedad.

Este escenario, que llamaremos “Colaboración para la realización de procesos administrativos”, requiere que ambos organismos hagan un acuerdo de datos a intercambiar, teniendo presente el proceso (o los procesos) en que está involucrado el intercambio. Para fijar ideas, podemos decir que el segundo organismo es cliente del primero. Entonces ambos organismos deben acordar qué consulta tiene que permitir el proveedor que el cliente realice (parámetros de entrada y datos de retorno) y en qué condiciones se puede usar dicha consulta. Puede ocurrir que la misma consulta pueda ser usada por diferentes clientes en diferentes condiciones (para diferentes procesos). Por esto los organismos que intervienen en el proceso deben acordar cómo se comunican el contexto del proceso en el que están trabajando.

En un caso más general, puede ocurrir que un proceso requiera la intervención de varios organismos en determinado orden, por lo que se deberá resolver nuevamente el problema del contexto del trámite y la coordinación del orden de intervención de los organismos. Otro problema que surge es que puede darse intercambio de información sensible, por lo que se requieren mecanismos de seguridad específicos, tanto para el acceso a las consultas, como para la transmisión de la información. Mientras que en el escenario anterior el objeto de la colaboración era la gestión de información geográfica, en este escenario se apunta a mejorar la gestión de procesos en general que utilizan información geográfica, siendo por lo tanto de aplicación mucho más amplia.

Dado que los procesos administrativos generalmente son gestionados desde sistemas de expediente, este escenario requerirá la integración del intercambio de información geográfica en dichos sistemas. Los usuarios destinatarios de este escenario son los funcionarios de los organismos involucrados en el proceso administrativo.

Este escenario ofrece la ventaja de incrementar la interacción online de los organismos, permitiendo agilizar los procesos administrativos y brindar mejores servicios a los funcionarios. Los principales

problemas para implementar este escenario son: la buena coordinación institucional (para lograr coordinar los sistemas de diferentes organismos) y el crecimiento de la complejidad cuando participan más de dos organizaciones. Aquí aparece una oportunidad de usar los servicios de coordinación de procesos de la Plataforma de Gobierno Electrónico.

De acuerdo al tipo de proceso puede ser necesario tanto brindar servicios de consulta de información, como servicios de actualización de información.

3.1.5 Público generando Información Geográfica

En varias áreas de aplicación es interesante contar con información provista por los usuarios y permitir la participación ciudadana. Esta modalidad se conoce en la literatura de GIS como Volunteered Geographic Information [43]. La modalidad VGI se puede aplicar al reporte de información del territorio sobre diferentes temas: estado de pavimento, tránsito, ocurrencia de fenómenos climáticos puntuales, etc. Para esto son necesarios mecanismos para que los ciudadanos puedan ingresar información y poder controlar el ciclo de vida de dicha información. Por un lado hay que brindar mecanismos amigables para que los ciudadanos puedan ingresar información fácilmente; pero por otro lado hay que auditar el proceso de ingreso de datos para lograr buena confianza en esos datos. Sin olvidar que para estimular la participación es necesario que la información ingresada quede accesible inmediatamente para la comunidad. Ejemplo: monitoreo medioambiental, reporte estadístico.

Este escenario, que llamaremos “Generación Comunitaria de Datos (VGI⁴)”, requiere que el organismo interesado en generar una comunidad para la generación colaborativa de datos geográficos brinde un sitio completo para esta comunidad. El usuario registrado en la comunidad podrá ingresar información, generalmente de granularidad muy fina (una ocurrencia de algún fenómeno en un punto), y consultar la información ingresada por otros miembros de la comunidad.

Este escenario nos permite tener información voluntaria de los ciudadanos que de otra forma sería muy difícil o costosa de obtener siguiendo los procedimientos tradicionales de generación de información geográfica. Aunque esta información no sea exhaustiva, puede ser usada como un insumo extra para análisis espaciales en organismos públicos y a su vez servir de referencia para los integrantes de la comunidad.

⁴ VGI: Volunteered Geographic Information

Sección 3.2 – Análisis Técnico de Escenarios

Esta sección presenta las características técnicas de los escenarios introducidos en la sección anterior.

3.2.1 Escenario I – Información Pública

Este escenario se caracteriza por incluir servicios de información geográfica pública destinados al público en general así como a funcionarios del estado. La información se publica por servicios web que pueden ser accedidos tanto desde Visualizadores en la Web como desde un software GIS de escritorio.

La IDE estatal tendrá su propio geoportal alojado en la Plataforma de Gobierno Electrónico, siendo este uno de los sitios a los que el público en general podrá acceder.

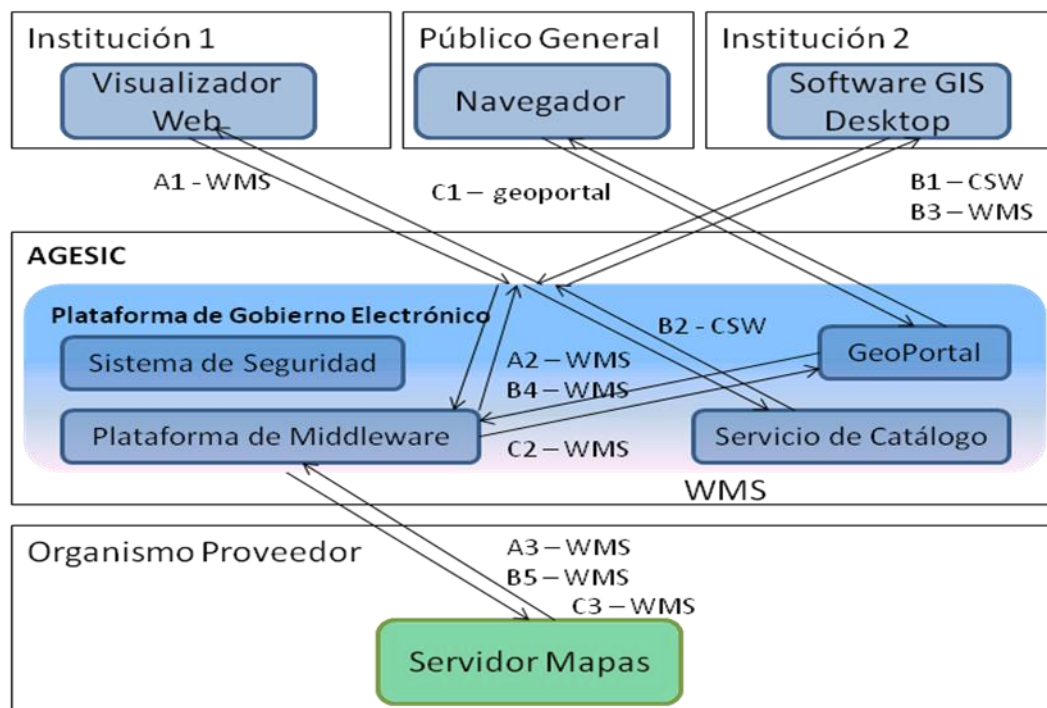


Figura 11 - Escenario de Información Pública

En la Figura 11 se muestra la arquitectura y el funcionamiento general de este escenario. Se consideran diferentes organismos: un Organismo Proveedor de la Información, la Plataforma de AGESIC como mediadora y varios clientes que pueden ser tanto instituciones como público en general. También se aprecia que al ofrecer la información geográfica a través de servicios estándar, se puede usar una variedad de clientes. En el dominio de AGESIC se muestra la Plataforma de Gobierno Electrónico y los servicios necesarios para este escenario.

En la Figura 11 se muestran los flujos de invocaciones que generan distintos tipos de usuarios al acceder a la información geográfica. El Flujo A (pasos A1, A2, A3) muestra cómo un usuario de una institución accede desde un Visualizador Web. El Flujo B (pasos B1, B2, B3, B4 y B5) muestra cómo un usuario avanzado consulta el catálogo de servicios y luego de conocer los datos del servicio realiza invocaciones

usando el protocolo WMS. El Flujo C (pasos C1, C2, C3) representa las invocaciones que se hacen cuando un usuario del público general acceder al Geoportal de la PGE.

Finalmente se muestra que el Organismo Proveedor solamente tiene que ofrecer servicios de mapas simples, dejando la complejidad de las comunicaciones en la Plataforma de Gobierno Electrónico. En las siguientes secciones entraremos en detalle sobre las interacciones que se muestran en la Figura 11.

Desde el punto de vista de seguridad y robustez lo que se prevé es balanceo de carga para asegurar la Calidad de Servicio (QoS) y permitir la protección ante posibles ataques de Denegación de Servicio (DoS).

Forma de Uso de la Plataforma

En este escenario la PGE tiene un rol de mediador ofreciendo además el Servicio de Catálogo, que sirve a los usuarios para localizar la información que necesitan. Como los Servicios de Mapas son Data Services, los metadatos almacenados en el Servicio de Catálogo contienen la descripción de la información que brinda el Organismo Proveedor.

En el caso A, el Servicio de Catálogo lo usa un desarrollador para programar en el visualizador web el acceso directo al servicio de mapas del Organismo Proveedor. En el caso B un usuario avanzado usa el Servicio de Catálogo para descubrir online la información disponible. Luego que elige el servicio que necesita configura su cliente desktop para que realice los pedidos al Servicio de Mapas. En el caso C el usuario (Público General) accede al Geoportal para consultar la información publicada. En este caso el Geoportal ya conoce el servicio que necesita.

En todos los casos los pedidos al Servicio de Mapas del Organismo Proveedor pasar por el mediador de la Plataforma de Gobierno Electrónico. De este modo la Plataforma puede proteger al servicio proveedor regulando la cantidad de pedidos que le envía y pudiendo aplicar estrategias de defensa ante ataques de DoS (Denial Of Service).

En resumen, en este escenario la plataforma brinda el acceso al servicio proveedor para los distintos tipos de clientes realizando una virtualización de servicios (siendo mediador de localización). Esto le permite realizar balanceo de carga y aplicar protección ante ataques.

Protocolos

En el esquema de la Figura 11 se muestra que los datos son accedidos mediante protocolo WMS. Como se describe en la sección 2.3, este protocolo es el más simple y eficiente para el acceso a información geográfica por parte de usuarios finales. El Organismo Proveedor puede ofrecer además servicios WFS básicos para los usuarios más avanzados que quieran obtener una versión procesable de los datos geográficos.

Para documentar qué información se está proveyendo se usan metadatos de información geográfica que se publican a través del protocolo CSW que es implementado por el Servicio de Catálogo. En este servicio se publica la estructura de la información geográfica, la temática, sus condiciones de uso (entre otros metadatos estándar de IG) y también la dirección del servicio de mapas que los brinda.

La restricción que plantea este escenario es que para acceder a los datos el cliente debe usar el mismo protocolo que el proveedor. El protocolo WMS es el más extendido en su uso y a no ser por problemas de versiones, no debería haber grandes incompatibilidades que impidan el acceso a la información. En el caso del protocolo WFS puede haber mayor variación ya que el protocolo define un conjunto de

operaciones obligatorias y otras opcionales. Si el usuario requiere alguna de las operaciones opcionales puede no tenerlas disponibles.

Tipos de Operaciones

Considerando el protocolo WMS los usuarios usarán (a través de los distintos clientes) las siguientes operaciones:

- **WMS – getMap** – esta operación recibe un conjunto de parámetros (lista de capas, área solicitada, tamaño de la imagen resultado, etc.) y devuelve una imagen que es la representación gráfica de la información solicitada (generalmente recibirá la información geométrica o espacial, pero no la información temática detallada). Esto es un mapa pensado para un usuario final que no es procesable automáticamente (solamente sirve para visualización). Si el usuario final desea obtener detalle de la información temática usará la siguiente operación.

- **WMS – getFeatureInfo** – esta operación recibe un conjunto de parámetros (lista de capas, punto de referencia, área de trabajo, etc.) y devuelve la información temática de las geometrías presentes en el punto de referencia (o cercanas con cierto radio de tolerancia). Entre los parámetros opcionales se puede considerar un límite máximo de “registros” a devolver.

El protocolo WFS tiene operaciones equivalentes de consulta de datos pero siempre devuelven la información en GML, permitiendo que el usuario reciba una “copia” digital completa de los datos. De esta forma el usuario podría realizar procesamientos posteriores con la información consultada.

En relación a los tipos de datos que se manejan y a su granularidad, como WMS devuelve una imagen de acuerdo al tamaño pedido, no surge un problema de sobrecarga en la información transferida ante una solicitud de una gran cantidad de entidades. Otra característica importante es que el WMS puede manejar tanto información vectorial como información raster para generar la imagen resultado. El protocolo WFS solamente maneja información vectorial y usa formatos XML para representar todas las variedades de datos: puntos, líneas, polígonos, etc.

Actores Involucrados

En este escenario el actor principal es el usuario final que accede a la información geográfica a través de distintos sistemas cliente: geoportal, visualizador web o cliente GIS desktop.

El mediador en las comunicaciones de acceso a la información geográfica es la PGE.

Finalmente quién juega el rol de proveedor es el Organismo que publica la Información Geográfica.

Mecanismos de Seguridad

Este escenario solamente requiere servicios de auditoría como mecanismo de seguridad (con baja prioridad), ya que la información publicada y accedida es pública y el usuario puede ser anónimo. Además de esto, se requiere que la Plataforma de Gobierno Electrónico brinde servicios de seguridad para asegurar el nivel del servicio proveedor; esto es, mecanismos de defensa ante posibles ataques y mecanismos de optimización en el uso de las comunicaciones.

Productos de Software

En este escenario se requiere el uso de los siguientes productos de software:

- Servidor de Mapas - servicios base en el Organismo Proveedor.
- Servidor Web – tanto para el geoportal como para el visualizador web.
- Servidor de Aplicaciones – para brindar el Catálogo de Servicios.
- ESB – cumple tareas de ruteo como Plataforma de Middleware para la mediación en la invocación de los servicios del organismo proveedor.
- Clientes - geoportal, visualizador web, software GIS

Coordinación Institucional

La implementación de este escenario requiere que el Organismo Proveedor coordine con AGESIC como organismo gestor de la Plataforma de Gobierno Electrónico. Esta coordinación se realiza en varios niveles.

A nivel técnico se requieren los acuerdos para establecer la mediación. El Organismo Proveedor debe establecer los Términos de Uso de la información geográfica que publica (aunque sean datos públicos se pueden establecer restricciones en su uso).

A más alto nivel, de la negociación entre el Organismo Proveedor y AGESIC surgirá la política de Nivel de Servicio que tendrá el servicio de mapas que se ofrece a través de la Plataforma de Gobierno Electrónico.

3.2.2 Escenario II – Servicios para públicos específicos

Este escenario está pensado para públicos específicos, que necesitan acceder a información detallada de un organismo proveedor. La información se publica a través de servicios web estándar para que pueda ser accedida por los clientes que la necesitan. El público serán funcionarios especializados que usan un Software GIS Desktop. Además del rol de mediador, la Plataforma de Gobierno Electrónico (PGE) realiza controles de Seguridad (autenticación y autorización).

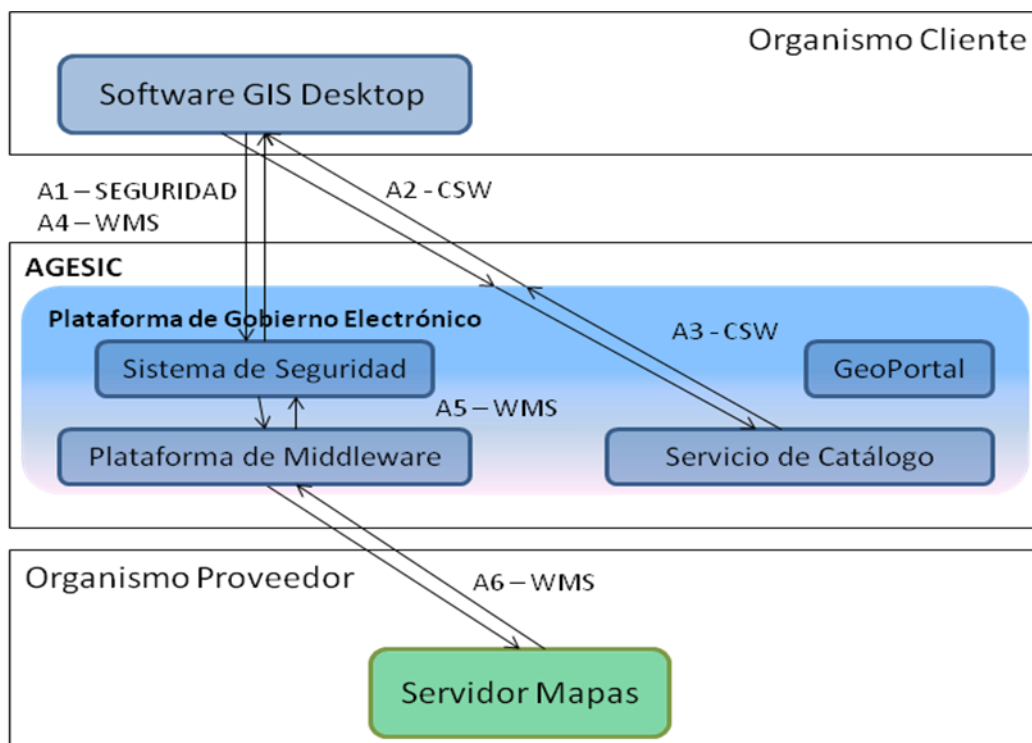


Figura 12 - Escenario de Información para público específico

En la Figura 12 se muestra la arquitectura y el funcionamiento general de este escenario. Se consideran diferentes organismos: un Organismo Proveedor de la Información, la PGE como mediadora y un Organismo Cliente que es el que requiere la información específica. Como esta información específica está pensada para los funcionarios de un Organismo Cliente, se usará el Sistema de Seguridad de la PGE para controlar accesos no autorizados a la información.

En este escenario se presenta un flujo de uso (A) en el que el usuario debe autenticarse ante los mecanismos de seguridad. Luego de esto puede consultar el servicio de catálogo para localizar la información que necesita. Con la información de localización de la información podrá realizar pedidos al Organismo Proveedor que pasarán siempre por el Sistema de Seguridad de la PGE. Los pedidos también pasan por la Plataforma de Middleware que brinda los mecanismos de localización del proveedor del servicio.

Forma de Uso de la Plataforma

En este escenario la PGE tiene un rol de mediador ofreciendo Servicios de Seguridad y el Servicio de Catálogo, que sirve a los usuarios para localizar la información que necesitan. Como los Servicios de

Mapas son Data Services, los metadatos almacenados en el Servicio de Catálogo contienen la descripción de la información que brinda el Organismo Proveedor.

Los usuarios deberán autenticarse para poder consultar la información específica y pasar controles de acceso de la PGE para asegurar que tiene los permisos para acceder a dicha información.

Luego de autenticado, el usuario avanzado usa el Servicio de Catálogo para descubrir online la información disponible. Hecho esto, elige el servicio que necesita y configura su cliente desktop para que realice los pedidos al Servicio de Mapas.

En todos los casos los pedidos al Servicio de Mapas del Organismo Proveedor pasar por el Sistema de Seguridad para que la PGE pueda aplicar las políticas de control de acceso a los datos. De allí el pedido pasará por el mediador de la PGE. De este modo la PGE puede proteger al servicio proveedor regulando la cantidad de pedidos que le envía y pudiendo aplicar estrategias de defensa ante ataques de DoS (Denial Of Service).

En resumen, en este escenario la plataforma brinda el acceso al servicio proveedor aplicando políticas de seguridad y realizando una virtualización de servicios (siendo mediador de localización). Esto le permite aplicar controles para asegurar la información, realizar balanceo de carga y aplicar protección ante ataques.

Protocolos

En el esquema de la Figura 12 se muestra que los datos son accedidos mediante protocolo WMS. Como se describe en la sección 2.3, este protocolo es el más simple y eficiente para el acceso a información geográfica por parte de usuarios finales. El Organismo Proveedor puede ofrecer además servicios WFS básicos para los usuarios que quieran obtener una versión procesable de los datos geográficos.

Para documentar qué información se está proveyendo se usan metadatos de información geográfica que se publican a través del protocolo CSW que es implementado por el Servicio de Catálogo. En este servicio se publica la estructura de la información geográfica, la temática, sus condiciones de uso (entre otros metadatos estándar de IG) y también la forma de acceder al servicio de mapas que los brinda. Esto no quita que el acceso se realiza a través de la PGE para usar la seguridad que la misma brinda.

La restricción que plantea este escenario es que para acceder a los datos el cliente debe usar el mismo protocolo que el proveedor. El protocolo WMS es el más extendido en su uso y tiene amplio soporte en los clientes desktop. En el caso del protocolo WFS se considera que para consultar información solamente se usarán los métodos del WFS Básico. Pudiendo el usuario usar cualquiera de los dos si el proveedor los soporta.

En lo que respecta a la PGE, los servicios de Seguridad se basan en los protocolos WS-Security que extienden la especificación de WS SOAP para permitir agregar credenciales de la identidad del usuario (y su pertenencia al organismo cliente). Los protocolos WMS y WFS no permiten el agregado de nuevos parámetros para mantener la sesión. Por esto, la responsabilidad de autenticar al usuario y aplicar los controles de acceso a lo largo de la sesión es una tarea compleja que debe realizar la PGE.

Tipos de Operaciones

Considerando el protocolo **WMS** los usuarios usarán las siguientes operaciones:

- **WMS – getMap** – esta operación recibe un conjunto de parámetros (lista de capas, área solicitada, tamaño de la imagen resultado, etc.) y devuelve una imagen que es la representación gráfica de la información solicitada (generalmente recibirá la información geométrica o espacial, pero no la información temática detallada). Esto es un mapa pensado para un usuario final que no es procesable automáticamente (solamente sirve para visualización). Si el usuario final desea obtener detalle de la información temática usará la siguiente operación.

- **WMS – getFeatureInfo** – esta operación recibe un conjunto de parámetros (lista de capas, punto de referencia, área de trabajo, etc.) y devuelve la información temática de las geometrías presentes en el punto de referencia (o cercanas con cierto radio de tolerancia). Entre los parámetros opcionales se puede considerar un límite máximo de “registros” a devolver.

El protocolo **WFS** provee operaciones equivalentes de consulta de datos pero siempre devuelven la información en GML, permitiendo que el usuario reciba una “copia” digital completa de los datos. De esta forma el usuario podría realizar consultas más complejas y procesamientos posteriores con la información consultada.

