Gobierno Brasileño

Comité Ejecutivo de Gobierno Electrónico

e-PING
Estándares de Interoperabilidad de Gobierno Electrónico

Documento de Referencia

Versión 2010

11 de diciembre de 2009

ÍNDICE

Presentación

La arquitectura e-PING – Estándares de Interoperabilidad de Gobierno Electrónico – define un conjunto mínimo de premisas, políticas y especificaciones técnicas que regulan la utilización de la Tecnología de la Información y Comunicación (TIC) en la interoperabilidad de Servicios de Gobierno Electrónico, estableciendo las condiciones de interacción con los demás Poderes y esferas de gobierno y con la sociedad en general.

Las áreas cubiertas por la e-PING están divididas en:

- Interconexión;
- Seguridad;
- Medios de Acceso;
- Organización e Intercambio de Informaciones;
- Áreas de Integración para Gobierno Electrónico.

Para cada uno de esos segmentos fueron especificados componentes, para los que son determinados estándares.

Todo el contenido de este documento de referencia está en conformidad con las directrices del Comité Ejecutivo de Gobierno Electrónico, creado por el Decreto de 18 de octubre de 2000, y está publicado en página específica en Internet (http://www.eping.e.gov.br), asegurando acceso público a las informaciones de interés general y transparencia propia de la iniciativa. El gobierno brasileño se compromete a garantizar que estas políticas y especificaciones permanezcan alineadas a las necesidades de la sociedad y a la evolución del mercado y de la tecnología.

El documento de referencia de la e-PING contiene:

- las bases de concepción, implantación y gestión de la e-PING, relacionando los beneficios esperados con el trabajo, definiendo los límites del alcance de la arquitectura e-PING y destacando las premisas consideradas y las políticas establecidas;
- el modelo de gestión de la e-PING, detallando responsabilidades, criterios de verificación de conformidad, gestión de alteraciones, divulgación y orientación para capacitación;
- las políticas y las especificaciones técnicas establecidas para todos los componentes de cada uno de los segmentos de la e-PING;
- Glosario de terminología técnica referenciada;
- relación de los integrantes y colaboradores de la presente versión de este documento.

Parte I – Visión General de la e-PING

1. Introducción

La base para la provisión de mejores servicios, adaptados a las necesidades de los ciudadanos y de los negocios, con costos más bajos, es la existencia de una infraestructura de Tecnología de la Información y Comunicación (TIC) que sirva como pilar para la creación de esos servicios. Un gobierno moderno, integrado y eficiente exige sistemas igualmente modernos, integrados e interoperables, trabajando de manera honesta, segura y coherente en todo el sector público.

En ese contexto, la interoperabilidad de tecnología, procesos, información y datos es condición vital para la provisión de servicios de calidad, volviéndose premisa para gobiernos en todo el mundo, como fundamento para los conceptos de gobierno electrónico, el *e-gov*. La interoperabilidad permite racionalizar inversiones en TIC, mediante compartición, reutilización e intercambio de recursos tecnológicos.

Gobiernos como el estadounidense, el canadiense, el británico, el australiano y el neozelandés invierten firmemente en el desarrollo de políticas y procesos y en el establecimiento de estándares en TIC, armando estructuras dedicadas para conseguir la interoperabilidad, con el objetivo de proveer servicios de mejor calidad con menores costos.

El gobierno brasileño está consolidando la arquitectura e-PING – "Estándares de Interoperabilidad de Gobierno Electrónico", que tiene por objetivo ser el paradigma para el establecimiento de políticas y especificaciones técnicas que posibiliten la prestación de servicios electrónicos de calidad a la sociedad.

¿Qué es la Interoperabilidad?

Para el establecimiento de los objetivos de la e-PING, es vital que se defina claramente lo que se considera *Interoperabilidad.* A continuación son presentados cuatro conceptos que cimentaron la concepción del gobierno brasileño a respecto del tema:

"Intercambio coherente de informaciones y servicios entre sistemas. Debe permitir el reemplazo de cualquier componente o producto utilizado en los puntos de interconexión por otro de especificación parecida, sin comprometer las funcionalidades del sistema." (gobierno del Reino Unido);

"Habilidad de transferir y utilizar informaciones de modo uniforme y eficiente entre varias organizaciones y sistemas de información." (gobierno de Australia);

"Habilidad de dos o más sistemas (ordenadores, medios de comunicación, redes, software y otros componentes de tecnologías de la información) de interactuar y de intercambiar datos en conformidad con un método definido, de manera a obtener los resultados esperados." (ISO);

"Interoperabilidad define si dos componentes de un sistema, desarrollados con herramientas diferentes, de proveedores diferentes, pueden o no actuar en conjunto." (Lichun Wang, Instituto Europeo de Informática – CORBA Workshops);

Interoperabilidad no es sólo Integración de Sistemas, ni sólo Integración de Redes. No se refiere únicamente al intercambio entre sistemas. No contempla sólo definición de tecnología.

Es, en realidad, la suma de todos esos factores, considerando también la existencia de un legado de sistemas, de plataformas de Hardware y Software instaladas. Parte de principios que tratan de la diversidad de componentes, con el uso de productos diferentes de proveedores distintos. Tiene por objetivo la consideración de todos los factores para que los sistemas puedan actuar cooperativamente, determinando las normas, las políticas y los estándares necesarios para consecución de esos objetivos.

Para que se conquiste la interoperabilidad, las personas deben estar comprometidas con un esfuerzo continuo para asegurar que sistemas, procesos y culturas de una organización sean administrados y direccionados para maximizar oportunidades de intercambio y reutilización de informaciones.

2. Descripción

Políticas y especificaciones claramente definidas para interoperabilidad y administración de informaciones son fundamentales para favorecer la conexión del gobierno, tanto en el ámbito interno como en el contacto con la sociedad y, en un nivel mayor de abarcadura, con el resto del mundo – otros gobiernos y empresas que actúan en el mercado mundial. La e-PING es concebida como una estructura básica para la estrategia de gobierno electrónico, aplicada inicialmente en el gobierno federal – Poder Ejecutivo, sin restringir la participación, por adhesión voluntaria, de otros poderes y esferas gubernamentales.

Los recursos de información del gobierno conforman valiosos activos económicos. Al garantizar que la información gubernamental pueda ser rápidamente localizada e intercambiada entre el sector público y la sociedad, mantenidas las obligaciones de privacidad y seguridad, el gobierno ayuda en el aprovechamiento máximo de este activo, impulsando y estimulando la economía nacional.

La arquitectura e-PING cubre el intercambio de informaciones entre los sistemas del gobierno federal – Poder Ejecutivo y las interacciones con:

- Ciudadanos;
- Otros niveles de gobierno (estatal y municipal);
- Otros Poderes (Legislativo, Judicial) y Ministerio Público Federal;
- Organismos Internacionales;
- Gobiernos de otros países;
- Empresas (en Brasil y en el mundo);
- Tercer Sector.

La figura a continuación representa esa relación.

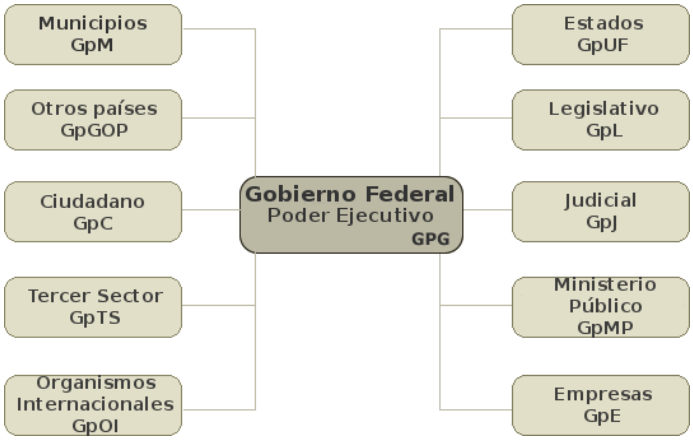

Figura 1 – Relaciones del gobierno federal.

2.1. Adhesión a la e-PING

La adopción de los estándares y políticas contenidos en la e-PING no puede imponerse a los ciudadanos y a las varias instancias gubernamentales, dentro y fuera del país. El gobierno brasileño, sin embargo, establece esas especificaciones como el estándar por el seleccionado y aceptado, o sea, estos son los estándares en que desea interoperar con las entidades externas al gobierno federal – Poder Ejecutivo Brasileño. La adhesión de esas entidades se dará de forma voluntaria y sin cualquier intromisión de la Coordinación de la e-PING.

Para los órganos del gobierno federal – Poder Ejecutivo brasileño, la adopción de los estándares y políticas contenidos en la e-PING es obligatoria.

El “gobierno federal – Poder Ejecutivo” brasileño incluye:

- Los órganos de la Administración Directa: Ministerios, Secretarías y otras entidades

gubernamentales de la misma naturaleza jurídica, relacionados directa o indirectamente a la Presidencia de la República de Brasil;

- Las Autarquías y fundaciones.
- En el ámbito de las entidades antes mencionadas, son obligatorias las especificaciones contenidas en la e-PING para:
- Todos los nuevos sistemas de información que sean desarrollados e implantados en el gobierno federal y que se encuadran en la descripción de la interacción, dentro del gobierno federal y con la sociedad en general;
- Sistemas de información legados que sean objeto de implementaciones que involucren provisión de servicios de gobierno electrónico o interacción entre sistemas;
- Otros sistemas que formen parte de los objetivos de colocar a disposición los servicios de gobierno electrónico.

La adhesión sucederá de forma gradual, conforme plan de implementación creado por el propio órgano, que considerará la situación de la institución en relación a las condiciones para adaptarse a las especificaciones y recomendaciones de la e-PING.

El contraste de la situación del órgano cuanto al uso efectivo de los estándares se realizará con base en el Modelo de Grado de Adopción de la e-PING – M-PING, actualmente en construcción.

Para los sistemas de información del gobierno que estén fuera de la descripción de obligatoriedad limitada, es recomendable que los responsables consideren la adaptación a los estándares de la e-PING siempre que sean planificados esfuerzos significativos de actualización.

Todas las compras y contrataciones del gobierno federal – Poder Ejecutivo dirigidas al desarrollo de servicios de gobierno electrónico y para actualizaciones de sistemas legados deben ser concordantes con las especificaciones y políticas contenidas en este documento.

La e-PING estimula la participación de todas las partes interesadas en el desarrollo y actualización continua de las especificaciones y recomendaciones que integran la arquitectura. La gestión de la e-PING prevé esa participación, con el uso de Internet (http://www.eping.e.gov.br) como medio preferencial para el contacto entre gestores de la e-PING y la sociedad.

2.2. Foco en la interoperabilidad

La e-PING no tendrá como foco de trabajo todos los asuntos del área de Tecnologías de la Información y Comunicación (TIC). Serán tratadas sólo especificaciones que sean relevantes para garantizar la interconexión de sistemas, integración de datos, acceso a servicio de gobierno electrónico y administración de contenido. La e-PING involucra los asuntos abarcados en la segmentación, descrita en el ítem 4 de este documento.

2.3. Asuntos no tratados

La e-PING no objetiva estandarizar la forma de presentación de las informaciones de los servicios de gobierno electrónico, limitándose a la definición de los requisitos de intercambio de datos y de las condiciones de disponibilidad de esos datos para los dispositivos de acceso.

Informaciones sobre directrices y políticas relativas a la presentación y accesibilidad de los portales y páginas del gobierno están disponibles en el portal del gobierno electrónico brasileño (http://www.governoeletronico.gov.br).

3. Políticas Generales

Están relacionadas a continuación las políticas generales utilizadas en la construcción de la e-PING y que cimentan las políticas y especificaciones técnicas de cada segmento:

3.1. Adopción Preferencial de Estándares Abiertos

La e-PING define que, siempre que sea posible, serán adoptados estándares abiertos en las especificaciones técnicas. Estándares propietarios son aceptados, de forma pasajera, manteniéndose las perspectivas de reemplazo cuando haya condiciones de migración disponibles. Sin perjudicar esas metas, serán respetadas las situaciones en que haiga necesidad de consideración de requisitos de seguridad e integridad de informaciones.

3.2. Software Público y/o Software Libre

La implementación de los estándares de interoperabilidad debe priorizar la utilización de software público y/o software libre, de acuerdo con directrices del Comité Ejecutivo del Gobierno Electrónico y normas definidas en el ámbito del SISP.

3.3. Transparencia

Los documentos de la e-PING estarán a disposición de la sociedad, por medio de Internet, previendo mecanismos de divulgación, recepción y evaluación de sugerencias. En ese sentido, serán definidos – y divulgados para amplio conocimiento – plazos y compromisos para implantación y gestión de sitio dedicado en Internet (http://www.eping.e.gov.br).

3.4. Seguridad

La interoperabilidad en la prestación de los servicios de gobierno electrónico debe considerar el nivel de seguridad requerido por el servicio, con la mayor transparencia posible.

3.5. Soporte de mercado

Todas las especificaciones contenidas en la e-PING contemplan soluciones ampliamente apoyadas por el mercado. La meta a ser alcanzada es la reducción de los costos y de los riesgos en la concepción y producción de servicios en los sistemas de informaciones gubernamentales.

La e-PING considera que la interoperabilidad involucra elementos técnicos, semánticos y organizacionales, siendo políticas generales directoras de esas dimensiones:

3.6. Dimensión técnica

3.6.1. Alineamiento con INTERNET

Todos los sistemas de información de la administración pública deberán estar alineados con las principales especificaciones utilizadas en Internet y con la *World Wide Web.*

3.6.2. Adopción del XML

Como estándar primario de intercambio de datos para todos los sistemas del sector público.

3.6.3. Adopción de navegadores (*browsers*)

Como principal medio de acceso: Todos los sistemas de información gubernamentales deberán ser

accesibles, preferencialmente, por medio de tecnología basada en *browser*; otras interfaces son permitidas en situaciones específicas, como en rutinas de actualización y captación de datos donde no haya alternativa tecnológica disponibles basada en navegadores.

3.6.4. Escalabilidad

Las especificaciones seleccionadas deberán tener la capacidad de atender alteraciones de demanda en el sistema, como cambios en volúmenes de datos, cantidad de transacciones o cantidad de usuarios. Los estándares establecidos no podrán ser un factor restrictivo, debiendo ser capaces de cimentar el desarrollo de servicios que atiendan de necesidades más específicas, involucrando pequeños volúmenes de transacciones y de usuarios, a demandas de abarcadura nacional, con tratamiento de gran cantidad de informaciones y envolvimiento de un gran contingente de usuarios.

3.7. Dimensión semántica

3.7.1. Desarrollo y mantenimiento de recursos de organización de la información

Buscando contribuir para la simplificación del acceso a documentos y servicios por el ciudadano brasileño, como vocabularios controlados, taxonomías, ontologías y otros métodos de organización y recuperación de informaciones.

3.7.2. Desarrollo y adopción de un Estándar de Metadatos del Gobierno Electrónico – e-PMG

Con base en estándares internacionalmente aceptados (http://www.eping.e.gov.br).

3.8. Dimensión organizacional

3.8.1. Simplificación administrativa

La aplicación de la e-PING busca contribuir para que las interacciones del gobierno con la sociedad sean realizadas de forma simple y directa, sin daños a la legislación vigente.

3.8.2. Promoción de la colaboración entre organizaciones

Mediante la integración entre objetivos institucionales y procesos de negocio de organizaciones con estructuras internas y procesos internos diferentes.

3.8.3. Garantía de la privacidad de información

Todos los órganos responsables por el ofrecimiento de servicios de gobierno electrónico deben asegurar las condiciones de preservación de la privacidad de las informaciones del ciudadano, empresas y órganos gubernamentales, respetando y cumpliendo la legislación que define las restricciones de acceso y divulgación.

4. Segmentación

La arquitectura e-PING fue divida en cinco partes, con el fin de organizar las definiciones de los estándares. Para cada uno de los **segmentos**, fue elaborado un grupo de trabajo, formado por profesionales que actúan en órganos de los gobiernos federal, estatal y municipal, especialistas en cada tema. Esos grupos fueron responsables por la elaboración de esta versión de la arquitectura, pilar para el establecimiento de los estándares de interoperabilidad del gobierno brasileño.

Los cinco segmentos – “Interconexión”, “Seguridad”, “Medios de Acceso”, “Organización e Intercambio de Informaciones" y "Áreas de Integración para el Gobierno Electrónico” – fueron subdivididos en **componentes**, para los que fueron determinadas las políticas y las especificaciones técnicas a ser adoptadas por el gobierno federal. A continuación son relacionados los componentes que forman cada uno de los cinco segmentos.

4.1. Interconexión

El segmento “Interconexión” estipula las condiciones para que los órganos gubernamentales se interconecten, además de fijar las condiciones de interoperación entre el gobierno y la sociedad.

