# Plataforma de Interoperabilidad

Andes 1365 piso 7º
Montevideo – Uruguay
Tel./Fax: (+598)  2901.2929*
Email: contacto@agesic.gub.uy

www.agesic.gub.uy

# Índice de contenidos




Andes 1365 piso 7º
Montevideo – Uruguay
Tel./Fax: (+598) 2901.2929*
Email: contacto@agesic.gub.uy

Andes 1365 piso 7º
Montevideo – Uruguay
Tel./Fax: (+598) 2901.2929*
Email: contacto@agesic.gub.uy

# Introducción

Este capítulo brinda una descripción técnica de la PGE, presentando sus principales componentes. En particular, se profundiza en dos de los componentes de la Plataforma de Interoperabilidad: el Sistema de Seguridad y la Plataforma de Middleware. Para cada uno de ellos, se describen las prestaciones más importantes que brindan y los mecanismos, productos y estándares utilizados para hacerlo.

# Descripción General de la PGE

La Plataforma de Gobierno Electrónico (PGE) del Estado Uruguayo tiene como objetivo general facilitar y promover la implementación de servicios de Gobierno Electrónico en Uruguay. Para esto, la PGE brinda mecanismos que apuntan a simplificar la integración entre los organismos del Estado y a posibilitar un mejor aprovechamiento de sus activos.

A nivel tecnológico, se implementó una Arquitectura Orientada a Servicios (Service Oriented Architecture, SOA) a nivel del Estado, la cual se apoya fuertemente en la tecnología de Web Services. De esta forma, los organismos proveen sus funcionalidades de negocio a través de servicios de Software que son descriptos, publicados, descubiertos, invocados y combinados de forma independiente a la plataforma tecnológica en la que fueron implementados. Esto facilita la integración entre los organismos, promoviendo la reutilización y el aprovechamiento de los recursos de información y tecnológicos con los que cuentan. Además, contribuye a poder responder de forma ágil ante cambios en requerimientos o regulaciones.

El soporte tecnológico a la PGE está dado por un conjunto de componentes que dan soporte a la Plataforma de Interoperabilidad y proveen Servicios Transversales. Estos componentes brindan mecanismos para implementar la SOA, garantizar la interacción segura entre los servicios y aplicaciones, e interactuar con los ciudadanos. La Figura 1

presenta una visión general de los componentes de la PGE y de los distintos actores involucrados.

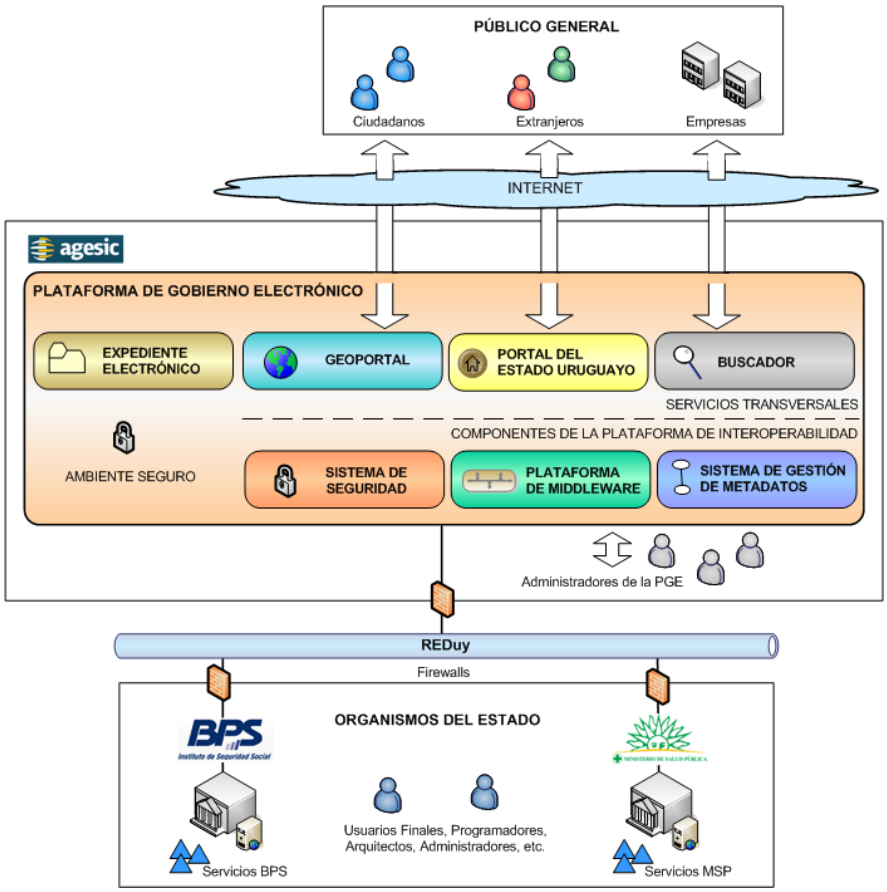


Figura 1 – Principales Componentes y Actores de la PGE

Los componentes de la Plataforma de Interoperabilidad son el Sistema de Seguridad, el Sistema de Gestión de Metadatos y la Plataforma de Middleware. En particular, el Sistema de Seguridad provee los mecanismos para que los componentes y servicios de la PGE se ejecuten en un ambiente seguro. Las Servicios Transversales proveen funcionalidades específicas y actualmente consisten en el Portal y el Buscador del Estado Uruguayo, el Sistema de Expediente Electrónico y el Geoportal.

Por otro lado, los principales actores de la PGE son el Público en General, los Organismos del Estado y el personal de AGESIC. El Público en General, que incluye ciudadanos, extranjeros y empresas, accede a los

servicios de la PGE a través de Internet utilizando, por ejemplo, el Portal del Estado Uruguayo. Los usuarios y Sistemas de Software en los Organismos del Estado, se apoyan en la infraestructura de conectividad provista por la REDuy para acceder a los servicios y componentes de la PGE. También utilizan esta infraestructura de conectividad para proveer, a través de la PGE, sus servicios al resto de los organismos. Por último, el personal de AGESIC se encarga de la administración de la plataforma.

# Infraestructura de Conectividad: REDuy

La REDuy [1] es una red de alta velocidad que provee la infraestructura de conectividad necesaria para que los organismos se interconecten, entre ellos y con la PGE, de manera segura y con adecuados niveles de servicio y seguridad informática. La REDuy está implementada sobre la red MPLS (MultiProtocol Label Switching) de AntelData y cuenta con velocidades de acceso mínimas de 10Mbps y máximas de 100Mbps. Cuenta además con un centro de soporte gestionado por AGESIC y es considerada un activo de información crítico del Estado, por lo que tiene especial atención del CERTuy [2].

La REDuy es una red metropolitana y actualmente conecta a varios organismos de Montevideo. Además, se planea extender su alcance para llegar también a los organismos del interior del país.

Como se presenta en la Figura 2, la conexión de los organismos a la REDuy está protegida por *firewalls* que controlan el tráfico de red de los organismos, desde y hacia la REDuy. La configuración y administración de estos *firewalls* está a cargo del equipo de soporte de AGESIC.