- **WFS – getFeature** – esta operación permite realizar consultas complejas pudiendo seleccionar qué capas se consultan, qué atributos se desean obtener y aplicar filtros (incluso condiciones espaciales) para obtener resultados en GML. De esta forma el software cliente puede obtener datos para hacer procesamientos posteriores.

En relación a los tipos de datos que se manejan y a su granularidad, como WMS devuelve una imagen de acuerdo al tamaño pedido, no surge un problema de sobrecarga en la información transferida ante una solicitud de una gran cantidad de entidades. Otra característica importante es que el WMS puede manejar tanto información vectorial como información raster para generar la imagen resultado. El protocolo WFS solamente maneja información vectorial y usa formatos XML para representar todas las variedades de datos: puntos, líneas, polígonos, etc.

En lo referente a las operaciones sobre la PGE, se requiere que brinde algún tipo de servicio de Autenticación y que luego aplique controles de acceso para asegurar que es el mismo usuario que autenticó el que está accediendo a la información. En la PGE de AGESIC la autenticación se realiza usando WS-Security y WS-Trust manejando identidad federada entre los diferentes organismos del estado.

Actores Involucrados

En este escenario el actor principal es un funcionario del Organismo Cliente que accede a la información geográfica a través de un cliente GIS desktop.

El mediador en las comunicaciones de acceso a la información geográfica es la PGE. La PGE también es la que brinda los servicios de seguridad y control de acceso.

Finalmente quién juega el rol de proveedor es el Organismo que publica la Información Geográfica.

Mecanismos de Seguridad

Este escenario requiere un fuerte uso de mecanismos de seguridad: Autenticación y Autorización, para asegurar que solamente los funcionarios del Organismo Cliente acceden a la información publicada por el Organismo Proveedor. También se usarán servicios de auditoría como mecanismo secundario de seguridad (con baja prioridad).

Además de esto, se requiere que la Plataforma de Gobierno Electrónico brinde servicios de seguridad para asegurar el nivel del servicio proveedor; esto es, mecanismos de defensa ante posibles ataques y mecanismos de optimización en el uso de las comunicaciones.

Productos de Software Involucrados

En este escenario se requiere el uso de los siguientes productos de software:

- Servidor de Mapas - servicios base en el Organismo Proveedor.
- Servidor de Aplicaciones – para brindar el Catálogo de Servicios.
- ESB – cumple tareas de ruteo como Plataforma de Middleware para la mediación en la invocación de los servicios del organismo proveedor.
- Clientes - software GIS desktop

Es de destacar que el cliente GIS desktop puede necesitar ser adaptado para poder cumplir los mecanismos de seguridad (autenticación y autorización).

Coordinación Institucional

La implementación de este escenario requiere que los Organismos (Proveedor y Cliente) coordinen entre ellos la especificación de la información a proveer/consultar. Además, ambos organismos deber coordinar con AGESIC como organismo gestor de la PGE, la forma de implementar la comunicación a través de la PGE y de definir las políticas de seguridad.

A nivel técnico se requieren los acuerdos para establecer los controles de seguridad y la mediación. Esto abarca desde las credenciales que presentarán los clientes hasta la dinámica de definición de las políticas de seguridad.

En otro nivel, el cliente y el proveedor deberán acordar la estructura de los datos a publicar, el nivel de detalle, la cobertura y la frecuencia de actualización, entre otros ítems.

A más alto nivel, de la negociación entre el Organismo Proveedor y AGESIC surgirá la política de Nivel de Servicio que tendrá el servicio de mapas que se ofrece a través de la PGE, de acuerdo al uso que se haga de las prestaciones de mediación.

3.2.3 Escenario III – Colaboración inter-institucional para la generación de Información Geográfica

Este escenario está pensado para la colaboración entre organismos en la generación de Información Geográfica. Los usuarios serán funcionarios de las Instituciones que colaboren con el Organismo Proveedor. Dicho organismo ofrecerá a sus colaboradores un servicio WFS-Transaccional a través del cual podrán ingresar y actualizar información. El Organismo Proveedor a su vez ofrece la información a otras instituciones para su consulta. La Plataforma de Gobierno Electrónico (PGE) cumple el rol de mediador y brinda los servicios de seguridad.

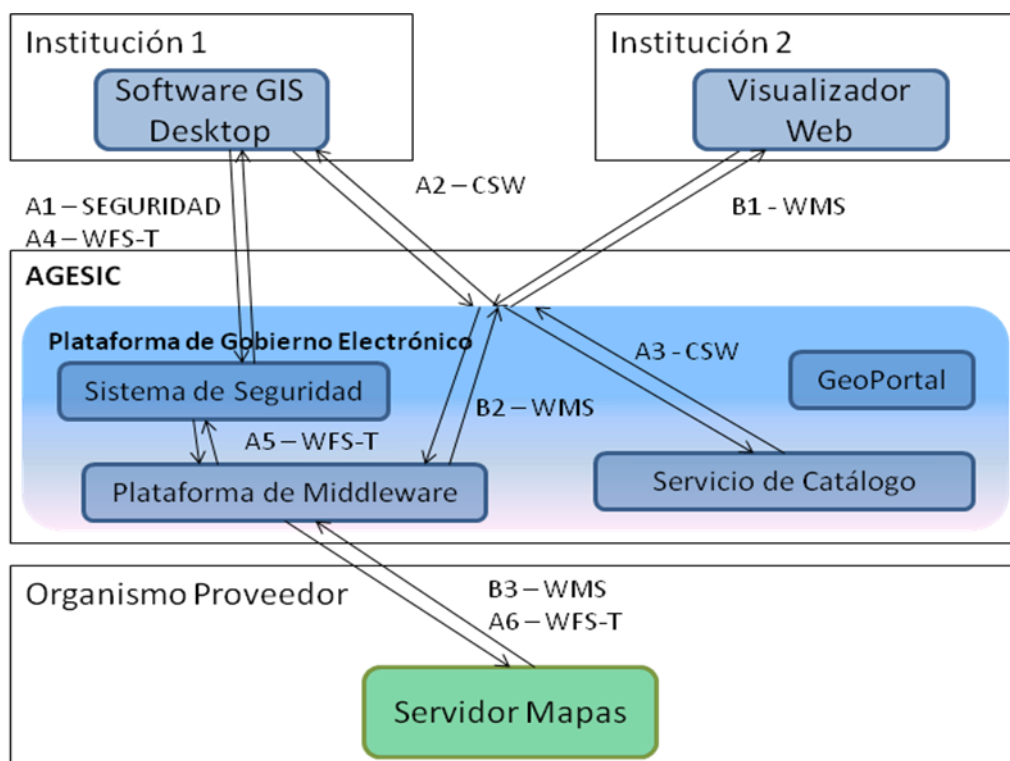


Figura 13 - Escenario de Colaboración para la Generación de Información Geográfica

En la Figura 13 se ve que la Institución 1 es una institución colaboradora, cuyos funcionarios, con los debidos controles de seguridad, pueden acceder al servicio WFS-T para ingresar información (Flujo A). Es posible que dichos funcionarios tengan que localizar el servicio a través de servicio de catálogo (pasos A2, A3).

En el Flujo B se muestra como otras instituciones consultan la información generada por las instituciones colaboradoras, accediendo a los servicios del Organismo Proveedor. Este acceso podría darse en las condiciones del Escenario I o del Escenario II. Además, el Organismo Proveedor puede realizar internamente la validación de la información que recibe de sus colaboradores. Esto le permite, por ejemplo, tener una versión de los datos recién recibidos y otra versión de los datos validados.

Forma de Uso de la Plataforma

En este escenario la PGE tiene un rol de mediador ofreciendo Servicios de Seguridad y el Servicio de Catálogo, que sirve a los usuarios para localizar la información que necesitan. Como los Servicios de Mapas son Data Services, los metadatos almacenados en el Servicio de Catálogo contienen la descripción de la información que brinda el Organismo Proveedor.

Los usuarios de las instituciones colaboradoras deberán autenticarse para poder ingresar y actualizar la información del Organismo Proveedor.

Luego de autenticado, el usuario avanzado puede usar el Servicio de Catálogo para descubrir la localización de los servicios WFS-T. Luego que elige el servicio que necesita, configura su cliente desktop para que se conecte al Servicio de Mapas.

En todos los casos los pedidos al Servicio de Mapas del Organismo Proveedor pasar por el Sistema de Seguridad para que la PGE pueda aplicar las políticas de control de acceso, permitiendo solamente el acceso a los funcionarios de las instituciones colaboradoras. De allí los pedidos pasarán por el mediador de la PGE. De este modo la PGE puede proteger al servicio proveedor regulando la cantidad de pedidos que le envía y pudiendo aplicar estrategias de defensa ante ataques de DoS (Denial Of Service).

En resumen, en este escenario la plataforma brinda el acceso al servicio proveedor aplicando políticas de seguridad y realizando una virtualización de servicios (siendo mediador de localización). Esto le permite aplicar controles para asegurar el acceso de escritura, realizar balanceo de carga y aplicar protección ante ataques.

Protocolos

El centro de este escenario es el protocolo WFS-Transaccional ofrecido por el Organismo Proveedor para que los funcionarios de las Instituciones Colaboradoras puedan acceder y modificar la información geográfica que les corresponde.

Además se puede requerir emplear el protocolo CSW para localizar los servicios deseados (o conocer su especificación detallada). También se usará el protocolo WMS para publicar la información generada colaborativamente.

Este escenario requiere que el Organismo Proveedor y las Instituciones Colaboradoras acuerden el formato de los datos a ingresar y su representación. Por ejemplo, las carreteras pueden representarse con líneas continuas o con secuencias de segmentos de líneas, e incluso se podrían emplear polígonos si queremos representar su superficie.

Por su parte, la PGE para brindar la seguridad emplea protocolos WS-Security para permitir la autenticación de los usuarios y el control de la autorización.

Tipos de Operaciones

Considerando el protocolo WFS-T los usuarios necesitarán las siguientes operaciones:

- **WFS - getFeature** – se usará para obtener la información actual. Dicha información puede ser editada o solamente usada como referencia.

- **WFS - Transaction** – se usará para editar la información correspondiente. Generalmente se editará un tipo de datos por vez (una capa) y se trabajará en una entidad geográfica a la vez. Esta operación recibe como uno de sus parámetros la función que se desea que se ejecute con los datos transferidos: Insert, Update, Delete.

- **WFS - LockFeature** –esta es una operación opcional que se podrá usar para evitar que dos usuarios editen la misma entidad a la vez, si el software cliente y el servidor de mapas la soportan.

Para conocer la estructura de los datos a la hora de editarlos, el cliente puede usar el método WFS – DescribeFeatureType. Esto le da la estructura en la que deberá ingresar los datos pero no la lógica de la representación. Como el protocolo WFS trabaja con estructuras XML se pueden intercambiar datos de cualquier granularidad: desde un solo objeto geográfico hasta un conjunto completo.

Este escenario también presenta la posibilidad de que luego se consulte la información actualizada mediante el protocolo WMS. Su uso y las operaciones que provee ya fueron presentados en el Escenario I.

Actores Involucrados

En este escenario los actores principales son los funcionarios de las Instituciones Colaboradoras que acceden a través de un cliente GIS desktop a los servicios del Organismo Proveedor para actualizar la información geográfica.

El mediador en las comunicaciones de acceso a la información geográfica es la PGE. La PGE también es la que brinda los servicios de seguridad y control de acceso.

Finalmente quién juega el rol de proveedor es el Organismo Proveedor que permite que actualicen su información. Luego el Organismo Proveedor puede publicar la información actualizada, pudiendo realizar controles de calidad de la misma en el proceso.

Mecanismos de Seguridad

Este escenario requiere un fuerte uso de mecanismos de seguridad: Autenticación y Autorización, para asegurar que solamente los funcionarios de las Instituciones Colaboradoras puedan acceder a actualizar la información del Organismo Proveedor. También se usarán servicios de auditoría como mecanismo secundario de seguridad (con baja prioridad).

Además de esto, se requiere que la Plataforma de Gobierno Electrónico brinde servicios de seguridad para asegurar el nivel del servicio proveedor; esto es, mecanismos de defensa ante posibles ataques y mecanismos de optimización en el uso de las comunicaciones.

Productos de Software Involucrados

En este escenario se requiere el uso de los siguientes productos de software:

- Servidor de Mapas - servicios base en el Organismo Proveedor.
- Servidor de Aplicaciones – para brindar el Catálogo de Servicios.
- ESB – cumple tareas de ruteo como Plataforma de Middleware para la mediación en la invocación de los servicios del organismo proveedor.

- Clientes - software GIS desktop (para edición), visualizador Web (para consulta)

Es de destacar que el cliente GIS desktop puede necesitar ser adaptado para poder cumplir los mecanismos de seguridad (autenticación y autorización).

Coordinación Institucional

La implementación de este escenario requiere que los Organismos (Proveedor e Instituciones Colaboradoras) coordinen entre ellos la especificación de la información sobre la cual trabajarán. Además, ambos organismos deben coordinar con AGESIC como organismo gestor de la PGE, la forma de implementar la comunicación a través de la PGE y de definir las políticas de seguridad.

A nivel técnico se requieren los acuerdos para establecer los controles de seguridad y la mediación. Esto abarca desde las credenciales que presentarán los clientes hasta la dinámica de definición de las políticas de seguridad.

En otro nivel, el cliente y el proveedor deberán acordar la estructura de los datos a trabajar: la estructura, la forma de representación, el área de trabajo de cada Institución Colaboradora (podría ser una Institución Departamental colaborando con un Organismo Nacional), la frecuencia de actualización, entre otros detalles del proceso de colaboración.

A más alto nivel, de la negociación entre el Organismo Proveedor y AGESIC surgirá la política de Nivel de Servicio que tendrá el servicio de mapas que se ofrece a través de la PGE, de acuerdo al uso que se haga de las prestaciones de mediación.

3.2.4 Escenario IV – Colaboración para la realización de procesos

Este escenario está pensado para la colaboración entre organismos para la realización de procesos administrativos. Los usuarios serán funcionarios de las Instituciones que colaboren para la realización de los procesos. Un organismo puede ofrecer servicios de consulta o de actualización de la información que él gestiona. De acuerdo a las necesidades del proceso distintos organismos colaboradores pueden jugar diferentes papeles y necesitar distintas formas de comunicación.

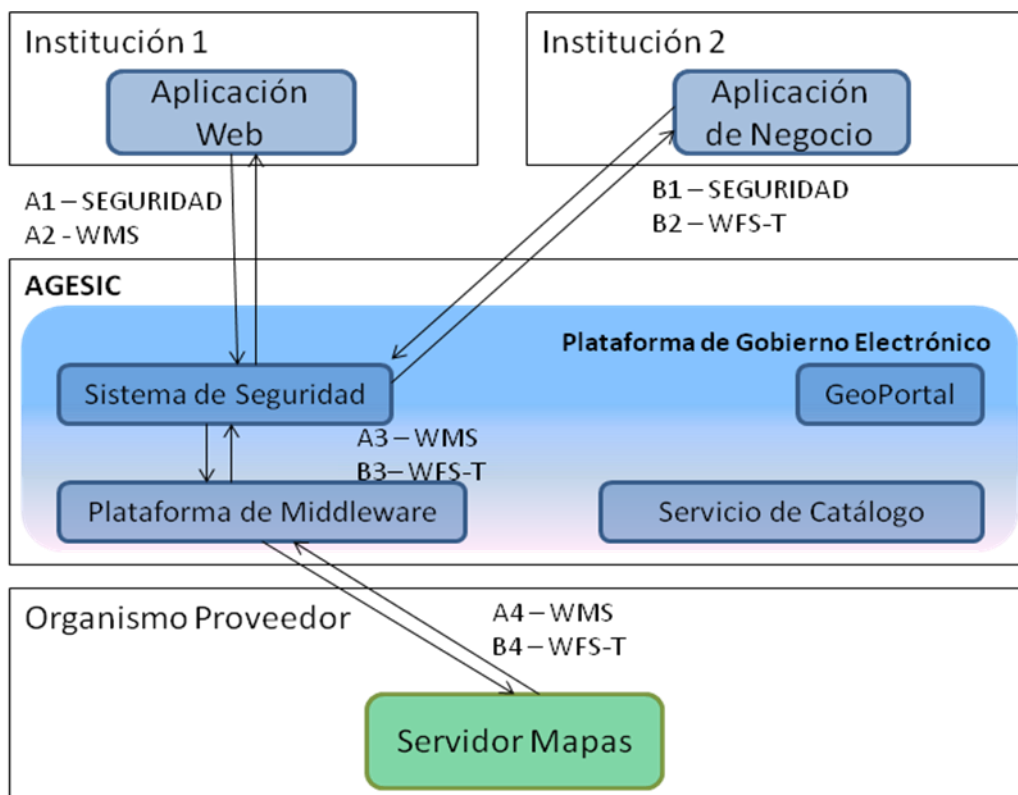


Figura 14 - Escenario IV Colaboración para la realización de procesos

En la Figura 14 se muestran dos posibles vinculaciones para la realización de procesos. En este caso el Organismo Proveedor brinda a la Institución 1 la posibilidad de consultar Información Geográfica (quizás restringida). En el Flujo A vemos que la Institución 1 posee una Aplicación Web responsable del proceso que realiza (podría ser un sistema de expediente o una aplicación hacia el público). Dicha aplicación puede solamente necesitar información de referencia del Organismo Proveedor, pero dicho Organismo necesita saber que es la Institución 1 quién la está solicitando. Por esto se necesitan controles de seguridad.

En el Flujo B se muestra otra posible interacción en la realización de procesos, la Institución 2 tiene que comunicarle información al Organismo Proveedor. Para esto el Organismo Proveedor, contando con los mecanismos de seguridad apropiados, ofrece un servicio WFS-T.

Forma de Uso de la Plataforma

En este escenario la PGE tiene roles de coordinación y mediación, ofreciendo los Servicios de Seguridad y de Catálogo como servicios básicos. También puede brindar mecanismos de coordinación de procesos de negocio si el proceso a implementar es muy complejo o se realiza entre más de dos organismos.

Los usuarios de las instituciones colaboradoras deberán autenticarse para poder ingresar y consultar o actualizar la información del Organismo Proveedor.

Luego de autenticado el usuario, desde el software en el que realiza el proceso, accederá a los servicios que necesite del Organismo Proveedor. Esto puede ser tanto una consulta como una actualización de información.

En todos los casos los pedidos al Servicio de Mapas del Organismo Proveedor pasar por el Sistema de Seguridad para que la PGE pueda aplicar las políticas de control de acceso, permitiendo solamente el acceso a los funcionarios de las instituciones participantes en el proceso. De allí los pedidos pasarán por el mediador de la PGE. De este modo la PGE puede proteger al servicio proveedor regulando la cantidad de pedidos que le envía y pudiendo aplicar estrategias de defensa ante ataques de DoS (Denial Of Service).

En resumen, en este escenario la plataforma brinda el acceso al servicio proveedor aplicando políticas de seguridad y realizando una virtualización de servicios (siendo mediador de localización). Esto le permite aplicar controles para asegurar el acceso de escritura, realizar balanceo de carga y aplicar protección ante ataques. La PGE también puede realizar funciones de coordinación central del proceso si esto es necesario.

Protocolos

De acuerdo a las necesidades del proceso a realizar pueden usarse tanto protocolos de consulta (WMS y WFS básico) como un protocolo que permita la actualización de la información: WFS-Transaccional.

A nivel de la PGE pueden usarse otros protocolos para la gestión del proceso administrativo, como por ejemplo funcionalidades de Orquestación de Servicios o coordinación.

Tipos de Operaciones

Para el caso en que el proceso solamente requiera consulta de información, estamos en el caso del Escenario II – Información para público específico. Aquí se pueden usar tanto los métodos de WMS como de WFS básico.

En el caso en que el proceso requiera actualizar (o ingresar) información, estaremos en la situación del Escenario III – Colaboración para la generación de Información. Aquí se necesitarán los métodos de WFS Transaccional. Dado que el proceso puede tener varios pasos puede ser necesario contar con la operación WFS – LockFeature (opcional según el estándar). En esa situación se tendrá que validar que el producto usado como Servidor de Mapas y el cliente soporten dicho método.

Actores Involucrados

En este escenario los actores principales son los funcionarios de las Instituciones que participan en el proceso. Dichos funcionarios usan tanto sistemas web como aplicaciones empresariales para llevar adelante los procesos administrativos.

El mediador en las comunicaciones de acceso a la información geográfica es la PGE. La PGE también es la que brinda los servicios de seguridad y control de acceso. Una función muy importante que cumple la PGE en este escenario es la coordinación de las invocaciones a lo largo del proceso.

Finalmente quién juega el rol de proveedor es el Organismo Proveedor que permite que otras instituciones consulten su información o hagan actualizaciones. Este Organismo puede a su vez tener rol de cliente frente a otras instituciones si él mismo necesita consultar información.

Mecanismos de Seguridad

Este escenario requiere un fuerte uso de mecanismos de seguridad: Autenticación y Autorización, para asegurar que solamente los funcionarios de las Instituciones participantes en el proceso puedan acceder a las funciones que brinda el Organismo Proveedor. También se usarán servicios de auditoría como mecanismo secundario de seguridad (con baja prioridad).

Además de esto, se requiere que la Plataforma de Gobierno Electrónico brinde servicios de seguridad para asegurar el nivel del servicio proveedor; esto es, mecanismos de defensa ante posibles ataques y mecanismos de optimización en el uso de las comunicaciones.

Productos de Software Involucrados

En este escenario se requiere el uso de los siguientes productos de software:

- Servidor de Mapas - servicios base en el Organismo Proveedor.
- ESB – cumple tareas de ruteo como Plataforma de Middleware para la mediación en la invocación de los servicios del organismo proveedor.
- Clientes – sistema Web, aplicación empresarial.

Es de destacar que tanto el sistema web como la Aplicación Empresarial deben poder cumplir con los mecanismos de seguridad (autenticación y autorización) y ser clientes del protocolo elegido para la comunicación.

Coordinación Institucional

La implementación de este escenario requiere que los Organismos participantes del proceso coordinen entre ellos la especificación de la información que intercambiarán. Además, los organismos deben coordinar con AGESIC como organismo gestor de la PGE, la forma de implementar la comunicación a través de la PGE y de definir las políticas de seguridad.