En este segmento, son establecidas las especificaciones para:

- Mensajería;
- Infraestructura de Red;
- Servicios de Red.

4.2. Seguridad

Este segmento aborda los aspectos de seguridad de TIC que el gobierno debe considerar. Son tratados los estándares para:

- Seguridad en la Comunicación de Datos;
- Seguridad de Correo Electrónico;
- Criptografía;
- Desarrollo de Sistemas;
- Servicios de Red;
- Redes Inalámbricas (Wireless);
- Respuesta a Incidentes de Seguridad de la Información;
- Políticas y Especificaciones para Tarjetas Inteligentes (*smart-cards*) y *tokens.*

4.3. Medios de Acceso

En el segmento “Medios de Acceso" son expuestas las cuestiones relativas a los estándares de los dispositivos de acceso a los servicios de gobierno electrónico. En esta versión son tratadas las políticas y las especificaciones para estaciones de trabajo, televisión digital y movilidad. En versiones futuras, serán abordados otros dispositivos. Está formado por tres subgrupos considerando los siguientes componentes:

Estándares para acceso mediante estaciones de trabajo:

- Navegadores (*browsers*);
- Conjunto de Letras y Alfabetos;
- Formato de Intercambio de Hipertexto;
- Archivos del Tipo Documento;
- Archivos del Tipo Planilla;
- Archivos del Tipo Presentación;
- Archivos del Tipo Banco de Datos para Estaciones de Trabajo;

- Especificación de Intercambio de Informaciones Gráficas e Imágenes Estáticas;
- Gráficos Vectoriales;
- Especificación de Estándares de Animación;
- Archivos del Tipo Audio y del Tipo Video;
- Compactación de Archivos de Uso General;
- Archivos para referencia geográfica;
- Programación Extendida (Plugins).

Movilidad:

- Definición;
- Protocolo de transmisión;
- Navegador;
- Estándar de Hipertexto;
- Programación Extendida;
- Mensajería;
- Archivos de Video y Audio;
- Archivos de Imagen;
- Archivos de Oficina;
- Lector de PDF.

TV Digital:

- Definición;
- Normas de la ABNT;
- Especificaciones de Estándares.

4.4. Organización e Intercambio de Informaciones

Aborda los aspectos relacionados al tratamiento y a la transferencia de informaciones en los servicios de gobierno electrónico. Incluye estándar de estructura de temas de gobierno y de metadatos, abarcando los siguientes componentes:

- Lenguaje para intercambio de datos;
- Lenguaje para transformación de datos;
- Definición de los datos para intercambiar;
- Vocabulario Controlado del Gobierno Electrónico (VCGE);
- Estándar de Metadatos del Gobierno (e-PMG).

4.5. Áreas de Integración para Gobierno Electrónico

El segmento establece la utilización o construcción de especificaciones técnicas basadas en el estándar XML para sostener el intercambio de informaciones en áreas transversales de la actuación gubernamental.

Las herramientas que apoyan la actuación del segmento son:

- Catálogo Estándar de Datos (CPD);
- Catálogo XML *Schemas*;
- Catálogo de Servicios Interoperables (*Web Services*).

5. Gestión de la e-PING

En este ítem son tratados los aspectos de gestión de la arquitectura e-PING, especificando la forma mediante la cual el gobierno brasileño pretende consolidar la implantación de las políticas y especificaciones técnicas como estándares efectivos adoptados tanto internamente, por los órganos que componen la Administración Pública Federal, como en la interoperación con las entidades externas, representadas por otras instancias de gobierno, por la iniciativa privada, por instituciones que actúan en el tercer sector y por el ciudadano.

5.1. Histórico

La arquitectura e-PING tiene por objetivo ser el paradigma de interoperabilidad para el gobierno federal, inicialmente en el ámbito del Pode Ejecutivo. La iniciativa de montaje de la arquitectura cupo a tres órganos de la esfera federal:

- Ministerio de la Planificación, Presupuesto y Gestión, mediante su Secretaría de Logística y Tecnología de la Información (SLTI/MP);
- Instituto Nacional de Tecnologías de la Información, de la Presidencia de la República (ITI);
- Servicio Federal de Procesamiento de Datos (SERPRO), empresa pública relacionada al Ministerio de Hacienda.

Esos tres órganos organizaron un Seminario, con colaboración de entidades del gobierno federal, en el ámbito del Poder Ejecutivo, teniendo como fin la formación de un comité entre órganos - denominado Comité Constituyente - para liderar los trabajos iniciales de montaje de la arquitectura.

Después de su institucionalización, por medio de la Portería Normativa nº 5, de 14 de julio de 2005, el Comité pasó a ser denominado Coordinación de la e-PING. Además de los tres organizadores, participan de ese grupo las siguientes entidades: Presidencia de la República, Ministerio de Relaciones Exteriores, Ministerio de la Salud, *Banco do Brasil, Caixa Econômica Federal*, DATAPREV y *Associação Brasileira de Entidades Estaduais de Tecnologia da Informação e Comunicação* (Asociación Brasileña de Entidades Estatales de Tecnologías de la Información y Comunicación - ABEP).

El Comités estableció el siguiente programa laboral:

- Definición de la forma inicial de elaboración y gestión de la arquitectura e-PING;
- Definición de la división de los temas a ser tratados por la e-PING;
- Creación de cinco grupos de trabajo responsables por las definiciones iniciales de políticas y especificaciones técnicas para cada uno de los segmentos;
- Establecimiento de un cronograma de trabajo con el objetivo de construcción y divulgación de la versión inicial de la arquitectura, denominada versión 0;
- Realización de consulta pública y audiencias públicas en RS, SP, DF, RJ, MG y PE, de modo que sean colectadas contribuciones, de la sociedad en general, sobre el contenido propuesto en la versión 0;
- Publicación de la versión 1, junto con la resolución de institucionalización de la e-PING en el ámbito de la APF – Poder Ejecutivo;
- Publicación de la versión 1.5, conteniendo las actualizaciones y revisión de las especificaciones técnicas y de la visión general de la e-PING. Las versiones 1.1 hasta 1.4 quedaron en discusión interna en los grupos de trabajo y en la coordinación de la e-PING.
- Realización de consulta pública y audiencias públicas de modo que sean colectadas contribuciones, de la sociedad en general, a cada nueva versión de documento de referencia;
- Publicación de la versión anual, conteniendo las actualizaciones y revisiones de las especificaciones técnicas y de la visión general de la e-PING.

Experiencias similares desarrolladas por gobiernos de otros países son constantemente analizadas. La e-GIF – *Government Interoperability Framework* – del gobierno británico fue adoptada como base para construcción de la arquitectura de interoperabilidad del gobierno brasileño. La gestión de la e-PING se apoya en la forma implementada por el gobierno del Reino

Unido, operante desde el año 2000, y, en el presente, con un grado de desarrollo internacionalmente reconocido como referencia.

5.2. Estrategia de Implantación

La divulgación de los estándares y especificaciones establecidos por el gobierno brasileño sigue el esquema de versiones. Está prevista la elaboración de una versión anual, con publicación intermediaria de actualizaciones, siempre que existan modificaciones significativas.

La presente versión consolidó el trabajo de los grupos armados para los cinco segmentos definidos. Todo su contenido fue colocado a disposición para consulta pública, con el objetivo de obtener contribuciones para las propuestas de estándares publicados en la minuta de la versión 2010.

5.3. Modelo de Gestión

En este ítem son especificadas las formas de gestión de la arquitectura e-PING, siendo relacionadas las principales atribuciones y la forma de implementación de esas actividades en la organización estructural del gobierno.

5.3.1. Atribuciones

La Gestión de la e-PING abarca el desempeño de atribuciones de orden administrativo y de orden técnico.

Entre las **atribuciones de carácter administrativo**, sobresalen:

- Definir los objetivos estratégicos y de gestión de gobierno para el establecimiento de los estándares;
- Administrar la arquitectura de interoperabilidad del gobierno brasileño, proveyendo la infraestructura administrativa necesaria para su correcta utilización y garantizando su actualización, considerando: Las prioridades y metas de gobierno, las necesidades de la sociedad y la disponibilidad de nuevas tecnologías maduras y soportadas por el mercado de TIC;
- Actuar como centro de coordinación de la arquitectura e-PING, buscando alineamiento de los esfuerzos de interoperabilidad, garantizando la coherencia de las iniciativas emprendidas por los órganos de gobierno;
- Específicamente para los segmentos de Interoperabilidad, administrar la relación del gobierno federal – Poder Ejecutivo – con las demás instancias definidas en el ítem 2 – Descripción;
- Administrar y operar la divulgación de los estándares de la e-PING, considerando:
  - Creación y administración de una página en Internet para la e-PING;
  - Coordinación del proceso de consultas públicas;
  - Coordinación del proceso de recepción y evaluación de proposiciones de alteración y complementación;
  - Coordinación del proceso de solicitación de sugerencias para la e-PING;
  - Publicación de las versiones actualizadas de la e-PING y de las actualizaciones intermediarias;
- Administrar la interacción con iniciativas del mismo propósito, lideradas por otros gobiernos, nacional e internacionalmente;
- Incentivar la capacitación de los equipos del gobierno federal, actuando en grupo con los órganos, en la consideración de la e-PING en los planes específicos de adiestramiento de cada uno de ellos, y en la realización de eventos corporativos dirigidos a la diseminación de los estándares e-PING;
- Establecer, implantar y divulgar indicadores de acompañamiento de los resultados obtenidos con la implantación de la e-PING;

- Administrar la interacción con organismos de especificación (W3C, IEEE, BSI, OMG, OGC, OASIS, IETF, Institutos Normativos de segmentos específicos, como ABNT, INMETRO, ISO, NIST, etc.); Estos organismos serán seleccionados a criterio de la coordinación de la e-PING, considerando su notorio reconocimiento internacional, competencia en su área de actuación y el establecimiento de estándares abiertos.
- Administrar la interacción con órganos de fomento nacionales e internacionales, para canalizar recursos, buscando atender las necesidades de creación de infraestructura de la e-PING y promover la investigación y desarrollo;
- Posibilitar la implantación y administrar el proceso de homologación de los estándares que serán estipulados para el gobierno;
- Posibilitar la implantación y administrar procesos de auditoría realizados con la finalidad de verificar el nivel de adhesión a las recomendaciones y especificaciones de la e-PING;
- Actuar cooperativamente, como apoyo a los órganos de gobierno, en la realización de los procesos necesarios para adaptación a los estándares e-PING; evaluar la posibilidad de patrocinar programas abarcadores que promuevan la utilización intensiva de los estándares propuestos.

Entre las **atribuciones de carácter técnico**, sobresalen:

- Establecer las formas de elaboración y de mantenimiento de las políticas y especificaciones técnicas que componen la e-PING, considerando:
  - Identificación, creación y gestión de grupos de trabajo específicos;
  - Establecimiento de convenios y definición de instituciones gubernamentales como responsables por las políticas y especificaciones técnicas de componentes específicos de los segmentos de interoperabilidad;
  - Identificación e implementación de formas alternativas de administración técnica de los temas contemplados en la abarcadura de actuación de la e-PING;

- Coordinar el desarrollo y mantenimiento, en el ámbito del gobierno federal – Poder Ejecutivo, de:
  - Estándar de Metadatos del Gobierno (e-PMG);
  - Vocabulario Controlado del Gobierno Electrónico (VCGE);
  - Catálogo de Estándares de Datos (CPD);
  - Catálogo de Referencia de los Esquemas XML;
  - Demás Estándares de Organización e Intercambio de Informaciones;
  - Estándares de Interconexión;
  - Estándares de Seguridad;
  - Estándares de Medios de Acceso a servicios electrónicos del gobierno;
  - Estándares de utilización de Tarjetas Inteligentes, *Tokens* y otros tipos de tarjeta;
- Garantizar la unicidad de concepción, conceptos, definiciones y establecimiento de estándares por parte de los responsables por los segmentos técnicos definidos para la e-PING.

5.3.2. Responsabilidades

La estructura gubernamental creada para administración de la e-PING es presentada en el esquema simplificado a seguir.

Figura 2 – Administración de la e-PING.

La SLTI/MP, mediante el instrumento del Sistema de Administración de los Recursos de Información e Información (SISP), instituido por el Decreto 1.048, de 21 de enero de 1994, es la responsable por la institucionalización y por la definición del formato jurídico de la Coordinación de la e-PING.

La actuación de la Coordinación de la e-PING será pautada por los siguientes ítems:

- Implantación de la arquitectura e-PING, forneciendo las actividades necesarias para consolidación de la versión actual y dinámica de su evolución;
- Gestión de la arquitectura e-PING;
- Establecimiento y gestión de las normas y de los instrumentos institucionales y legales que garanticen la efectividad de las recomendaciones y especificaciones de la e-PING;
- Administración de los estándares considerados en la e-PING;
- Garantía de mantenimiento de la actualización de los varios catálogos de la e-PING;
- Gestión de los procesos de Comunicación y Divulgación de los estándares, de las decisiones y de las actividades de la e-PING, incluyendo la publicación de nuevas versiones y de las actualizaciones intermediarias;
- Creación de un sello e-PING y administración de proceso que certifique la adhesión de determinado servicio o producto a la e-PING;
- Provisión de criterios y subsidios para la elaboración de la Ley Presupuestaria Anual del gobierno federal;
- Gestión de los procesos de contratación de los servicios y de establecimiento de convenios para realización de las atribuciones necesarias para consolidación de los estándares, como, por ejemplo, evaluación de propuestas de proyectos de e-gov destinados a la Administración Pública Federal, homologación de estándares y verificación de conformidad;
- Establecimiento de los puntos de contacto con los diversos órganos de la Administración Pública Federal;
- Administración de los Grupos de Trabajo – GT, definiendo su composición y determinando las directrices laborales, basadas en las políticas técnicas, generales y específicas, en las necesidades de gobierno y en el monitoreo del panorama tecnológico.

Los Grupos de Trabajo de la e-PING, constituidos por representantes indicados por los varios órganos de la APF y por representantes de instituciones de otras esferas gubernamentales, son responsables por:

- Tatar los temas que componen los segmentos de la e-PING;
- Monitorear sistemáticamente el mercado, principalmente para los segmentos bajo su responsabilidad, con el objetivo de detectar las necesidades de actualización tecnológica de las políticas y especificaciones técnicas;
- Subsidiar la actuación de la Coordinación de la e-PING, en la performance de sus atribuciones administrativas y técnicas.

Los coordinadores de los Grupos de Trabajo tendrán lugar en la Coordinación de la e-PING.

5.4. Actividades adicionales

Además de las atribuciones de carácter administrativo y técnico para implantación y mantenimiento evolutivo de la arquitectura e-PING, otras actividades estarán bajo responsabilidad de la Coordinación de la e-PING.

5.4.1. Selección y Homologación de Estándares Tecnológicos

Las políticas técnicas incluidas en este documento cimentan los estándares de la e-PING, sirviendo como referencia en la selección de los componentes para los que son establecidas las especificaciones técnicas.

La e-PING prevé un proceso de análisis de los estándares candidatos a integrar la arquitectura. Ese proceso abarca la selección, la homologación y la clasificación de las especificaciones seleccionadas en cinco niveles de situaciones, que caracterizan el grado de adhesión a las políticas técnicas generales y específicas de cada segmento.

Esos cinco niveles son los siguientes:

• **Adoptado (A):** Ítem adoptado por el gobierno como estándar en la arquitectura e-PING, habiéndose sometido a un proceso formal de homologación realizado por una institución gubernamental o por otra institución con delegación formal para realizar el proceso. También se lo considera homologado cuando se basa en una proposición debidamente cimentada por la coordinación del segmento, publicada en la página y aprobado por la Coordinación de la e-PING;

• **Recomendado (R):** Ítem que coincide con las políticas técnicas de la e-PING, es reconocido como un ítem que debe utilizarse en el ámbito de las instituciones gubernamentales, pero aún no fue sometido a un proceso formal de homologación;

• **En Transición (T):** Ítem que el gobierno no recomienda, por no cumplir con uno o más requisitos establecidos en las políticas generales y técnicas de la arquitectura; está incluido en la e-PING por causa de su utilización significativa en instituciones gubernamentales, tendiendo a ser desactivado cuando algún otro componente, en una de las dos situaciones anteriores, presente condiciones totales para reemplazarlo. Puede llegar a ser considerado un componente “recomendado” caso se adapte a todas las políticas técnicas establecidas. Conviene resaltar que el desarrollo de nuevos servicios o la reconstrucción de partes significativas de los ya existentes debe evitar la utilización de componentes clasificados como pasajeros;

• **En Estudio (E):** Componente que está siendo evaluado y podrá ser encasillado en una de las situaciones anteriores, cuando el proceso evaluador haya terminado;

• **Estudio Futuro (F):** Componente aún no analizado y que será sometido posteriormente a evaluación.