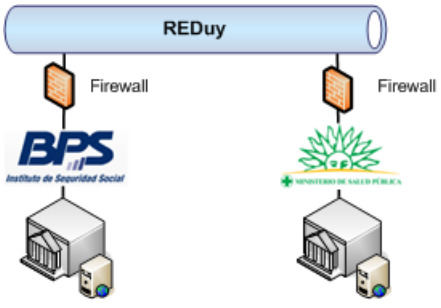


Figura 2 - *Firewalls* REDuy

El tráfico desde los organismos hacia la REDuy está permitido libremente. Sin embargo, el tráfico hacia los organismos desde la REDuy, debe ser habilitado en los *firewalls* por el equipo de soporte de AGESIC.

# Servicios provistos por Organismos

Los Organismos del Estado proveen sus funcionalidades de negocio a través de la tecnología de Web Services. Generalmente, los sistemas informáticos correspondientes, accesibles a través de Web Services, se alojan en los servidores de los propios organismos, aunque también es posible alojarlos en la PGE, en caso que se tengan requerimientos especiales que no se puedan satisfacer en los organismos.

Los Web Services se pueden implementar utilizando distintas tecnologías como Java EE, la plataforma .NET y PHP, entre otras. Para mejorar el nivel de interoperabilidad, se requiere que las implementaciones de los Web Services se ajusten a los perfiles Basic Profile [3] y Basic Security Profile [4] definidos por la organización Web Services Interoperability (WS-I).

Cabe recalcar que los Web Services pueden exponer las funcionalidades de negocio de Sistemas Legados alojados en los organismos, aprovechando de esta forma los recursos de información y tecnológicos existentes.

# Componentes de la Plataforma de Interoperabilidad

Los componentes de la Plataforma de Interoperabilidad de la PGE [5] son la Plataforma de Middleware, el Sistema de Seguridad y el Sistema de Gestión de Metadatos.

La **Plataforma de Middleware** provee mecanismos que facilitan el desarrollo, despliegue e integración de servicios y aplicaciones. Además, cuenta con los componentes necesarios para la implementación de la SOA a nivel del Estado. En la sección “Plataforma de Middleware” se brinda una descripción más detallada de la misma, junto con los productos y tecnologías que la implementan.

El **Sistema de Seguridad** constituye un componente esencial de la PGE, dado que provee servicios de seguridad al resto de los componentes. Este sistema brinda mecanismos que permiten realizar auditorías de seguridad en la PGE, aplicar políticas de acceso asociadas a los servicios publicados en la plataforma, y facilitar el acceso seguro de los organismos a la PGE. En la sección "Sistema de Seguridad" se brinda una descripción más detallada del mismo, junto con los productos y tecnologías que lo implementan.

Por último, el **Sistema de Gestión de Metadatos** provee una especificación de alto nivel de los conceptos relativos a servicios públicos, de forma de evitar, o eventualmente resolver, ambigüedades en el manejo de estos conceptos por parte de los organismos. El Conocimiento en este sistema se maneja a través de ontologías, utilizando OWL [6] (Web Ontology Languge) como lenguaje de especificación y Protégé [7] como herramienta de modelado. El Sistema de Gestión de Metadatos expone interfaces, a través de Web Services, para que otros sistemas puedan interactuar con él.

# Servicios Transversales de la PGE

Los Servicios Transversales de la PGE son actualmente el Portal y el Buscador del Estado Uruguayo, el Sistema de Expediente Electrónico y el Geoportal.

El **Portal del Estado Uruguayo** es uno de los principales puntos de entrada al Gobierno Electrónico, permitiendo la interacción de los ciudadanos con contenidos, servicios y trámites de interés público. Desde el punto de vista tecnológico, el portal está basado en la herramienta WebSphere Portal [8] de IBM, complementada con un manejador de contenido y herramientas de estadística. Entre sus principales características se encuentran el soporte a estándares de la industria, como las especificaciones de Portlets Java [9][10] y Web Services for Remote Portlets (WSRP) [11], su capacidad dinámica de personalización y su cumplimiento con pautas de accesibilidad de sitios Web.

El **Buscador del Estado Uruguayo** tiene como objetivo instrumentar una herramienta de búsqueda orientada a las necesidades del gobierno electrónico en Uruguay. La principal ventaja del buscador, con respecto a

otros como Google, es que está específicamente optimizado para realizar búsquedas de información del Estado Uruguayo. A nivel tecnológico, está implementado utilizando el producto Google Search Appliance [12] complementado con indexación de texto, búsqueda por palabras claves, detección de errores de digitación y errores ortográficos, glosarios y taxonomías.

El **Sistema de Expediente Electrónico** tiene como objetivo principal informatizar el manejo de Expedientes a nivel del Estado Uruguayo y facilitar la interoperabilidad de los mismos a través de los diferentes organismos. El principal componente del sistema es una aplicación de gestión de expedientes electrónicos, que puede ser utilizada bajo la modalidad de *software* como servicio (Software as a Service, SaaS) o puede ser instalada localmente en los organismos del Estado. Una aplicación Web ofrecerá a ciudadanos y organismos la posibilidad de consultar a través de Internet la trazabilidad de los expedientes en que está involucrado. Finalmente, un módulo de ruteo y trazabilidad permitirá el intercambio y trazabilidad de todas las actuaciones realizadas sobre todos los expedientes.

Por último, el **Geoportal** es un portal de información geográfica que permite la consulta y análisis vía Web de la información geográfica proveniente de los organismos. El Geoportal, se encuentra enmarcado en el proyecto IDE (Infraestructura de Datos Espaciales), el cual tiene como objetivo principal crear un servicio en red para acceder y compartir datos geográficos entre los Organismos del Estado.

# Plataforma de Middleware

El objetivo de la Plataforma de Middleware es fomentar la interoperabilidad entre los diferentes Organismos del Estado proveyendo los mecanismos necesarios para facilitar el desarrollo, despliegue e integración de servicios y aplicaciones. Estos mecanismos brindan a su vez, la infraestructura base para la implementación de la SOA a nivel del Estado.

A continuación, se brinda un ejemplo de funcionamiento de la Plataforma de Middleware, para luego describir sus principales componentes.

# Ejemplo de Uso de la Plataforma de Middleware

El ejemplo de uso de la Plataforma de Middleware consta de un servicio "Cédula de Identidad" (CI), que permite, a partir de un número de cédula, obtener información pública de una persona. El servicio es provisto por los organismos A y B, pero con las diferencias que se presentan en la Tabla 1.

| Característica | Servicio (del organismo) A | Servicio (del organismo) B |
|---|---|---|
| Información | Oficial | Réplica de datos provenientes del organismo A. El proceso de réplica se ejecuta de forma mensual. |
| Cantidad máxima de pedidos concurrentes | 100 | 500 |
| Formato de datos de entrada | Número de CI sin puntos, ni dígito verificador. P. ej: 25694581 | Número de CI con puntos y dígito verificador. P ej: 2.569.458-1 |

Tabla 1 – Diferencias entre servicio A y el servicio B

Los principales consumidores del servicio de CI son los funcionarios del organismo C, los cuales acceden al mismo a través de la PGE por intermedio de aplicaciones de escritorio y Web. Asimismo, los Ciudadanos Uruguayos son otros potenciales consumidores, los cuales acceden al servicio utilizando el Portal del Estado Uruguayo.