A nivel técnico se requieren los acuerdos para establecer los controles de seguridad y la mediación. Esto abarca desde las credenciales que presentarán los clientes hasta la dinámica de definición de las políticas de seguridad.

En otro nivel, los organismos deberán coordinar la secuencia del proceso a realizar y la información a intercambiar, teniendo en cuenta aspectos legales. Algunos de estos procesos pueden ser trámites legales que siguen reglamentos formales o incluso determinada legislación.

A más alto nivel, de la negociación entre el Organismo Proveedor y AGESIC surgirá la política de Nivel de Servicio que tendrá el servicio de mapas que se ofrece a través de la PGE, de acuerdo al uso que se haga

de las prestaciones de mediación. También se tendrá que negociar la forma de coordinación del proceso, si es necesario que está se implemente a través de la PGE.

3.2.5 Escenario V – Generación Comunitaria de Datos (VGI)

Este escenario está pensado para que un organismo ponga a disposición del público en general mecanismos para la generación comunitaria de información geográfica (VGI⁵) [43]. Un organismo puede ofrecer los recursos técnicos para apoyar a una comunidad con interés en un tema, de forma que esta pueda generar y compartir información. Por ejemplo: el Ministerio de Medio Ambiente puede tener un sitio donde el público en general ingrese para reportar avistamiento de especies.

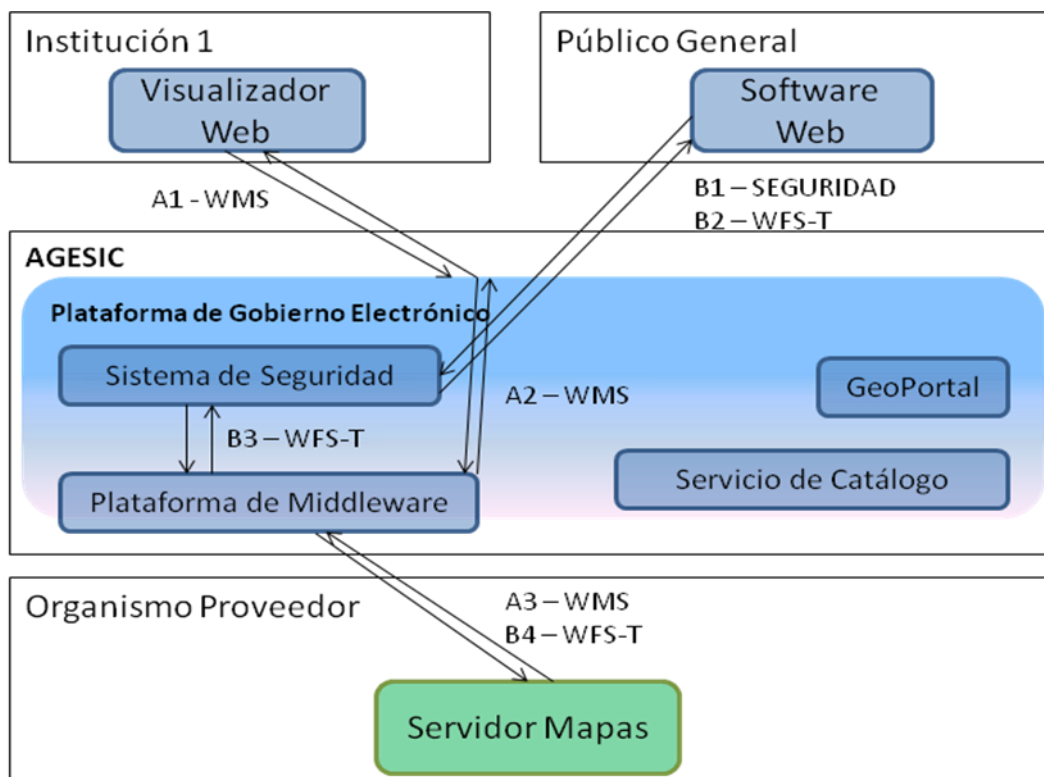


Figura 15 - Escenario de obtención de VGI

En la Figura 15 se ve que el público en general (o los integrantes de la comunidad de interés) usan un software web a través del cual se gestiona la comunidad y que permite el ingreso de información geográfica. Este sistema se apoya en los servicios de seguridad de la PGE y usa el protocolo WFS-T para enviar la información (Flujo B).

En el Flujo A se muestra como otras instituciones consultan la información generada por la comunidad de usuarios, accediendo a los servicios del Organismo Proveedor. Para esto se usarán los mismos mecanismos que para acceder a información pública. En este escenario los mecanismos de auditoría y validación de la información suelen estar incorporados en la gestión de la comunidad y lo hacen los mismos usuarios.

⁵ VGI: Volunteered Geographic Information

Forma de Uso de la Plataforma

En este escenario la PGE tiene el rol de mediación, ofreciendo los Servicios de Seguridad y de ruteo.

Los usuarios de la comunidad deberán autenticarse para poder ingresar información, pero la información y consultar o actualizar la información del Organismo Proveedor.

En todos los casos los pedidos al Servicio de Mapas del Organismo Proveedor pasar por el Sistema de Seguridad para que la PGE pueda aplicar los mecanismos de seguridad. De allí los pedidos pasarán por el mediador de la PGE. De este modo la PGE puede proteger al servicio proveedor regulando la cantidad de pedidos que le envía y pudiendo aplicar estrategias de defensa ante ataques de DoS (Denial Of Service).

En resumen, en este escenario la plataforma brinda el acceso al servicio proveedor aplicando políticas de seguridad y realizando una virtualización de servicios (siendo mediador de localización). Esto le permite aplicar controles para asegurar el acceso de escritura, realizar balanceo de carga y aplicar protección ante ataques.

Protocolos

En este escenario se usará el protocolo WFS-Transaccional ofrecido por el Organismo Proveedor para recibir la información ingresada por los usuarios.

También se usará el protocolo WMS para publicar la información generada colaborativamente, de forma que otras instituciones puedan consultarlos.

Este escenario requiere que el Organismo Proveedor brinde un software web sencillo para el ingreso de la información. Dicha información puede ser tanto geométrica como temática.

Por su parte, la PGE tiene que brindar el soporte de infraestructura para permitir gestionar la comunidad de usuarios de acuerdo a cómo esta se defina. Por ejemplo, puede haber usuarios ingresando información y otros usuarios que actúen como validadores (o moderadores) de la información ingresada, además de usuarios administradores de la comunidad. Esto implica un sistema de registro de usuarios, asignación de roles y control de acceso bastante complejo y que a su vez pueda ser administrado por miembros de la comunidad (o un funcionario del organismo que apoya a la comunidad).

Tipos de Operaciones

Para la obtención de la información generada por los usuarios el Organismo Proveedor brindará servicios WFS-Transaccionales. Aquí se necesitará que provea los métodos de un servicio WFS básico y el método WFS-Transaction.

Actores Involucrados

En este escenario los actores principales son los usuarios finales, es decir el público en general o una comunidad. Dichos usuarios generan colaborativamente la información geográfica y a su vez son los que la consultan. Para el ingreso de la información deberán usar un software específico provisto por la Institución que apoya a dicha comunidad. La información generada puede ser consultada desde

El mediador en las comunicaciones de acceso a la información geográfica es la PGE. La PGE también es la que brinda los servicios de seguridad, tanto de autenticación como de protección del servicio.

Finalmente quién juega el rol de proveedor es el Organismo Proveedor que brinda la infraestructura para almacenar la información generada por los usuarios.

Mecanismos de Seguridad

Este escenario requiere un uso de mecanismos de seguridad, más específicamente de autenticación y auditoría. Dado que los usuarios estarán ingresando información, es bueno que se identifiquen para poder disponer de estadísticas de participación en la comunidad. También se usarán servicios de auditoría como mecanismo secundario de seguridad (con baja prioridad).

Además de esto, se requiere que la Plataforma de Gobierno Electrónico brinde servicios de seguridad para asegurar el nivel del servicio proveedor; esto es, mecanismos de defensa ante posibles ataques y mecanismos de optimización en el uso de las comunicaciones.

Productos de Software Involucrado

En este escenario se requiere el uso de los siguientes productos de software:

- Servidor de Mapas - servicios base en el Organismo Proveedor.
- ESB – cumple tareas de ruteo como Plataforma de Middleware para la mediación en la invocación de los servicios del organismo proveedor.
- Clientes – sistema Web específico.

Es de destacar que el sistema web debe poder cumplir con los mecanismos de seguridad (autenticación y autorización) y ser clientes del protocolo elegido para la comunicación.

Coordinación Institucional

La implementación de este escenario requiere que el Organismo Proveedor coordine con AGESIC como organismo gestor de la Plataforma de Gobierno Electrónico. Esta coordinación se realiza en varios niveles.

A nivel técnico se requieren los acuerdos para establecer la mediación. El Organismo Proveedor debe establecer los Términos de Uso de la información geográfica que recibe y publica (aunque sean datos públicos se pueden establecer restricciones en su uso).

A más alto nivel, de la negociación entre el Organismo Proveedor y AGESIC surgirá la política de Nivel de Servicio que tendrá el servicio de mapas que se ofrece a través de la Plataforma de Gobierno Electrónico.

Sección 3.3 - Resumen Análisis Escenarios

El siguiente cuadro resume las características técnicas de cada escenario.

Item	Escenario I	Escenario II	Escenario III	Escenario IV	Escenario V
Plataforma	Localización	Localización, seguridad	Localización, seguridad	Localización, seguridad, orquestación	seguridad
Protocolos	GIS: WMS, WFS, CSW PGE: ninguno	GIS: WMS, WFS, CSW PGE: WS-Security, WS-Trust	GIS: WMS, WFS-T, CSW PGE: WS-Security, WS-Trust	GIS: WMS, WFS-T, CSW PGE: WS-Security, WS-Trust, WS-Coordination	GIS: WMS, WFS-T, CSW PGE: WS-Security, WS-Trust
Operaciones	Solo Lectura	Solo Lectura	Lectura, escritura	Lectura, escritura	Lectura, escritura
Actores	Público en General, Funcionarios	Funcionarios de organismo cliente	Funcionarios de organismos	Funcionarios de organismos	Public en general
Seguridad	No requiere	Control de Acceso	Control de Acceso	Control de Acceso	Control de Acceso
Software	Cliente web y cliente GIS desktop	cliente GIS desktop adaptado	Cliente GIS desktop adaptado	Aplicaciones de negocio	Software Comunidad Web
Coordinación Institucional	Solo acuerdo de uso de la PGE	Acuerdo cliente-proveedor	Acuerdos con organismos proveedores	Acuerdos entre organismos	Herramientas de la comunidad

Tabla 1 - Resumen Análisis Escenarios

Las principales diferencias entre los protocolos de Web Services utilizados por plataformas de middleware para gobierno electrónico (WS-SOAP, WS*) y los utilizados por Sistemas de Información Geográficos consisten en:

- **La forma de invocación.** En los Web Services de tipo geográficos la invocación es directa componiendo los parámetros de la llamada en la misma invocación. Los estándares están definidos en base al protocolo HTTP usando solamente los métodos GET y POST. En cambio, los Web Services de uso general están especificados sobre el protocolo SOAP que está orientado a mensajes. Tanto el método elegido como los parámetros son parte del cuerpo del mensaje,

mientras que en el cabecal del mensaje se pone la información necesaria para el direccionamiento del mensaje (que puede recorrer un camino complejo y pasar por intermediarios).

- **La existencia de WSDL.** En los Web Services de tipo geográfico no hay un documento que describa al servicio y pueda ser consultado en registros. El estándar establece que el servicio tiene un método para consultar las características del mismo. Este método devuelve un conjunto operativo de metadatos sobre los datos, que aseguran que el cliente pueda realizar invocaciones. Los Web Services de uso general son descritos con un documento WSDL, que describe los métodos que brinda el servicio, las estructuras de datos necesarias para el uso del servicio y puede ser extendido para agregar más información. El WSDL suele ser publicado en Servicios de Registro de Web Services, que además de brindar la descripción del servicio, especifican la forma de comunicarse con el servicio.
- **Las políticas de uso.** En los Web Services geográficos la política de uso viene dada por la política de uso del conjunto de datos que el servicio provee. Estas políticas suelen documentarse en los metadatos del conjunto de datos, los que pueden ser almacenados en servicios de catálogos. Dichos metadatos describen el conjunto de datos y aunque pueden incluir algún dato del servicio, estos no son obligatorios, ya que el conjunto de datos existe por sí mismo independiente del servicio que lo provea. En los Web Services de uso general, se han definido extensiones del documento WSDL para describir las políticas de uso del servicio, políticas de seguridad, etc.
- **La seguridad.** En los Web Services geográficos, las especificaciones de los estándares son funcionales y se propone un estándar aparte para políticas de control de acceso (GeoXACML). En este estándar se propone una arquitectura donde el servidor de mapas brinda los servicios siguiendo los estándares y el control de acceso lo realiza otro servidor. En esta arquitectura el servidor de mapas no recibe ni envía ningún tipo de información en seguridad. En los Web Services de uso general se puede especificar la seguridad de diferente forma para cada servicio (e incluso para cada método). Aunque se prevee la presencia de servidores con funciones específicas de control de la seguridad, en la descripción del servicio se pueden poner requisitos de seguridad y en los mensajes de invocación (y respuesta) al servicio se puede agregar información de seguridad.

Estas diferencias obligan a implementar diferenciadamente las invocaciones correspondientes, lo cual genera problemas en el contexto de plataformas de interoperabilidad, tales como la de gobierno electrónico, principalmente debido a la pérdida de independencia con respecto a la implementación. Tales problemas se presentan principalmente en funciones de:

- **Descubrimiento de servicios** – Los Web Services geográficos (WS GIS) no proveen mecanismos para el descubrimiento automático de servicios. Por lo que el cliente debe conocer la URL del servicio que desea invocar. Por otro lado, es importante señalar que los WSGIS tienen métodos fijos estandarizados y en particular el método `getCapabilities` brinda los metadatos de los datos provistos por el servicio. En los Web Services de uso general se proveen mecanismos bien estructurados para el descubrimiento automático de servicios, ya que la información de invocación se publica en forma estructurada a través del WSDL y existen directorios de dichas descripciones.

- **Aplicación de Seguridad** – los estándares de seguridad que aplica la plataforma de gobierno electrónico se basan en extensiones del protocolo SOAP (WS-Security, WS-Trust), agregando información a los mensajes y a la descripción de los servicios. De este modo se puede controlar la seguridad tanto en servidores intermedios como en el servidor final que provee el servicio. En los protocolos WS-GIS no hay mecanismos de seguridad incorporados, sino que tiene que implementarlo un servidor aparte del servidor de mapas.
- **Invocación** – La invocación de los servicios WS GIS se hace directamente a una URL de acuerdo al protocolo HTTP. La invocación de WS-SOAP se realiza a un punto de entrada del servicio, enviando un mensaje SOAP. En este caso el protocolo de transporte puede ser HTTP o no. Esto hace que para poder mediar en la invocación de un WS-GIS haya que realizar análisis de la invocación a bajo nivel (HTTP) en lugar de hacer análisis del mensaje SOAP, mucho más estructurado.
- **Virtualización de Servicios** – esta es una funcionalidad fundamental en las plataformas de gobierno electrónico, porque permite gestionar mejor el acceso a los servicios que proveen los organismos. Para esto las aplicaciones clientes envían las invocaciones a la plataforma de gobierno electrónico usando un alias del servicio que desean invocar y ella los redirige al servicio real del organismo proveedor.
- **Retorno de Información** – en los protocolos WS-GIS los datos se retornan sincrónicamente en la misma conexión HTTP. En los WS-SOAP la información de retorno puede enviarse por otros canales ya que es otro mensaje SOAP (y puede ser asincrónicamente). Esto hace que al pasar un pedido WS-GIS por una plataforma de middleware se tenga que guardar información de la conexión para devolver la respuesta, ya que la respuesta puede ser en algunos casos solamente una imagen, sin mucho contexto de la solicitud que la originó.

En resumen, los protocolos de WS para GIS no son compatibles con los protocolos WS-*, como por ejemplo los de seguridad (WS-Security, WS-Trust, WS-Policy). Esto genera problemas importantes para la integración de servicios de información geográficos en plataformas con mecanismos de seguridad porque los protocolos WS-* extienden el protocolo SOAP y los Web Services geográficos no usan protocolo SOAP.

A continuación se detallan los principales problemas de compatibilidad detectados para el uso Web Services geográficos (WS-GIS) en una Plataforma de Gobierno Electrónico (PGE):

- 1 Ruteo – el ruteo en la PGE se basa en la extensibilidad del protocolo SOAP, pudiendo agregarse información extra en los mensajes SOAP (destinatario, ruta, prioridad, etc.). Como los WS-GIS no usan SOAP, hay que desarrollar mecanismos propietarios de ruteo inspeccionando elementos de bajo nivel como las conexiones HTTP. Esta problemática afecta a todos los escenarios planteados en la sección 3.2.
- 2 Asincronismo – los WS-GIS están definidos en forma Request-Response sincrónica, mientras que las comunicaciones en la PGE son en forma de mensajes que pueden ser asincrónicos. Esto genera que un cliente WS-GIS al hacer un pedido se quedará esperando respuesta manteniendo la conexión. Esta es una limitante que afecta especialmente al Escenario IV.
- 3 Control de Acceso – en la PGE el control de acceso se implementa en base a los estándares WS-Security y WS-Trust porque se tiene identidad federada de los usuarios. Estos estándares se

apoyan en el protocolo SOAP. A excepción del Escenario I, todos los demás requieren control de acceso, por lo que se verán afectados por este problema.

- 4 Sesión – los WS-GIS son funcionales pero no tienen identificación de los usuarios. En los escenarios de escritura de datos es necesario que la PGE brinde los mecanismos para mantener la sesión de los usuarios. Esto es como complemento a los mecanismos de control de acceso.
- 5 Seguridad – los WS-GIS tienen los mismos problemas básicos que el protocolo HTTP en el que se basan [42], para lograr características avanzadas de seguridad como confidencialidad por ejemplo.
- 6 Directorio de Servicios – la PGE basa su gestión en un directorio de servicios (basado en UDDI). Como los WS-GIS no tienen descripción en WSDL no se pueden registrar en el directorio de la PGE en forma directa.
- 7 Servicio de Catálogos – los estándares GIS proponen un servicio de catálogos que es un servicio para la localización de datos a través de sus metadatos. Estos conjuntos de datos pueden o no estar accesibles a través de un WS-GIS.

Capítulo 4 – Propuesta de Solución

Sección 4.1 - Visión General de la Solución

4.1.1 Introducción

En este capítulo se presentan encares de solución a los problemas presentados en el capítulo anterior. Nos concentramos en el análisis para los flujos de datos en la Plataforma de Gobierno Electrónico (PGE) y especialmente en el uso más eficiente y extenso de la plataforma por parte de las organizaciones. También se prioriza el criterio de generar el menor impacto posible a los organismos clientes y proveedores.

Para la propuesta de solución se unifican las características comunes de los escenarios tomando como centro los escenarios II, III y IV. A nivel de los flujos dentro de la plataforma, los escenarios I y V quedan cubiertos implícitamente. En esta propuesta al centrarnos en los flujos dentro de la PGE, no entraremos en detalle sobre los distintos clientes y sus funciones al usuario final.

En la Figura 16 se muestra la Arquitectura Unificada sobre la que se basa la propuesta de solución. Aumentando el nivel de abstracción de los protocolos de Web Services Geográficos, los trabajaremos como pedidos y respuestas, centrándonos en cómo estos pedidos y respuesta siguen un Flujo dentro de la PGE.

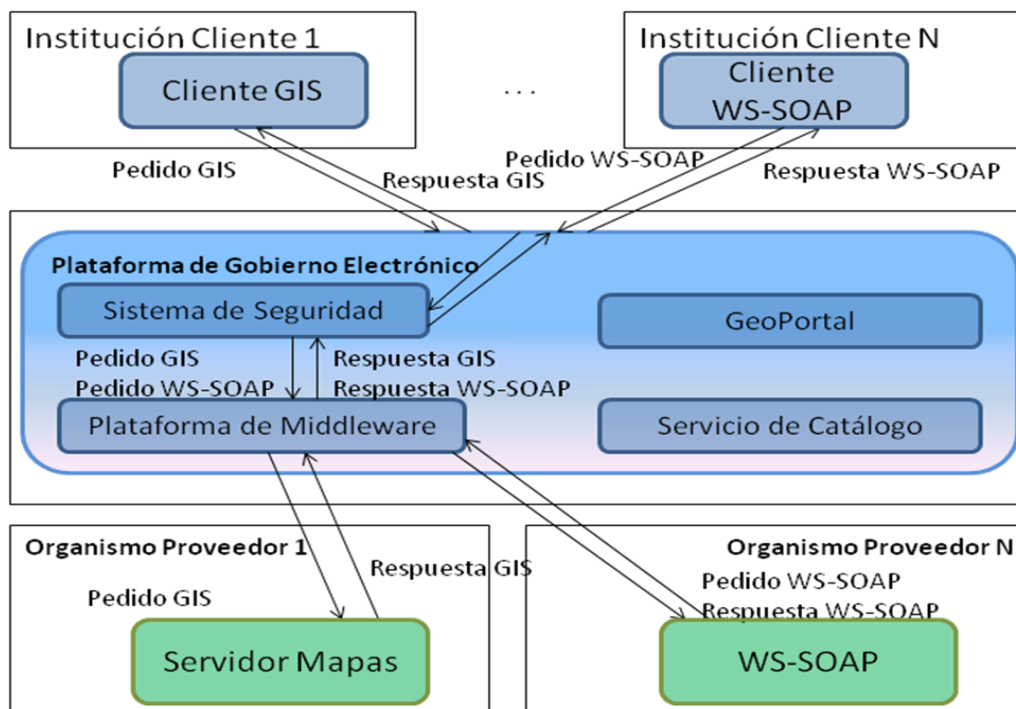


Figura 16 - Arquitectura Unificada

Se considera además que los clientes pueden realizar tanto pedidos de Web Services Geográficos como pedidos de Web Services SOAP. A su vez, dentro de la PGE puede ocurrir que para atender un pedido de Web Services SOAP la PGE internamente tenga que realizar pedidos a Web Services Geográficos. En esta situación, la plataforma debe distinguir el tipo de pedido que está recibiendo y tratarlos de distinta forma.