El proceso de selección de los componentes adoptados por la e-PING y su consecuente clasificación en las situaciones antes indicadas es de responsabilidad de los Grupos de Trabajo formados por profesionales especialistas que actúan en el gobierno y en instituciones con las cuales esté establecido algún tipo de sociedad o contrato específicamente para ese fin.

La selección es realizada por medio de sugerencias formalizadas, demandas internas de los órganos del gobierno federal, Poder Ejecutivo, y encuestas realizadas por los Grupos de Trabajo.

Ya la homologación deberá ser objeto de estudio más profundizado por parte de los gestores de la e-PING. En virtud de la gran variedad de componentes abordados por la arquitectura, habrá necesidad de elaboración de una sistemática de homologación que contemple desde procesos en que sea indispensable la evaluación de características físicas de determinados componentes (Tarjetas Inteligentes, por ejemplo) hasta otros en que sean requeridos estudios de aspectos que involucren el uso del componente en el desarrollo y construcción de servicios (organización e intercambio de informaciones y seguridad, por ejemplo).

En ese caso, el gobierno deberá establecer sociedades o acreditar instituciones para elaboración de exámenes de conformidad, siempre definiendo cuáles componentes deben ser sometidos a procesos de homologación, cuáles son los criterios para examinar los resultados y cuáles son las condiciones de realización de los procedimientos.

La definición completa del proceso de selección y homologación, considerando las especificidades de los segmentos, quedará al mando de la Coordinación de la e-PING.

5.4.2. Auditoría de Conformidad

El cumplimiento de las especificaciones y recomendaciones por parte de los órganos del gobierno federal – Poder Ejecutivo es el factor crítico de éxito en la implantación y consolidación de la e-PING. Los gestores de la e-PING recomendarán la realización de procesos de auditoría para verificación del cumplimiento de las especificaciones y políticas de la arquitectura.

Podrá haber delegación de responsabilidad para equipos especialmente formados para ese fin, compuestos por técnicos de gobierno con experiencia en procedimientos de esa proveniencia.

La forma preferencial de realización de ese tipo de procedimiento, sin embargo, será el uso de las estructuras propias en los órganos responsables por auditoría de sistemas. La Coordinación de la e-PING actuará en el sentido de sugerir los criterios básicos que los órganos deberán seguir. Para eso, fue organizado, mediante la Portería nº 8, de 31 de octubre de 2008, de la SLTI/MP, Grupo de Trabajo para estudiar, analizar y proponer modelo de auditoría a respecto de la adhesión de los estándares de la e-PING. Esa propuesta también considerará el modelo de grado de la e-PING (M-PING).

Otra cuestión a ser considerada será la participación de órganos gubernamentales actuantes en el área, previéndose contactos con instituciones de otros Poderes y esferas gubernamentales.

5.4.3. Creación y Mantenimiento de la Página

Todo el proceso de intercambio de informaciones sobre la e-PING con usuarios, colaboradores e interesados es realizado preferentemente, por Internet, en la dirección http://www.eping.e.gov.br. En su etapa más avanzada de funcionamiento, la página de la e-PING tendrá, como principales funcionalidades:

- Divulgación completa de la documentación relacionada a la arquitectura: Versiones oficiales y correspondientes actualizaciones de la arquitectura, versiones para consulta pública, documentación técnica de apoyo, documentación legal e institucional correspondiente;
- Disponibilidad de las recomendaciones, determinaciones, especificaciones técnicas y políticas para validación, homologación y recepción de comentarios y sugerencias de la sociedad;
- Publicación de solicitación de comentarios relacionados a la especificación de componentes para la arquitectura;
- Disponibilidad de medio electrónico para recepción de sugerencias;
- Disponibilidad de enlaces a documentos, estándares, normas o cualquier otro tipo de referencia constante en la e-PING.

5.4.4. Acompañamiento Legal e Institucional

La e-PING tendrá apoyo constante del equipo de Asesoría Jurídica del Ministerio de Planificación, Presupuesto y Gestión para asegurar la adhesión a las normas e instrumentos legales vigentes en el país del contenido de los documentos que componen la arquitectura.

Adicionalmente, esa Asesoría también tendrá la responsabilidad de preparar toda la parte institucional necesaria para garantizar que las adaptaciones y recomendaciones de la e-PING compongan el conjunto de instrumentos legales de TIC en el país.

La coordinación de la e-PING podrá actuar estableciendo una forma de colaboración con algún otro órgano de gobierno que tenga condiciones de proveer su estructura de soporte jurídico para realización de esa actividad.

5.4.5. Divulgación

Será dada total publicidad a todo el contenido de la e-PING. Las principales formas de divulgación previstas, además de la página en Internet, son:

- Realización de eventos específicos para divulgación, como Seminarios, Talleres y presentaciones en general;
- Participación en eventos gubernamentales en el área de TIC y correlacionadas;
- Participación en eventos destinados a públicos específicos
- Publicación de todas las versiones de la e-PING y de las actualizaciones intermediarias;
- Intercambio con otras esferas y otros Poderes gubernamentales, con instituciones públicas, privadas y del tercer sector y con gobiernos de otros países.

5.4.6. Capacitación

Formarán parte de la agenda de implantación y gestión de la e-PING eventos dirigidos a la capacitación. También está prevista la utilización intensiva de Aprendizaje a Distancia (CAD).

La Coordinación de la e-PING elaborará y publicará un currículo estándar de adiestramiento, de forma que cada órgano de la APF posea subsidios para planificar y estimar inversiones necesarias para capacitación de los profesionales involucrados en el proceso de adaptación a las recomendaciones de la e-PING.

Cada órgano gubernamental deberá observar las definiciones de estándar de la e-PING en el montaje de sus planes particulares de capacitación, asegurando la provisión de adiestramiento adecuado para los componentes de sus equipos técnicos.

5.5. Relación con Gobierno y Sociedad

En este ítem son tratadas las formas de relación de la e-PING con las entidades que componen el gobierno y la sociedad.

5.5.1. Organizaciones del Gobierno Federal – Poder Ejecutivo

En el ámbito del Poder Ejecutivo, la participación de todos los niveles jerárquicos de la Administración Pública Federal, sus agencias y organismos reguladores y las empresas e instituciones públicas es esencial para la promoción y consolidación de la interoperabilidad en el sector público.

Aunque las directrices generales sean administradas por la Coordinación de la e-PING, cada institución en particular tendrá su responsabilidad en la gestión y garantía de uso de los estándares e-PING. Entre las atribuciones de esa proveniencia, sobresalen:

- Contribuir para el desarrollo y mejoría continua de la e-PING;
- Asegurar que sus estrategias organizacionales de TIC consideren que los sistemas integrantes de servicios de gobierno electrónico bajo su responsabilidad estén adaptados a las recomendaciones de la e-PING;
- Disponer de un plan de implementación y adaptación de la infraestructura de TIC de la organización a la arquitectura e-PING;
- Garantizar que sean de dominio de los equipos de la institución las habilidades para definir y utilizar las especificaciones requeridas para interoperabilidad, dando soporte de adiestramiento cuando necesario;
- Establecer punto de contacto en las instituciones, para intercambio de informaciones y de necesidades con la Coordinación de la e-PING;
- Destinar y suplir recursos para dar apoyo a sus procesos de adaptación a la e-PING;
- Aprovechar la oportunidad para racionalizar procesos (como el resultado del aumento de la interoperabilidad) de forma a mejorar la calidad y reducir costos de provisión de los servicios de e-gov.

5.5.2. Otras Instancias de Gobierno (otros Poderes Federales, Gobiernos Estatales y Municipales)

La adopción de la e-PING es obligatoria para los órganos y entidades del gobierno federal – Poder Ejecutivo. Para los otros Poderes (Judicial, Legislativo) y otras esferas de gobierno (estatal y municipal) la adopción es opcional.

La coordinación de la e-PING actúa de forma proactiva buscando la adopción de la e-PING por los entes integrantes de otras esferas y poderes, dada la importancia del intercambio de informaciones entre esferas y poderes para la eficiencia, eficacia y efectividad de la actuación gubernamental y para la construcción de servicios de gobierno electrónico orientados a la sociedad, especialmente al ciudadano.

Para facilitar la adopción de la e-PING por los gobiernos estatales, la ABEP participa de la coordinación de la e-PING, actuando junto con la coordinación en la construcción de una matriz de intereses federativos para el intercambio de informaciones.

5.5.3. Organizaciones del Sector Privado y del Tercer Sector

La e-PING prevé la interacción con el Sector Privado y con el Tercer Sector mediante los mecanismos de Consulta Pública, Solicitación de Comentarios y Recepción de Sugerencias.

Todas las entidades de esa proveniencia que participen de procesos licitatorios para provisión de productos y servicios para el Poder Ejecutivo Federal deberán cumplir con las especificaciones y recomendaciones de la e-PING.

Otras formas de participación de esas instituciones en la e-PING pueden considerarse, estableciéndose criterios que garanticen la transparencia y equidad de oportunidades.

5.5.4. Ciudadano

Gobierno electrónico significa, esencialmente, el gobierno sirviendo mejor a las necesidades del ciudadano utilizando los recursos de Tecnología, Información y Comunicación. La arquitectura e-PING permite la integración y coloca a disposición servicios de forma honesta, segura y coherente, posibilitando obtener mejores niveles de eficiencia en el gobierno.

El gobierno debe estimular la sociedad a opinar, comentar y contribuir con sugerencias de innovaciones que puedan ayudarlo a mejorar el acceso a la información y la prestación de sus servicios. Todos los procesos de divulgación y de interrelación de la e-PING prevén la participación activa del ciudadano y de la sociedad en general, en el proceso de construcción y gestión de la arquitectura.

Parte II – Especificación Técnica de los Componentes de la e-PING

6. Interconexión

6.1. Interconexión: Políticas Técnicas

Las políticas técnicas para interconexión son:

6.1.1. Los órganos de la APF deberán interconectarse usando IPv4 y planear su futura migración a IPv6. Nuevas contrataciones y actualizaciones de redes deben prever soporte a la coexistencia de los protocolos IPv4 e IPv6 y a productos que soporten ambos protocolos.

6.1.2. Los sistemas de correo electrónico deben utilizar SMTP/MIME para el envío de mensajes. Para acceso a los mensajes, deben utilizarse los protocolos POP3 y/o IMAP, siendo alentado el uso de interfaces *web* para correo electrónico, observados cuando necesario los aspectos de seguridad.

6.1.3. Los órganos de la APF deben obedecer la política de nomenclatura de dominios del gobierno federal, política que está establecida en la Resolución nº 7, accesible en la dirección electrónica

https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm.

6.1.4. El DNS debe utilizarse para resolución de nombres de dominios en Internet, convirtiéndolos en direcciones IP e, inversamente, convirtiendo IPs en nombres de dominios, por medio del mantenimiento de los mapas directo y reverso, respectivamente.

6.1.5. Los protocolos FTP y/o HTTP deben utilizarse para transferencia de archivos, observando sus funcionalidades para recuperación de interrupciones y seguridad, cuando sea necesario. El HTTP debe ser preferido para transferencias de archivos provenientes de páginas de Internet.

6.1.6. Siempre que posible[1], debe utilizarse tecnología basada en la *web* en aplicaciones que utilizaron Emulación de Terminal anteriormente.

6.1.7. La tecnología de *Web Services* es recomendada como solución de interoperabilidad de la e-PING. Se recomienda la utilización del protocolo *Simple Object Access Protocol* (SOAP) para interconexión en arquitecturas descentralizadas y/o distribuidas para implementación de servicios en sistemas de cualquier porte. De forma alternativa, para servicios web de pequeño porte, se considera posible el desarrollo de proyectos basados en REST, que utiliza el protocolo HTTP.

6.2. Interconexión: Especificaciones Técnicas

Cuadro 1 – Especificaciones para Interconexión – Mensajería[2]

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Direcciones de caja postal electrónica	Las reglas para definición de los nombres de las cajas postales de correo electrónico deberán seguir lo establecido en el documento “Cajas Postales Individuales-Funcionales en el gobierno federal”, disponible en la dirección electrónica http://www.e.gov.br/correios/cp_individ.htm	**A**	
Envío de mensaje	Utilizar productos de mensajería electrónica que	**R**	

[1] Existen productos que pueden proveer acceso por el *Browser* a los sistemas legados, sin necesidad de alterar esos sistemas; generalmente estos productos pueden proveer acceso directo a las pantallas de legado o ser reemplazados por interfaces gráficas (GUIs). Debe prestarse atención a cualquier implicación se seguridad en relación a su uso.

[2] Las RFCs pueden ingresarse en http://www.ietf.org/rfc.html

Componente	Especificación	SIT	Observaciones
electrónico	soporten interfaces acordes a SMTP/MIME para envío de mensajes. RFCs correlacionadas: RFC 2821; RFC 2822; RFC 2045; RFC 2046; RFC 3676; RFC 2047; RFC 2231 (actualización de las RFCs 2045, 2047 y 2183); RFC 2183; RFC 4288; RFC 4289; RFC 3023 y RFC 2049..		
Acceso a la caja postal	A menos que las exigencias de seguridad lo determinen de otro modo, programas de correo que proveen facilidades de acceso a correspondencia deberán, como mínimo, estar de acuerdo con POP3 para acceso remoto a la caja postal. RFCs correlacionada: RFC 1939 (actualizada por la RFC 1957 y RFC 2449).	**T**	
	Donde sean necesarias facilidades adicionales, a menos que requisitos de seguridad lo establezcan de forma contraria, los programas de correo que proveen facilidades avanzadas de acceso a la correspondencia, deberán estar en conformidad con el IMAP para acceso remoto a la caja postal. RFCs correlacionadas: RFC 2342; RFC 2910 (actualizada por la RFC 3510); RFC 2971; RFC 3501; RFC 3502 y RFC 3503.	**R**	
Mensajería en Tiempo Real	El modelo y requisitos para *Instant Messaging and Presence Protocol* (IMPP) son definidos por las RFC 2778 y 2779.	**T**	
	El modelo y requisitos para *Extensible Messaging and Presence Protocol* (XMPP) son definidos por las RFC 3920 y 3921.	**R**	
Servicio de Mensajes Cortos	El Servicio de Mensajes Cortos (SMS) deberá utilizar el protocolo SMPP, como definido por el SMS *Forum* httop://smsforum.net	**R**	

Cuadro 2 – Especificaciones para Interconexión – Infraestructura de Red

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Transporte	TCP (RFC 793)	**A**	
	UDP (RFC 768) cuando sea necesario, sujeto a las limitaciones de seguridad.	**A**	
Intercomunicación LAN/WAN	IPv4 (RFC 791)	**A**	
	IPv6 (RFC 2460)	**E**	
Tránsito avanzado	Cuando sea necesario, el tráfico de red puede ser mejorado mediante uso del MPLS (RFC 3031). este debe poseer, como mínimo, cuatro clases de servicio.	**A**	
Calidad de servicio	Adopción de una arquitectura para servicios diferenciados por el uso del Diffserv (RFC 2475).	**E**	

Componente	Especificación	SIT	Observaciones
Red metropolitana inalámbrica (wireless)	IEEE 802.16, conforme determinaciones del *WimaxForum* (http://www.wimaxforum.org) y normas de Anatel (http://www.anatel.gov.br).	**E**	
Red local inalámbrica (wireless)	IEEE 802.11 b/g, conforme determinaciones del *Wi-Fi Alliance* (http://www.wi-fi.org) y normas de Anatel (http://www.anatel.gov.br).	**R**	
Red de acceso por cableado eléctrico	*Power Line Communication* (PLC)*, según las normas de Anatel* (http://www.anatel.gov.br) y de Aneel (http://www.aneel.gov.br).	**F**	

Cuadro 3 – Especificaciones para Interconexión – Servicios de Red

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Protocolo de transferencia de hipertexto	Utilizar HTTP/1.1 (RFC 2616).	**A**	
Protocolos de transferencia de archivos	FTP (RFCs 959 y 2228) (con re inicialización y recuperación) y HTTP (RFC 2616) para transferencia de archivos.	**R**	
Directorio	LDAP v3 deberá utilizarse para acceso general al directorio, conforme RFC 4510.	**A**	
Sincronismo de tiempo	RFC 1305 IETF – *Network Time Protocol* – NTP versión 3.0. RFC 4330 IETF - *Simple Network Time Protocol* - SNTP versión 4.0.	**R**	
Servicios de Nomenclatura de Dominio	El DNS debe utilizarse para resolución de nombres de dominios de Internet, conforme RFC 1035. A su vez, las directivas de nomenclatura de dominio del gobierno brasileño son encontradas en la Resolución Nº 7 del Comité Ejecutivo del Gobierno Electrónico, en la dirección electrónica https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm Además de esas directivas, por decisión del Comité Gestor de Internet en Brasil, la nomenclatura de dominios obedece las orientaciones del Ministerio de Planificación, Presupuesto y Gestión, a quien corresponde administrar los dominios .GOV.BR. Las particularidades de otros niveles de gobierno, como por ejemplo, los dominios de los gobiernos de las Unidades de la Federación, que incluyen la sigla de la UF en la composición de las direcciones, son tratadas en la dirección electrónica http://registro.br/faq/faq1.html#12.	**A**	
Protocolos de señalización	Uso del Protocolo de Inicialización de Sesión (SIP), definido por la RFC 3261, como protocolo de control en la camada de aplicación (señalización) para crear,	**R**	

Componente	Especificación	SIT	Observaciones
	modificar y terminar sesiones con uno o más participantes.		
Protocolos de administración de red	Uso del protocolo SNMP, definido por las RFCs 3411 y 3418, como protocolo de administración de red.	**T**	Versión 2
		R	Versión 3
Protocolo de intercambio de informaciones estructuradas en plataforma descentralizada y/o distribuida	SOAP v1.2, como definido por el W3C http://www.w3.org/TR/soap12-part1/ http://www.w3.org/TR/soap12-part2/ Especificaciones del protocolo SOAP pueden ser encontradas en http://www.w3.org/TR/soap12-part0/	**A**	
Protocolo de análisis de tráfico de red	IPFix	**F**	

6.3. Mensaje Electrónico (Correo Electrónico)

Para efectos de clarificación, la e-PING utilizará los siguientes conceptos:

Envío de mensaje electrónico

El envío de mensaje electrónico es definido como la interface entre dos sistemas de correo.