La invocación de los servicios de la PGE se hace mediante el envío de mensajes. Por lo que, para consumir el servicio de CI, los funcionarios y ciudadanos deben enviar, a través de la aplicación en uso, un mensaje a la PGE con los datos de su solicitud.

Una vez que el mensaje llega a la PGE, y pasa los controles de seguridad necesarios, es reenviado a la Plataforma de Middleware que se encarga de realizar las siguientes acciones:

1. Verificación sintáctica: Se realizan validaciones de integridad como la verificación de nulos, estructuras de datos incompletas o errores en tipos de datos. En caso de encontrar errores, el mensaje es rechazado y se notifica al cliente los motivos.

2. Verificación de políticas de seguridad: Se realizan validaciones para determinar si el mensaje satisface las restricciones de seguridad definidas por la Ley 18.331 de Protección de Datos Personales y acción de Habeas Actas [13], y otras políticas definidas por la PGE. En casos de encontrar errores, el mensaje es rechazado y se notifica al cliente los motivos.

3. Elección del destino del mensaje: Se elige el mejor destino del mensaje. En este ejemplo, existen dos posibles destinos: 1) el servicio A y 2) el servicio B. La política de direccionamiento de mensajes de la PGE define que "*Siempre se enviará el mensaje al servicio del organismo A si hay menos de 100 pedidos concurrentes pendientes. En caso contrario, se redirigirán los pedidos al servicio del organismo B.*"

4. Transformación de datos: En casos donde se haya optado por dirigir el mensaje al servicio B, es necesario transformar el pedido, ingresando la información faltante (puntos y guiones a la CI).

5. Envío del mensaje al servicio: Se envía el mensaje al servicio destino.

La Figura 3 presenta de forma gráfica el ejemplo descrito anteriormente.

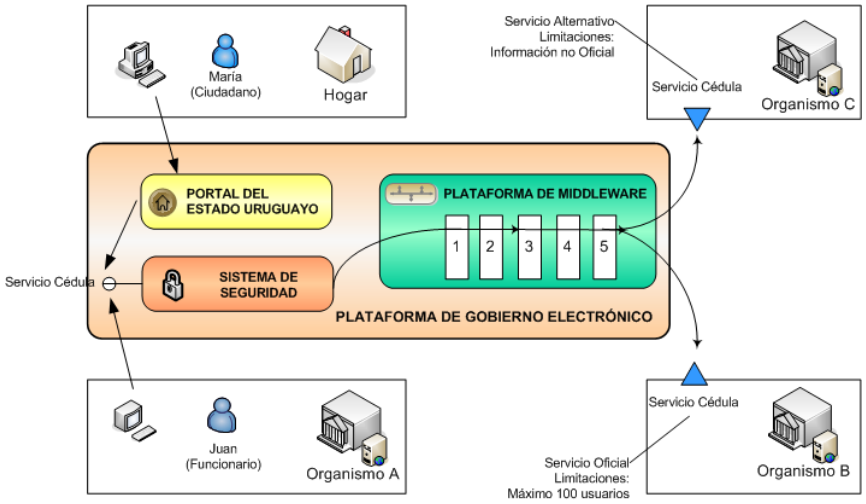


Figura 3 – Ejemplo de Funcionamiento de la Plataforma de Middleware

La Tabla 2 presenta los principales beneficios que obtienen consumidores y productores de servicios del ejemplo al utilizar la PGE.

| Beneficios | Consumidor | Productor |
|---|---|---|
| Transparencia en la ubicación de los servicios | Los consumidores no conocen la ubicación real del servicio. La PGE identifica el mejor destino y se encarga de manejar posibles errores (caída del servicio, etc). | No tienen que hacer pública la ubicación real de sus servidores, brindando un mayor nivel de seguridad para los mismos. |
| Balanceo de Carga | Dado que los servicios no se saturan, los tiempos de respuesta al consumidor no se ven degradados. | La PGE realiza un balanceo de carga de los pedidos de acuerdo a capacidades de los servicios, evitando su saturación. |
| Transformación de formatos | Los clientes no necesitan reconfigurarse debido a (algunos) cambios en el formato de los mensajes recibidos por el servicio. | La PGE puede aprovechar servicios con formatos legados haciendo transparente la transformación de formatos a los clientes. |
| Verificación de datos | | Los servicios sólo procesan pedidos válidos. Procesamiento dedicado exclusivamente al negocio. |

Tabla 2 – Beneficios del uso de la PGE (en el ejemplo) para Consumidores y Productores

# Componentes de la Plataforma de Middleware

La Figura 4 presenta una visión general de la Plataforma de Middleware, en la que se distinguen tres grandes bloques: entornos de ejecución para Aplicaciones y Servicios, un Registro de Servicios y productos de tipo Enterprise Service Bus.

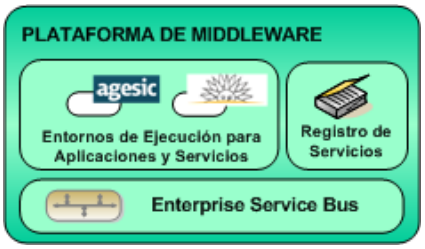


Figura 4 - Plataforma de Middleware

## Entornos de Ejecución

Si bien en general las aplicaciones y servicios de la PGE se alojan en los propios organismos, la Plataforma de Middleware provee entornos de ejecución para alojar aplicaciones y servicios en la propia PGE. Estos entornos se basan en tecnologías de Middleware tales como Servidores de Aplicaciones, entre otros.

Los organismos pueden aprovechar estos entornos para alojar en la PGE servicios o aplicaciones que requieran infraestructura de *hardware* o *software* avanzada, no disponible en los mismos. Esta infraestructura puede ser necesaria para garantizar determinados niveles de calidad de servicio en relación, por ejemplo, a tiempos de respuesta y disponibilidad.

Por otro lado, los entornos de ejecución se utilizan también para servicios, componentes o aplicaciones que brindan funcionalidades comunes o utilitarias. A modo de ejemplo, existe actualmente en la PGE un servicio "Timestamp" provisto por AGESIC, el cual provee la fecha y hora actual. La Figura 5 presenta gráficamente este servicio[1].

[1] [ip-srv-pge] corresponde a la dirección IP del servidor donde está alojado el servicio


Figura 5 - Servicio de Timestamp

La Plataforma de Middleware proporciona entornos de ejecución a través de dos de las principales plataformas para el desarrollo de aplicaciones empresariales: la plataforma .NET [14] de Microsoft y la plataforma Java Enterprise Edition (Java EE) [15]. Esta última se provee a través del JBoss Enterprise SOA Platform [16]. Además de estos dos entornos de ejecución, la plataforma cuenta con otros componentes que también permiten la implementación y ejecución de lógica de negocio. A modo de ejemplo, se cuenta con motores para la ejecución de procesos y reglas de negocio, como motores WS-BPEL.

## Registro de Servicios

El Registro de Servicios de la PGE provee funcionalidades para que los organismos publiquen, describan, busquen y descubran servicios en la PGE.