Los puntos técnicos problemáticos comunes a los escenarios son: el ruteo de los pedidos y respuestas, el manejo de asincronismo y la seguridad, considerando control de acceso y sesión. En la PGE el ruteo se resuelve en base a WS-Addressing sobre Web Services SOAP, la seguridad se resuelve en base a mecanismos de WS-Security y el asincronismo con atributos avanzados de WS-Addressing.

Como estrategia general para poder integrar en la PGE pedidos de Web Services Geográficos, los mismos serán transformados a paquetes SOAP y se les agregará información para su tratamiento. Concretamente, luego de tener los pedidos como paquetes SOAP necesitamos agregarle información para que la PGE pueda usar sus mecanismos asincrónicos, de ruteo y de seguridad, de acuerdo a lo que se necesite en el caso de aplicación (en qué escenario estamos). En una última etapa, cuando la PGE va a enviar el pedido al Servidor de Mapas, se debe volver a transformar el paquete SOAP que viajó dentro de la plataforma en el pedido original. Los puntos de aplicación de las transformaciones se muestran en la Figura 17 con la etiqueta CTP (Componente de Transformación de Protocolos). Cabe destacar que, luego de dichas transformaciones, dentro de la plataforma se procesarán pedidos y respuestas correspondientes a Web Services Geográficos en forma transparente a la PGE.

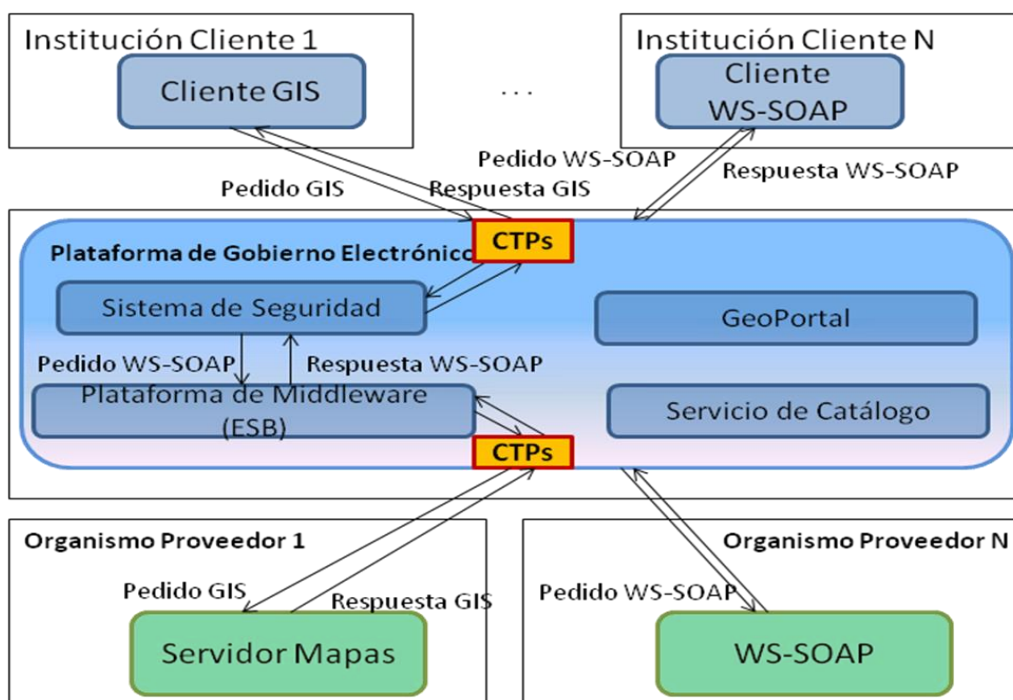


Figura 17 - Arquitectura con los Componentes de Transformación de Protocolos

En la siguiente sección se presentan las descripciones de los Flujos y las Transformaciones propuestas.

4.1.2 Flujos y Transformaciones

De acuerdo a lo presentado en la sección anterior, la propuesta de solución se basa en realizar Transformaciones que permitan que los pedidos WS-GIS se conviertan en pedidos WS-SOAP para su procesamiento dentro de la PGE. A su vez se define cómo estos pedidos pueden viajar dentro de la PGE mediante la definición de Flujos. Estos Flujos toman en cuenta los mecanismos internos de la PGE para tratar los pedidos de WS-SOAP usuales. De acuerdo al escenario de aplicación en que nos encontremos los pedidos seguirán distintos flujos, ya que, por ejemplo, en algunos casos pasarán controles de seguridad y en otros no. Dependiendo del Flujo a recorrer, al realizar la transformación del pedido WS-GIS en WS-SOAP se usarán diferentes mecanismos de transformación. Por esto se definen distintas transformaciones que consideran distintos aspectos necesarios en los diferentes flujos. A la hora de implementar un flujo en particular se podrán componer las transformaciones. A continuación se presenta una primera aproximación a la caracterización de los Flujos y las Transformaciones que se proponen. Luego, en la Sección 4.2 se realiza la especificación formal de ambos.

Flujo de Ruteo

Cuando la PGE recibe un pedido WS-GIS, se debe transformar en un paquete WS-SOAP para que sea compatible con los paquetes que maneja la PGE. Esto permite que la PGE pueda aplicar sus mecanismos de ruteo como lo haría con cualquier otro paquete WS-SOAP. Aquí ya surge la primera transformación que llamaremos T1, que genera un paquete SOAP a partir de un pedido WS-GIS. Cuando la PGE determina el destino final del pedido, se aplicará una transformación inversa a T1, para generar el pedido WS-GIS original y así enviarlo al servicio deseado. Aquí surge una segunda transformación que llamaremos T1inv, ya que realiza la transformación inversa a la transformación T1.

Luego de realizada la invocación al Web Service Geográfico, la PGE recibe la respuesta WS-GIS. Esta respuesta debe ser transformada en un paquete SOAP para recorrer el camino de regreso en la PGE y ser devuelta al cliente. Aquí definimos el par de transformaciones T2 y T2inv que empaquetan y desempaquetan la respuesta del WS-GIS en un paquete SOAP. En la Sección 4.2 Especificación de la solución se definirá más formalmente este flujo y las transformaciones asociadas.

Flujos con Asincronismo

Aunque los pedidos WS-GIS son sincrónicos, dentro de la plataforma los paquetes WS-SOAP pueden ser tratados tanto en forma sincrónica como asincrónica. También puede ocurrir que al integrar servicios WS-GIS con servicios WS-SOAP tengamos que invocar servicios asincrónicos. Por esto se consideran Flujos con características asíncronas, que requieren información adicional para su tratamiento.

Dado que ya se tiene resuelta la transformación del pedido WS-GIS a un paquete SOAP (T1 y T2), podemos agregar la información extra necesaria a dicho paquete SOAP. Aquí aparece una nueva transformación T3 que toma un paquete SOAP y le agrega información para soportar invocaciones asincrónicas, la cual consistiría, por ejemplo, en el punto de retorno de la respuesta al pedido realizado. Con esta información en el paquete SOAP la PGE no solamente lo puede rutear, sino que también tiene la información extra para manejar el flujo de la respuesta. Nuevamente, cuando la PGE va a enviar el pedido al servicio destino, deberá transformar el paquete SOAP guardando en su contexto la

información para el retorno de la respuesta. Para esto se usará una transformación T3inv que realiza esta tarea.

Cuando la PGE recibe la respuesta del pedido, se realiza nuevamente el empaquetamiento de la respuesta en un paquete SOAP como se presenta en el Flujo de Ruteo. Además, al estar en un escenario asíncrono, deberemos tomar del contexto de ejecución la información del punto de retorno. Esto lo realizará una transformación que llamaremos T4 y que agrega la información necesaria al paquete SOAP de la respuesta. La PGE ahora puede rutear el paquete de respuesta al destinatario correcto (que quizás no es el origen del pedido). Antes de que la PGE pueda entregar la respuesta, se deberá desempaquetar la misma, aplicando las transformaciones inversas de las utilizadas. Para esto se usará una transformación T4inv que quita la información de ruteo asíncrono.

Dentro del conjunto de flujos asíncronos distinguimos dos casos particulares que generan conflictos:

Caso 1: un cliente WS-GIS consulta un WS-SOAP asíncrono, esperando un comportamiento sincrónico.

Caso 2: un cliente WS-SOAP que consulta un WS-GIS suponiendo un comportamiento asíncrono.

En el Caso 1 las Transformaciones a usar solamente agregarán información de ruteo y le asignarán alta prioridad al pedido para lograr el mejor tiempo de respuesta posible. En este caso la respuesta deberá devolverse al mismo punto en que partió el pedido (que es la misma conexión del pedido).

En el Caso 2, las Transformaciones agregarán la información de ruteo guardado el punto de retorno en el contexto de ejecución. La PGE actuará como cliente sincrónico ante el WS-GIS pero responderá al cliente WS-SOAP como un servicio asíncrono.

Flujos con Seguridad

En algunos casos los pedidos WS-GIS deberán ser considerados en contextos seguros, considerando tanto la autenticación del cliente que realiza el pedido, como su autorización para realizar ese pedido. Para esto la PGE ya cuenta con mecanismos para controlar la seguridad que se basan en WS-Security, WS-Trust y WS-Policy, todos estándares para trabajar con paquetes WS-SOAP. En estos casos, ya contando con las transformaciones del Flujo de Ruteo, podemos considerar que tenemos resuelto el empaquetamiento del pedido WS-GIS en un paquete SOAP.

Sin embargo los pedidos WS-GIS no incluyen información de seguridad. Ante este problema, se definen transformaciones que agregan al paquete SOAP la información necesaria, tomándola del contexto de ejecución del pedido. Se consideran varias transformaciones con tareas distintas: una transformación T5 que agrega la información del usuario autenticado, lo que nos permite tener una sesión asociada al pedido. Como los servidores de WS-GIS no consideran esta información, la transformación T5inv retira dicha información del pedido. Se definen un par de transformaciones T6 y T6inv que trabajan con la información de sesión sobre un paquete de respuesta a un pedido GIS.

Para que la PGE pueda gestionar la autorización en los pedidos, se definen transformaciones encargadas de agregar información sobre los permisos que tiene el cliente para acceder al servicio deseado. Aquí se tomará información del contexto de ejecución, tanto de la información asociada al pedido como

información disponible en la misma PGE. En algunos casos la autorización puede estar asociada a la institución a la que pertenece el usuario cliente y en otros casos puede ser debido al perfil del usuario. Definimos la transformación T7 para agregar dicha información al pedido GIS en el paquete SOAP y una transformación T7inv para retirar dicha información antes de enviar el pedido al servicio GIS destino. Luego se usarán transformaciones T8 y T8inv para gestionar esta información en la respuesta de retorno.

Transformaciones

A continuación se resumen las transformaciones identificadas y los Flujos y aspectos que cubren.

Transformación	Flujo relacionado	Función
T1: Req WS-GIS \Rightarrow SOAP-Req	Flujo de Ruteo	Genera un paquete SOAP a partir de un pedido WS-GIS.
T1inv: SOAP-Req \Rightarrow Req WS-GIS	Flujo de Ruteo	Arma el pedido WS-GIS original a partir de un paquete SOAP.
T2: respWS-GIS \Rightarrow SOAP-Resp	Flujo de Ruteo	Empaqueta en un paquete SOAP con una respuesta del WS-GIS.
T2inv: SOAP \Rightarrow respWS-GIS	Flujo de Ruteo	Desempaqueta la respuesta del WS-GIS en un paquete SOAP.
T3: SOAP-Req \Rightarrow T3SOAP-Req	Flujos con Asincronismo	Toma un paquete SOAP y le agrega información para soportar invocaciones asincrónicas. Se utiliza compuesta con T1.
T3inv: T3SOAP-Req \Rightarrow SOAP-Req	Flujos con Asincronismo	Transforma un paquete SOAP guardando en el contexto la información para el retorno de la respuesta. Se utiliza compuesta con T1inv.
T4: SOAP-Resp \Rightarrow T4SOAP-Resp	Flujos con Asincronismo	Toma un paquete de respuesta SOAP y le agrega información de direccionamiento asincrónico. Se utiliza compuesta con T2.
T4inv: T4SOAP-Resp \Rightarrow SOAP-Resp	Flujos con Asincronismo	Transforma un paquete SOAP en otro quitando la información de direccionamiento. Se utiliza compuesta con T2inv.
T5: SOAP-Req \Rightarrow T5SOAP-Req	Flujos con Seguridad - Sesión	Transforma un paquete SOAP en otro agregando la información del usuario autenticado. Se utiliza compuesta con T1.
T5inv: T5SOAP-Req \Rightarrow SOAP-Req	Flujos con Seguridad - Sesión	Transforma un paquete SOAP en otro retirando la información del

		usuario autenticado. Se utiliza compuesta con T1inv.
T6: SOAP-Resp \Rightarrow T6SOAP-Resp	Flujos con Seguridad - Sesión	Transforma un paquete SOAP en otro agregando información de sesión. Se utiliza compuesta con T2.
T6inv: T6SOAP-Resp \Rightarrow SOAP-Resp	Flujos con Seguridad - Sesión	Transforma un paquete SOAP en otro retirando la información de sesión. Se utiliza compuesta con T2inv.
T7: SOAP-Req \Rightarrow T7SOAP-Req	Flujos con Seguridad - Autorización	Transforma un paquete SOAP en otro agregando la información del perfil de usuario. Se utiliza compuesta con T1.
T7inv: T7SOAP-Req \Rightarrow SOAP-Req	Flujos con Seguridad - Autorización	Transforma un paquete SOAP en otro retirando la información del perfil de usuario. Se utiliza compuesta con T1inv.
T8: SOAP-Resp \Rightarrow T8SOAP-Resp	Flujos con Seguridad - Autorización	Transforma un paquete SOAP en otro agregando la información del perfil de usuario en respuesta. Se utiliza compuesta con T2.
T8inv: T8SOAP-Resp \Rightarrow SOAP-Resp	Flujos con Seguridad - Autorización	Transforma un paquete SOAP en otro retirando la información del perfil de usuario en la respuesta. Se utiliza compuesta con T2inv.

4.1.3 Comparación de Protocolos de Web Services

En esta sección se comparan los protocolos de Web Services SOAP y Web Services Geográficos: WMS y WFS, a los efectos de conocer en detalle las similitudes y diferencias de estructuras y comportamiento, así como de definir la semántica de las transformaciones entre los mismos.

Mensajes SOAP y WS Geográficos

La siguiente tabla presenta las características de los mensajes en los protocolos.

	WS SOAP	WS Geográficos	Problemas generados
Estructura del Mensaje	Cabecales y Cuerpo	Key Value Pairs o XML	Flexibilidad en los contenidos del mensaje
Codificación de Parámetros	XML (namespaces)	Fijos: obligatorios y opcionales	(im)Posibilidad de extensión
Selección de método a invocar	Parámetro	Parámetro	
Destinatario	Codificado en el cabecal	Codificado en el pedido	(im)Posibilidad de ruteo
Origen	Codificado en el cabecal	Detectable estudiando el pedido HTTP	(im)Posibilidad de ruteo
Mecanismo de Falla	Codificado en el mensaje	Respuesta plana	

Tabla 2 - Comparación de aspectos de los protocolos

Formas de Comunicación e Invocación

Uno de los problemas de compatibilidad entre los Web Services SOAP y los Web Services Geográficos es la forma de comunicación e invocación entre cliente y servidor.

Los Web Services SOAP se basan en el envío de mensajes SOAP entre nodos SOAP de alto nivel. La forma de conectarse entre los nodos está dada por el protocolo de transporte, siendo el más usado HTTP (aunque puede haber otros).

Los Web Services Geográficos se basan en invocaciones directas sincrónicas de un cliente a la URL de atención de un servidor de mapas usando los métodos básicos del protocolo HTTP: get y post.

Los Web Services SOAP tienen la posibilidad de ser tanto sincrónicos como asincrónicos y la gestión de pedidos en la PGE se basa en mecanismos asincrónicos.

Protocolos (extendidos): WS-* y WS Geográficos

Para lograr características de seguridad en los WS-SOAP se usan los estándares WS-Security, WS-Trust y WS-Policy. Estos estándares proponen extensiones al paquete SOAP que agregan información sobre las credenciales que tiene el cliente que realiza el pedido al servicio. Dichas credenciales se pueden validar directamente en la PGE o pueden ser validadas en forma distribuida consultando a los diferentes organismos que usan la plataforma.

El estándar WS-Addressing permite agregar información de direccionamiento a los paquetes SOAP. Esto habilita el uso de mecanismos asincrónicos tipo call-back, permitiendo agregar información de un punto de retorno de la respuesta. Este estándar también es utilizado para la virtualización de servicios, pudiendo la PGE redirigir un pedido a un proveedor de servicios diferente cuando sea necesario.

Sección 4.2 Especificación de la solución

En esta sección se presenta una especificación formal de la solución propuesta. La misma se organiza en las siguientes sub-secciones:

1. Definiciones Previas
2. Especificación formal de transformaciones.
3. Especificación formal de flujos, incluyendo transformaciones definidas antes.
4. Demostración, por derivación, de las propiedades de las transformaciones en los flujos.

4.2.1 Definiciones previas

En esta sección se definen las estructuras de datos y funciones que se usarán en la especificación de la solución.

Estructuras

Definición 4.1 – Mensaje SOAP

Mensaje SOAP es una estructura de datos con un envelope compuesta por dos secciones: header y body. Dicha estructura se representará en un formato XML.

Definición 4.2 – Paquete WS-GIS

Paquete WS-GIS es la unión del pedido WS-GIS y los atributos del request HTTP.

En el pedido WS-GIS distinguimos las siguientes partes:

- Endpoint - URL a la que se envió el pedido.
- Servicio - protocolo sobre el que se hace el pedido.
- Método - método del protocolo al que se invoca.
- Parámetros - toda otra información de la invocación.

Definición 4.3 – Respuesta WS-GIS

Respuesta WS-GIS es todo el conjunto de información que genera un Servidor de Mapas ante un pedido WS-GIS. En la estructura se llamará contenido a la información retornada por el servidor de mapas. Los diferentes métodos WS-GIS pueden retornar diferentes tipos de información (desde imágenes hasta xml).

Definición 4.4 – Contexto de Operación y Seguridad

Contexto de Operación y Seguridad es el espacio en la plataforma que gestiona un pedido a un servicio. Esto incluye la información sobre si hay una sesión establecida, quién es el usuario conectado, a qué organismo pertenece, etc.

Predicados

- **PaqueteSOAP (p) = true** sii p es un paquete SOAP válido.
- **WS-GIS (p) = true** sii p es un pedido GIS válido.
- **RespWS-GIS (p) = true** sii p es una respuesta a un pedido WS-GIS.
- **T1(p) = true** sii $p \equiv \text{Post}(T1)$
- **T1inv(p) = true** sii $p \equiv \text{Post}(T1\text{inv})$
- **T2(p) = true** sii $p \equiv \text{Post}(T2)$
- **T2inv(p) = true** sii $p \equiv \text{Post}(T2\text{inv})$
- **T3(p) = true** sii $p \equiv \text{Post}(T3)$
- **T3inv(p) = true** sii $p \equiv \text{Post}(T3\text{inv})$
- **T4(p) = true** sii $p \equiv \text{Post}(T4)$
- **T4inv(p) = true** sii $p \equiv \text{Post}(T4\text{inv})$
- **T5(p) = true** sii $p \equiv \text{Post}(T5)$
- **T5inv(p) = true** sii $p \equiv \text{Post}(T5\text{inv})$
- **T6(p) = true** sii $p \equiv \text{Post}(T6)$
- **T6inv(p) = true** sii $p \equiv \text{Post}(T6\text{inv})$
- **T7(p) = true** sii $p \equiv \text{Post}(T7)$
- **T7inv(p) = true** sii $p \equiv \text{Post}(T7\text{inv})$
- **T8(p) = true** sii $p \equiv \text{Post}(T8)$
- **T8inv(p) = true** sii $p \equiv \text{Post}(T8\text{inv})$

Funciones

Se define además una función auxiliar **servMapas** que realiza la invocación al servidor de mapas.

servMapas(p-gis:WS-GIS):respWS-GIS

Esta función recibe un pedido para un web service geográfico y lo ejecuta, devolviendo el resultado que obtiene del Servidor de Mapas.

4.2.2 Transformaciones

En esta sección se presenta una definición formal de las Transformaciones propuestas. Se sigue la notación de Precondiciones y Poscondiciones de acuerdo a “Guarded Command Language” de Anne Kaldewaij [47], siguiendo la corriente de Dijkstra de especificaciones formales que permiten la derivación de algoritmos y su prueba formal simultáneamente.

Notación

Se especificarán las transformaciones en base a su firma, precondiciones y poscondiciones.

La firma contiene la definición de la variable de entrada y su tipo, y el tipo de respuesta de la Transformación. A continuación se muestra un prototipo de firma para una transformación genérica T que tiene como entrada una variable “var_name” de tipo “VAR_TYPE” y devuelve información de tipo “RET_TYPE”.

Transformación T(input: var_name: VAR_TYPE):RET_TYPE

Las precondiciones y poscondiciones se especifican en lenguaje lógico de primer orden usando los predicados definidos en la sección previa. Nota: se usa el símbolo “:=” para la asignación a la variable de salida de la transformación. En las condiciones lógicas que se cumplen en las precondiciones y poscondiciones el símbolo “=” solamente se refiere a la comparación lógica.

Las precondiciones son las propiedades que valen para la variable de entrada que recibe la transformación. Las poscondiciones establecen las propiedades que valen sobre la variable de salida y su relación con la información recibida como entrada.

Especificación

Transformación T1 (input: p-gis: WS-GIS): SOAP

Convierte un paquete WS-GIS a SOAP, con toda la información que trae. Identifica el origen del mensaje y el destinatario.

Pre \equiv {p-gis / WS-GIS(p-gis)}

Post \equiv {p-gis-soap := T1(p-gis) / (p-gis-soap = PaqueteSOAP(T1(p-gis))) AND (p-gis-soap.header \supset p-gis.endpoint as “receiver”) AND (p-gis-soap.body \supset p-gis.servicio, p-gis.metodo, p-gis.parametros)}

Se exige como precondición para esta transformación la existencia de un pedido a un WS-GIS. Al aplicar la transformación se cumple, como poscondición, que retorna un paquete SOAP (p-gis-soap) y que el paquete contiene en su **header** información del servicio destino y en el **body** todos los atributos del pedido: servicio, método y parámetros.