Acceso a la caja postal

Acceso a la caja postal es definido como la interface entre un cliente de correo y un sistema de correo.

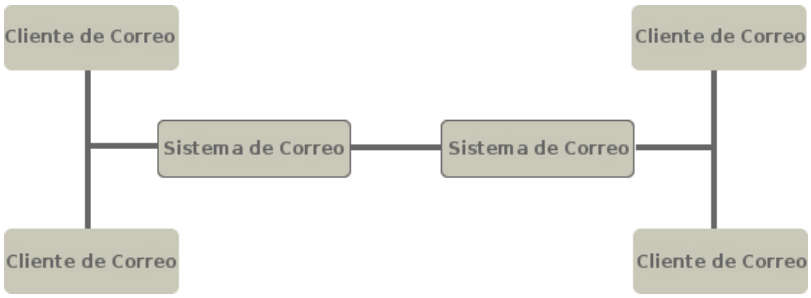

Figura 3 – Interfaces entre sistemas y clientes de Correo.

6.4. VPN

Virtual Private Network (VPN), o Red Privada Virtual, es un túnel virtual privativo construido sobre la infraestructura de una red pública o privada. En vez de usar circuitos dedicados o redes de paquetes para conectar redes remotas, se utiliza generalmente la infraestructura de Internet.

Tal utilización, como infraestructura de conexión entre *hosts* de la red privada, es una buena solución en términos de costos, pero no en términos de privacidad, pues los datos en tránsito pueden ser leídos por cualquier equipo, siendo necesario el uso de VPN.

Los túneles virtuales transportan datos criptografados sobre redes públicas o privadas, formando un canal virtual seguro mediante esas redes. Para eso, son utilizados protocolos de túnel.

Los dispositivos responsables por la administración de la VPN deben ser capaces de asegurar privacidad, integridad y autenticidad de los datos.

Las especificaciones sobre VPN están presentes en el segmento de seguridad.

6.5. Redes peer-to-peer

Los Sistemas *Peer-to-Peer* (P2P) son sistemas distribuidos que consisten en nodos interconectados, con capacidad de auto organizarse en topologías de red, con el fin de compartir recursos como procesamiento, almacenaje y ancho de banda, capaces de adaptarse a fallas y acomodar poblaciones pasajeras de nodos, mientras mantiene conectividad y desempeño aceptables, sin depender de la intercesión o soporte de una autoridad (servidor) central.

Aunque los sistemas P2P puedan contribuir para compartición de recursos y colaboración en larga escala, con control descentralizado y bajo acople, aún son sensibles a varios problemas de seguridad, impidiendo el uso sistemático de redes P2P. Este asunto será tratado futuramente.

7. Seguridad

7.1. Seguridad: Políticas Técnicas

7.1.1. Los datos, informaciones y sistemas de información del gobierno deben ser protegidos contra amenazas de manera a reducir riesgos y garantizar la integridad, confidencialidad, disponibilidad y autenticidad.

7.1.2. Los datos e informaciones deben mantenerse con el mismo nivel de protección, independiente del medio en que estén siendo procesados, almacenados o transitando.

7.1.3. Las informaciones sensibles que transitan en redes no seguras, incluyendo las inalámbricas, deben ser criptografadas, de manera adecuada, de acuerdo con los componentes de seguridad especificados en este documento.

7.1.4. Los requisitos de seguridad de la información, de los servicios y de infraestructura deben ser identificados y tratados conforme la clasificación de la información, niveles de servicio definidos y resultado del análisis de riesgos.

7.1.5. La seguridad debe ser tratada de manera preventiva. Para los sistemas que apoyan procesos críticos, deben elaborarse planes de continuidad, donde serán tratados los riesgos residuales, buscando atender los niveles mínimos de producción.

7.1.6. La seguridad es un proceso que debe estar incluido en todas las etapas del ciclo de desarrollo de un sistema.

7.1.7. Los sistemas deben tener registros históricos (*logs*) para permitir auditorías y pruebas materiales, siendo imprescindible la adopción de un sistema de sincronismo de tiempo centralizado, bien como la utilización de mecanismos que garanticen la autenticidad de los registros almacenados, siempre que posible con firma digital.

7.1.8. Los servicios de seguridad de XML deben estar acordes a las especificaciones del W3C.

7.1.9. En las redes inalámbricas metropolitanas se recomienda la adopción de valores aleatorios en las asociaciones de seguridad, diferentes identificadores de cada servicio y la limitación del tiempo de vida de las llaves autorizadoras.

7.1.10. El uso de criptografía y certificación digital, para la protección del tráfico, almacenaje de datos, control de acceso, firma digital y firma de código, debe estar acorde a las reglas de ICP-Brasil.

7.1.11. La documentación de los sistemas, de los controles de seguridad y de las topologías de los ambientes debe ser mantenida actualizada y protegida, manteniéndose un grado de sigilo compatible.

7.1.12. Los usuarios deben conocer sus responsabilidades en relación a la seguridad y deben ser capaces de realizar sus tareas y utilizar correctamente los medios de acceso.

7.1.13. Los órganos de la APF, buscando la mejoría de la seguridad, deben tener como referencia las normas NBR ISO/IEC 27002:2005 – código de práctica para la gestión de la seguridad de la información; NBR ISO/IEC 27001:2006 – sistemas de gestión de seguridad de la información; NBR 15999-1:2007 y 15999-2:2008 – gestión de continuidad de negocios; NBR ISO/IEC 27005:2008 - gestión de riegos de seguridad de la información; Instrucción Normativa nº 01/2000, Norma Complementaria nº 02/2009, 04/2009 y 05/2009.

7.1.14. Para especificaciones sobre tarjetas inteligentes y *tokens* deberán ser adoptados los requisitos contenidos en los normativos que tratan de la homologación de equipos y sistemas en el ámbito de la Infraestructura Brasileña de Llaves Públicas – ICP-Brasil (http://www.icpbrasil.gov.br/). Estos requisitos, observados por productos homologados en ICP-Brasil, tal como medias que almacenan los certificados digitales y correspondientes lectoras, además de los sistemas y equipos necesarios para la realización de la certificación digital, determinan estándares y especificaciones técnicas mínimas, con el fin de asegurar su interoperabilidad y la confiabilidad de los recursos de seguridad de la información utilizados por ellos. Es importante observar que los datos almacenados en una determinada tarjeta inteligente o *token* no podrán estar protegidos por cualquier tipo de licencia que prohíba su lectura por cualquier otro software que no sea el del proveedor de aquella tarjeta inteligente o *token*.

7.2. Seguridad: Especificaciones Técnicas

Cuadro 4 – Especificaciones para Seguridad – Comunicación de datos

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Transferencia de datos en redes no seguras por los protocolos HTTP, LDAP, IMAP, POP3, Telnet.	TLS – *Transport Layer Security*, RFC 2246 (http://www.ietf.org/rfc/rfc2246.txt) Caso sea necesario el protocolo TLS v1 puede emular el SSL v3. HTTP sobre TLS, RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt) Pudiendo implementar los siguientes algoritmos criptográficos: - Algoritmos para cambio de llaves de sesión, durante el *handshake*: RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA; - Algoritmos para definición de la llave de cifrado: RC4,, IDEA, 3DES y AES; - Algoritmos que implementan la función de *hash* para definición del MAC: SHA-256 o SHA-512. - Tipo de Certificado Digital – X 509 v3 – ICP-Brasil, http://www.iti.gov.br SASL – *Simple Authentication and Security Layer*, RFC 4422 (http://www.ietf.org/rfc/rfc4422.txt)	**R**	
Seguridad de redes IPv4	*IPSec Authentication Header* RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt) y RFC 4835 (http://www.ietf.org/rfc/rfc4303.txt) para autenticación de cabecera de IP. IKE – *Internet Key Exchange*, RFC 4306 (http://www.ietf.org/rfc/rfc4306.txt), debe utilizarse siempre que sea necesario para negociación de asociación de seguridad entre dos entidades para intercambio de material de llaveado. ESP – *Encapsulating Security Payload*, RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt) Requisito para VPN – Virtual Private Network.	**A**	
Seguridad de redes IPv4 para protocolos de aplicación	El S/MIME v3 RFC 2633 (http://www.ietf.org/rfc/rfc2633.txt) deberá utilizarse cuando sea adecuado para seguridad de mensajes generales de gobierno.	**A**	

Componente	Especificación	SIT	Observaciones
Seguridad de redes IPv6 en la camada de red	El IPv6 definido en la RFC 2460 (http://www.ietf.org/rfc/rfc2460.txt) presenta implementaciones de seguridad nativas en el protocolo. Las especificaciones del IPv6 definieron dos mecanismos de seguridad: La autenticación de la cabecera AH (*Authentication Header*) RFC 4302 (http://www.ietf.org/rfc/rfc4302.txt) o autenticación IP, y la seguridad del encapsulado IP, ESP (*Encrypted Security Payload*) RFC 4303 (http://www.ietf.org/fc/rfc4303.txt).	**R**	

Cuadro 5 – Especificaciones para Seguridad – Correo Electrónico

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Acceso a cajas postales	El acceso a la caja postal deberá suceder mediante el cliente del software de correo electrónico utilizado, considerando las facilidades de seguridad originarias del cliente. Cuando no sea posible utilizar el cliente específico o sea necesario entrar a la caja postal por medio de redes no seguras (por ejemplo: Internet) debe utilizarse HTTPS conforme los estándares de seguridad de transporte descritos en la RFC 2595 (http://www.ietf.org/rfc/rfc2595.txt), que aborda el uso del TLS con IMAP, POP3 y ACAP.	**A**	
Contenido de mensaje	El S/MIME V3 deberá utilizarse cuando sea adecuado para seguridad de mensajes generales de gobierno. Eso incluye la RFC 3369 (http://www.ietf.org/rfc/rfc3369.txt), RFC 3370 (http://www.ietf.org/rfc/rfc3370.txt), RFC 2631 (http://www.ietf.org/rfc/rfc2631.txt), RFC 3850 (http://www.ietf.org/rfc/rfc3850.txt), RFC 3851 (http://www.ietf.org/rfc/rfc3851.txt) y RFC 3852 (http://www.ietf.org/rfc/rfc3852.txt).	**A**	
Envío de mensaje	Utilizar SPF (*Sender Policy Framework*) acorde a los términos de la RFC 4408 (http://www.ietf.org/rfc/rfc4408.txt).	**R**	
Firma	Utilizar certificado estándar ICP-Brasil para firma de mensaje, cuando sea exigido. Conforme lo dispuesto en la Medida Provisoria nº 2.200-2, de 24/08/2001, y Decreto nº 3.996 de 31/10/2001.	**A**	Ver Resolución nº 65, de 09/06/2009, del Comité Gestor de la Infraestructura Brasileña de Llaves Públicas - ICP-Brasil.

Cuadro 6 – Especificaciones para Seguridad – Criptografía

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F – Estudio Futuro		
Algoritmo de cifrado	3DES o AES	**R**	
Algoritmo para firma/hashing	SHA-256 o SHA-512	**R**	Los sistemas deben tener soporte para el algoritmo de *hash* MD5 con RSA, para asegurar compatibilidad con implementaciones anteriores.
Algoritmos para firma/hashing	SHA-224 o SHA-238	**E**	Considerando que fueron incluidas en el Informe Final del Grupo de Trabajo de Criptografía I, instituido por el Gabinete de Seguridad Institucional de la Presidencia de la República, pero aún no se transformaron en norma en la Administración Pública Federal.
Algoritmo para transporte de llave criptográfica de contenido/sesión	RSA	**A**	
Algoritmos criptográficos basados en curvas elípticas	ECDSA 256 y ECDSA 512 (rfc 5480 – http://www.ietf.org/rfc/rfc5480.txt). ECIES 256 y ECIES 512 (Resolución nº 65, de 09/06/2009, del Comité Gestor de la Infraestructura Brasileña de Llaves Públicas – ICP-Brasil). ECMQV y ECDH, ambos para acuerdo de llaves, de acuerdo con la RFC 3278. (http://www.ietf.org/rfc/rfc3278.txt).	**A** **E**	ECDSA, para firmas digitales, y ECIES para cifrado y envío seguro de llaves criptográficas. Consultar errata para la RFC 5480 en http://rfc-editor.org/errata_search.php?rfc=5480.

Componente	Especificación	SIT	Observaciones
Requisitos de seguridad para módulos criptográficos	Homologación de ICP-Brasil NSH-2 y NSH-3; FIPS 140-1 y FIPS 140-2.	**R**	Ver Resolución nº 65, de 09/06/2009, del Comité Gestor de la Infraestructura Brasileña de Llaves Públicas (ICP-Brasil).

Cuadro 7 – Especificaciones para Seguridad – Desarrollo de Sistemas

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F – Estudio Futuro		
Firmas XML	Sintaxis y Procesamiento de firma XML (XMLsig) acorde a lo definido por el W3C http://www.w3.org/TR/xmldsig-core/	**A**	
Cifrado XML	Sintaxis y Procesamiento de Cifrado XML (XMLenc) conforme definido por el W3C http://www.w3.org/TR/xmlenc-core/	**R**	
Forma y cifrado XML	Transformación de descifrado para firma XML acorde a lo definido por el W3C http://www.w3.org/TR/xmlenc-decrypt	**R**	
Principales administraciones XML cuando un ambiente PKI es utilizado	XML – *Key Management Specification* (XKMS 2.0) (Especificaciones de Administración de Llave XML) acorde a lo definido por el W3C http://www.w3.org/TR/xkms2/	**R**	
Autenticación y autorización de acceso XML	SAML – acorde a lo definido por OASIS cuando un ambiente ICP es utilizado http://www.oasis-open.org/committees/security/index.shtml	**R**	
Intermediación o Federación de Identidades	WS-Security 11.1 – andamiaje de estándares para asegurar integridad y confidencialidad en mensajes SOAP. (http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf). WS-Trust 1.3 – extensiones para el estándar WS-Security, definiendo el uso de credenciales de seguridad y gerencia de confianza distribuida. (http://docs.oasis-open.org/ws-sx/ws-trust/200512).	**R**	El componente anterior (SAML) podrá juntarse a este componente después de exámenes.
Navegadores	Sólo utilizar testigos de conexión de carácter permanente (*cookies*) con la concordancia del usuario. Resolución nº 7 del Comité Ejecutivo del Gobierno Electrónico (Capítulo II, Art.7º).	**A**	

Cuadro 8 – Especificaciones para Seguridad – Servicios de Red

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F – Estudio Futuro		
Directorio	Portería Normativa Nº 2, de 3 de octubre de 2002 – Publicada en el D.O. del día 4 de octubre de 2002. Sección 1, página 85. LDAPv3 RFC 2251 (http://www.ietf.org/rfc/rfc2251.txt). LDAP v3 extensión para TLS RFC2830 (http://www.ietf.org/rfc/rfc2830.txt).	**R**	
DNSSEC	Resolución nº 7 de 29/07/2002 – Comité Ejecutivo del Gobierno Electrónico *Práticas de Segurança para Administradores de Redes Internet* (Prácticas de Seguridad para Administradores de Redes Internet) *Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil* (Centro de Estudios, Respuestas y Tratamiento de Incidentes de Seguridad en Brasil – CERT.BR) http://www.cert.br/docs/seg-adm-redes/seg-adm-chklist.pdf Versión .2, 16 de mayo de 2003.	**R**	
Transferencia de archivos en forma segura	HTTPS RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt).	**R**	
Transferencia de archivos en forma segura	SSH FTP	**E**	Los documentos aún están en formato de borrador.
Transferencia de archivos en forma segura	Proteger o FTP con TLS, RFC 4217 http://www.faqs.org/rfcs/rfc4217.html y RFC 2246 http://faqs.org/rfcs/rfc2246.html.	**E**	
Mensaje instantáneo	RFC 2778 (http://www.ietf.org/rfc/rfc2778.txt), RFC 3261 (http://www.ietf.org/rfc/rfc3261.txt), RFC 3262 (http://www.ietf.org/rfc/rfc3262.txt), RFC 3263 (http://www.ietf.org/rfc/rfc3263.txt), RFC 3264 (http://www.ietf.org/rfc/rfc3264.txt) y RFC 3265 (http://www.ietf.org/rfc/rfc3265.txt).	**E**	
Sincronismo de tiempo	RFC 2030 IETF - *Simple Network Time Protocol* – SNTP versión 4.0 (http://www.ietf.org/rfc/rfc2030.txt).	**E**	
Sello de tiempo	RFC 3628 TSAs – *Policy Requirements for Time-Stamping Authorities* (http://www.ietf.org/rfc/rfc3628.txt). *Time-Stamp Protocol*, RFC 3161 ETSI TS101861 (*Time-Stamping Profile*) (http://www.ietf.org/rfc/rfc3161.txt).	**R**	El servicio de sello de tiempo deberá estar conforme a la Resolución nº 58, de 28/11/2008, y demás normas de ICP-Brasil.