La Figura 6 presenta, por ejemplo, dos de los servicios publicados en el Registro de Servicios. En primer lugar, se encuentra el servicio "Certificado de Nacidos Vivos" provisto por el Ministerio de Salud Pública (MSP). En segundo lugar, se encuentra el servicio "Timestamp", descripto previamente y provisto por AGESIC.

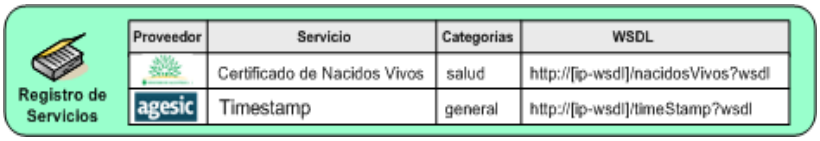


Figura 6 - Directorio de Servicios[2]

[2] [ip-wsdl] corresponde a la dirección IP del servidor donde están alojadas las descripciones de los servicios

Además de los nombres, proveedores y categorías de los servicios, es posible acceder a la descripción de los mismos, especificada en WSDL, que brinda los datos necesarios para que una aplicación cliente pueda invocarlos.

Si bien actualmente el Registro de Servicios se maneja de forma interna a AGESIC, se planea brindar un registro UDDI [17] a través del cual los organismos podrán buscar y descubrir servicios de acuerdo a distintos criterios. A modo de ejemplo, la Figura 7 presenta dos búsquedas que se podrían realizar en un registro UDDI y sus resultados. En el primer caso, el usuario Juan busca servicios cuyo proveedor es "AGESIC"; la búsqueda retorna entonces el servicio "Timestamp". En el segundo caso, la usuaria Ana busca servicios en la categoría "salud"; la búsqueda retorna entonces el servicio "Certificado de Nacidos Vivos". El resultado de una búsqueda retorna la información necesaria para poder invocar a los servicios que se retornan.


Figura 7 - Búsqueda de Servicios

## Productos Enterprise Service Bus

Los productos de ESB de la Plataforma de Middleware proveen mecanismos que pueden ser utilizados por los organismos para el consumo y provisión de servicios. La Plataforma de Middleware cuenta con dos productos de tipo ESB: JBoss ESB [16] y Microsoft Biztalk Server [18] complementado con el Biztalk ESB Toolkit [19].

A continuación se describen algunos de los principales mecanismos que brindan estos productos en el marco de la PGE.

## Transparencia de Ubicación

Los productos de ESB proveen mecanismos que permiten a la PGE brindar transparencia en la ubicación de los servicios que se acceden a través de ella, esto es, las aplicaciones cliente no conocen la dirección real (física) de los servicios que invocan. Cuando una aplicación cliente quiere invocar un servicio, debe enviar un pedido a la PGE especificando, a través de una dirección lógica, el servicio que se quiere invocar. Esta dirección lógica identifica al servicio en la plataforma.

El mapeo entre direcciones lógicas y físicas es gestionado en los ESBs. De esta forma, si la ubicación de un servicio cambia, las aplicaciones cliente no deben ser modificadas dado que basta con configurar la nueva dirección en el ESB. Por otro lado, los proveedores de servicios se benefician de este mecanismo, ya que no tienen que hacer pública la ubicación real de sus servidores, brindando un mayor nivel de seguridad para los mismos.

Para especificar la dirección lógica del servicio que se quiere invocar, una aplicación cliente debe utilizar el estándar WS-Addressing [20]. En la sección "**¡Error! No se encuentra el origen de la referencia.**" se describe con más detalle cómo debe especificarse esta dirección en el mensaje SOAP utilizado en la invocación del servicio.

## Mecanismos de Mensajería Confiable

Los productos de ESB de la PGE permiten brindar mecanismos de mensajería confiable utilizando los modelos *point-to-point* y *publish-and-subscribe* [21].

En particular, el modelo *publish-and-subscribe* se basa en una comunicación de tipo *broadcast*, donde un emisor/productor envía un mensaje que reciben varios receptores/consumidores. En este modelo, los consumidores se suscriben a un determinado evento/tópico de información y cada vez que los productores generan un mensaje sobre un tópico/evento determinado, éste es automáticamente redirigido a los consumidores suscritos al mismo.

El modelo *publish-and-subscribe* puede ser aplicado, por ejemplo, a la modificación de padrones del territorio nacional, donde existen varios

interesados en esta información. En este escenario, el evento/tópico es "modificación de padrón", el productor es la Dirección Nacional de Catastro (DNC) y los consumidores pueden ser la Dirección General de Registro (DGR) y la Intendencia Municipal de Montevideo (IMM). Estos últimos, se suscribirán al tópico "modificación de padrón" y cada vez que DNC genere un mensaje para este tópico, el sistema de mensajería reenviará dicho mensaje a la IMM y DNC. En caso que éstos no estén activos, podrán posteriormente consultar el almacén de mensajes en busca de notificaciones perdidas.

## Transformación y Enriquecimiento de Mensajes

Los productos de ESB de la PGE proveen varios mecanismos para transformar y enriquecer mensajes que fluyen entre clientes y servicios, por ejemplo, a través del estándar XSLT [22]. Estos mecanismos de transformación pueden utilizarse para abordar distintos requerimientos, como la resolución de discrepancias entre los formatos de datos intercambiados. A modo de ejemplo, si un cliente maneja datos en formato XML y un servicio espera datos en formato CSV[3], se podría utilizar XSLT para transformar los datos XML en datos CSV.

Además, las transformaciones podrían utilizarse para minimizar el impacto, en las aplicaciones cliente, ante cambios en los servicios. Por ejemplo, si un servicio cambiara su interfaz funcional, en ciertas ocasiones se podrían utilizar transformaciones para que los mensajes enviados por clientes se ajusten a la nueva interfaz. Dado que esto se resuelve en el ESB, los cambios en los servicios no tendrían impacto en las aplicaciones cliente.

## Ruteo Basado en Contenido

Otra funcionalidad que proveen los productos de ESB de la PGE, es la posibilidad de direccionar mensajes de acuerdo a su contenido. Los Content Based Routing (CBR) Services son servicios especializados que pueden ser introducidos entre cliente y servicio con el fin de inspeccionar el mensaje y a partir de su contenido redirigirlo a un determinado servicio.

[3] CSV – Comma-separated values (Valores Separados por Coma)

Un ejemplo de un servicio CBR es el servicio de Ruteo de Mensajes de la PGE, el cual examina el mensaje para determinar su destino. En particular, se consulta el cabezal WS-Addressing "To", el cual contiene el servicio que se quiere invocar.

## Monitoreo

Los productos de ESB cuentan con varias funcionalidades nativas que permiten el monitoreo de distintos tipos de información como tiempos de respuesta de los servicios, contenido de los mensajes, cantidad de invocaciones a los servicios, etc.

## Otros Posibles Mecanismos

Dado el rol mediador de los ESBs, es de esperar que se implementen otros mecanismos que podrían ser utilizados por los organismos, tanto consumidores como proveedores de servicios. Algunos ejemplos de estos mecanismos son:

- **Tolerancia a Fallas**

  Este mecanismo permitiría que en caso de que un servicio no esté disponible o falle por algún motivo, se pueda invocar a otro equivalente de forma transparente al cliente que efectúa la invocación.