Transformación T1inv (input: p-gis-soap: SOAP): WS-GIS

Convierte un paquete WS-SOAP a un pedido WS-GIS.

Pre \equiv {p-gis-soap / PaqueteSOAP(p-gis-soap) AND (p-gis-soap.header \supset "receiver") AND (gis-soap.body \supset servicio, metodo, parametros)}

Post \equiv {p-gis:= T1inv(p-gis-soap), / WS-GIS(p-gis) AND (p-gis.endpoint = p-gis-soap.header.receiver) AND (p-gis.servicio= p-gis-soap.body.servicio) AND (p-gis.metodo= p-gis-soap.body.metodo) AND (p-gis.parametros= p-gis-soap.body.parametros)}

La precondition consiste en que, como entrada, se recibe un paquete SOAP que contiene información en su **header** y en su **body**. En el **header** viene la identificación del servicio destinatario del pedido. En el **body** se incluye información sobre el servicio invocado, el método elegido y los parámetros a pasar. Al aplicar la transformación **T1inv** se genera un pedido gis que se estructura con la información que trae el paquete SOAP. En el pedido GIS se usa el atributo que viene en el **header** como "endpoint" y los atributos que vienen en el **body** como método y parámetros.

Transformación T2 (input: resp-gis:Resp-WS-GIS): SOAP

Convierte una respuesta WS-GIS a un paquete WS-SOAP

Pre \equiv {resp-gis / WS-GIS(resp-gis)}

Post \equiv { resp-gis-soap:=T2(resp-gis), / (resp-gis-soap = PaqueteSOAP(T2(resp-gis))) AND (resp-gis-soap.body.contenido = resp-gis.contenido)}

Esta Transformación tiene como precondition que recibe un paquete de información correspondiente a la respuesta que brinda un servidor de Mapas. Al aplicar la transformación devuelve un paquete SOAP que tiene toda la información de la respuesta en el **body** del paquete SOAP.

Transformación T2inv (input: p-gis-soap:SOAP): RespWS-GIS

Convierte un paquete WS-SOAP a una respuesta WS-GIS, con toda la información que incluye.

Pre \equiv {p-gis-soap / PaqueteSOAP(p-gis-soap) AND (gis-soap.body \supset contenido)}

Post \equiv {resp-gis:= T2inv(p-gis-soap), / RespWS-GIS(resp-gis) AND resp-gis.contenido= p-gis-soap.body.contenido}

Esta Transformación tiene como precondition que recibe un paquete SOAP que tiene información de contenido en el **body**. Luego de aplicar la transformación se obtiene un paquete de respuesta a un pedido de WS-GIS cuyo contenido es igual al incluido en el body del paquete SOAP de entrada.

Transformación T3 (input: p-gis-soap:SOAP):SOAP

Recibe un paquete WS-SOAP y le agrega información de direccionamiento devolviendo otro paquete SOAP.

Pre \equiv {p-soap / PaqueteSOAP(p-soap) AND T1(p-soap)}
Post \equiv { p-soapA:=T3(p-soap), / p-soapA.header.to = p-soap.header.receiver AND p-soapA.header.action = p-soap.body.metodo AND p-soapA.body=p-soap.body}

Esta Transformación tiene como precondition que recibe un paquete SOAP que cumple las poscondiciones de la Transformación T1. Al aplicar la Transformación T3 se obtiene otro paquete SOAP que cumple como poscondición que en el **header** tiene un campo **to** con la información que el paquete traía en el campo **receiver** y en el campo action del **header** lleva la información que el paquete traía en el campo **metodo** del **body** y el contenido del **body** es igual al del paquete de entrada.

Transformación T3inv (input: p-gis-soap:SOAP):SOAP

Recibe un paquete WS-SOAP con información de direccionamiento y la quita devolviendo otro paquete SOAP

Pre \equiv {p-soapA / PaqueteSOAP(p-soapA) AND T3(p-soapA)}
Post \equiv { p-soap:=T3inv(p-soapA), / \neg (p-soap.header \supset p-soapA.header.to) AND \neg (p-soap.header \supset p-soapA.header.action) AND (p-soap.body=p-soapA.body)}

Esta transformación tiene como precondition que recibe un paquete SOAP (p-soapA) que cumple las poscondiciones de la Transformación T3. Al aplicar la Transformación T3inv se obtiene otro paquete SOAP que cumple que en el **header** no hay un campo **to** ni un campo **action** y la información en el body es igual a la que trae el paquete de entrada.

Transformación T4 (input: p-gis-soap:SOAP):SOAP

Recibe un paquete WS-SOAP con una respuesta WS-GIS y le agrega información de ruteo devolviendo otro paquete SOAP

Pre \equiv {resp-gis-soap / PaqueteSOAP(resp-gis-soap) AND T2(resp-gis-soap)}
Post \equiv { resp-gis-soapA:=T4(resp-gis-soap), / (resp-gis-soapA = PaqueteSOAP(T2(resp-gis-soap))) AND (resp-gis-soapA.header.destino = S_context.client) AND (resp-gis-soap.body=p-soapA.body)}

Esta Transformación tiene como precondition que recibe un paquete SOAP que cumple las poscondiciones de la Transformación T2. Al aplicar la Transformación T4 se obtiene otro paquete SOAP que cumple como poscondición que en el **header** tiene un campo **destino** con información del contexto de ejecución que indica quién es el cliente y el contenido del **body** es igual al del paquete de entrada.

Transformación T4inv (input: p-gis-soap:SOAP):SOAP

Recibe un paquete WS-SOAP con información de ruteo y la quita devolviendo otro paquete SOAP

Pre \equiv { p-soapA / PaqueteSOAP(p-soapA) AND T4(p-soapA) }

Post \equiv { p-soap:=T4inv(p-soapA), / \neg (p-soap.header \supset p-soapA.header.destino) AND (p-soap.body=p-soapA.body) }

Esta transformación tiene como precondition que recibe un paquete SOAP (p-soapA) que cumple las poscondiciones de la Transformación T4. Al aplicar la Transformación T4inv se obtiene otro paquete (p-soap) SOAP que cumple que en el **header** no hay un campo **destino** y la información en el **body** es igual a la que trae el paquete de entrada.

Transformación T5 (input: p-gis-soap:SOAP):SOAP

Recibe un paquete WS-SOAP y le agrega información de sesión devolviendo otro paquete SOAP

Pre \equiv { p-soap / PaqueteSOAP(p-soap) AND T1(p-soap) }

Post \equiv { p-soapS:=T5(p-soap), / (p-soapS.header.token = S_context.token) AND (p-soapS.body=p-soap.body) }

Esta transformación tiene como precondition que recibe un paquete SOAP (p-soap) que cumple las poscondiciones de la transformación T1. Al aplicar la transformación T5 se obtiene otro paquete SOAP (p-soapS) que cumple como poscondición que en el **header** se agrega un campo **token** que contiene un token de seguridad obtenido del contexto de seguridad y que el contenido del **body** es igual al body del paquete de entrada.

Transformación T5inv (input: p-gis-soap:SOAP):SOAP

Recibe un paquete WS-SOAP con información de sesión y la quita devolviendo otro paquete SOAP

Pre \equiv { p-soapS / PaqueteSOAP(p-soapS) AND T5(p-soapS) }

Post \equiv { p-soap:=T5inv(p-soapS), / \neg (p-soap.header \supset p-soapS.header.token) AND (p-soap.body=p-soapS.body) }

Esta transformación tiene como precondition que recibe un paquete SOAP (p-soapS) que cumple las poscondiciones de la transformación T5. Al aplicar la transformación T5inv se obtiene otro paquete SOAP (p-soap) que no contiene el campo **token** en el **header** y el body es igual al que trae el paquete de entrada.

Transformación T6 (input: resp-gis-soap:SOAP): SOAP

Convierte una respuesta WS-GIS-SOAP a un paquete WS-SOAP con información de Sesión.

<pre> Pre \equiv {resp-gis-soap / PaqueteSOAP(resp-gis-soap) AND T2(resp-gis-soap)} Post \equiv { resp-gis-soapS:=T6(resp-gis-soap), / (resp-gis-soapS.header.token = S_context.token) AND (resp-gis-soapS.body.contenido = resp-gis-soap.body.contenido)} </pre>

Esta transformación tiene como precondition que recibe un paquete SOAP (resp-gis-soap) que cumple las poscondiciones de la transformación T2. Al aplicar la transformación T6 se obtiene otro paquete SOAP (resp-gis-soapS) que contiene en el **header** un campo **token** con información de un token de sesión obtenido del contexto de seguridad y el contenido del **body** es igual al paquete de entrada.

Transformación T6inv (input: resp-gis-soapA:SOAP): SOAP

Convierte un paquete SOAP a otro paquete SOAP, quitando la información de sesión que trae.

<pre> Pre \equiv {resp-gis-soapS / PaqueteSOAP(resp-gis-soapS) AND T6(resp-gis-soapS)} Post \equiv {resp-gis-soap := T6inv(resp-gis-soapS), / PaqueteSOAP(resp-gis-soap) AND \neg ((resp-gis-soap.header \supset resp-gis-soapS.header.token) AND (resp-gis-soap.body.contenido = resp-gis-soapS.body.contenido))} </pre>
--

Esta transformación tiene como precondition que recibe un paquete SOAP (resp-gis-soapS) que cumple las poscondiciones de la transformación T6. Al aplicar la transformación T6inv se obtiene otro paquete SOAP que cumple las poscondiciones de no incluir el campo **token** en el **header** y tener en el **body** el mismo contenido que el paquete de entrada.

Transformación T7 (input: p-gis-soap: SOAP): SOAP

Convierte un paquete SOAP a otro paquete SOAP agregando información de Autorización.

<pre> Pre \equiv {p-gis-soap / PaqueteSOAP (p-gis-soap) AND T1(p-gis-soap)} Post \equiv {p-gis-soapA:=T7(p-gis-soap), / (PaqueteSOAP(p-gis-soapA)) AND (p-gis-soapA.header.auth \supset S_contexto.auth) AND (p-gis-soapA.body=p-gis-soap.body)} </pre>

Esta transformación tiene como precondition que recibe un paquete SOAP (p-gis-soap) que cumple las poscondiciones de la transformación T2. Al aplicar la transformación T7 se obtiene otro paquete SOAP (resp-gis-soapA) que contiene en el **header** un campo **auth** con información de un token de autorización obtenido del contexto de seguridad y el contenido del **body** es igual al paquete de entrada.

Transformación T7inv(input: p-gis-soapA:SOAP): SOAP

Convierte un paquete SOAP a otro paquete SOAP quitando la información de Autorización.

Pre $\equiv \{p\text{-gis-soapA} / \text{PaqueteSOAP}(p\text{-gis-soapA}) \text{ AND } T7(p\text{-gis-soapA})\}$

Post $\equiv \{p\text{-gis-soap} := T8inv(p\text{-gis-soapA}), / \text{PaqueteSOAP}(p\text{-gis-soap}) \text{ AND } \neg (p\text{-gis-soap.header} \supset S_context.auth) \text{ AND } (p\text{-gis-soap.body}=p\text{-gis-soapS.body})\}$

Esta transformación tiene como precondition que recibe un paquete SOAP (p-gis-soapA) que cumple las poscondiciones de la transformación T7. Al aplicar la transformación T7inv se obtiene otro paquete SOAP que no contiene en el **header** el campo **auth** y el contenido del **body** es igual al del paquete de entrada.

Transformación T8 (input: resp-gis-soap:SOAP): SOAP

Convierte un paquete SOAP a otro paquete SOAP agregando información de Autorización.

Pre $\equiv \{resp\text{-gis-soap} / \text{PaqueteSOAP}(resp\text{-gis-soap}) \text{ AND } T2(resp\text{-gis-soap})\}$

Post $\equiv \{resp\text{-gis-soapA}:=T8(resp\text{-gis-soap}), / (\text{PaqueteSOAP}(resp\text{-gis-soapA})) \text{ AND } (resp\text{-gis-soapA.header.auth} = S_context.auth) \text{ AND } (resp\text{-gis-soapA.body}=resp\text{-gis-soap.body})\}$

Esta transformación tiene como precondition que recibe un paquete SOAP (resp-gis-soap) que cumple las poscondiciones de la Transformación T2. Al aplicar la transformación T8 se obtiene otro paquete SOAP que contiene en el **header** un campo **auth** con un **token** de autorización obtenido del contexto de seguridad y el contenido del **body** es igual al del paquete de entrada.

Transformación T8inv(input: resp-gis-soap: SOAP):SOAP

Convierte un paquete SOAP a otro paquete SOAP quitando la información de Autorización.

Pre $\equiv \{resp\text{-gis-soapA} / \text{PaqueteSOAP}(resp\text{-gis-soapA}) \text{ AND } T8(resp\text{-gis-soapA})\}$

Post $\equiv \{resp\text{-gis-soap} := T8inv(resp\text{-gis-soapA}), / \text{PaqueteSOAP}(resp\text{-gis-soap}) \text{ AND } \neg (resp\text{-gis-soap.header} \supset S_context.auth) \text{ AND } (resp\text{-gis-soapA.body}=resp\text{-gis-soap.body})\}$

Esta transformación tiene como precondition que recibe un paquete SOAP (resp-gis-soapA) que cumple las poscondiciones de la transformación T8. Al aplicar la transformación T8inv se obtiene otro paquete SOAP que no contiene en el **header** el campo **auth** y el contenido del **body** es igual al del paquete de entrada.

4.2.3 Flujos

En esta sección se presenta una especificación de los Flujos analizados en la sección 4.1. Los Flujos representan las comunicaciones que recibe y envía el componente encargado de las transformaciones y muestran la secuenciación en el uso de las transformaciones de acuerdo a cada necesidad.

En cada flujo se considera como precondition que existen los actores que participan en el mismo:

- Un cliente que genera pedidos WS-GIS.
- La PGE que brinda su infraestructura para que esos pedidos se realicen.
- Un servidor de mapas que atiende los pedidos WS-GIS.

La poscondición de los flujos es que la aplicación de todo el flujo sobre el pedido del cliente le devuelve exactamente lo que el servidor generó ante su pedido.

Flujo 1 - Ruteo de pedido Request-Response

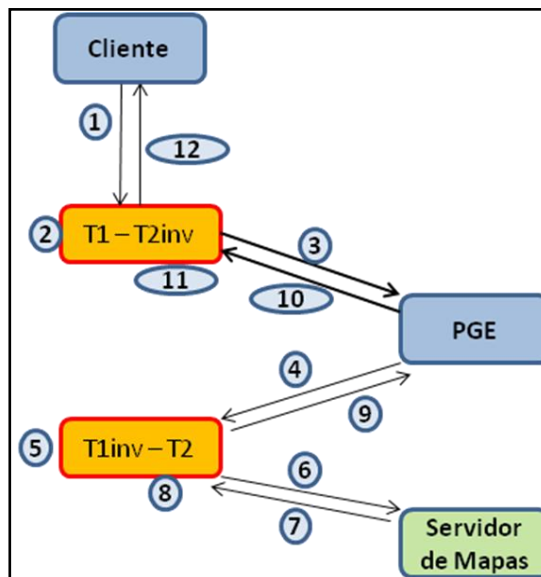
Pre $\equiv \{\exists \text{ Cliente, PGE, Servidor de Mapas}\}$

Flujo 1 - Request-Response

- 1 - llega pedido p-gis / WS-GIS(p-gis) de **Cliente**
- 2 - genero p-gis-soap := T1(p-gis)
- 3 - envío p-gis-soap a **PGE**
- 4 - recibo p-gis-soap de **PGE**
- 5 - genero p-gis:=T1inv(p-gis-soap)
- 6 - envío p-gis a **Servidor de Mapas**

resp-gis: = servMapas(p-gis)

- 7 - recibo resp-gis de **Servidor de Mapas**
- 8 - genero resp-gis-soap:=T2(resp-gis)
- 9 - envío resp-gis-soap a **PGE**
- 10 - recibo resp-gis-soap de **PGE**
- 11 - genero resp-gis:=T2inv(resp-gis-soap)
- 12 - envío resp-gis a **Cliente**



Post $\equiv \{\text{Flujo1(p-gis)=resp-gis=servMapas(p-gis)}\}$

El Flujo 1 define el ruteo de un pedido WS-GIS y las transformaciones que se aplican en los Componentes de Transformación de Protocolos. A la izquierda se presenta un detalle de los pasos del Flujo, a la derecha se muestra un esquema gráfico de las comunicaciones. La poscondición del Flujo es que el cliente recibe como respuesta exactamente lo que el servidor de mapas genera como respuesta ante su pedido. Es decir que con la aplicación del Flujo, el servidor de mapas recibe exactamente el pedido que el cliente realizó y el cliente recibe exactamente la respuesta que el servidor de mapas generó.

Flujo 2 - Ruteo de pedido Asincrónico

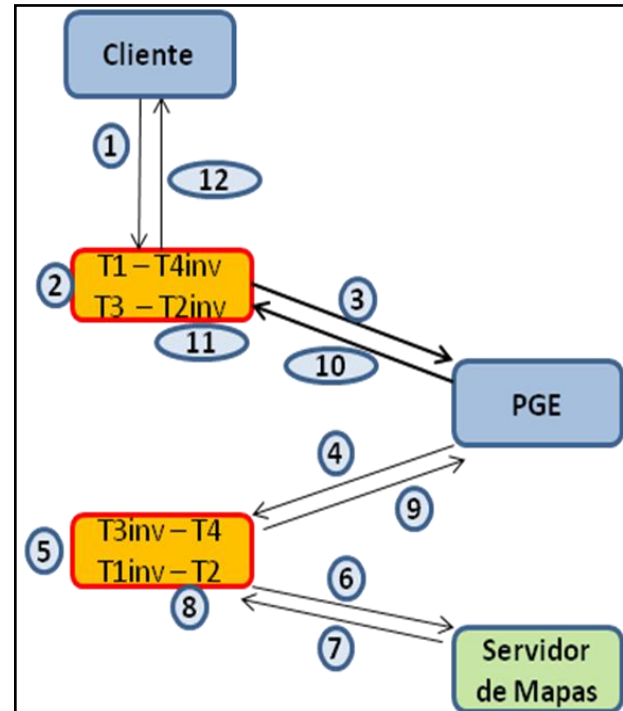
Pre $\equiv \{\exists \text{ cliente, PGE, Servidor de Mapas}\}$

Flujo 2 – pedido Asincrónico

- 1- llega pedido p-gis / WS-GIS(p-gis) de **Cliente**
- 2- genero p-gis-soap := T1(p-gis)
- 2- genero p-gis-soapA := T3(p-gis-soap)
- 3- envío p-gis-soapA a **PGE**
- 4- recibo p-gis-soapA de **PGE**
- 5- genero p-gis-soap := T3inv(p-gis-soapA)
- 5- genero p-gis := T1inv(p-gis-soap)
- 6- envío p-gis a **Servidor de Mapas**

resp-gis = servMapas(p-gis)

- 7 - recibo resp-gis de **Servidor de Mapas**
- 8 - genero resp-gis-soap:=T2(resp-gis)
- 8 - genero resp-gis-soapA:= T4(resp-gis-soap)
- 9 - envío resp-gis-soapA a **PGE**
- 10 - recibo resp-gis-soapA de **PGE**
- 11 - genero resp-gis-soap:= T4inv(resp-gis-soapA)
- 11 - genero resp-gis:= T2inv(resp-gis-soap)
- 12 - envío resp-gis a **Cliente**



Post $\equiv \{\text{Flujo2}(\text{p-gis}) = \text{resp-gis} = \text{servMapas}(\text{p-gis})\}$

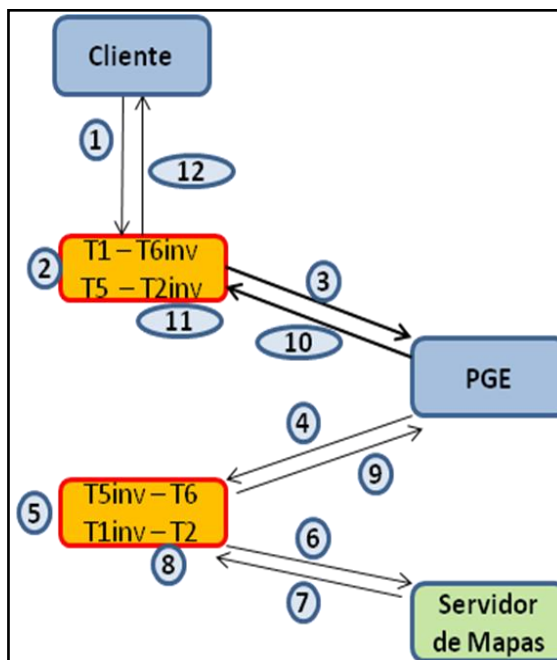
El Flujo 2 define el ruteo de un pedido WS-GIS con Asincronismo y las Transformaciones que se aplican en los Componentes de Transformación de Protocolos. A la izquierda se presenta un detalle de los pasos del Flujo, a la derecha se muestra un esquema gráfico de las comunicaciones. La poscondición del Flujo es que el cliente recibe como respuesta exactamente lo que el servidor de mapas genera como respuesta ante su pedido. Es decir que con la aplicación del Flujo, el servidor de mapas recibe exactamente el pedido que el cliente realizó y el cliente recibe exactamente la respuesta que el servidor de mapas generó.