Cuadro 9 – Especificaciones para Seguridad – Redes Inalámbricas (Wireless)

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F – Estudio Futuro		
MAN[3] inalámbrico 802.16-2004[4] 802.16.2-2004[5] 802.16e[6] y 802.16f[7]	Usar PKM-EAP (*Privacy Key Management - Extensible Autentication Protocol*) con: • EAP – TLS o TTLS; • AES[8] (Advanced Encryption Standard).	**E**	
LAN inalámbrico 802.11	Utilizar la especificación WPA2 (Wi-Fi *Protect Access*).	**R**	

Cuadro 10 – Especificaciones para Seguridad – Respuesta a Incidentes de Seguridad de la Información

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Preservación de registros	*Guidelines for Evidence Collection and Archiving,* RFC 3227 (http://www.ietf.org/rfc/rfc3227.txt).	**R**	
Tratamiento y respuesta a incidentes en redes de ordenadores	*Expectations for Computer Security Incident Response,* RFC 2350 (http://www.ietf.org/rfc/rfc2350.txt). Creación de equipos de tratamiento y respuesta a incidentes en redes de ordenadores de acuerdo con la Norma Complementaria nº 05/09 (http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf)	**R**	
Informática Forense	*Guide to Integrating Forensic Techniques into Incident Response* – NIST – *Special Publication* 800-86 – (http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf).	**A**	

[3] El 802.16 es definido por el IEEE como una interface tecnológica para redes de acceso inalámbricas metropolitanas o WMAN (*Wireless Metropolitan Access Network*).
[4] http://standards.ieee.org/getieee802/download/802.16-2004.pdf.
[5] http://standards.ieee.org/getieee802/download/802.16.2-2004.pdf.
[6] http://standards.ieee.org/getieee802/download/802.16e-2005.pdf.
[7] http://standards.ieee.org/getieee802/download/802.16f-2005.pdf.
[8] http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf.

8. Medios de Acceso

8.1. Medios de Acceso: Políticas Técnicas

Las políticas técnicas para posibilitar el acceso a los servicios electrónicos del gobierno federal para la sociedad en general – ciudadanos, otras esferas gubernamentales, otros Poderes, servidores públicos, empresas privadas y otras instituciones – son:

8.1.1. Los sistemas de información del gobierno deben ser proyectados de forma a respetar la legislación brasileña, dando recursos de accesibilidad a los ciudadanos con necesidades especiales, a grupos étnicos minoritarios y aquellos con riesgo de exclusión social o digital. La atención vía mostrador de prestación de servicios debe ser considerada en toda su abarcadura, de manera a permitir que los beneficios resultantes del uso de los servicios de gobierno electrónico sean extendidos a la camada de la población que no puede tener acceso directo a esos servicios mediante los dispositivos previstos.

8.1.2. Sistemas de información del gobierno que proveen servicios de gobierno electrónico:

- Cuando utilicen Internet como medio de comunicación y estaciones de trabajo como dispositivo de acceso, serán preferentemente diseñados para dar acceso a sus informaciones con utilización de tecnologías y protocolos de comunicación de la *web* basados en navegadores (*browsers*);
- Cuando utilicen otros dispositivos de acceso, por ejemplo, celulares y televisión digital, podrán usar otras interfaces además de los navegadores *web*;
- Deberán ser diseñados para colocar a disposición de los usuarios servicios de gobierno electrónico por medio de varias formas de acceso;
- En esta versión, la e-PING trata de los siguientes medios de acceso:
  - Estaciones de Trabajo;
  - Movilidad;
  - TV Digital.

8.1.3. Los sistemas de información del gobierno, construidos para soportar un determinado dispositivo de acceso deben seguir, de forma obligatoria, las especificaciones publicadas en la e-PING para dicho dispositivo.

8.1.4. Todos los sistemas de información del gobierno que provean servicios electrónicos deben ser capaces de utilizar Internet como medio de comunicación, sea de forma directa o por medio de servicios de terceros.

8.1.5. El desarrollo de los servicios de gobierno electrónico debe ser orientado de forma a proveer atención a los usuarios que no tengan acceso a las tecnologías más recientes disponibles en el mercado. Por otro lado, también se debe considerar la necesidad de atención a aquellos usuarios con necesidades especiales, requisito que involucra el uso de recursos más sofisticados y de uso específico. De forma a conciliar esas necesidades, deberán observarse las recomendaciones del Modelo de Accesibilidad de Gobierno Electrónico (e-MAG)[9].

8.1.6. Cuando Internet sea utilizada como medio de comunicación, los sistemas de información del gobierno deben ser diseñados de forma que el máximo de informaciones pueda ser trabajado a partir de navegadores que cumplan con el estándar mínimo expresado por el soporte a las especificaciones técnicas pertinentes previstas en la sección 8.2. De forma complementaria, la e-PING recomienda que todo servicio de gobierno electrónico especifique, claramente y de preferencia en su página inicial, las versiones mínimas de navegadores que soportan las funcionalidades requeridas por el servicio asociado.

En el cumplimiento del estándar mínimo arriba mencionado, deben considerarse las excepciones que involucren cuestiones de seguridad en el tratamiento de informaciones.

8.1.7. Cuando Internet sea utilizada como medio de comunicación, *middleware* o *plug-ins* adicionales podrán ser utilizados, si no hay alternativa técnicamente viable, para mejorar la

[9] BRASIL. Ministerio de Planificación, Presupuesto y Gestión. Recomendaciones de Accesibilidad para la construcción y adaptación de contenidos del Gobierno Brasileño en Internet: modelo de accesibilidad. Versión 2.0. Brasília, 2005. Disponible en: (http://www.governoeletronico.gov.br/emag/). Accedido en: 13/07/2006.

funcionalidad del navegador en las estaciones de trabajo. En este caso, ese software adicional deberá ser ofrecido sin el pago de impuesto de licencia y deberá estar acorde a todas las especificaciones técnicas correspondientes discriminadas en la e-PING. Además, deberá ser colocado a disposición en repositorio seguro mantenido por el órgano gubernamental responsable por la aplicación.

8.1.8. Los servicios de gobierno electrónico deben ser diseñados de forma a asegurar a os usuarios la autenticidad del contenido mediante emisión de certificado digital, de acuerdo con los estándares difundidos por ICP-Brasil. Referencia: http://www.icpbrasil.gov.br/. En ese sentido, todas las páginas *web* deberán, obligatoriamente, utilizar “https” en vez de “http”.

8.1.9. La necesidad de la sociedad aliada a la posibilidad del gobierno de desarrollar e implantar servicios electrónicos respaldará la definición de las especificaciones técnicas exigidas por los medios de acceso disponibles. Podrán ser utilizadas técnicas de administración de contenido y tecnologías que posibiliten adecuación de los dispositivos para soportar los servicios de gobierno electrónico para simplificar el acceso por medio del estándar mínimo de navegador *web* (de acuerdo con el ítem 3, Políticas Generales) y para volver variable el uso de quioscos públicos, de mostradores y de Centrales de Atención al ciudadano (como, por ejemplo, Telecentros).

8.1.10. Los sistemas de información del gobierno federal deben prever, cuando sea necesario y técnica/económicamente viable, la construcción de adaptadores que permitan el acceso a las informaciones de los servicios electrónicos en *web* para una variedad de ambientes, presentando tiempos de respuesta aceptables y costos reducidos.

Esos adaptadores pueden ser utilizados para filtrar, convertir y reformatear, de forma dinámica, el contenido *web*, de modo a adaptarse a las exigencias y a las capacidades de exhibición del dispositivo de acceso. Pueden, todavía, permitir la modificación del contenido de una página *web*, basándose en protocolos de datos, XML, XSL, preferencias del usuario y parametrización de red y de dispositivos de acceso.

Esos adaptadores también podrán ser usados como método alternativo de permitir el acceso a minorías étnicas, personas con deficiencia visual (por ejemplo: por el uso de traductores de textos, fuentes y gráficos mayores, sonido, etc.). Tales aspectos son tratados por la Resolución nº 7 del Comité Ejecutivo de Gobierno Electrónico. Referencia:

https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm

8.1.11. serán considerados preferenciales aquellos tipos de archivo que tienen como estándar de empaquetado el “xml”, de manera a facilitar la interoperabilidad entre los servicios de gobierno electrónico.

8.1.12. Los servicios de gobierno electrónico que coloquen documentos a disposición de sus usuarios deberán hacerlo empleando en el propio enlace de acceso al documento información clara cuanto a su proveniencia, versión, fecha y formato. Por fecha de publicación se entiende aquella en que el documento fue publicado en diario oficial, para los casos en que esta medida sea exigida, o la fecha de disponibilidad en la página, para los demás casos. Otras informaciones sobre el documento, como autor, redactor, emisor, fecha tópica u otros datos relevantes a su precisa caracterización, deberán constar en el campo propiedades del propio documento.

8.2. Medios de Acceso: Especificaciones Técnicas para Estaciones de Trabajo

Para elaboración de minutas de documentos o trabajos que deban ser creados colaborativamente por más de una personas y/u órgano, pueden ser utilizados los formatos previstos en el Cuadro 11.

Ya para la elaboración de la versión final de documentos, que deba ser enviada a otros órganos o archivada en forma digital, se recomienda la utilización del formato pdf/a. Documentos que necesiten garantía de integridad y/o autoría, además de estar en formato pdf/a, deben ser formados digitalmente por su autor, utilizando certificado ICP-Brasil.

La mención a los productos que generan los formatos de los archivos citados en el Cuadro 11 tiene como único fin la identificación de una **referencia mínima** a partir de la cual los servicios de e-gov deben intercambiar informaciones, siendo capaces de recibir o enviar archivos en **versiones iguales o posteriores** a las mencionadas.

Cuadro 11 – Especificaciones para Medios de Acceso – Estaciones de Trabajo

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Navegadores (*browsers*)	Deben estar adheridos a los estándares W3C y a los ítems Adopción de Navegadores y Adopción Preferencial de Estándares Abiertos en Políticas Generales.	**R**	
Conjunto de letras y alfabetos	UNICODE *standard* versión 4.0, latin-1, UTF8, ISBN 0-321-18578-1.	**R**	
Formato de intercambio de hipertexto	HTML versión 4.01 (.html o .htm), creado conforme especificaciones del W3C[10].	**A**	
	XHTML versiones 1.0 o 1.1 (.xhtml), creado conforme especificaciones del W3C[11].	**R**	
	XML versiones 1.0 o 1.1 (.xml), creado conforme especificaciones del W3C[12].	**A**	
	SHTML (.shtml).	**R**	
	MHTML (.mhtl o .mht)[13].	**T**	
Archivos del tipo documento	XML versiones 1.0 o 1.1 (.xml) o con formateo (opcional) XSL (.xsl), creado conforme especificaciones del W3C[14].	**R**	
	Open Document (.odt), creado conforme especificaciones del estándar ISO/IEC 26300[15].	**A**	
	Rich Text Format (.rtf).	**T**	
	PDF (.pdf).	**T**	
	PDF versión abierta PDF/A[16].	**R**	
	Texto puro (.txt).	**A**	
	HTML versión 4.01 (.html o .htm), creado conforme especificaciones del W3C.	**R**	
Archivos del tipo	Open Document (.ods), creado conforme	**A**	

[10] *HTML 4.01 Specification - W3C Recommendation 24 December 1999*. Disponible en: http://www.w3.org/TR/html4/.
[11] *XHTML 1.0 The Extensible HyperText Markup Language (Second Edition): A Reformulation of HTML 4 in XML 1.0 - W3C Recommendation 26 January 2000, revised 1 August 2002*. Disponible en: http://www.w3.org/TR/xhtml1/.
[12] *Extensible Markup Language (XML) 1.0 (Third Edition) - W3C Recommendation 04 February 2004*. Disponible en: http://www.w3.org/TR/2004/REC-xml-20040204/.
Extensible Markup Language (XML) 1.1 - W3C Recommendation 04 February 2004, edited in place 15 April 2004. Disponible en: http://www.w3.org/TR/2004/REC-xml11-20040204/.
[13] Formato de empaquetado de archivos *web* de Microsoft (*Mime Enscapsulation of Aggregate HTML Documents*).
[14] *Extensible Stylesheet Language (XSL) Version 1.0 - W3C Recommendation 15 October 2001*. Disponible en: http://www.w3.org/TR/xsl/.
[15] *Open Document Format for Office Applications (OpenDocument)* v1.0 – estándar ISO/IEC 26300. Disponible en: http://www.iso.org/.
[16] *Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A -1)* – estándar ISO 19005-1:2005. Disponible en: http://www.iso.org/.