- **Control y Balanceo de Carga**

  En este caso, un organismo podría solicitar a AGESIC que se controle la cantidad de invocaciones a un determinado servicio, para que reciba como máximo un número dado de invocaciones por período de tiempo.

- **Validaciones**

  Un organismo que sabe que gran parte de las invocaciones a sus servicios no son válidas, podría solicitar realizar validaciones en los productos de ESB para no saturar a sus servidores con estas invocaciones. Esto además, reduciría el tráfico de red.

- **Aplicación de Políticas**

AGESIC podría implementar controles, por ejemplo asociados a la ley de Protección de Datos Personales, en base a las funcionalidades de los productos de ESB.

# Sistema de Seguridad

El Sistema de Seguridad de la PGE provee un conjunto de mecanismos que facilitan la implementación de requerimientos de seguridad a aplicaciones, servicios o componentes en el marco de la PGE. En particular, permite que los organismos deleguen a la PGE la tarea de controlar el acceso a los servicios que proveen.

A continuación, se describe el funcionamiento, componentes y prestaciones del Sistema de Seguridad.

## Ejemplo de Uso del Sistema de Seguridad

En esta sección se brinda un ejemplo de uso del Sistema de Seguridad, con el fin de proveer una idea general de su funcionamiento para controlar el acceso a los servicios de la PGE.

El control de acceso en la plataforma se realiza a nivel de métodos, por lo que cuando un organismo publica un servicio debe especificar quién tiene acceso a cada método del mismo. En este ejemplo, como se presenta en la Figura 8, el organismo B provee el servicio de CI que tiene dos métodos: getNombre y getFechaNacimiento. El organismo B brinda acceso a los funcionarios del organismo A para invocar únicamente al método getNombre. De esta forma, si un funcionario del organismo A intenta invocar el método getFechaNacimiento, la PGE le negará el acceso al mismo.

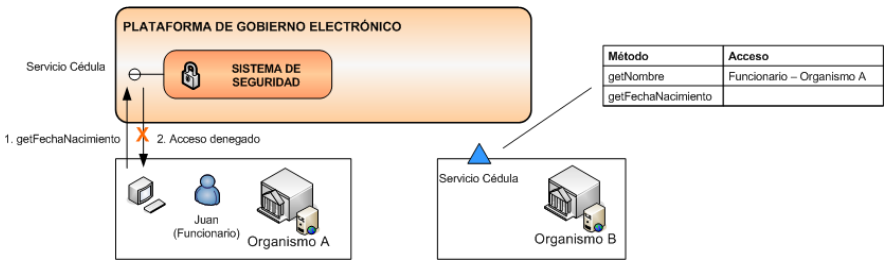


Figura 8 – Ejemplo de Funcionamiento del Sistema de Seguridad

Como se presenta en el ejemplo, el organismo proveedor del servicio puede delegar al Sistema de Seguridad de la PGE el control de acceso a los servicios que provee, por lo que no debe preocuparse ni invertir recursos en esta tarea.

# Componentes del Sistema de Seguridad

Como se puede observar en la Figura 9, el Sistema de Seguridad se puede dividir en tres grandes bloques: Sistema de Auditoría, Sistema de Control de Acceso y Servicio Periféricos de Seguridad.


Figura 9 - Sistema de Seguridad

## Sistema de Auditoría

El Sistema de Auditoría provee las herramientas necesarias para realizar auditorías de seguridad sobre la PGE. Este sistema recolecta información y realiza análisis y reportes de auditoría. El Sistema de Auditoría está implementado por el producto Tivoli Compliance Insight Manager (TCIM)[23].

## Servicios Periféricos de Seguridad

Los Servicios Periféricos de Seguridad tienen la finalidad de brindar los mecanismos necesarios para facilitar a los organismos el acceso seguro a la PGE. Como se observa en la Figura 10, en este componente existen dos servicios principales: Autoridad Certificadora (Certification Authority, CA) y Servicio de Directorio.


Figura 10 - Servicios Periféricos de Seguridad

La **CA** tiene como cometido emitir y gestionar los certificados de propósito general que se utilicen en la PGE. Por ejemplo, la CA tiene a cargo la emisión de los certificados que deben utilizar los servidores de los organismos para establecer conexiones seguras con la PGE. La CA es provista por el producto Windows 2003 Server.

El **Servicio de Directorio** provee servicios de directorio a través del protocolo LDAP, y tiene cuatro funciones principales [25]:

- replicar automáticamente las estructuras de directorio de los organismos que cuenten con este servicio
- proveer servicio de directorio a aplicaciones de la PGE
- proveer servicio de directorio a organismos que no cuenten con este servicio
- brindar una visión unificada de las estructuras de directorio de los organismos y la PGE

El Servicio de Directorio está implementado principalmente por los productos IBM Directory Server, Tivoli Identity Manager (TIM) [36] y Tivoli Directory Integrator (TDI) [37].

La Figura 11 presenta la estructura base del árbol de directorio manejado por la PGE, y a partir de dónde se integran los árboles de directorio de los organismos.

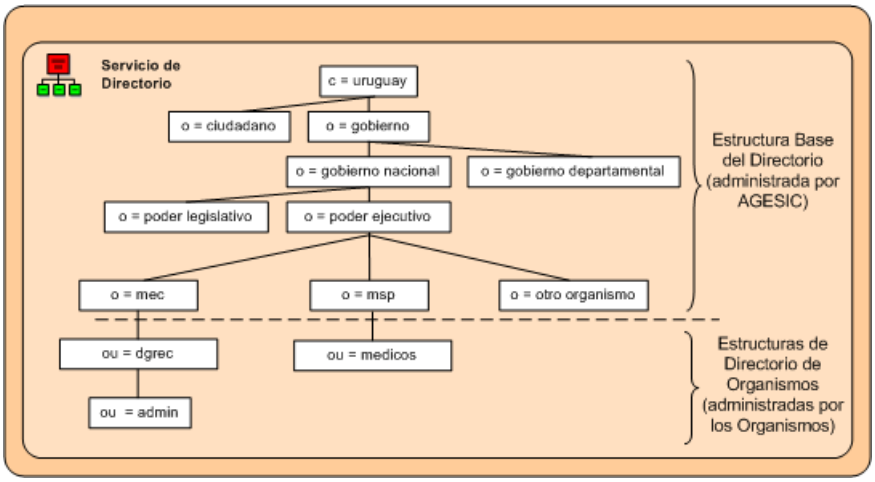


Figura 11 - Estructura Base del Directorio

A modo de ejemplo, se puede observar que hay definida una Organización "mec" que corresponde al Ministerio de Educación y Cultura (o =mec), la cual tiene una Unidad Organizacional denominada "dgrec" (ou = dgrec) que corresponde a la Dirección General de Registro del Estado, en la cual existen una entrada denominada "admin" que corresponde a un rol existente en la unidad organizacional.

## Sistema de Control de Acceso

La finalidad del Sistema de Control de Acceso de la PGE es brindar los mecanismos para aplicar políticas de control de acceso sobre los servicios publicados y las aplicaciones disponibles en la PGE. El control de acceso en la PGE se realiza siguiendo un esquema RBAC, utilizando el rol del usuario que quiere acceder al servicio o aplicación, y las políticas de acceso definidas en la PGE. En esta sección se describen las principales características, los componentes y el funcionamiento de este sistema, para realizar el control de acceso sobre los servicios.