Flujo 3 - Ruteo de pedido con Seguridad - Sesión

Pre $\equiv \{\exists \text{ Cliente, PGE, Servidor de Mapas}\}$

Flujo 2 – pedido con Seguridad

- llega pedido p-gis / WS-GIS(p-gis) de **cliente**
- genero p-gis-soap := T1(p-gis)
- genero p-gis-soapS := T5(p-gis-soap)
- envío p-gis-soapS a **PGE**
- recibo p-gis-soapS de **PGE**
- genero p-gis-soap := T5inv(p-gis-soapS)
- genero p-gis:=T1inv(p-gis-soap)
- envio p-gis a **servidor de mapas**
- recibo resp-gis de **servidor de mapas**
- genero resp-gis-soap:=T2(resp-gis)
- genero resp-gis-soapS:= T6(resp-gis-soap)
- envio resp-gis-soapS a **PGE**
- recibo resp-gis-soapS de **PGE**
- genero resp-gis-soap:= T6inv(resp-gis-soapS)
- genero resp-gis:= T2inv(resp-gis-soap)
- envio resp-gis a **cliente**



Post $\equiv \{\text{Flujo3(p-gis)} = \text{resp-gis} = \text{servMapas(p-gis)}\}$

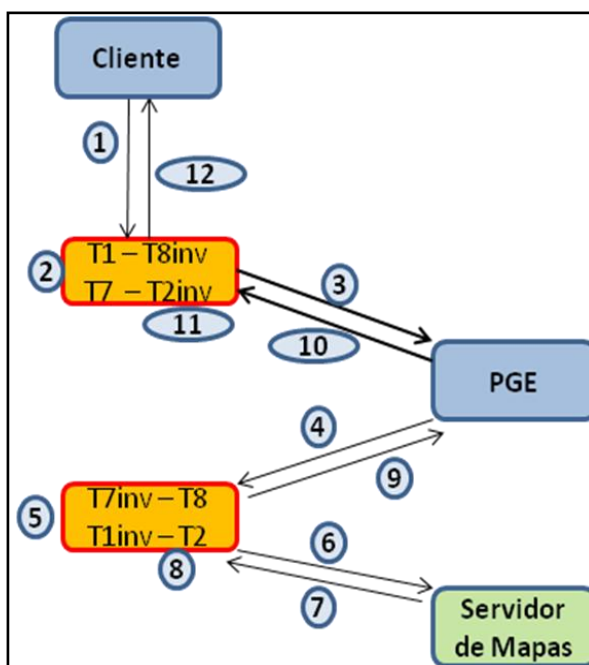
El Flujo 3 define el ruteo de un pedido WS-GIS con Seguridad y las transformaciones que se aplican en los Componentes de Transformación de Protocolos. A la izquierda se presenta un detalle de los pasos del Flujo, a la derecha se muestra un esquema gráfico de las comunicaciones. La poscondición del Flujo es que el cliente recibe como respuesta exactamente lo que el servidor de mapas genera como respuesta ante su pedido. Es decir que con la aplicación del Flujo, el servidor de mapas recibe exactamente el pedido que el cliente realizó y el cliente recibe exactamente la respuesta que el servidor de mapas generó.

Flujo 3 - Ruteo de pedido con Seguridad - Autorización

Pre $\equiv \{\exists \text{ Cliente, PGE, Servidor de Mapas}\}$

Flujo 2 – pedido con Seguridad

- llega pedido p-gis / WS-GIS(p-gis) de **cliente**
- genero p-gis-soap := T1(p-gis)
- genero p-gis-soapS := T7(p-gis-soap)
- envío p-gis-soapS a **PGE**
- recibo p-gis-soapS de **PGE**
- genero p-gis-soap := T7inv(p-gis-soapS)
- genero p-gis:=T1inv(p-gis-soap)
- envio p-gis a **servidor de mapas**
- recibo resp-gis de **servidor de mapas**
- genero resp-gis-soap:=T2(resp-gis)
- genero resp-gis-soapS:= T8(resp-gis-soap)
- envio resp-gis-soapS a **PGE**
- recibo resp-gis-soapS de **PGE**
- genero resp-gis-soap:= T8inv(resp-gis-soapS)
- genero resp-gis:= T2inv(resp-gis-soap)
- envio resp-gis a **cliente**



Post $\equiv \{\text{Flujo3(p-gis)} = \text{resp-gis} = \text{servMapas(p-gis)}\}$

El Flujo 3 define el ruteo de un pedido WS-GIS con Seguridad y las transformaciones que se aplican en los Componentes de Transformación de Protocolos. A la izquierda se presenta un detalle de los pasos del Flujo, a la derecha se muestra un esquema gráfico de las comunicaciones. La poscondición del Flujo es que el cliente recibe como respuesta exactamente lo que el servidor de mapas genera como respuesta ante su pedido. Es decir que con la aplicación del Flujo, el servidor de mapas recibe exactamente el pedido que el cliente realizó y el cliente recibe exactamente la respuesta que el servidor de mapas generó.

4.2.4 Demostraciones

En esta sección se muestra como aplicando las transformaciones a lo largo de un flujo se cumplen las propiedades deseadas. Las demostraciones se hacen por construcción aplicando las definiciones previas y las definiciones de las transformaciones. Se muestran las transformaciones de datos generadas por el Componente de Transformación de Protocolos (CTP).

A la izquierda se muestran las transformaciones de datos que realiza el CTP y a la derecha las propiedades que se aplican. De este modo se llega a que la poscondición del flujo vale.

Teorema 4.1 El Flujo 1 cumple con las condiciones establecidas en la poscondición.

Hipótesis: dados un cliente, la Plataforma de Gobierno Electrónico, un Servidor de Mapas y el Componente de Transformación de Protocolos. Teniendo en cuenta la definición del Flujo 1.

Tesis: para todo pedido p-gis del cliente vale la Poscondición:

Post $\equiv \{\text{Flujo1}(\text{p-gis}) = \text{resp-gis} = \text{servMapas}(\text{p-gis})\}$

Demostración:

1 - Se recibe pedido p-gis formado por: endpoint, servicio, metodo, parametros.	(Definición 4.2)
2 - Se genera p-gis-soap := T1(p-gis) que cumple: p-gis-soap.header.receiver= p-gis.endpoint p-gis-soap.body.servicio = p-gis.servicio p-gis-soap.body.metodo = p-gis.metodo p-gis-soap.body.parametros = p-gis.parametros	(por Definición 4.1, Transformación T1)
3 - Se genera pf-gis:=T1inv(p-gis-soap) que cumple: pf-gis.endpoint = p-gis-soap .header.receiver pf-gis.servicio= p-gis-soap .body.servicio pf-gis.metodo= p-gis-soap .body.metodo pf-gis.parametros= p-gis-soap .body.parametros	(por Definición 4.2, Transformación T1inv)
4 - se obtiene resp-gis := servMapas(pf-gis)	(por Definición función servMapas)
5 - se genera resp-gis-soap:=T2(resp-gis) que cumple: resp-gis-soap.body.contenido = resp-gis.contenido	(por Definiciones 4.1 y 4.3, Transformación T2)
6 - se genera respf-gis:=T2inv(resp-gis-soap) que cumple: respf-gis.contenido=resp.gis-soap.body.contenido	(por Definición 4.3, Transformación T2inv)
<p>Por los pasos 2 y 3 se deduce que pf-gis = p-gis, el servidor de mapas recibe un pedido igual al generado por el cliente. Por el paso 4 se obtiene resp-gis=servMapas(pf-gis)=servMapas(p-gis). Por los pasos 5 y 6 se deduce que respf-gis=resp-gis, el cliente recibe una respuesta igual a la generada por el servidor de Mapas. Entonces:</p>	
<p>Flujo1(p-gis) = respf-gis que es equivalente a resp-gis=servMapas(pf-gis) y como pf-gis=p-gis vale resp-gis=servMapas(p-gis).</p>	

Teorema 4.2 El Flujo 2 cumple con las condiciones establecidas en la poscondición.

Hipótesis: dados un cliente, la Plataforma de Gobierno Electrónico, un Servidor de Mapas y el Componente de Transformación de Protocolos. Teniendo en cuenta la definición del Flujo 2.

Tesis: para todo pedido p-gis del cliente vale la Poscondición:

Post $\equiv \{\text{Flujo2}(\text{p-gis}) = \text{resp-gis} = \text{servMapas}(\text{p-gis})\}$

Demostración:

1 - Se recibe pedido p-gis formado por: endpoint, servicio, metodo, parametros.	(Definición 4.2)
2 - Se genera p-gis-soap := T1(p-gis) que cumple: Transformación T1) p-gis-soap.header.receiver= p-gis.endpoint p-gis-soap.body.servicio = p-gis.servicio p-gis-soap.body.metodo = p-gis.metodo p-gis-soap.body.parametros = p-gis.parametros	(por Definición 4.1,
3 - Se genera pf-gis:=T1inv(p-gis-soap) que cumple: pf-gis.endpoint = p-gis-soap .header.receiver pf-gis.servicio= p-gis-soap .body.servicio pf-gis.metodo= p-gis-soap .body.metodo pf-gis.parametros= p-gis-soap .body.parametros	(por Definición 4.2, Transformación T1inv)
4 - Se obtiene resp-gis := servMapas(pf-gis)	(por Definición función servMapas)
5 - se genera resp-gis-soap:=T2(resp-gis) que cumple: resp-gis-soap.body.contenido = resp-gis.contenido	(por Definiciones 4.1 y 4.3, Transformación T2)
6 - Se genera respf-gis:=T2inv(resp-gis-soap) que cumple: respf-gis.contenido=resp.gis-soap.body.contenido	(por Definición 4.3, Transformación T2inv)
Por los pasos 2 y 3 se deduce que pf-gis = p-gis, el servidor de mapas recibe un pedido igual al generado por el cliente. Por el paso 4 se obtiene resp-gis=servMapas(pf-gis)=servMapas(p-gis). Por los pasos 5 y 6 se deduce que respf-gis=resp-gis, el cliente recibe una respuesta igual a la generada por el servidor de Mapas. Entonces:	
Flujo1(p-gis) = respf-gis que es equivalente a resp-gis=servMapas(pf-gis) y como pf-gis=p-gis vale resp-gis=servMapas(p-gis).	

Teorema 4.3 El Flujo 3 cumple con las condiciones establecidas en la poscondición.

Hipótesis: dados un cliente, la Plataforma de Gobierno Electrónico, un Servidor de Mapas y el Componente de Transformación de Protocolos. Teniendo en cuenta la definición del Flujo 3.

Tesis: para todo pedido p-gis del cliente vale la Poscondición:

Post $\equiv \{\text{Flujo3}(\text{p-gis}) = \text{resp-gis} = \text{servMapas}(\text{p-gis})\}$

Demostración:

Se recibe pedido p-gis formado por: endpoint, servicio, metodo, parametros.	(Definición 4.2)
Se genera p-gis-soap := T1(p-gis) que cumple:	(por Definición 4.1, Transformación T1)
p-gis-soap.header.receiver = p-gis.endpoint p-gis-soap.body.servicio = p-gis.servicio p-gis-soap.body.metodo = p-gis.metodo p-gis-soap.body.parametros = p-gis.parametros	
Se genera pf-gis:=T1inv(p-gis-soap) que cumple:	(por Definición 4.2, Transformación T1inv)
pf-gis.endpoint = p-gis-soap .header.receiver pf-gis.servicio= p-gis-soap .body.servicio pf-gis.metodo= p-gis-soap .body.metodo pf-gis.parametros= p-gis-soap .body.parametros	
Se obtiene resp-gis := servMapas(pf-gis)	(por Definición función servMapas)
se genera resp-gis-soap:=T2(resp-gis) que cumple:	(por Definiciones 4.1 y 4.3, Transformación T2)
resp-gis-soap.body.contenido = resp-gis.contenido	
Se genera respf-gis:=T2inv(resp-gis-soap) que cumple:	(por Definición 4.3, Transformación T2inv)
respf-gis.contenido=resp-gis-soap.body.contenido	
Por los pasos 2 y 3 se deduce que pf-gis = p-gis, el servidor de mapas recibe un pedido igual al generado por el cliente. Por el paso 4 se obtiene resp-gis=servMapas(pf-gis)=servMapas(p-gis).	
Por los pasos 5 y 6 se deduce que respf-gis=resp-gis, el cliente recibe una respuesta igual a la generada por el servidor de Mapas. Entonces:	
Flujo1(p-gis) = respf-gis que es equivalente a resp-gis=servMapas(pf-gis) y como pf-gis=p-gis vale resp-gis=servMapas(p-gis) .	

Sección 4.3 - Alternativas de Implementación

En esta sección se presentan posibles mecanismos de implementación de la solución propuesta considerando la Plataforma de Gobierno Electrónico de AGESIC: PGEUy.

4.3.1 Descripción General

Los componentes centrales de la PGE usada para la propuesta de solución se corresponden con los componentes de la PGE de AGESIC como se muestra en la siguiente figura. El GeoPortal (1-izquierda) de la propuesta se corresponde con la Aplicación GeoPortal (1-derecha) de la PGE de AGESIC. Lo mismo ocurre con el Sistema de Seguridad (2) y la Plataforma de Middleware (3), ambos componentes base en la PGE de AGESIC. El componente de Servicio de Catálogo (4) tiene información sobre la Información Geográfica disponible y se comporta en forma similar al Sistema de Gestión de Metadatos de la PGE de AGESIC.

Los servicios ofrecidos por organismos proveedores (5) se corresponden a los Organismos del Estado que se interconectan a través de la REDUy. Estos organismos pueden ofrecer tanto servicios de negocio SOAP como Servicios de Mapas.

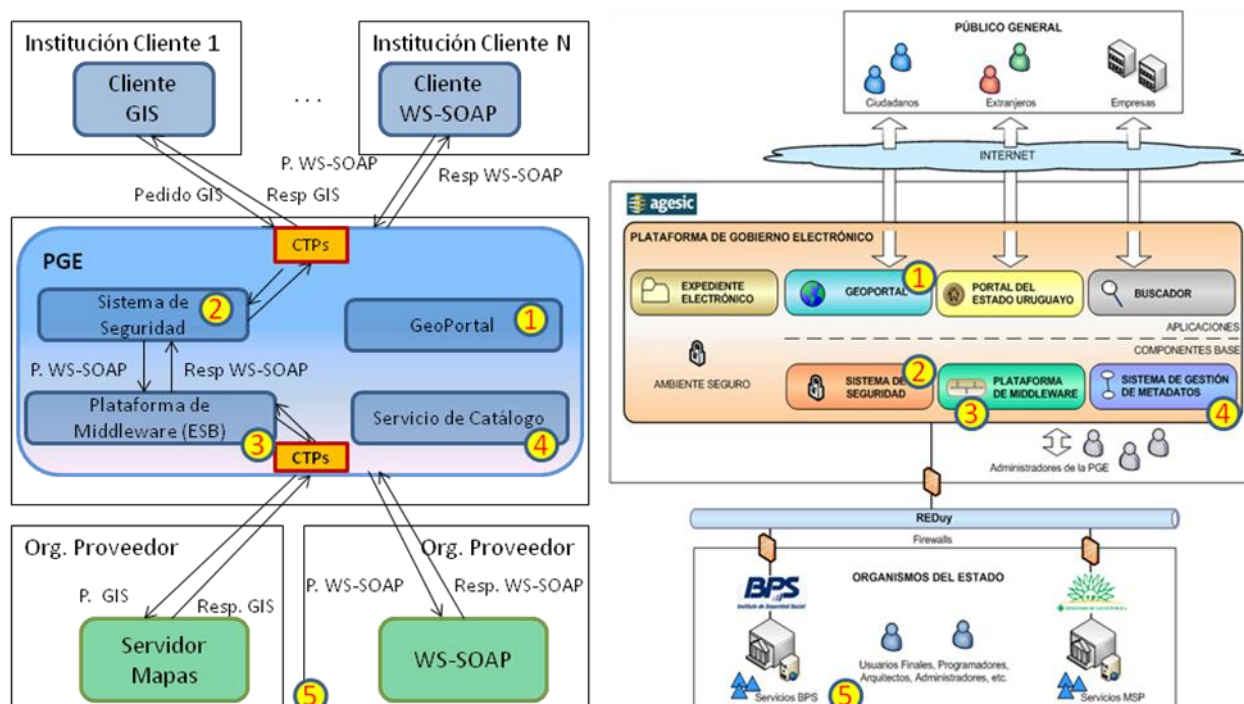


Figura 18 - Mapeo de la Solución a la PGE Uy

De acuerdo a la Plataforma de Gobierno Electrónico que se use las Transformaciones propuestas en esta tesis pueden implementarse de diferentes formas. En particular, el Contexto de Operación y Seguridad puede ser guardado por la PGE y ofrecido a través de algún servicio de consulta interno.

Clientes

Como se mencionó en el capítulo 2 hay varios productos tanto de Visualizadores Web como de Clientes GIS Desktop que ya tienen implementados los clientes de los Web Services Geográficos. En la solución propuesta no se tienen que cambiar estos clientes, sino que siguen funcionando como hasta ahora.

Los clientes deberán realizar sus pedidos a un Proxy que está en la PGE en lugar de ir directamente al Servidor de Mapas del organismo proveedor. El proxy se encargará de aplicar las transformaciones para que los pedidos viajen dentro de la plataforma.

Ruteo de pedidos

Usando las características de virtualización de servicios que provee la PGE se definirán Endpoints en la plataforma que representan los diferentes servicios geográficos registrados. De acuerdo a las características del servicio geográfico se definirán los atributos del endpoint en la plataforma. Este será un endpoint virtual que representa al servidor de mapas destino. El Endpoint mandará el pedido a través del ESB a un componente Gateway.

Componentes de Transformación de Protocolos

Las Transformaciones de Protocolos serán aplicadas a los pedidos y respuestas de Web Services Geográficos por los componentes que llamamos Proxy y Gateway. Ambos pueden ser implementados como servicios en la PGE y el Proxy será el punto de referencia para los clientes de WS-GIS. El componente Gateway será el responsable de comunicarse con los servidores de mapas y recibir sus respuestas.

Seguridad

A nivel de la PGE y de acuerdo a las políticas de acceso a la información que se definan entre los organismos, se tendrán que configurar las políticas en el componente de Seguridad. Dado que las transformaciones agregan información para la evaluación de las políticas de seguridad, el componente de seguridad podrá aplicar las políticas a los pedidos GIS transformados en paquetes SOAP como a cualquier otro pedido SOAP.

Servicios Geográficos

Servidor de Mapas – el componente que ofrece los Web Services Geográficos podrá ser cualquiera de los ya existentes en el mercado y no requiere modificación alguna para la implementación de la solución propuesta.

4.3.2 Implementación de las Transformaciones de Protocolos

Para la implementación de las Transformaciones se tiene en cuenta la estructura de la PGEUy.

Las transformaciones T1, T1inv, T2 y T2inv arman y desarman los pedidos originales a paquetes SOAP. La transformación T1 tiene que ser aplicada antes de que los pedidos lleguen a la PGE. Por esto se propone como una alternativa de implementación que los clientes usen un Componente de Transformación de Protocolos a modo de Proxy. Dicho componente puede instalarse en la PGE para recibir todos los pedidos de los clientes de WS-GIS o puede ser implementado como un plugin de los clientes.

Otras transformaciones se aplican antes de enviar el pedido al Servidor de Mapas y al recibir sus respuestas. Estas se agruparán en un componente que llamaremos Gateway.

En la siguiente figura se muestra la ubicación de las Transformaciones en relación a los componentes de la PGE considerando solamente clientes GIS y el Servidor de Mapas.

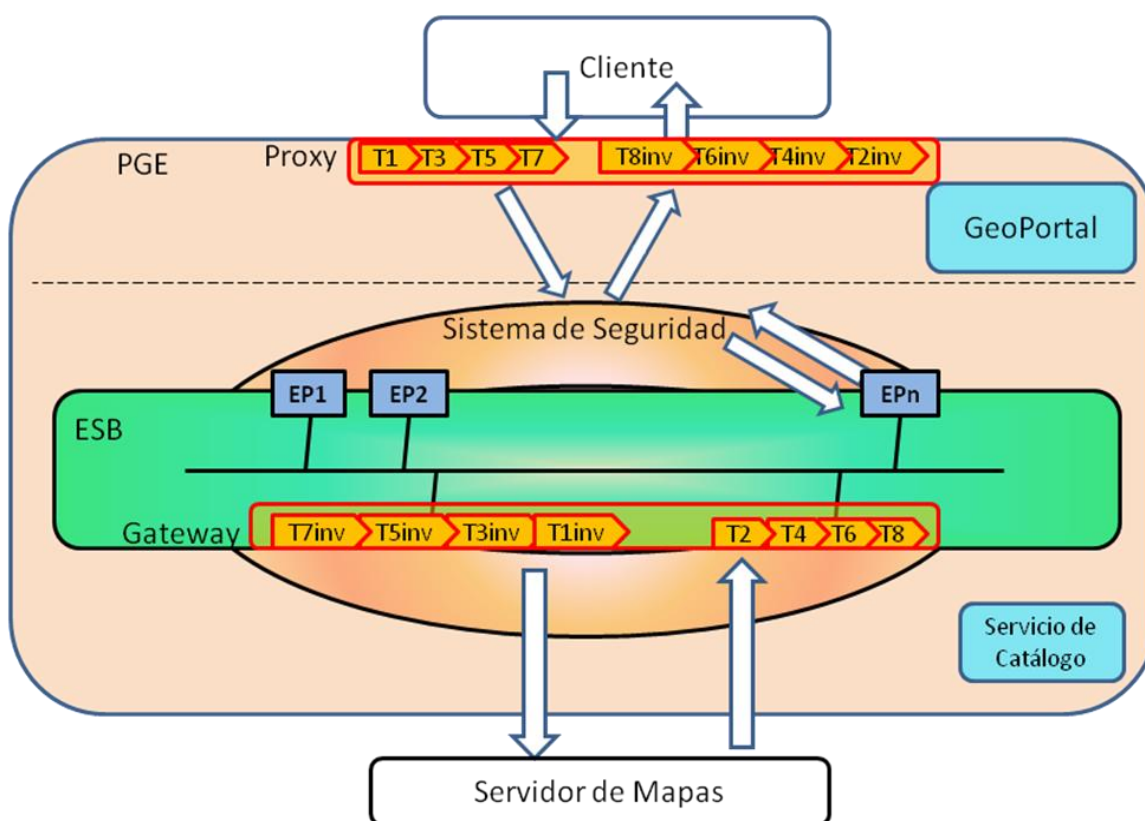


Figura 19 - Ubicación de los Transformadores

Las Transformaciones con número impar (T1, T3, T5, T7) se alojan en el proxy que usa el cliente para conectarse a la plataforma, ya que arman los pedidos en los paquetes SOAP. Las transformaciones con número impar inversas (T1inv, T3inv, T5inv, T7inv) están en un Gateway que desarma los pedidos para ser enviados al Servidor de Mapas.

Las Transformaciones con número par (T2, T4, T6, T8) están en el Gateway que recibe la respuesta desde el servidor de mapas, armándola en un paquete SOAP. Las Transformaciones con número par inversas (T2inv, T4inv, T6inv, T8inv) se aplican en el componente Proxy, desarmando los paquetes SOAP de respuesta para enviárselas al cliente.