Componente	Especificación	SIT	Observaciones
planilla	especificaciones del estándar ABNT NBR ISO/IEC 26300.		
Archivos del tipo presentación	Open Document (.odp), creado conforme especificaciones del estándar ABNT NBR ISO/IEC 26300.	**A**	
	HTML (.html o .htm), creado conforme especificaciones del W3C.	**R**	
Archivos del tipo “banco de datos” para estaciones de trabajo	XML versiones 1.0 o 1.1 (.xml)	**R**	En las opciones texto plano (txt) y csv, debe incluirse obligatoriamente el layout de los campos, de forma de los campos, de manera a posibilitar su tratamiento.
	MySQL Database (.myd, .myi), creados en los formatos del MySQL, versión 4.0 o superior.	**R**	
	Texto puro (.txt)	**A**	
	Texto Puro (.csv) - comma-separated values	**A**	
	Archivo de la Base (.odb), creado conforme especificaciones del estándar ISO/IEC 26300.	**R**	
Intercambio de informaciones gráficas e imágenes estáticas	PNG (.png), creado de acuerdo con especificaciones del W3C[17] – ISO/IEC 15948:2003 (E).	**A**	
	TIFF (.tif)[18].	**R**	
	SVG (.svg), creado acorde a especificaciones del W3C[19].	**R**	
	JPEG File Interchange Format (.jpeg, .jpg o .jfif) [20].	**R**	
	Open Document (.odg), creado conforme especificaciones del estándar ABNT NBR ISO/IEC 26300.	**A**	
	BMP (.bmp).	**T**	
	GIF (.gif), creado conforme las especificaciones GIF87a y GIF89a[21].	**T**	
Gráficos vectoriales	SVG (.svg), creado acorde a especificaciones del W3C.	**R**	
	Open Document (.odg), creado conforme especificaciones del estándar ABNT NBR ISO/IEC 26300.	**R**	
Especificación de estándares de animación	SVG (.svg), creado acorde a especificaciones del W3C.	**R**	
	GIF (.gif), creado conforme la especificación GIF89a.	**T**	
Archivos del tipo	.mpg	**R**	

[17] *Portable Network Graphics (PNG) Specification (Second Edition). W3C Recommendation 10 November 2003.*
ISO/IEC 15948:2003 (E) - Information technology - Computer graphics and image processing - Portable Network Graphics (PNG): Functional specification. Disponible en: http://www.w3.org/TR/2003/REC-PNG-20031110/. Accedido en: 7 dic 2005.
[18] *Tagged Image File Format (Adobe Systems).*
[19] *Scalable Vector Graphics (SVG) 1.1 Specification. W3C Recommendation 14 January 2003. Disponible en: http://www.w3.org/TR/2003/REC-SVG11-20030114/*. Accedido en: 7 dic. 2005.
[20] *JPEG File Interchange Format (version 1.02) 1 September 1992. Disponible en: http://www.jpeg.org/public/jfif.pdf*. Accedido en: 7 dic. 2005.
[21] *Graphics Interchange Format (CompuServe/America Online, Inc.).*

Componente	Especificación	SIT	Observaciones
audio y del tipo video	Audio y video MPEG-4, Part 14 (.mp4)[22]	**R**	
	MIDI (.mid)[23]	**R**	
	Áudio Ogg Vorbis I (.ogg)[24]	**R**	
	Audio-Video Interleaved (.avi), con codificación Xvid.	**R**	
	Audio-Video Interleaved (.avi), con codificación divX..	**T**	
	Audio MPEG-1, Audio Layer 3 (.mp3)[25]	**T**	
	WAVE (.wav)	**T**	
Compactación de archivos de uso general	ZIP (.zip).	**R**	
	GNU ZIP (.gz).	**R**	
	Paquete TAR (.tar).	**R**	
	Paquete TAR compactado (.tgz o .tar.gz).	**R**	
	BZIP2 (.bz2).	**R**	
	Paquete TAR compactado con BZIP2 (.tar.bz2).	**R**	
	MS Cabinet (.cab).	**T**	
Informaciones referenciadas geográficamente – estándares de archivos para intercambio entre estaciones de trabajo	GML versión 2.0 o superior[26].	**A**	Indicado para estructuras vectoriales complejas, involucrando primitivas geográficas como polígonos, puntos, líneas, superficies, colecciones, y atributos numéricos o textuales sin límite de caracteres.
	ShapeFile[27].	**A**	Indicado para estructuras vectoriales limitadas a líneas, puntos y polígonos, cuyos atributos textuales no sobrepasen los 256 caracteres. También puede almacenar las dimensiones M y Z.
	GeoTIFF[28].	**A**	Indicado para estructuras matriciales limitadas a matrices de pixeles.
	SFS.	**E**	SFS (*Simple Features Interface Standard*) es un estándar OGC

[22] *ISO/IEC 14496-14:2003 - Information Technology - Coding of audio-visual objects - Part 14: MP4 file format.*

[23] Musical Instrument Digital Interface, conforme la especificación *The Complete MIDI 1.0 Detailed Specification*. Version 96.1, 2.ed., nov. 2001. Disponible en: http://www.midi.org/about-midi/specinfo.shtml. Accedido en: 30 mai. 2007.

[24] Xiph.Org Foundation. Especificación disponible en: http://xiph.org/vorbis/doc/Vorbis_I_spec.html.

[25] *ISO/IEC 11172-3:1993 - Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1,5Mbit/s - Part 3: Audio.*
ISO/IEC 11172-3:1993/Cor 1:1996.

[26] *Geography Markup Language*. Especificaciones disponibles en: http://www.opengeospatial.org/standards/gml.

[27] *ESRI Shapefile Technical Description*. Disponible en: http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf.

[28] *GeoTIFF Format Especification*. Disponible en: http://remotesensing.org/geotiff/geotiff.html.

Componente	Especificación	SIT	Observaciones
			(http://www.opengeospatial.org/standards/sfa) que define la forma en que las aplicaciones almacenarán (crear, actualizar y excluir) y entrarán en sistemas administradores de banco de datos objetos relacionales. OpenGIS *Simple Features* (facciones simples) sin facciones espaciales descritas utilizando elementos como puntos, líneas y polígonos.
Programación Extendida (Plug-ins)	Tema para consideración futura.	**F**	

8.3. Medios de Acceso: Especificaciones Técnicas para Movilidad

El número de dispositivos de telefonía móvil ya sobrepasó la cantidad de telefonía fija, volviéndose así un amplio canal de comunicación con el ciudadano. Además, la oferta de ordenadores personales con recursos de movilidad a precios más accesibles para el ciudadano crece a cada día, estimulada por incentivos gubernamentales y reducción del gasto de producción. De esa forma, se vuelve un gran desafío para el gobierno permitir el acceso de la sociedad a los productos y servicios del gobierno electrónico, a partir de dispositivos móviles, en general portátiles, como *laptops*, celulares, *smartphones* y similares, anhelando el aumento de la inclusión digital mediante la movilidad.

Un concepto que está consolidándose para la interface de aplicaciones para los usuarios es el de “web universal”, que sea para todos, en cualquier lugar, a cualquier momento, independiente del dispositivo de acceso. Este concepto debe aplicarse a los servicios a ser colocados a disposición mediante los dispositivos móviles.

Cuadro 12 – Especificaciones para Medios de Acceso – Movilidad

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Protocolo de Transmisión	Debe ser adherente a los estándares W3C – *Mobile Best Practices* 1.0, disponibles en la dirección electrónica: http://www.w3.org/TR/mobile-bp	**R**	
Navegador	Debe ser adherente a los estándares W3C – *Mobile Best Practices* 1.0, disponibles en la dirección electrónica: http://www.w3.org/TR/mobile-bp	**R**	
Estándar Hipertexto	Debe ser adherente a los estándares W3C – *Mobile Best Practices* 1.0, disponibles en la dirección electrónica: http://www.w3.org/TR/mobile-bp	**R**	
Programación Extendida	Debe ser adherente a los estándares W3C – *Mobile Best Practices* 1.0, disponibles en la dirección electrónica: http://www.w3.org/TR/mobile-bp	**R**	

Componente	Especificación	SIT	Observaciones
Mensajería	Debe ser adherente a los estándares W3C – *Mobile Best Practices* 1.0, disponibles en la dirección electrónica: http://www.w3.org/TR/mobile-bp	**R**	
Archivos de Video y Audio	Debe ser adherente a los estándares W3C – *Mobile Best Practices* 1.0, disponibles en la dirección electrónica: http://www.w3.org/TR/mobile-bp	**R**	
Archivos de Imagen	Debe ser adherente a los estándares W3C – *Mobile Best Practices* 1.0, disponibles en la dirección electrónica: http://www.w3.org/TR/mobile-bp	**R**	
Archivos de Oficina	Debe ser adherente a los estándares W3C – *Mobile Best Practices* 1.0, disponibles en la dirección electrónica: http://www.w3.org/TR/mobile-bp	**R**	
Lector de PDF	Debe ser adherente a los estándares W3C – *Mobile Best Practices* 1.0, disponibles en la dirección electrónica: http://www.w3.org/TR/mobile-bp	**R**	

8.4. Medios de Acceso: Especificaciones Técnicas para TV Digital

Considerando el alto nivel de la presencia de dispositivos receptores de señal de televisión en las casa brasileñas y la inminente implantación del Sistema Brasileño de TV Digital, que permite interacción con los telespectadores, este se transforma en canal de gran potencial de relaciones entre gobierno y sociedad. De esa manera, surgen nuevas posibilidades de acceso a los productos y servicios del gobierno electrónico, por medio de los nuevos dispositivos de TV Digital.

Su uso ofrece más que una señal de calidad, proporcionando interactividad y accesibilidad con Servicios Comerciales como: Compras, juegos y acceso a bancos, y también Servicios Sociales, como: Consultas al FGTS, PIS, Programas Sociales del Gobierno, teleeducación y otros, haciendo que los ciudadanos pasen de una actividad esencialmente pasiva a una acción participativa.

La TV Digital se vuelve un estándar de comunicación entre diferentes perspectivas como: la tecnológica, con la migración del sistema analógico al digital; la económica, con la migración de nuevas posibilidades de servicios y negocios; la social, con oferta de diversidad de contenidos e inclusión social al utilizar Internet a través de una TV; la política, con la posibilidad de incentivar la discusión de un nuevo marco regulador y la comportamental, con la posibilidad de participación activa de las audiencias por medio del uso de diferentes niveles de interactividad en la TV Digital.

Para atender las cuestiones técnicas, el Foro del Sistema Brasileño de TV Digital Terrestre – SBTVD, publicado junto a la Asociación Brasileña de Normas Técnicas – ABNT, agrupa varias normas en la página: http://www.forumsbtvd.org.br/materias.asp?id=112, donde se referencia un conjunto de especificaciones, estandarizado y libre de impuestos, denominado GINGA.

Cuadro 13 – Especificaciones para Medios de Acceso – TV Digital

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Transmisión	**ABNT NBR 15601** Parte 1 – Sistema de transmisión	**R**	

Componente	Especificación	SIT	Observaciones
Codificación	**ABNT NBR 15602** Parte 1 – Codificación de Video. Parte 2 – Codificación de Audio. Parte 3 – Sistema de multiplexado de señales.	**R**	
Multiplexado	**ABNT NBR 15603** Parte 1 – Servicios de información del sistema de radiodifusión. Parte 2 – Sintaxis y definiciones de la información básica de SI. Parte 3 – Sintaxis y definiciones de la información extendida de SI.	**R**	
Receptores	**ABNT NBR 15604** Parte 1 – Receptores.	**R**	
Seguridad	**ABNT NBR 15605** Parte 1 – Tópicos de seguridad.	**R**	
Middleware	**ABNT NBR 15606** Parte 1 – Codificación de datos. Parte 2 – Ginga-NCL para receptores fijos y móviles – Lenguaje de aplicación XML para codificación de aplicaciones. Parte 3 - Especificación de transmisión de datos. Parte 5 – Ginga-NCL para receptores fijos y móviles – Lenguaje de aplicación XML para codificación de aplicaciones. Parte 4	**R** **F**	
Canal de Interactividad	**ABNT NBR 15607** Parte 1 – Protocolos, interfaces físicas e interfaces de software.	**R**	
Guía Operacional	**ABNT NBR 15608** Parte 1 – Sistema de Transmisión – Guía para implementación de la ABNT NBR 15601. Parte 2 – Codificación de video, audio y multiplexado – Guía para implementación de la ABNT NBR 15602. Parte 3 – Multiplexado y servicio de informaciones (SI) – Guía de implementación de la ABNT NBR 15603.	**R**	

9. Organización e Intercambio de Informaciones

9.1. Organización e Intercambio de Informaciones: Políticas Técnicas

Las políticas técnicas para sistemas de organización e intercambio de informaciones y datos son:

9.1.1. Uso de XML para intercambio de datos.

9.1.2. Uso de Esquema XML y de la UML (cuando sea el caso) para definición de los datos para intercambio.

9.1.3. Uso de XSL para transformación de datos.

9.1.4. Uso de un estándar de metadatos para la gestión de contenidos electrónicos.

9.2. Organización e Intercambio de Informaciones: Especificaciones Técnicas

Cuadro 14 – Especificaciones para Organización e Intercambio de Informaciones

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Lenguaje para intercambio de datos	XML (*Extensible Markup Language*) como definido por el W3C http://www.w3.org/XML	**A**	
Transformación de datos	XSL (*Extensible Stylesheet Language*) como definido por el W3C http://www.w3.org/TR/xsl XSL *Transformation* (XSLT) como definido por el W3C http://www.w3.org/TR/xslt	**A**	
Definición de los datos para intercambiar	Esquema XML como definido por el W3C: - XML *Schema Part 0: Primer* http://www.w3.org/TR/2004/REC-xmlschema-0-20041028/ - XML *Schema Part 1: Structures* http://www.w3.org/TR/xmlschema-1/structures - XML *Schema Part 2: Datatypes* http://www.w3.org/TR/xmlschema-2/datatypes UML (*Unified Modeling Language*) como definido por el OMG http://www.omg.org/gettingstarted/specsandprods.htm/	**A**	
Descripción de datos	RDF (*Resource Description Framework*) Como definido por la W3C.	**F**	
Elementos de Metadatos para administración de contenidos	e-PMG – Estándar de Metadatos para el Gobierno Electrónico.	**E**	
Taxonomía para navegación	LAG – Lista de Asuntos del Gobierno, Versión 1.0. acorde a lo definido en http://www.eping.e.gov.br	**A**	En 2010 la LAG pasará a denominarse VCGE – Vocabulario Controlado del Gobierno Electrónico.

Componente	Especificación	SIT	Observaciones
Sistema de resolución de Identificadores	*Handle system* (http://www.handle.net).	**E**	

9.3. Notas sobre XML y *Middleware*

No todos los sistemas deben tener capacidad de comunicarse directamente en XML, como está representado en la Figura 4. Cuando sea apropiado, es aceptable el uso de *middleware* conforme la ilustración de la Figura 5.

Aunque las configuraciones a continuación presenten soluciones en potencia, el modelo XML directo (Figura 4) es preferencial, siendo posible el uso del modelo indirecto, en la Figura 5, en casos donde haiga razones fundamentales que justifiquen su uso.

Figura 4 – Modelo XML Directo – Intercambio Directo.

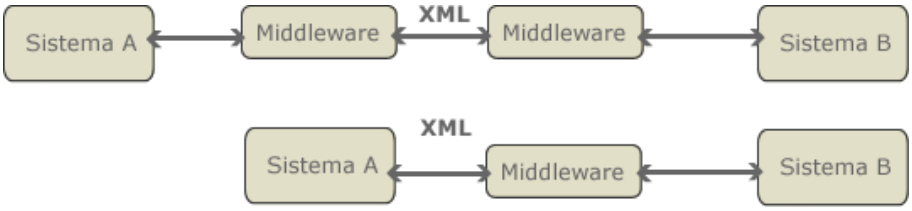

Figura 5 – Intercambios por medio de *middleware.*

En casos específicos como aquellos que necesitan la transferencia de un gran volumen de datos entre sistemas en un corto espacio de tiempo y en los intercambios en que el tiempo de respuesta es crítico, la adopción del XML como lenguaje para intercambio podrá ocurrir de forma gradual.

Es importante resaltar que el XML es adoptado en la e-PING como un lenguaje para intercambio de datos. Como solución de interoperabilidad (interconexión) observe los ítems 6.1.7 y 10.1.4 sobre *Web Services* y SOAP.

9.4. Nota sobre la utilización de UML

Para la descripción de datos complejos buscando una mejor explicitación es recomendado, cando corresponda, el uso del diagrama de clases de la UML.

9.5. Nota sobre la LAG

En 2010 la LAG pasará a denominarse VCGE – Vocabulario Controlado del Gobierno Electrónico.

10. Áreas de Integración para Gobierno Electrónico

10.1. Áreas de Integración para Gobierno Electrónico: Políticas Técnicas

10.1.1. En este segmento, son tratados componentes relacionados a temas transversales a las Áreas de Actuación de Gobierno, cuya estandarización sea relevante para la interoperabilidad de servicios de Gobierno Electrónico, tal como Procesos e Informaciones Geográficas.

10.1.2. Como directriz técnica para integración de sistemas de información se recomienda la adopción gradual de la Arquitectura Orientada a Servicios (SOA), basándose en la iniciativa "**Arquitectura Referencial de Interoperabilidad de los Sistemas Informatizados de Gobierno (AR)**" para la implementación, modelo de Arquitectura Orientada a Servicios, adaptado a la realidad de los Sistemas Informatizados del Gobierno Federal, disponible en la página http://www.eping.e.gov.br.

10.1.3. La arquitectura e-PING – Estándares de Interoperabilidad de Gobierno Electrónico – promueve la adopción del XML y el desarrollo de Esquemas XML como pilares para la integración e interoperabilidad electrónica del gobierno.

10.1.4. Se recomienda el uso de *Web Services* para demandas de integración entre sistemas de información de gobierno. De forma que, independiente de las tecnologías en que fueron implementados, se pueda adoptar un estándar de interoperabilidad que asegure escalabilidad, facilidad de uso, además de permitir actualización de forma simultánea y en tiempo real.

10.1.5. Está disponible, en el Portal del Gobierno Electrónico, el **Guía de Interoperabilidad de Servicios de Gobierno** para orientar el uso de las herramientas y tecnologías producidas por el segmento.

10.1.6. El segmento actuará buscando la identificación, acompañamiento de la producción y análisis de estándares de datos de interés general de la Administración Pública, junto a grupos representativos del gobierno y de la sociedad, reportándose a instancias competentes en lo que respecta a la priorización.

10.1.7. El formato de los Datos de interés general del gobierno debe ser colocado a disposición en el **Catálogo de Interoperabilidad**, según las reglas de uso de esta herramienta.