Como se presenta en la Figura 12, el Sistema de Control de Acceso para Servicios consiste de tres componentes: un Servicio de Tokens de Seguridad, un Administrador de Políticas de Seguridad y un Firewall XML.


Figura 12 – Sistema de Control de Acceso para Servicios

El **Servicio de Tokens de Seguridad (Security Token Service, STS)** tiene la responsabilidad de emitir los *tokens* de seguridad necesarios para que las aplicaciones cliente puedan invocar a los servicios publicados en la PGE. Este componente soporta el estándar WS-Trust v1.3[24] y es implementado por el producto Tivoli Federated Identity Manager (TFIM) [25].

Para emitir los *tokens* de seguridad la PGE confía en las autenticaciones realizadas en los sistemas de los organismos, verificando la autenticidad de las solicitudes mediante el uso de Firma Electrónica [31].

Cuando una aplicación cliente de un organismo quiere consumir un servicio publicado en la plataforma, debe solicitar un *token* de seguridad al STS de la PGE utilizando el estándar WS-Trust. En esta solicitud se debe incluir otro *token* de seguridad que incluya, entre otros datos, el rol de usuario con el que se quiere acceder al servicio. Este *token* debe especificarse utilizando el estándar SAML v1.1 o v2.0 y debe además estar firmado electrónicamente por el organismo cliente.

Cuando la PGE recibe un pedido para el STS, verifica la firma digital del *token* de seguridad incluido en el pedido, de forma de corroborar que se trata de un consumidor en el que se confía. Además, se verifica que el rol del usuario, incluido en el *token* de seguridad, exista en el Directorio LDAP. Si la firma digital es verificada y el rol de usuario existe, el STS emite un *token* de seguridad firmado por la PGE. Este *token* de seguridad se especifica utilizando el estándar SAML v1.1 e incluye, entre otros datos, el rol del usuario.

La comunicación entre las aplicaciones cliente y el STS de la PGE se debe realizar a través de HTTPS. En la sección “Conexiones SSL con la PGE” se brindan más detalles sobre las conexiones SSL que se deben

establecer, entre los organismos y la PGE, para cumplir con este requerimiento.

La Figura 13 presenta un resumen de los pasos que debe seguir una aplicación cliente para solicitar un *token* de seguridad al STS de la PGE.

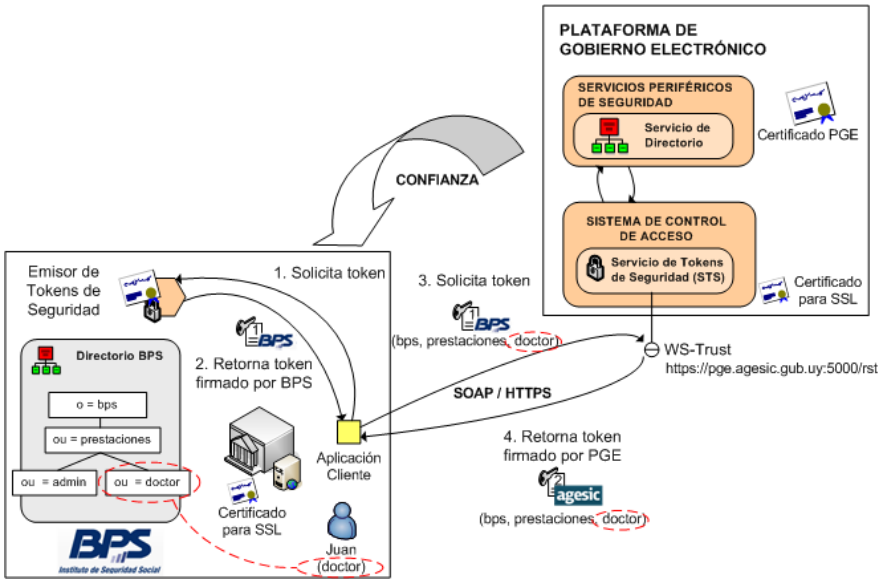


Figura 13 - Security Token Service

Primero, en los pasos 1 y 2, la aplicación cliente obtiene un *token* de seguridad firmado por el organismo, en este caso BPS. Para esto, se puede utilizar el estándar WS-Trust o cualquier otro mecanismo interno al organismo. Luego, en el paso 3, la aplicación cliente envía una solicitud de *token* de seguridad al STS de la PGE. Para esto se debe utilizar el estándar WS-Trust e incluir el *token* previamente obtenido. Finalmente, en el paso 4, si la firma del *token* enviado es verificada y el rol de usuario especificado en el *token* existe en el directorio LDAP, el STS emite un *token* de seguridad firmado por la PGE.

En la sección "**¡Error! No se encuentra el origen de la referencia.**" se especifica con más detalle los datos que se deben incluir en la solicitud del *token* al STS de la PGE, y los datos que se devuelven en la respuesta.

El **Administrador de Políticas de Seguridad** actúa como Punto de Decisión de Políticas (Policy Decision Point, PDP) siendo responsable por tomar la decisión de autorizar, o no, los pedidos de invocación a

servicios de la PGE. Este componente es implementado por el producto Tivoli Security Policy Manager (TSPM) [35].

En este componente se especifica qué roles tienen acceso a los métodos de los servicios de la PGE. Para esto, es necesario definir los Perfiles de Usuario que accederán a cada servicio, los métodos a los que tienen acceso estos perfiles, y con qué roles (de los organismos) se corresponden.

A modo de ejemplo, la Figura 14 presenta las políticas que se pueden definir para el servicio "Certificado de Nacidos Vivos".

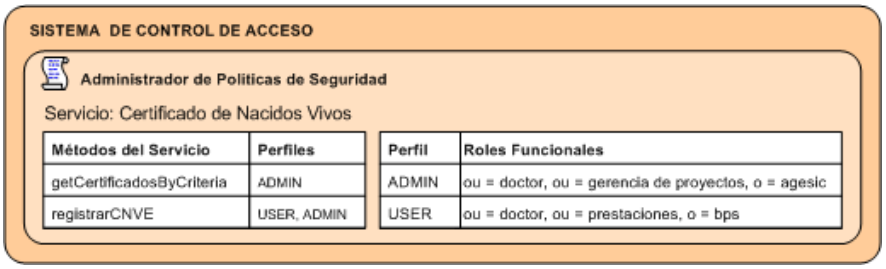


Figura 14 - Administrador de Políticas de Seguridad

En este caso se definen dos Perfiles de Usuario: ADMIN y USER. El Perfil de Usuario ADMIN tiene acceso al método "getCertificadosByCriteria" y está asociado al rol funcional "ou=doctor, ou=gerencia de proyectos, o=agesic". De forma similar, el Perfil de Usuario USER tiene acceso al método "registrarCNVE" y está asociado al rol funcional "ou=doctor, ou=prestaciones, o=bps".