En la Figura 20 - Arquitectura de Implementación los Endpoints (EP) corresponden tanto a servicios de negocio basados en el protocolo SOAP publicados en la PGE como a un endpoint virtual que representa a un a servicio geográfico.

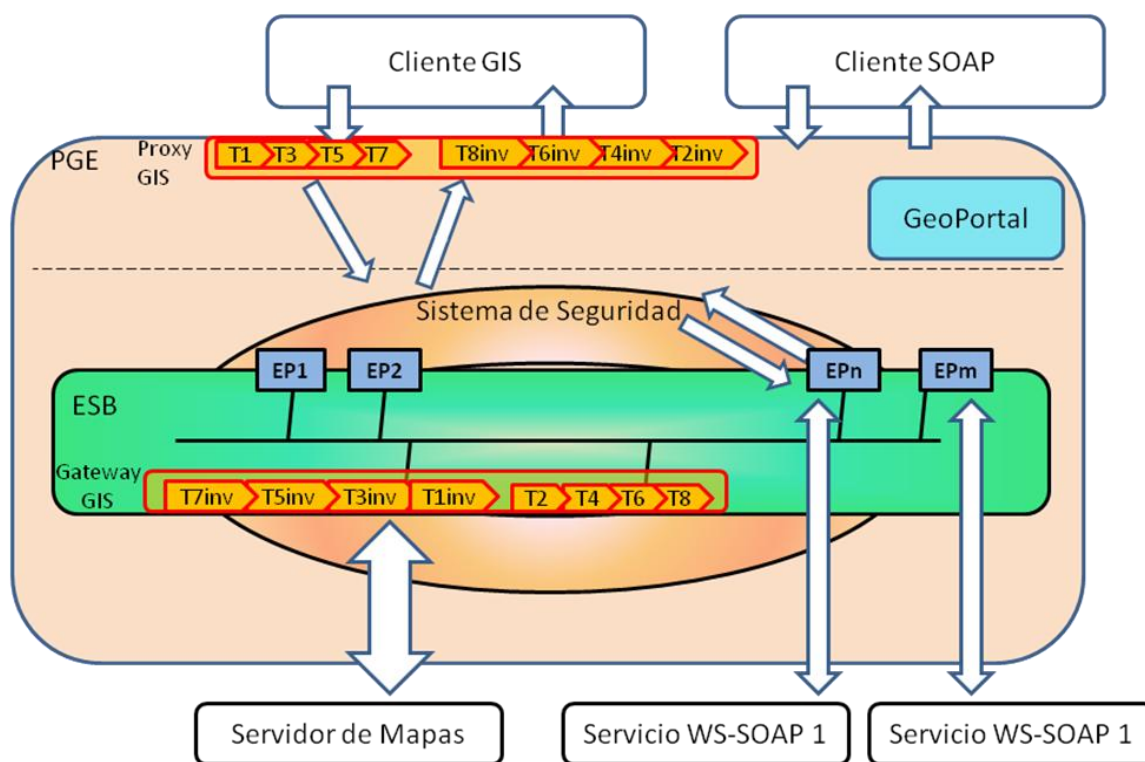


Figura 20 - Arquitectura de Implementación

En la Figura 20 se muestra la solución planteada con la inclusión de servicios basados en SOAP y clientes SOAP. Los pedidos de los clientes SOAP van directo a los endpoints de los servicios WS-SOAP en el ESB. Este endpoint es el que hace el llamado al servicio real en el Organismo Proveedor.

4.3.3 Implementación de Flujos

La implementación de los flujos no requiere ningún desarrollo adicional. Al definir los EndPoints de los servicios y definir sus características usando las herramientas del ESB, los flujos se pueden ejecutar directamente en la PGE usando las herramientas que ésta ya posee.

Para el Flujo 1, de acuerdo a su especificación, se usarán las Transformaciones T1, T1inv, T2 y T2inv. En este caso al publicar el servicio geográfico en la PGE, se creará un endpoint en el ESB con estos requerimientos: servicio de acceso público que no requiere seguridad. El cliente envía pedidos WMS o WFS al componente Proxy GIS (Paso 1). Este componente al recibir el pedido será el que al consultar las características del servicio a invocar aplicará la Transformación T1 y enviará el pedido SOAP a la plataforma para que vaya al endpoint que corresponde (Paso 2). El pedido pasará por el Sistema de seguridad (Paso 3). Cuando el pedido llega al endpoint, se ruteará al servicio real en el Servidor de Mapas destino a través del Gateway quién aplicará la transformación T1inv (Paso 4). La respuesta que genera el Servidor de Mapas la toma el Gateway (Paso 5) y aplicando la transformación T2 la devuelve al endpoint dentro de la plataforma para que envíe la respuesta de regreso (Paso 6). Dicha respuesta pasa

por el Proxy GIS que aplica la Transformación T2inv para desarmar el paquete SOAP y enviar la respuesta al cliente (8).

En la Figura 21 se muestra el recorrido del Flujo 1 a través de la Plataforma de Gobierno Electrónico.

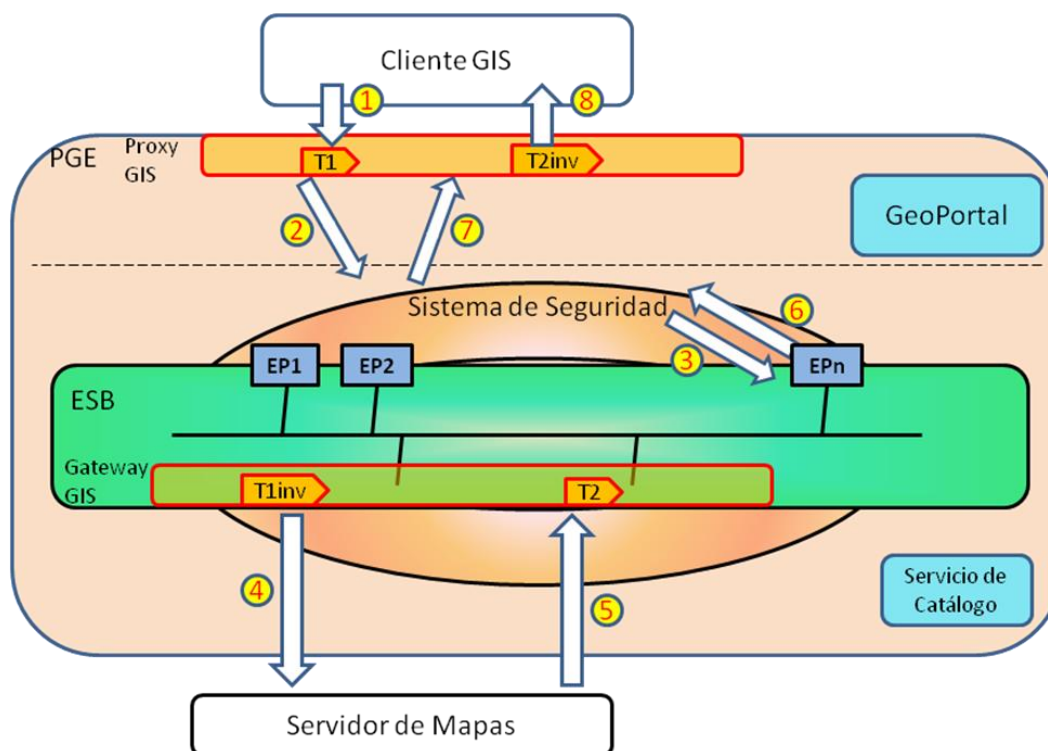


Figura 21 - Flujo 1

Para el Flujo 2, de acuerdo a su especificación, se usarán las Transformaciones T1, T1inv, T2, T2inv, T3, T3inv, T4 y T4inv. En este caso al publicar el servicio geográfico en la PGE, se creará un endpoint SOAP en el ESB con estos requerimientos: servicio de acceso público que no requiere seguridad y que puede responder en forma Asíncrona. El cliente envía pedidos WMS o WFS al componente Proxy GIS (Paso 1). Este componente al recibir el pedido será el que al consultar las características del servicio a invocar aplicará las Transformaciones T1 y T3. Luego enviará el pedido SOAP a la plataforma para que vaya al endpoint que corresponde (Paso 2). El pedido pasará por el Sistema de seguridad para llegar al endpoint (Paso 3). Cuando el pedido llega al endpoint, se ruteará al servicio real en el Servidor de Mapas destino a través del Gateway quién aplicará las transformaciones T1inv y T3inv para desarmar el paquete SOAP y mandar el pedido original al Servidor de Mapas (Paso 4). La respuesta que genera el Servidor de Mapas la toma el Gateway (Paso 5) y aplicando las transformaciones T2 y T4 la devuelve al endpoint dentro de la plataforma para que envíe la respuesta de regreso (Paso 6). Dicha respuesta pasa por el Proxy GIS que aplica las transformaciones T2inv y T4inv para desarmar el paquete SOAP y enviar la respuesta al destino (8). Este recorrido es el que se muestra en la Figura 22 a continuación.

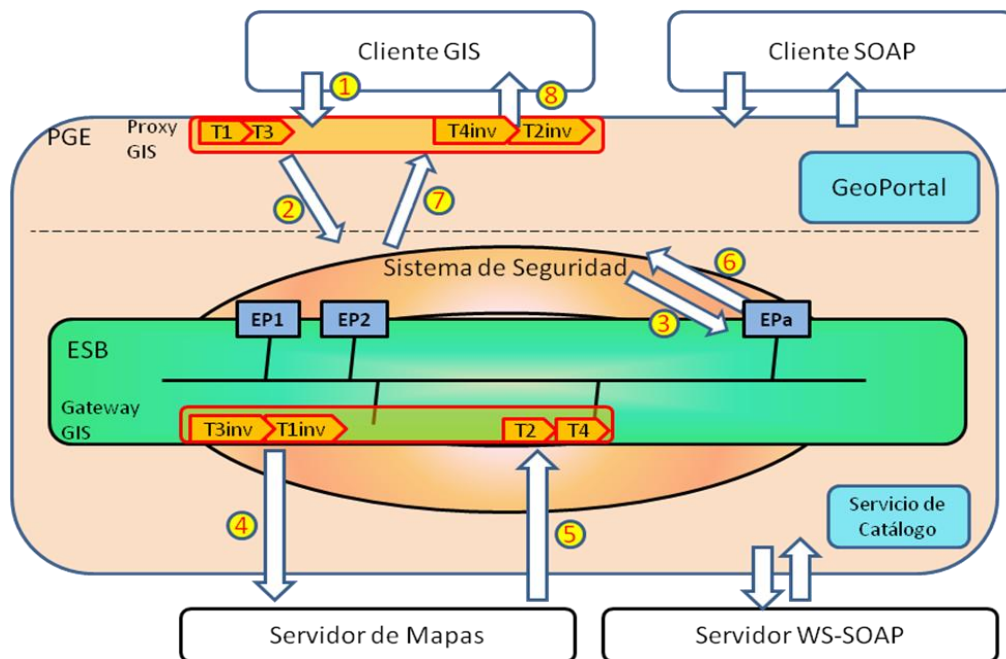


Figura 22 - Flujo 2

Para el Flujo 3, de acuerdo a su especificación, se usarán las Transformaciones T1, T1inv, T2, T2inv, T5, T5inv, T6, T6inv, T7, T7inv, T8 y T8inv. En este caso al publicar el servicio geográfico en la PGE, se creará un endpoint en el ESB con estos requerimientos: servicio que requiere credenciales de seguridad. El cliente envía pedidos WMS o WFS al componente Proxy GIS (Paso 1). Este componente al recibir el pedido verá que al consultar las características del servicio a invocar aplicará las transformaciones T1, T5 y T7 y enviará el pedido SOAP a la plataforma para que vaya al endpoint que corresponde (Paso 2). El pedido pasará por el Sistema de Seguridad que validará las credenciales (Paso 3). Cuando el pedido llega al endpoint, se ruteará al servicio real en el Servidor de Mapas destino a través del Gateway quién aplicará las transformaciones T7inv, T5inv y T1inv (Paso 4). La respuesta que genera el Servidor de Mapas la toma el Gateway (Paso 5) y aplicando las transformaciones T2, T6 y T8 la devuelve al endpoint dentro de la plataforma para que envíe la respuesta de regreso (Paso 6). Dicha respuesta pasa por el Proxy GIS que aplica las transformaciones T8inv, T6inv y T2inv para desarmar el paquete SOAP y enviar la respuesta al cliente (8).

En la Figura 23 se muestra el Flujo 3 completo a través de la PGE. En este caso se asume el escenario de mayor seguridad, que requiere autenticación (una sesión) y autorización.

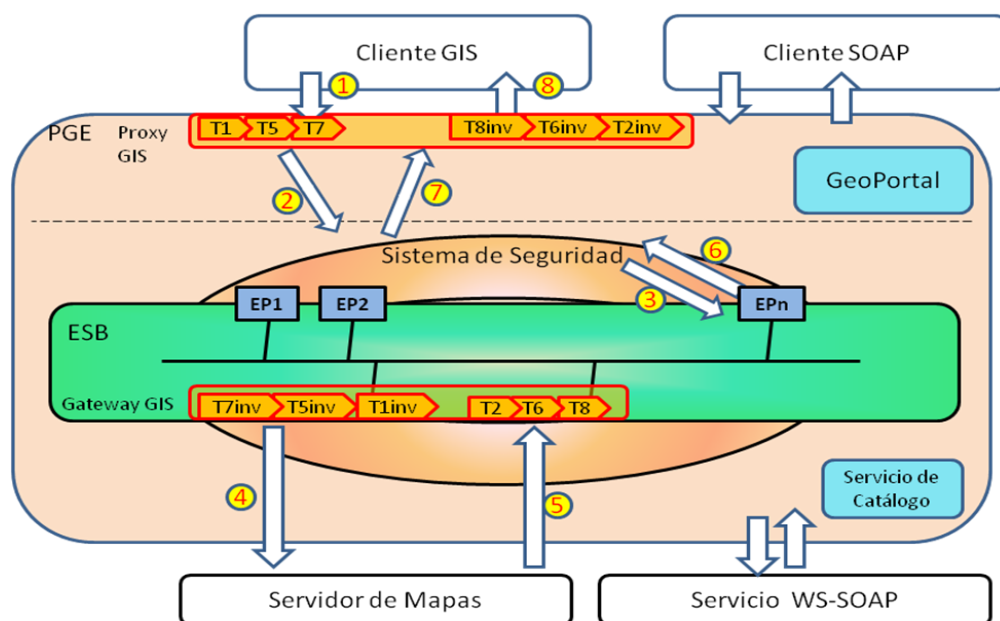


Figura 23 - Flujo 3

4.3.4 Relación Escenarios – Flujos

El análisis de aplicaciones de integración de web services geográficos se basó en escenarios de uso. Dichos escenarios iban aumentando la complejidad de la aplicación. Al realizar el análisis técnico para proponer una solución nos centramos en los Flujos de Información en la Plataforma de Gobierno Electrónico. En esta sección se presenta cómo dichos Flujos cumplen con los escenarios de aplicación propuestos.

Escenario I – Flujo 1

Este escenario lo origina un cliente para solicitar datos públicos. Por lo tanto con lo que brinda el Flujo 1 de ruteo de pedidos sin seguridad, se podrá ejecutar el pedido.

Escenario II – Flujo 3

Este escenario lo origina un cliente específico para solicitar datos restringidos a cierto público. Por lo tanto con lo que brinda el Flujo 3 de ruteo de pedidos con seguridad, se puede ejecutar el pedido.

Escenario III – Flujo 3

Este escenario lo origina un cliente específico para solicitar o ingresar datos restringidos a cierto público. Por lo tanto con lo que brinda el Flujo 3 de ruteo de pedidos con seguridad, se puede ejecutar el pedido. Aquí la diferencia es el tipo de pedido realizado, pero esto es transparente para los Componentes de Transformación de Protocolos.

Escenario IV – Flujos 2 y 3

Este escenario propone que los pedidos WS-GIS sean encadenados con otros pedidos a servicios de negocio. Usando las transformaciones de acuerdo al Flujo 3 se aseguran las propiedades de seguridad

que este requiere y usando el Flujo 2 se asegura que los pedidos y las respuestas puedan ser manejados en forma asincrónica por la Plataforma de Gobierno Electrónico.

Escenario V - Flujo 3

A nivel de la Plataforma de Gobierno Electrónico este escenario es idéntico al Escenario III, ya que las diferencias en funcionalidades son brindadas por el portal de la comunidad. En este caso, a nivel de seguridad, los usuarios en lugar de ser identificados por el organismo al que pertenecen, lo serán por la comunidad a la que pertenecen. Eso provoca que las credenciales de seguridad sean distintas, pero igual son codificadas en un token de seguridad.

Capítulo 5 – Conclusiones y Trabajos Futuros

En este Capítulo, en la Sección 5.1 se presenta un resumen del trabajo realizado y sus principales contribuciones, y en la Sección 5.2, se describen las actuales líneas de trabajo y se esbozan otras posibles líneas a futuro.

Sección 5.1 - Resumen y Contribuciones

Esta tesis presenta un análisis de escenarios de integración de Servicios de Información Geográfica a Plataformas de Gobierno Electrónico, identificando problemas de incompatibilidades entre los protocolos utilizados por los middleware utilizados en ambos tipos de sistemas, y proponiendo soluciones para los mismos.

El análisis de escenarios presentado en el Capítulo 3 aporta una visión general sobre los contextos de integración de servicios de información geográfica a plataformas de gobierno electrónico, los cuales han estado tradicionalmente separados. En este sentido, el conocimiento existente muestra un desarrollo muy importante de tecnologías y herramientas en ambos tipos de plataformas, pero basados en estándares y protocolos con diferencias tales que impiden su interacción automática. De este análisis cabe concluir, más allá del alcance de esta tesis, el enorme potencial de uso de servicios geográficos en Gobierno Electrónico, destacándose en particular el escenario de participación ciudadana interactuando con este tipo de información en servicios públicos en lo que se conoce como *Volunteered Geographic Information* (VGI) [43].

A partir de los escenarios de integración y de los protocolos utilizados para Web Services Geográficos y de uso general en Gobierno Electrónico, esta tesis identifica en detalle los problemas de compatibilidad entre los mismos que resulta relevantes para la integración de Servicios Geográficos en plataformas de Gobierno Electrónico. En resumen, estos problemas corresponden principalmente a diferencias en los formatos de paquetes de datos, en particular a que los paquetes, basados en SOAP, utilizados como principales en el middleware de uso general (Web Services y ESB), incluyen más información que los utilizados por los servidores de datos geográficos.

El encare de solución propuesto aborda los problemas de incompatibilidades antes mencionados en base a arquitecturas, tecnologías y plataformas actuales de última generación, de forma de que puedan aplicarse en forma incremental sobre plataformas y servicios existentes. Teniendo en cuenta la complejidad técnica y organizacional de los servicios de Gobierno Electrónico, tanto para su desarrollo como para su mantenimiento y evolución, consideramos de particular interés la exploración de soluciones que puedan aplicarse como agregados externos a sistemas existentes, utilizando al máximo los potenciales de las plataformas de middleware de tipo ESB, y minimizando los cambios en aplicaciones o servidores geográficos. Los resultados obtenidos muestran la factibilidad de este encare basado en la inserción de *Componentes de Transformación de Protocolos* en los puntos de integración de la plataforma de Gobierno Electrónico con los sistemas servidores y clientes de información geográfica.

Asimismo, entendemos importante destacar el aporte de la especificación formal de las transformaciones, que provee un marco para la demostración formal del cumplimiento de las propiedades de las transformaciones. Además del resultado obtenido en esta tesis, consistente en la especificación de transformaciones y demostraciones concretas realizadas, este encare permite avanzar en la aplicación de métodos formales para validar la correctitud de transformaciones y flujos que se especifiquen en este contexto de integración de sistemas.

Finalmente, con respecto a las perspectivas de implementación, las opciones presentadas, basadas en la Plataforma de Gobierno Electrónico (PGE) del Uruguay, muestran la posibilidad de uso mayoritario de software existente. Sin embargo, se identifica la necesidad de implementar un componente de tipo *Gateway* para la interacción de los Servidores de Mapas con la PGE.

En síntesis, entendemos que los aportes principales de esta tesis se encuentran en el análisis de escenarios de integración, el análisis técnico de los problemas de compatibilidad entre middleware usado en servidores geográficos y plataformas de gobierno electrónico de uso general, y la propuesta de solución planteada para lograr la integración. Como resultado general, los resultados obtenidos muestran la factibilidad de un encare de solución “no invasivo” y utilizando el potencial de los Enterprise Service Bus. Asimismo, la tesis aporta vías de solución directamente aplicables en el Uruguay.

Sección 5.2 - Trabajo en Curso y a Futuro

Esta tesis se inscribe en un marco de actividades académicas sobre Sistemas de Información Geográficos⁶, así como actividades en el contexto de la AGESIC para su aplicación en servicios públicos⁷, por lo que constituye naturalmente un paso intermedio más que un resultado final.

El trabajo en curso consiste en la profundización sobre la aplicación de tecnologías de middleware avanzado para la mejora de los Servicios de Información Geográficos y de su integración con otros sistemas, especialmente en el marco del Gobierno Electrónico. En particular, se avanza en el análisis de aplicación de otros mecanismos provistos por los Enterprise Service Bus así como en el uso de protocolos basados en REST. Asimismo, en coordinación con AGESIC, se realizan actividades de asesoramiento a instituciones públicas que desean utilizar servicios de información geográfica en un marco integrado de servicios públicos [45] [46].

Por otro lado, los resultados de esta tesis permiten identificar varios temas que resulta candidatos a trabajos a futuro.

1. Utilización de mecanismos basados en eventos y asincronismo provistos por los Enterprise Service Bus para potenciar las plataformas integradas. Se trata de investigar sobre la aplicación de estos mecanismos en la integración de servicios de información geográfica.
2. Uso de middleware orientado a la interacción del usuario (servidores de Portales, Mashup, otras Web 2.0, etc) en servicios de gobierno electrónico con información geográfica.

⁶ Grupo de Tecnologías en la Información Geoespacial - <http://www.fing.edu.uy/ia/grupos/gtig>

⁷ Grupo de Trabajo en Infraestructuras de Datos Espaciales Uruguay - <http://www.agesic.gub.uy/innovaportal/v/665/1/agesic/IDE.html>.