10.1.8. Los Servicios Interoperables (*Web Services*) de interés general deben ser colocados a disposición en el **Catálogo de Interoperabilidad**, pero aún así existe la necesidad de observar reglas de uso de los servicios de acceso restringido por los respectivos órganos.

10.1.9. El **Catálogo de Interoperabilidad** es un elemento central del ambiente de interoperabilidad del Gobierno Federal. Su uso es considerado equivalente a la situación Adoptado (A).

10.2. Catálogo de Interoperabilidad

10.2.1. El Catálogo de Interoperabilidad está disponible en la página http://www.eping.e.gov.br, estando formado por el Catálogo Estándar de Datos (CPD) y por el Catálogo de Servicios Interoperables.

10.2.2. El Catálogo Estándar de Datos (CPD) tiene por fin determinar estándares de tipos e ítems de datos que se aplican a las interfaces de los sistemas de forman parte del sector público, siendo dividido en dos documentos:

- Volumen 1, que establece los principios generales, o sea, las razones, abordajes y reglas para el uso de los estándares de Tipo e Ítems de Datos; y
- Volumen 2, que presenta los Tipos e Ítem de Datos estandarizados.

10.2.3. La Coordinación de la e-PING está encargada del Catálogo de Interoperabilidad, en especial por la definición de las reglas para la administración de los procesos de alteraciones y por fomentar que los estándares sean utilizados en desarrollos futuros.

10.2.4. El desarrollo y mantenimiento del Catálogo de Interoperabilidad es de responsabilidad del Grupo Áreas de Integración para Gobierno Electrónico que tiene la participación de diferentes segmentos del gobierno en las esferas federal y estatal.

10.3. Modelos para documentación de *Web Services* y otras modalidades de intercambio de datos

10.3.1. Como forma de documentar los servicios interoperables, se recomienda el uso, en cada caso, del modelo de documentación para *Web Services* y delo modelo de documentación para servicios de forma general (no *Web Services*), como intercambio de archivos, FTP, etc. Esos modelos están accesibles en la página de la e-PING.

10.3.2. La adopción de los modelos de documentación posee status equivalente a la situación Recomendada (R)**.**

10.3.4. Se solicita a los órganos que utilicen los Modelos de Documentación que envíen la documentación de las interfaces al correo electrónico: eping@planejamento.gov.br.

10.4. Áreas de Integración para Gobierno Electrónico: Nota explicativa sobre los Catálogos Estándar de Datos y Esquemas XML

10.4.1. Consideraciones Iniciales

Los Catálogos Estándar de Datos y Esquemas XML están disponibles en el portal del Gobierno Electrónico en la página http://www.governoeletronico.gov.br/.

El Catálogo Estándar de Datos tiene por fin determinar estándares de tipos e ítems de datos que se aplican a las interfaces de los sistemas de forman parte del sector público, siendo dividido en dos documentos:

- Volumen 1, que establece los principios generales, o sea, las razones, abordajes y reglas para el uso de los estándares de Tipo e Ítems de Datos; y
- Volumen 2, que presenta los Tipos e Ítem de Datos estandarizados.

El Catálogo Esquemas XML tiene por objetivo determinar estándares de Esquemas XML que se aplican a las interfaces de sistemas que apoyen la oferta de servicios de Gobierno Electrónico.

El Catálogo Esquemas XML contiene los estándares aceptados, en la forma de Esquemas XML, para intercambio de datos involucrando el sector público. Tales estándares pueden constituirse tanto en un único esquema, como en un conjunto de Esquemas XML, mientras que el conjunto se refiera a un mismo tema dentro del Área de Integración asociada.

La publicación de Esquemas XML no implica automáticamente una garantía de acceso a los contenidos correspondientes o servicios asociados, para lo que pueden ser definidas normas específicas por su respectivo gestor.

10.4.2. Propiedad y Responsabilidad

La Coordinación de la e-PING está encargada del Catálogo de Interoperabilidad, en especial por la definición de las reglas para la administración de los procesos de alteraciones y por fomentar que los estándares sean utilizados en desarrollos futuros.

En este sentido, se recomienda que el desarrollo o mantenimiento de sistemas que apoyen la oferta de servicios de Gobierno Electrónico correlativos a áreas/áreas derivadas de actuación del gobierno contempladas en el Catálogo consideren los Esquemas XML publicados.

El desarrollo y mantenimiento del Catálogo de Interoperabilidad es de responsabilidad del Grupo Áreas de Integración para Gobierno Electrónico que tiene la participación de diferentes segmentos del gobierno en las esferas federal y estatal.

10.4.3. Mecanismos de Gestión del Catálogo de Esquemas XML

Las entradas en el catálogo XML pueden darse por medio de las siguientes situaciones:

a) Proposición seguida de aprobación de propuesta de contenido para el Catálogo de Estándares de Datos (CPD);

b) Análisis seguido de aprobación de propuesta de contenido para la Arquitectura Referencial de Interoperación de los Sistemas Informatizados de Gobierno (AR);

c) Envío, por profesional vinculado al sector público, de contenido directamente al Catálogo de Esquemas XML, por medio de formulario electrónico disponible a partir de la página de la e-PING.

La proposición de registro de Esquemas XML será sometida a análisis de los integrantes del Grupo Áreas de Integración para Gobierno Electrónico mediante formulario electrónico específico disponible en la página de la e-PING (www.e-ping.e.gov.br). Serán mantenidas en el Catálogo sólo las proposiciones aceptadas, siendo que las que aún estén analizándose, las rechazadas y las versiones anteriores de Esquemas XML aceptadas serán mantenidas en ambiente “de pruebas” a ser oportunamente elaborado e implementado.

Los criterios evaluadores empleados incluirán:

- Reconocimiento por la comunidad usuaria;
- Acuerdo del gestor del área/área derivada (caso no sea el proponente); y
- Adherencia a los estándares de la e-PING.

O sea, la ocurrencia de envíos en que el proponente de determinado Esquema XML no sea el gestor del área está previsto, pero tendrá como condición adicional de aprobación la concordancia del gestor, a partir de interlocución realizada por el mismo proponente y/o por el Grupo Áreas de Integración para Gobierno Electrónico.

Solicitaciones de alteración para Esquemas XML ya publicados serán analizada previamente por los integrantes del Grupo Áreas de Integración para Gobierno Electrónico. La decisión de aprobación será responsabilidad de la Coordinación Central de la e-PING, que podrá adoptar las alteraciones propuestas de acuerdo con su abarcadura o someterlas a consulta pública, por medio de la página http://www.governoeletronico.gov.br.

Para esta versión del documento e-PING, se eligió colocar a disposición el contenido del Catálogo de Esquemas XML sólo en la herramienta desarrollada para la gestión de él, siendo eliminada la publicación en el documento de las referencias a ellos. Esa elección está cimentada en el objetivo de estimular el uso y mantenimiento de los Esquemas XML en la herramienta apropiada y permitir más flexibilidad de la gestión de los Esquemas XML.

10.5. Áreas de Integración para Gobierno Electrónico: Especificaciones Técnicas

Las especificaciones para las Áreas de Integración para Gobierno Electrónico son:

Cuadro 15 – Especificaciones para Áreas de Integración para Gobierno Electrónico – Temas transversales a Áreas de Actuación del Gobierno

Temas	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
PROCESOS – Lenguaje para Ejecución de Procesos	BPEL4WS V1.1, conforme definido por OASIS http://www.oasis-open.org/committees/download.php/2046/BPEL%20V1-1%20May%205%202003%20Final.pdf	**R**	El grupo acompañará la evolución del BPEL$WS versión 2.0. Estudios referentes al orquestado de procesos y coreografía serán futuramente liderados por el grupo.
PROCESOS –	BPMN 1.0, conforme definido por OMG	**R**	

Temas	Especificación	SIT	Observaciones
Notación de Modelado de Procesos	http://www.bpmn.org/Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf		
Intercambio de Informaciones Financieras	XBRL – *eXtensible Business Reporting Language* http://www.xbrl.org/SpecRecommendations/	**F**	www.xbrl.org
Legislación, Jurisprudencia y Proposiciones Legislativas	LexML v. 1.0 http://projeto.lexml.gov.br	**R**	Proyecto LexML define recomendaciones para la identificación y estructuración de documentos legislativos y jurídicos.
Planificación Estratégica	StratML – *Strategy Markup Language* http://xml.gov/stratml/index.htm	**F**	
INFORMACIONES REFERENCIADAS GEIGRÁFICAMENTE – Interoperabilidad entre sistemas de información geográfica	WMS versión 1.0 o posterior http://www.opengeospatial.org/standards	**A**	
	WFS versión 1.0 o posterior http://www.opengeospatial.org/standards	**A**	
	WCS versión 1.0 o posterior http://www.opengeospatial.org/standards	**A**	
	CSW versión 2.0 o posterior http://www.opengeospatial.org/standards/cat	**A**	
	WFS-T versión 1.0 o posterior http://www.opengeospatial.org/standards/wfs	**R**	Observar estándares y políticas de seguridad indicados por el GT2, principalmente WS-Security.
	WKT/WKB http://www.opengeospatial.org/standards/sfa	**R**	Para codificar coordenadas en servicios Web convencionales. Las coordenadas deben estar en Lat/Long utilizando el datum SIRGAS2000 o WGS-84. Usar GML siempre que sea posible.

Cuadro 16 – Especificaciones para Áreas de Integración para Gobierno Electrónico – *Web Services*[29]

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Infraestructura de registro	Especificación UDDI v3.0.2 (*Universal Description, Discovery and Integration*) definida por OASIS http://uddi.org/pubs/uddi_v3.htm	**R**	

[29] Las cuestiones de seguridad relacionadas a *Web Services* son tratadas en el capítulo 7.

Componente	Especificación	SIT	Observaciones
	ebXML (*Electronic Business using eXtensible Markup Language*). La especificación puede encontrarse en http://www.ebxml.org/specs/index.htm	**E**	
Lenguaje de definición del servicio	WSDL 1.1 (*Web Service Description Language*) como definido por W3C. La especificación puede encontrarse en http://www.w3.org/TR/wsdl	**A**	
	WSDL 2.0 (*Web Service Description Language*) como definido por W3C. La especificación puede encontrarse en http://www.w3.org/TR/wsdl20/	**E**	
Perfil básico de interoperabilidad	*Basic Profile 1.1 Second Edition,* como definido por WS-I http://www.ws-i.org/Profiles/BasicProfile-1.1.html	**E**	La versión 1.2 del Basic Profile está como borrador (*Working Draft*) en http://www.ws-i.org/Profiles/BasicProfile-1.2.html
Portlets remotos	WSRP 1.0 (Web Services for Remote Portlets) como definido por OASIS http://www.oasis-open.org/committees/wsrp	**E**	

11. Glosario de Siglas y Terminología Técnica[30]

En este ítem son presentados los significados de los principales términos técnicos utilizados en la e-PING.

ABNT – Asociación Brasileña de Normas Técnicas: Publica normas que orientan a respecto de la preparación y el compilado de referencias de material utilizado para la producción de documentos y para inclusión en bibliografías, resúmenes, reseñas, recensiones y otros.

ACAP – *Application Configuration Access Protocol* (Protocolo de Acceso a Configuración de Aplicación): Protocolo internet para acceso a opciones de programa cliente, configuraciones e informaciones preferenciales remotamente. Es una solución para el problema de movilidad de cliente en Internet.

APF – Administración Pública Federal: Reúne órganos de la administración directa (servicios integrados en la estructura administrativa de la Presidencia de la república y de los Ministerios) e indirecta (Autarquías, Empresas Públicas, sociedades de Economía Mixta y Fundaciones Públicas) del Poder Ejecutivo. https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm.

BPM – *Business Process Management* Visión de los procesos de negocio de una organización como flujo de servicios utilizando estándares de representación de notación, ejecución y coordinación en XML, cuyo rigor semántico permite su interoperabilidad entre sistemas de plataformas diferentes, siendo de esa forma un pilar para la implementación de soluciones basada en arquitectura orientada a servicios. Cuando la coordinación de la ejecución de los servicios se realiza con subordinación a un proceso maestre, en general, dentro de la organización, se denomina a esa coordinación como Orquestado. Cuando la coordinación es realizada sin la subordinación a un proceso maestre, en general, entre organizaciones, se la denomina Coreografía.

***Browser*:** Navegador de la *web* – Un aplicación cliente que permite al usuario visualizar contenidos de la *World Wide Web* en otra red o en el ordenador del usuario, acompañar los vínculos de hipertexto y transferir archivos.

Catálogo de Esquemas XML: Directorio de informaciones sobre los Esquemas XML.

Criptografía: Técnica de protección de información que consiste en cifrar el contenido de un mensaje o una señal, transformándolo en in texto ilegible, mediante la utilización de algoritmos matemáticos complejos.

CSW – *Catalogue Services for the Web*: Especificación OGC que define interfaces para publicar, ingresar, navegar y consultar metadatos sobre informaciones referenciadas geográficamente en Internet (HTTP).

Dispositivo: Componente físico (estación de trabajo, teléfono celular, tarjeta inteligente, *hand-held*, televisión digital con acceso a Internet).

DNS – *Domain Name System* (Sistema de Nombres de Dominio): Forma como los nombres de dominio son encontrados y traducidos en la dirección de protocolo de Internet. Un nombre de dominio es un recurso fácil de recordar cuando referenciado como una dirección en Internet.

FTP – *File Transfer Protocol* (Protocolo de Transferencia de Archivo): Es un protocolo aplicativo que utiliza los protocolos TCP/IP de Internet, siendo la forma más simple de intercambiar archivos entre ordenadores en Internet.

GML – *Geography Markup Language*: Especificación OGC basada en XML desarrollada para permitir el transporte y almacenado de informaciones geográficas/espaciales.

***Hand-helds*:** Computadora de mano, también conocida como PDA, pocket PC o palm top. Equipo portátil desarrollado para servir como dispositivo de acceso.

[30] Microsoft Press. Diccionario de informática. Traductor y consultor editorial Fernando Barcellos Ximenes – KPMG Peat Marwick. Editora Campos Ltda, 1993. ISBN 85-7001-748-0.

Thing, Lowell (ed.). Diccionario de Tecnología. Traducción de Bazán Tecnologia e Lingüística e Texto Digital. São Paulo: Futura, 2003. ISBN 85-7413-138-5.

***Handshake*:** En una comunicación por teléfono, intercambio de informaciones entre dos módems y el resultante acuerdo sobre cual protocolo utilizar antes de cada conexión telefónica.

***Hashing*:** Es la transformación de una cadena de caracteres en un valor de tamaño fijo normalmente menor o en una llave que representa la cadena original. Es utilizada para indexar y recuperar ítems en un banco de datos, porque es más rápido encontrar el ítem utilizando la menor llave transformada que del valor original. También es utilizada en algoritmos de criptografía.

HELO: Parámetros que limitan la entrega de correo electrónico comercial no solicitado. http://www.postfix.org/uce.html.

HTTP – *Hyper Text Transfer Protocol* (Protocolo de Transferencia de Hipertexto): Conjunto de reglas para intercambio de archivos (texto, imágenes gráficas, sonido, video y otros archivos multimedia) en la *World Wide Web.*

HTTPS – *Secure Hyper Text Transfer Protocol* (Protocolo de Transferencia de Hipertexto Seguro): Protocolo *web* desarrollado por Netscape y acoplado al navegador. Criptografa y criptoanaliza solicitaciones y retornos de páginas retornadas por el servidor *web.* El HTTPS es sólo el uso del SSL (*Secure Sockets Layer*) del Netscape como una camada secundaria bajo la organización normal de los programas de las aplicaciones HTTP.

ICP – Brasil: Conjunto de técnicas, prácticas y procedimientos, a implementarse por las organizaciones gubernamentales y privadas brasileñas con el fin de estipular los fundamentos técnicos y metodológicos de un sistema de certificación digital basado en llave pública. http://www.icpbrasil.gov.br.

IEEE – *Institute of Electrical and Electronics Engineers* (Instituto de Ingenieros Eléctricos y Electrónicos): Promueve el desarrollo de estándares y normas que con frecuencia se vuelven nacionales e internacionales.

IETF – *Internet Engineering Task Force* (Grupo de Trabajo en Ingeniería de Internet): Entidad que define protocolos operacionales estándar de Internet, como el TCP/IP.

IMAP – *Internet Message Access Protocol* (Protocolo de Acceso a Mensajes en Internet): Protocolo estándar para entrar a correo electrónico a partir del servidor local. IMAP es un protocolo cliente-servidor en que el correo electrónico es recibido y guardado por el servidor de Internet.

IP – *Internet Protocol* (Protocolo de Internet): Protocolo que permite la comunicación entre dispositivos en la red. De forma genérica, puede considerárselo como un conjunto de números que representa el local de un determinado equipo (normalmente ordenadores) en una red pública o privada.