Para que el Administrador de Políticas pueda tomar la decisión de autorizar, o no, la invocación a un método de un servicio, el cliente debe especificar el servicio y método que se quiere invocar. Para esto se utiliza el estándar WS-Addressing como se detalla en la sección "**¡Error! No se encuentra el origen de la referencia.**".

Además, como se menciona anteriormente, en la invocación del servicio se incluye también el rol funcional del usuario con el que se quiere realizar la invocación.

De esta forma, cuando la PGE recibe un pedido de invocación para a un método de un servicio, el Administrador de Políticas de Seguridad cuenta con toda la información necesaria para permitir o negar el acceso.

Por último, el **Firewall XML** actúa como Punto de Aplicación de Políticas (Policy Enforcement Point, PEP) de acuerdo a lo que decida el Administrador de Políticas de Seguridad. Este componente está implementado por el producto IBM Websphere Datapower Xi50 [29].

Para que el Firewall XML pueda actuar como PEP, para cada servicio de la PGE se despliega un Servicio Proxy en dicho Firewall. A modo de ejemplo, la Figura 15 presenta los Servicios Proxy de los servicios "Timestamp" y "Certificado de Nacidos Vivos". Una aplicación que quiera invocar a estos servicios debe hacerlo a través de sus Servicios Proxy. En caso de que se permita el acceso, el Firewall XML redirige el pedido a la Plataforma de Middleware, la cual envía la solicitud al servicio real.

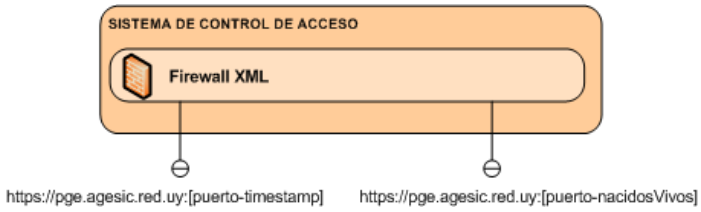


Figura 15 - Firewall XML

La comunicación entre las aplicaciones cliente y Servicios Proxy, así como la comunicación entre la PGE y los servicios en los organismos se realiza a través de HTTPS. En la sección "Conexiones SSL con la PGE" se brindan más detalles sobre las conexiones SSL que se deben establecer, entre los organismos y la PGE, para cumplir con este requerimiento.

A modo de resumen, la Figura 16 presenta los pasos que debe realizar una aplicación cliente para acceder a un servicio de la PGE.

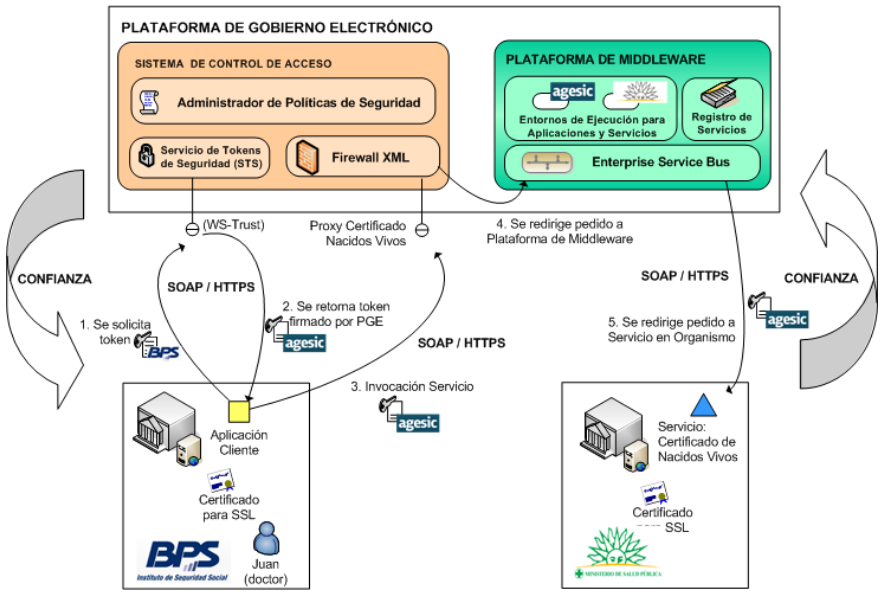


Figura 16 –Acceso a un Servicio de la PGE

En el paso 1 la aplicación cliente solicita un *token* de seguridad al STS[4] de la PGE, incluyendo en la solicitud un *token* firmado por el organismo, en este caso BPS, que contiene el rol del usuario. Si la firma del *token* es verificada y el rol del usuario existe en el Directorio LDAP, el STS, en el paso 2, devuelve a la aplicación un *token* de seguridad firmado por la PGE. Luego en el paso 3, la aplicación cliente invoca al servicio, a través de su Servicio Proxy, incluyendo en la invocación el *token* de seguridad firmado por la PGE. El Firewall XML permite o niega el acceso al servicio invocado, basándose en la decisión que tome el Administrador de Políticas de Seguridad. En caso de que el acceso sea permitido, el Firewall XML redirige el pedido, en el paso 4, a la Plataforma de Middleware la cual finalmente, en el paso 5, redirige el pedido al servicio[5].

[4] El acceso al STS se efectúa también a través del Firewall XML pero se omite para simplificar los diagramas.

[5] La comunicación entre la Plataforma de Middleware y el servicio también pasa a través del Firewall XML, pero se omite para simplificar los diagramas.

En la sección "**¡Error! No se encuentra el origen de la referencia.**" se explica en detalle este procedimiento especificando la información que se debe enviar en la invocación al servicio.

# Conectividad con la PGE

Para que un organismo pueda comunicarse con la PGE, ya sea para proveer o consumir servicios, es necesario que:

- el organismo esté conectado a la REDuy
- los *firewalls* de REDuy estén configurados para habilitar el tráfico de red requerido
- se puedan establecer conexiones SSL entre el organismo y la PGE

En esta sección se describen cada uno de estos requerimientos, especificando cómo debe proceder un organismo para cumplirlos.

## Conexión con REDuy

Como se menciona previamente en este documento, la REDuy provee la infraestructura de conectividad necesaria para que los organismos se interconecten entre sí, y con la PGE.

Para que un organismo provea un servicio en la PGE es necesario, entonces, que el organismo en el que se aloja el servicio esté conectado a la REDuy.

De forma similar, para que un organismo pueda consumir un servicio de la PGE, es necesario que el organismo en el que se aloja la aplicación cliente esté conectado a la REDuy.

En caso de no contar con conexión a la REDuy, un organismo puede solicitarla enviando un correo electrónico a soporte@agesic.gub.uy, especificando en el asunto del correo "[Conexión a REDuy] *Nombre del Organismo Solicitante*".

# Configuración de Firewalls de REDuy

Como se menciona previamente en este documento, la conexión de los organismos a la REDuy está protegida por *firewalls* que controlan el tráfico de red de los organismos, desde y hacia la REDuy.

Para que un organismo provea un servicio en la PGE es necesario, entonces, que estos *firewalls* estén configurados para habilitar el tráfico de red desde la PGE hacia el servidor donde se aloja el servicio.

La configuración de los firewalls está a cargo del equipo de soporte de AGESIC y se realiza una vez que se recibe y aprueba la petición de publicación de un servicio. Esta solicitud se realiza mediante el "**¡Error! No se encuentra el origen de la referencia.**" que se encuentra en el Apéndice 2.