3. Aporte de las tecnologías de middleware avanzadas a la implementación de escenarios de *Volunteered Geographic Information*, abordando los aspectos de gobierno electrónico relativos al fortalecimiento de la participación ciudadana.

Referencias

1. AGESIC – Agencia de Gobierno Electrónico y Sociedad de la Información - www.agesic.gub.uy (visitado julio 2011)
2. “Plataforma de eGob de Uruguay”, AGESIC.
http://www.agesic.gub.uy/innovaportal/v/452/1/agesic/plataforma_de_gobierno_electronico.html?menuderecho=5 (visitado julio 2011).
3. “Guía de Uso de la Plataforma de GE del Estado uruguayo”, AGESIC.
http://www.agesic.gub.uy/innovaportal/v/1454/1/agesic/guia_de_uso_de_la_plataforma_de_ge_del_estado_uruguayo.html (visitado julio 2011).
4. Portal de la Intranet Gubernamental – República de Colombia - <http://www.intranet.gov.co/> (visitado julio 2011)
5. “Benefits and challenges of using geographic information systems to enhance social security services”, R. Sosa, L. González, B.Rienzi, P.Foti – 6th International Policy and Research Conference on Social Security "Emerging trends in times of instability: New challenges and opportunities for social security" ISSA, 29.09.2010 - 01.10.2010 | Luxembourg
6. Environmental Protection Agency – USA <http://www.epa.gov/> (visitado Julio 2011)
7. "Transformative and Innovative E-Gov for the Next Generation: Linkages of Back Offices for One-stop Portal" Osamu Sudoh, Yumiko Kinoshita, E-Government, E-Services and Global Processes. Joint IFIP TC 8 and TC 6 International Conferences EGES 2010, Brisbane, Australia, September 2010. Proceedings.
8. “Information Systems for eGovernment A Quality-of-Service Perspective”, Viscusi, Batini, Mecella, ISBN 978-3-642-13570-5, Springer Heidelberg Dordrecht London New York 2010
9. IDEUy – <http://www.agesic.gub.uy/innovaportal/v/665/1/agesic/IDE.html> (visitado julio 2011)
10. “Bases para una Estrategia Iberoamericano de Interoperabilidad”, D. J. Ignacio Criado, XII Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, Buenos Aires, Argentina, 1-2 de julio 2010
11. W3C - Web Services - <http://www.w3.org/standards/webofservices/> (visitado julio 2011)
12. W3C – SOAP - <http://www.w3.org/TR/soap12-part0/> (visitado julio 2011)
13. OASIS Estandards - <http://www.oasis-open.org/standards> (visitado julio 2011)
14. M. Papazoglou, Web Services: Principles and Technology, 1st ed. Prentice Hall, September 2007, ISBN: 0321155556

15. OGC Standards - <http://www.opengeospatial.org/standards/> (visitado marzo 2011)
16. OGC Web Services - <http://www.opengeospatial.org/standards/common> (visitado marzo 2011)
17. "Enterprise Service Bus: Theory in Practice", David Chappell, O'Reilly Media, Junio 2004, ISBN: 0596006756
18. "Service oriented architectures: approaches, technologies and research issues", M. Papazoglou and W. Heuvel, The VLDB Journal, vol. 16, no. 3, pp. 389-415, 2007
19. SDI Cookbook – GSDI - http://www.gsdi docs.org/GSDIWiki/index.php/Main_Page (visitado marzo 2011)
20. "United Nations E-Government Survey 2010" - http://www2.unpan.org/egovkb/documents/2010/E_Gov_2010_Complete.pdf (visitado marzo 2011)
21. PGEUy – Plataforma de Gobierno Electrónico AGESIC http://www.agesic.gub.uy/innovaportal/v/452/1/agesic/plataforma_de_gobierno_electronico.html (visitado marzo 2011)
22. SGM – Servicio Geográfico Militar – Ministerio de Defensa <http://www.ejercito.mil.uy/cal/sgm/principal1024.html> (visitado marzo 2011)
23. WMS – Web Map Service - <http://www.opengeospatial.org/standards/wms> (visitado marzo 2011)
24. WFS – Web Feature Service - <http://www.opengeospatial.org/standards/wfs> (visitado marzo 2011)
25. CSW – Catalog Web Service - <http://www.opengeospatial.org/standards/cat> (visitado marzo 2011)
26. "Web GIS: Technologies and Its Applications", AA. Alesheikh, H. Helali, HA. Behroz, IAPRS, Vol. XXXIV, part 4, ISSN 1682-1750 <http://www.isprs.org/proceedings/XXXIV/part4/pdfpapers/422.pdf> (visitado marzo 2011)
27. GeoXACML - <http://www.opengeospatial.org/standards/geoxacml> (visitado marzo 2011)
28. XACML - <http://www.oasis-open.org/standards#xacmlv2.0> (visitado julio 2011)
29. Google Maps – <http://maps.google.com> (visitado julio 2011)
30. "Análisis comparativo de Servidores de Mapas", L. Monge de la Cruz, J. Torres Herrera, L. López Chico, C. Navarro Cota. Revista GeoFocus Nro 10 Año 2010 ISSN 1578-5157
31. OpenLayers - <http://openlayers.org/> (visitado Julio 2011)

32. I3Geo – <http://mapas.mma.gov.br/i3geo> (visitado julio 2011)
33. MapServer - <http://mapserver.org/> (visitado Julio 2011)
34. GeoServer - <http://geoserver.org/display/GEOS/Welcome> (visitado Julio 2011)
35. ArcGis - <http://www.esri.com/software/arcgis/> (visitado julio 2011)
36. INSPIRE – <http://inspire.jrc.ec.europa.eu/> (visitado julio 2011)
37. IDEE – <http://www.idee.es> (visitado julio 2011)
38. DNM – Dirección Nacional de Meteorología – Ministerio de Defensa
<http://www.meteorologia.gub.uy/> (visitado julio 2011)
39. gvSIG - <http://www.gvsig.org> (visitado Julio 2011)
40. Quantum GIS - <http://www.qgis.org/> (visitado Julio 2011)
41. W3C Web Services Activity <http://www.w3.org/2002/ws/Activity> (visitado julio 2011)
42. HTTP Security Considerations - <http://www.w3.org/Protocols/rfc2616/rfc2616-sec15.html>
(visitado julio 2011)
43. Goodchild, M.F. (2007). "Citizens as sensors: the world of volunteered geography". *GeoJournal* **69** (4): 211–221. [doi:10.1007/s10708-007-9111-y](https://doi.org/10.1007/s10708-007-9111-y) (visitado julio 2011)
44. Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) <http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf> (visitado julio 2011)
45. Dirección Nacional de Catastro – Ministerio de Economía <http://www.catastro.gub.uy/> (visitado Julio 2011)
46. Dirección Nacional de Topografía MTOP – Ministerio de Transporte y Obras Públicas
<http://www.dntopografia.gub.uy/> (visitado Julio 2011)
47. "Programming: The Derivation of Algorithms", Anne Kaldewaij, Prentice Hall International Series in Computer Science, 1990, ISBN: 0132041081
48. "Monitoreo y Control de Problemas de Salud mediante SIG" Raquel Sosa, P. Pazos, R. Ordeix, J. Pintos – Primer Congreso Uruguayo IDE – octubre 2010
http://www.agesic.gub.uy/innovaportal/v/1181/1/agesic/primer_congreso_uruguayo_de_infraestructura_de_datos_espaciales.html (visitado julio 2011)
49. "Seguridad y Control de Acceso para Servidores de Mapas" Raquel Sosa, R. Ordeix, J. Pintos y M. Souto – Primer Congreso Uruguayo IDE – octubre 2010

http://www.agesic.gub.uy/innovaportal/v/1181/1/agesic/primer_congreso_uruguayo_de_infraestructura_de_datos_espaciales.html (visitado julio 2011)

50. “Elaboración de escenarios prospectivos con gvSIG”, Rosario Casanova, Raquel Sosa, Sebastián Rodríguez. 1as Jornadas gvSIG Uruguay. Junio 2011
<http://www.gvsig.org/web/community/events/jornadas-uruguay/2011/ponencias> (visitado julio 2011)
51. “Web Services Geográficos y Gobierno Electrónico”, Raquel Sosa, Reporte Técnico PEDECIBA *RT 11-04* <http://www.fing.edu.uy/inco/pedeciba/bibliote/reptec/TR1104.pdf> (vistado julio 2011)
52. “Primer Congreso Uruguayo sobre Infraestructuras de Datos Espaciales”
http://www.agesic.gub.uy/innovaportal/v/1181/1/agesic/primer_congreso_uruguayo_de_infraestructura_de_datos_espaciales.html (visitado julio 2011)

Anexo - Caso de Estudio

Descripción

La Dirección Nacional de Meteorología (DNM) [1] brinda la información meteorológica oficial en el Uruguay. “La DNM será responsable de la realización de la observación, concentración, control de calidad, intercambio nacional e internacional, análisis e investigación, suministro, difusión y conservación de la información oficial en meteorología.”

Dentro de la DNM hay áreas distintas con diferentes tareas que brindan respuesta a las necesidades de diferentes públicos:

- Pronóstico – informa las previsiones del estado del tiempo a futuro en cortos períodos de tiempo. Por ejemplo: temperaturas máximas y mínimas para el día siguiente y hasta una semana hacia adelante; o posibilidades de eventos climáticos adversos: precipitaciones, tormentas, granizo, vientos fuertes.
- Climatología – informa las mediciones de las variables climáticas constatadas a la fecha y datos históricos. Genera análisis de la variación de las variables climáticas detectando anomalías con respecto a años o temporadas anteriores.

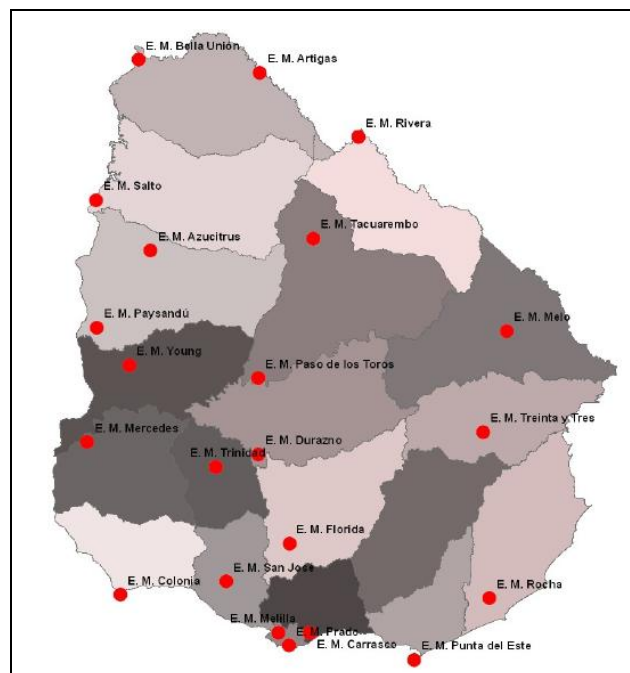


Figura 24 - Ubicación de las Estaciones Meteorológicas

Toda la información que trabaja meteorología es georreferenciable, desde la ubicación de las estaciones meteorológicas hasta la interpolación de sus mediciones a todo el territorio. En la Figura 1 se ve la

ubicación de las estaciones meteorológicas a lo largo de todo el país. Con las mediciones tomadas luego se procesa la información para interpolar los valores de las variables en todo el territorio.

Actualmente la DNM publica la información para el usuario final en su página web y genera boletines. Para acceder a la información histórica detallada se le solicita un informe a la DNM y ésta lo brinda en formato papel.

En este caso de estudio se presenta un ejemplo de servicios de información meteorológica que se podrían brindar a través de la plataforma de Gobierno Electrónico. De acuerdo al público, se considera que se puede estar en el Escenario I, Escenario II o Escenario IV.

Datos y Servicios

La Dirección Nacional de Meteorología puede ofrecer la información meteorológica a través de Web Services Geográficos. Se puede considerar que se generan 30 capas (una por cada variable) diarias y mensualmente las capas de información resumida y analizada. En la Figura 2 se ve un tipo de información histórica agregada: Precipitación Acumulada para un mes.

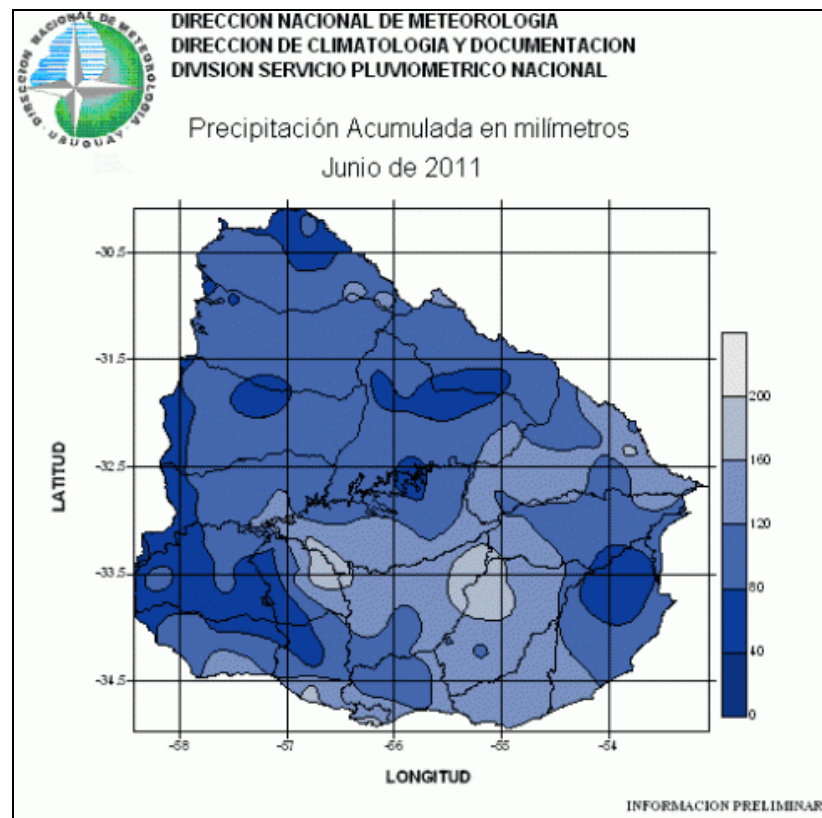


Figura 25 - Información de Precipitaciones Acumuladas

La Dirección de Meteorología podría brindar la información de pronóstico por servicios WMS y la información de climatología por WFS. A efectos ilustrativos veamos el caso de los datos de precipitación acumulada siendo accedidos por público general.

En este caso nos encontramos en el Escenario I y se seguirá el Flujo 1 aplicando las transformaciones T1, T1inv, T2 y T2 inv.

Ejemplo 1

Tomemos como ejemplo un pedido getMap para el servicio WMS. El software cliente generará el siguiente pedido mediante un GET HTTP:

[http://www.meteorologia.gub.uy/wms?bbox=-35,-59,-30,-52
&styles=precip&format=jpeg&info_format=text/plain&request=GetFeatureInfo&layers=meteo:precip_junio11&query_layers=meteo:precip_junio11&width=550&height=250&x=170&y=160](http://www.meteorologia.gub.uy/wms?bbox=-35,-59,-30,-52&styles=precip&format=jpeg&info_format=text/plain&request=GetFeatureInfo&layers=meteo:precip_junio11&query_layers=meteo:precip_junio11&width=550&height=250&x=170&y=160)

Esto al pasar por el proxy de ruteo de pedidos lo enviará a los CTP de la plataforma, que generarán el siguiente paquete SOAP usando la transformación T1.

```
<?xml version="1.0"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <Receiver>http://www.meteorologia.gub.uy/</Receiver>
  </soap:Header>

  <soap:Body>
    <Servicio>WMS</Servicio>
    <Metodo>GetMap</Metodo>
    <Parametros>
      bbox=-35,-59,-30,-52&styles=precip&format=jpeg&info_format=text/plain&
      request=GetFeatureInfo&layers=meteo:precip_junio11&query_layers=meteo:precip_junio11&width=550&height=250&x=170&y=160
    </Parametros>
  </soap:Body>
</soap:Envelope>
```

Este paquete SOAP podrá ser tratado por la PGE como cualquier otro paquete SOAP, siendo ruteado al endpoint correspondiente a Meteorología. Antes de enviar el pedido, los CTP en el Gateway reconstruirán el pedido original usando la transformación T1inv para mandarlo al servidor de mapas.

La respuesta del servidor de mapas a este pedido es una imagen en formato jpeg. Dicha respuesta será empaquetada en un paquete SOAP por la transformación T2. De acuerdo a la plataforma de implementación, puede ser codificada en base64 o mantenerse una codificación binaria de la misma. Finalmente el proxy recibirá el paquete SOAP de respuesta y extraerá la imagen para reenviarla al cliente.

Ejemplo 2

Tomemos como segundo ejemplo una consulta WFS – GetFeature que busca conocer la precipitación en la zona de Florida (coordenadas -34, -56). El software cliente manda un pedido tipo POST HTTP como el siguiente:

http://www.meteorologia.gub.uy/wfs - POST

```
<wfs:GetFeature service="WFS" version="1.1.0"
  xmlns:meteo="http://www.meteorologia.gub.uy/meteo"
  xmlns:wfs="http://www.opengis.net/wfs"
  xmlns="http://www.opengis.net/ogc"
  xmlns:gml="http://www.opengis.net/gml"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.opengis.net/wfs
    http://schemas.opengis.net/wfs/1.1.0/wfs.xsd">

  <wfs:Query typeName="meteo:precip_junio11">
    <Filter>
      <Intersects>
        <PropertyName>the_geom</PropertyName>
        <gml:Point srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
          <gml:coordinates>-34,-56</gml:coordinates>
        </gml:Point>
      </Intersects>
    </Filter>
  </wfs:Query>
</wfs:GetFeature>
```

Se destaca que la consulta busca la información de la capa precip_junio11 que se intersecta con el punto (-34,-56) que son las coordenadas aproximadas de Florida. El proxy enviará este pedido al CTP que aplicando la transformación T1 generará el siguiente paquete SOAP:

```

<?xml version="1.0"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
<soap:Header>
<Receiver>http://www.meteorologia.gub.uy</Receiver>
</soap:Header>

<soap:Body>
<Servicio>WFS</Servicio>
<Metodo>GetFeature</Metodo>
<Parametros>
<wfs:GetFeature service="WFS" version="1.1.0"
  xmlns:meteo="http://www.meteorologia.gub.uy/meteo"
  xmlns:wfs="http://www.opengis.net/wfs"
  xmlns="http://www.opengis.net/ogc"
  xmlns:gml="http://www.opengis.net/gml"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.opengis.net/wfs
  http://schemas.opengis.net/wfs/1.1.0/wfs.xsd">
<wfs:Query typeName="meteo:precip_junio11">
<Filter>
<Intersects>
<PropertyName>the_geom</PropertyName>
<gml:Point srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
<gml:coordinates>-34,-56</gml:coordinates>
</gml:Point>
</Intersects>
</Filter>
</wfs:Query>
</wfs:GetFeature>
</Parametros>
</soap:Body>
</soap:Envelope>

```

Este paquete será tratado dentro de la PGE como cualquier otro paquete SOAP. El componente Gateway se encargará de aplicarle la transformación T1inv para armar el pedido original y enviarlo al servidor de mapas.

Un ejemplo de respuesta del servidor de mapas se muestra en el recuadro en la siguiente página. Usando la transformación T2 el componente Gateway empaquetará esta respuesta en un paquete SOAP. En este caso toda la respuesta se guardará en el Body como contenido. Luego el componente Proxy aplicará la transformación T2inv para obtener solamente la respuesta a enviar al cliente.

```

<wfs:FeatureCollection xmlns="http://www.opengis.net/wfs" xmlns:wfs="http://www.opengis.net/wfs"
xmlns:meteo="http://www.meteorologia.gub.uy/meteo"
xmlns:gml="http://www.opengis.net/gml" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.meteorologia.gub.uy/meteo
http://www.meteorologia.gub.uy/geoserver/wfs?service=WFS&version=1.0.0&request=DescribeFeatur
eType&typeName=meteo:precip_junio11 http://www.opengis.net/wfs
http://www.meteorologia.gub.uy/geoserver/schemas/wfs/1.0.0/WFS-basic.xsd">

<gml:boundedBy>
<gml:null>unknown</gml:null>
</gml:boundedBy>

<gml:featureMember>
<meteo:precip_junio11 fid="precip_junio11.5">
<meteo:the_geom>
<gml:MultiPolygon srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
<gml:polygonMember>
<gml:Polygon>
<gml:outerBoundaryIs>
<gml:BoundingBox>
<gml:coordinates xmlns:gml="http://www.opengis.net/gml" decimal="." cs="," ts=" ">
-34.41,-56.51 -33.08,-55.06
</gml:coordinates>
</gml:BoudigBox>
</gml:outerBoundaryIs>
</gml:Polygon>
</gml:polygonMember>
</gml:MultiPolygon>
</meteo:the_geom>
<meteo:valor>80</meteo:valor>
</meteo:precip_junio11>
</gml:featureMember>
</wfs:FeatureCollection>

```

Usuarios y Software Cliente

La Información de Pronóstico es de interés del público en general. Esta información puede ser accedida por portales (como el geoportal) u otros portales comerciales.

La Información climática analizada es de interés para la Dirección Nacional de Medio Ambiente y para los investigadores en temas de Cambio Climático. Podemos considerar a este público como usuarios avanzados que requieren servicios con posibilidades de consultas avanzadas (no solamente ver el mapa en general). Lo usual es que este público maneje sistemas de software GIS Desktop que tiene la posibilidad de conectarse a servicios.

La Información histórica detallada es de interés para los Juzgados Civiles, en casos de accidentes de tránsito; y para las compañías de seguros tanto en los casos de accidentes vehiculares como en los casos de seguros agropecuarios para pagar daños causados por eventos climáticos extremos. En este caso la consulta en el software cliente será programada a medida en algún software.

Referencias

1. Póster - “Aplicaciones de SIG a Meteorología” - R. Sosa, R. Casanova, H. Bermúdez, A. Lofredo, B. Rienzi. Primer Congreso Uruguayo de Infraestructuras de Datos Espaciales.
http://www.agesic.gub.uy/innovaportal/file/1248/1/APLICACIONES_DE_SISTEMAS_DE_INFORMACION.pdf