Por otro lado, para que un organismo consuma servicios en la PGE, no es necesario realizar ninguna configuración adicional en los *firewalls*, dado que el tráfico hacia la REDuy se habilita al momento de instalarlos.

# Conexiones SSL con la PGE

Como se menciona en secciones anteriores, al consumir servicios de la PGE, la comunicación entre las aplicaciones cliente y la PGE, así como la comunicación entre la PGE y los servicios, se realiza a través de mensajes SOAP sobre HTTPS. Para esto es necesario establecer conexiones SSL entre la PGE y los organismos.

Para poder establecer estas conexiones, un organismo debe seguir los siguientes pasos:

1. Solicitar a AGESIC un certificado digital emitido por la CA de la PGE. La solicitud debe realizarse a través de un pedido de certificado en formato PKCS#10, el cual debe enviarse por correo electrónico a soporte@agesic.gub.uy junto con el "**¡Error! No se encuentra el origen de la referencia.**" o el "**¡Error! No se encuentra el origen de la referencia.**" (que se encuentran en el Apéndice 2), según el caso.

2. Instalar el certificado raíz de la CA de la PGE en los servidores o computadores del organismo, en donde se encuentran los servicios o aplicaciones que interactuarán con la PGE.

Por otro lado, las conexiones SSL que se establecen entre los organismos y la PGE deben cumplir los siguientes requisitos:

- Ser compatible con SSL v3.0
- Utilizar client_authentication con Certificados Digitales X.509 v3
- Utilizar certificados digitales emitidos por la CA de la PGE
- Soportar algunas de las CipherSuite especificadas en la Tabla 3

| |
|---|
| RC4_MD5_EXPORT Cipher |
| RC4_MD5_US Cipher |
| RC4_SHA_US Cipher |
| RC4_56_SHA_EXPORT1024 Cipher |
| TRIPLE_DES_SHA_US Cipher |
| TLS_RSA_WITH_AES_128_CBC_SHA Cipher |
| TLS_RSA_WITH_AES_256_CBC_SHA Cipher |
| AES_SHA_US Cipher |

Tabla 3 - CipherSuites para SSL

# Referencias

[1] AGESIC – REDuy. http://www.agesic.gub.uy/innovaportal/v/759/1/agesic/REDuy.html [Accedida en Abril de 2010]

[2] Centro Nacional de Respuesta a Incidentes en Seguridad Informática (CERTuy) http://www.cert.uy/ [Accedida en Abril de 2010]

[3] Basic Profile. http://www.ws-i.org/Profiles/BasicProfile-1.1.html [Accedida en Mayo de 2010]

[4] Basic Security Profile. http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html [Accedida en Mayo de 2010]

[5] AGESIC – Plataforma de Gobierno Electrónico. http://www.agesic.gub.uy/innovaportal/v/771/1/agesic/Plataforma-de-Gobierno-Electrónico.html [Accedida en Abril de 2010]

[6] Web Ontology Language (OWL) http://www.w3.org/2004/OWL/ [Accedida en Mayo de 2010]

[7] Protégé. http://protege.stanford.edu/ [Accedida en Mayo de 2010]

[8] WebSphere Portal. http://www-01.ibm.com/software/websphere/portal/ [Accedida en Mayo de 2010]

[9] JSR 168: Portlet Specification. http://jcp.org/en/jsr/detail?id=168 [Accedida en Mayo de 2010]

[10] JSR 286: Portlet Specification 2.0. http://jcp.org/en/jsr/detail?id=286, [Accedida en Mayo de 2010]

[11] Web Services for Remote Portlets (WSRP). http://www.oasis-open.org/committees/wsrp/ [Accedida en Mayo de 2010]

[12] Google Search Appliance. http://www.google.com/enterprise/gsa/ [Accedida en Mayo de 2010]

[13] Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data. http://www.protecciondedatos.gub.uy/sitio/Leyes/Ley-18.331.pdf [Accedida en Junio de 2010]

[14] Microsoft .NET Framework. http://www.microsoft.com/net/ [Accedida en Mayo de 2010]

[15] Java Enterprise Edition. http://java.sun.com/javaee/ [Accedida en Mayo de 2010]

[16] JBoss Enterprise SOA Platform. http://www.jboss.com/products/platforms/soa/ [Accedida en Noviembre de 2010]

[17] OASIS UDDI Specification TC http://www.oasis-open.org/committees/uddi-spec/ [Accedida en Agosto de 2010]

[18] Microsoft Biztalk Server. http://www.microsoft.com/biztalk/ [Accedida en Mayo de 2010]

[19] Biztalk ESB Toolkit. http://msdn.microsoft.com/en-us/biztalk/dd876606.aspx [Accedida en Mayo de 2010]

[20] Web Services Addressing Working Group. http://www.w3.org/2002/ws/addr/ [Accedida en Junio de 2010]

[21] Dave Chappell. Enterprise Service Bus. O'Reilly. 2004.

[22] XSL Transformations (XSLT). http://www.w3.org/TR/xslt [Accedida en Mayo de 2010]

[23] Tivoli Compliance Insight Manager. http://www-01.ibm.com/software/tivoli/products/compliance-insight-mgr/ [Accedida en Abril de 2010]

[24] WS-Trust 1.3. http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html [Accedida en Junio de 2010]

[25] Sistema de Seguridad de la Plataforma de Gobierno Electrónico. Presentación. 2009. http://www.agesic.gub.uy/innovaportal/file/758/1/seguridad.pdf [Accedida en Abril de 2010]

[26] Tivoli Federated Identity Manager. http://www-01.ibm.com/software/tivoli/products/federated-identity-mgr/ [Accedida en Abril de 2010]

[27] Tivoli Access Manager. http://www-01.ibm.com/software/tivoli/products/access-mgr-productline/ [Accedida en Abril de 2010]

[28] Tivoli Security Policy Manager. http://www-01.ibm.com/software/tivoli/products/security-policy-mgr/ [Accedida en Abril de 2010]

[29] WebSphere DataPower Integration Appliance XI50. http://www-01.ibm.com/software/integration/datapower/xi50/ [Accedida en Abril de 2010]

[30] JXplorer – Java LDAP Browser. http://jxplorer.org/ [Accedida en Mayo de 2010]

[31] Ley Nº 18.600. Documento Electrónico y Firma Electrónica http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18600 [Accedida en Mayo de 2010]

[32] Basic Profile. http://www.ws-i.org/Profiles/BasicProfile-1.1.html [Accedida en Mayo de 2010]

[33] Basic Security Profile. http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html [Accedida en Mayo de 2010]

[34] AGESIC. Guía de Programación Java para la Plataforma de Gobierno Electrónico. Junio 2010.

[35] Tivoli Security Policy Manager. http://www-01.ibm.com/software/tivoli/products/security-policy-mgr/ [Accedida en Mayo de 2010]

[36] Tivoli Identity Manager. http://www-01.ibm.com/software/tivoli/products/identity-mgr/ [Accedida en Mayo de 2010]

[37] Tivoli Directory Integrator. http://www-01.ibm.com/software/tivoli/products/directory-integrator/ [Accedida en Mayo de 2010]