IPSec – *Internet Protocol Security* (Seguridad de Protocolo de Internet): Estándar de desarrollo relacionado a la seguridad en la camada de la red o del procesamiento de paquetes de la comunicación en red. Una gran ventaja del IPsec es que las disposiciones de seguridad pueden ser manejadas sin exigir alteraciones en los ordenadores de usuarios individuales. El IPsec provee dos opciones de servicios de seguridad: *Authentication Header* (AH), que esencialmente permite la autenticación del remitente de datos, y *Encapsulating Security Payload* (ESP), que soporta la autenticación del remitente bien como la codificación criptográfica de datos.

IPv4 – *Internet Protocol Version 4* (Protocolo de Internet Versión 4): Es la versión del protocolo IP más utilizada hoy en día. Está formada por un número de 32 bits escrito con cuatro octetos en el formato decimal, separados por puntos (ejemplo: 161.148.1.18). La primera parte de la dirección identifica una red específica en la interred y la segunda parte identifica un equipo (host) de esa red.

IPv6 – *Internet Protocol Version 6* (Protocolo de Internet Versión 6): Es la versión más actual del protocolo IP. Está formada por un número de 128 bits escrito en ocho campos de cuatro dígitos hexadecimales, separados por dos puntos (ejemplo: 3ffe:6a88:85a3:08d3:1319:8a2e:0370:7344); e incluye prefijo de red y sufijo de host. Está implantándose gradualmente en Internet y debe funcionar lado a lado con el IPv4, en una situación técnicamente llamada de “batería doble”, por algún tiempo. A largo plazo, el IPv6 tiene como fin reemplazar el IPv4, que sólo soporta cerca de 4 billones (4 x 109) de direcciones, contra alrededor de 3,4 x 1038 direcciones del nuevo protocolo.

LAN – *Local Area Network* (Red Local): Grupo de ordenadores y dispositivos asociados que comparten una misma línea de comunicación y normalmente los recursos de un único procesador o servidor en una pequeña área geográfica. Normalmente, el servidor posee aplicaciones y almacenaje de datos compartidos por varios usuarios en diferentes ordenadores.

LDAP – *Lightweight Directory Access Protocol* (Protocolo Leve de Acceso a Directorio): Protocolo de software para permitir la localización de organizaciones, de personas y de otros recursos como archivos y dispositivos en una red, sea en Internet pública o en una red de intranet corporativa.

Medios de Acceso: Conjunto de componentes físicos (dispositivos de acceso) y de no físicos (software básico, aplicativos, etc.) que permite AL usuario el acceso a un servicio de gobierno electrónico.

Mensajería en Tiempo Real o Mensaje Instantáneo: Es un tipo de comunicación que permite que un usuario cambie mensajes en vivo con otro usuario también conectado a la red.

Metadatos: Conocidos como "datos sobre datos", los metadatos son usados para registrar atributos sobre un recurso informacional buscando facilitar la recuperación, la gestión, la interoperabilidad, dar soporte a la identificación digital y dar soporte al archivado y preservación.

Middleware: Es un término general que sirve para mediar dos programas separados y generalmente ya existentes. Aplicaciones diferentes pueden comunicarse a través del servicio *Messaging*, proveído por programas *Middleware.*

Newsgroup (Grupo de Noticias): Discusión sobre un determinado asunto que consiste en mensajes enviados a una página central en Internet y redistribuidos por la Usenet, una red global de grupos de discusión de noticias. Los usuarios pueden enviar mensajes a grupos de noticias existentes, responder a mensajes anteriores y crear nuevos grupos de noticias.

OGC – *Open Geospatial Consortium* (consorcio internacional *Open Geospatial*): Posee la misión de "desarrollar especificaciones para interfaces espaciales que serán colocadas a disposición libremente para uso general".

Estándar Abierto:

I – posibilita la interoperabilidad entre diversas aplicaciones y plataformas, internas y externas;

II – permite aplicación sin cualquier restricción o pago de impuestos;

III – puede implementarse plena e independientemente por múltiples proveedores de programas de ordenador, en varias plataformas, sin cualquier gravamen relativo a la propiedad intelectual para la tecnología necesaria.

Estándar de Metadatos: Un estándar de metadatos establece un conjunto de elementos de metadatos para una comunidad, incluyendo la especificación de cada elemento y esquemas de codificación para permitir la interoperabilidad entre los sistemas que utilizan el estándar.

***Plug-in*:** Un programa accesorio que agrega capacidades al programa principal. Normalmente, en aplicaciones *web*, son programas que pueden ser fácilmente instalados y utilizados como parte del navegador. Una aplicación de plug-in es reconocida automáticamente por el navegador y la función es integrada a la página HTML que está siendo presentada.

POP3 – *Post Office Protocol* 3 (Protocolo de los Correos 3): Versión más reciente del protocolo estándar para recuperar mensajes. El POP3 es un protocolo de cliente/servidor donde el mensaje es recibido y guardado por el servidor de Internet.

Portal: Página en Internet que agrega servicios, noticias y gran volumen de contenido informativo o de entretenimiento.

Red Gobierno: Es el portal de entrada para todas las páginas del gobierno federal en Internet. http://www.federativo.bndes.gov.br/destaques/egov/egov_redegoverno.htm.

Resolución n 7 del Gobierno Electrónico: Establece reglas y directrices para las páginas en Internet de la Administración Pública Federal (gov.br y mil.br). Dividida en 7 capítulos, la resolución trata de la estructura de la información, del control y monitoreo, de la gestión de los elementos interactivos, del modelo organizacional, de la entidad visual y de la seguridad de las páginas gubernamentales en la red mundial de ordenadores. http://www.governoeletronico.e.gov.br.

RFC – *Request for Comments* (Solicitación de Comentarios): Documento formal de la IETF, resultado de modelos y revisiones de partes interesadas. La versión final del RFC se volvió un estándar donde no son permitidos alteraciones ni comentarios. Las alteraciones pueden suceder, sin embargo, por medio de RFCs subsecuentes que reemplazan o elaboran partes del RFCs anteriores. RFC también es la sigla para Remote Function Call (llamada funcional remota).

RSA - *Rivest-Shamir-Adleman*: Cifrado de Internet y un sistema de autenticación que utiliza un algoritmo desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman.

Servicios Electrónicos de Gobierno (*relacionados* Servicios de Gobierno Electrónico, Servicios Electrónicos):

Gobierno electrónico puede definirse por el uso de la tecnología para aumentar el acceso y mejorar la provisión de servicios del gobierno a ciudadanos, proveedores y servidores. En general, las funciones características del gobierno son:

1. Prestación electrónica de informaciones y servicios.
2. Reglamentación de las redes de información, involucrando principalmente gobernanza, certificación y tributación.
3. Prestación de cuentas públicas, transparencia y monitoreo de la ejecución presupuestaria.
4. Aprendizaje a distancia, alfabetización digital y mantenimiento de bibliotecas virtuales.
5. Difusión cultural enfatizando las identidades locales, promoción y preservación de culturas locales.
6. e-procurement, o sea, adquisición de bienes y servicios por medio de Internet, como licitaciones públicas electrónicas, remates electrónicos, bolsas de compras públicas virtuales y otros tipos de mercados digitales para los bienes adquiridos por el gobierno.
7. Incentivo a los negocios electrónicos, por medio de la creación de ambientes de transacciones seguras, en especial para pequeñas y medianas empresas. http://www.governoeletronico.gov.br/r1.

Sistemas de Información del Gobierno Federal: Sistemas que apoyan las actividades de:

- Gestión de gobierno: Planificación, Presupuesto, Ejecución Presupuestaria, Administración financiera, Administración de Recursos Humanos, Administración de Servicios Generales, Gestión de Documentación e Informaciones, Organización y Modernización Administrativa, Recursos de Información e Informática y Control Interno;
- Actuación final de gobierno: Actividades finalísticas de los varios órganos de la estructura gubernamental, como infraestructura (transporte, comunicaciones, energía, administración de recursos naturales), Agricultura, Salud, Educación, etc.

Referencia: http://www.redegoverno.gov.br/projetos/reg_gestao.asp.

SFS – *Simple Features Specification for* SQL: Especificación OGC que define la estandarización del esquema SQL que soporta almacenaje, recuperación, consulta y actualización sobre informaciones referenciadas geográficamente.

Smart Cards: Tarjeta de plástico, de la medida aproximada de una tarjeta de crédito, con un microchip embutido que puede ser cargado con datos, usado para realizar llamadas telefónicas, pagos electrónicos en dinero y otros usos. Es actualizado periódicamente para recibir usos adicionales.

S/MIME – *Secure Multi-Purpose Internet Mail Extensions* (Extensiones de Correo de Internet Multipropósito Seguras): Método seguro de enviar mensaje que utiliza el sistema de cifrado RSA (Rivest-Shamir-Adleman). S/MIME describe como pueden ser incluidas informaciones encriptadas y un certificado digital como parte del cuerpo del mensaje.

SMTP/MIME – *Simple Mail Transfer Protocol/Multi-purpose Internet Mail Extensions* (Protocolo de Transferencia de Mensaje Simple – Extensiones de Correo de Internet Multipropósito): SMTP es un protocolo TCP/IP utilizado en el envío y recepción de mensajes. MIME es una extensión de protocolo del mensaje original de Internet que permite el intercambio de diferentes tipos de archivos dados por Internet.

SOA – *Service Oriented Architecture* (Arquitectura Orientada a Servicios): Es un paradigma para organización y uso de competencias distribuidas bajo control de diferentes dominios propietarios. La arquitectura SA es usada para interoperabilidad de sistemas mediante conjunto de interfaces de servicios débilmente acoplados (*loosely coupled*), donde los servicios no necesitan detalles técnicos de la plataforma de los otros servicios para que el intercambio de informaciones sea realizado.

SOAP – *Simple Object Access Protocol* (Protocolo simple para Acceso a Objetos): Describe un modelo para el empaquetado de preguntas y respuestas XML. El envío de mensajes SOAP ES usado para permitir el intercambio de una variedad de informaciones XML. La norma de SOAP asume la tarea de transmitir pedidos y respuestas sobre servicios entre usuarios y proveedores de servicios.

Software Libre: Programa de ordenador disponible por medio de su código fuente y con la permisión para que cualquiera lo use, copie o distribuya, en su forma original o modificada, de forma gratuita o paga. El software libre es necesariamente no propietario, pero es importante no confundir software libre con software gratuito.

SPAM: Mensaje no solicitado en Internet. Del punto de vista del remitente, esa es una forma de mensaje en masa, generalmente a una lista separada de personas inscritas en un grupo de discusión Usenet u obtenida por empresas especialistas en crear listas de distribución de mensajes. Para el destinatario, el *spam* es normalmente considerado como basura.

SSL – *Secure Sockets Layer* (Camada de Soquetes Segura): Es un protocolo comúnmente utilizado para administrar la seguridad de una transmisión de mensaje en Internet.

Taxonomía para Navegación: Es un vocabulario controlado de términos y frases, organizado y estructurado jerárquicamente, conforme relaciones naturales o presumidas, objetivando simplificar a los usuarios de páginas y portales de Internet la descubierta de información por medio de la navegación.

TCP – *Transmission Control Protocol* (Protocolo de Control de Transmisión): Conjunto de reglas utilizadas con el IP para enviar datos en forma de unidades de mensaje entre ordenadores por Internet. Mientras el IP lidia con la entrega real de los datos, el TCP controla las unidades individuales de los datos en que un mensaje es dividido para distribución eficiente por medio de Internet.

Telnet: La forma de ingresar al ordenador de otra persona, asumiendo que esté permitido. Más técnicamente, Telnet es un comando del usuario y un protocolo subliminar TCP/IP para ingresar a ordenadores remotos.

TLS – *Transport Layer Security* (Seguridad de Nivel de Transporte): Protocolo que garantiza la privacidad entre las aplicaciones de comunicación y sus usuarios en Internet. Cuando un servidor y el cliente se comunican, el TLS asegura que ninguna otra parte podrá ver o recibir ese mensaje.

Token: Un objeto de datos estructurado o un mensaje que circula continuamente entre las conexiones de una red *token ring* y describe el estado actual de la red.

UDDI – *Universal Description Discovery and Integration* (Descripción, Descubierta e Integración Universales): Es el repositorio donde los investigadores registran los *Web Services* disponibles que permiten a los clientes la descubierta y uso de los servicios localizados en Extranet e Intranets.

UDP – *User Datagram Protocol* (Protocolo de Datagrama de Usuarios): Protocolo de comunicación que ofrece una cantidad limitada de servicio cuando los mensajes son intercambiados entre ordenadores de una red que utiliza el IP. El UDP es una alternativa para el uso del TCP y, con el IP, es referido como UDP/IP. Así como el TCP, el UDP utiliza el IP para llevar una unidad de datos de un ordenador a otro. A diferencia del TCP, el UDO no provee el servicio de dividir un mensaje en paquetes y rearmarlo en el otro extremo. El UDP no provee la secuencia de los paquetes en que los datos llegan. O sea, el programa de aplicación que utiliza el UDP debe asegurar que el mensaje entero llegó y está en orden. Las aplicaciones de red que quieren salvar el tiempo de procesamiento porque tienen unidades muy pequeñas de datos para intercambiar pueden preferir el UDP al TCP.

UML – *Unified Modeling Language* (Lenguaje de Modelado Unificado): La UML es más que la estandarización de una notación. Eso significa que es un lenguaje estándar para la elaboración de la estructura de proyectos de *software*, incluyendo aspectos conceptuales como procesos de negocios y funciones del sistema, además de ítems concretos como las clases escritas en determinado lenguaje de programación, esquemas de banco de datos y componentes de *softwares* reutilizables. La UML puede emplearse para la visualización, la especificación, la construcción y la documentación de artefactos de sistemas de *software*, también pudiendo usarse en el modelado de negocios y otros tipos de sistemas, no sólo de *software.*

URI – *Uniform Resource Identifier* (Identificador de Recurso Único): Estándar de codificación de

nombres y direcciones en Internet. Una URI está formada por un nombre (ej.: file, http, ftp, news, mailto, gopher), seguido por dos puntos y, finalmente, un camino, estandarizado por una lista de esquemas que sigue la RFC 1630. La URI agrupa los conceptos URNs y URLs.

Usenet: Colección de notas y mensajes enviados por usuarios sobre varios asuntos a los servidores en una red mundial. Cada colección de notas enviadas es conocida como un newsgroup.

VPN – *Virtual Private Networks* (Red Privada Virtual): Red particular, que utiliza la infraestructura de una red pública de telecomunicaciones, como Internet, por ejemplo, para la transmisión de informaciones confidenciales. Los datos transmitidos están encriptados. Su uso sucede por medio de túneles virtuales, por los cuales transitan las informaciones, protegiéndolas del acceso de usuarios desautorizados.

W3C – *World Wide Web Consortium* (Consorcio de la Red Mundial *Web*): Asociación de industrias que busca promover estándares para la evolución de la *web* e interoperabilidad entre productos para WWW produciendo softwares de especificación y referencia.

WAN – *Wide Area Network* (Red de Gran Área): Red de ordenadores que abarca extensa área geográfica como una provincia, un país o un continente.

WCS – *Web Coverage Service*: Especificación OGC que define la interface de un servicio para acceder a informaciones referenciadas geográficamente que poseen valores en todo el espacio considerado, sin fronteras bien definidas (geo-campos).

Web Services: Aplicación lógica, programable que vuelve compatibles entre sí las más diferentes aplicaciones, independiente del sistema operacional, permitiendo la comunicación y el intercambio de datos entre diferentes redes.

WFS – *Web Feature Service*: Especificación OGC que define la interface de un servicio que permite ingresar y manejar datos geográficos codificados en GML en Internet (HTTP). Pueden definirse dos clases de servicios:

- **WFS Básico (WFS):** Implementa operaciones de sólo lectura, que permiten obtener los datos espaciales.
- **WFS Transaccional (WFS-T):** Implementa las operaciones transaccionales, utilizadas para manejar los datos de forma remota.

WMS – *Web Map Service*: Especificación OGC que define la interface de un servicio para colocar a disposición mapas (datos geográficos editados) o imágenes en Internet (HTTP).

WSDL – *Web Services Definition Language* (Lenguaje para Definición de Servicios *Web*): Es un formato XML para descripción de servicios *web* y sus informaciones para acceso. Él describe las funcionalidades de los servicios ofrecidos por el proveedor de servicios, bien como su localización y forma de acceso.

XML – *eXtensible Markup Language* (Lenguaje Markup Extensible): Forma flexible para crear formatos de informaciones comunes y compartir ambos formatos y datos en la *World Wide Web,* en las Intranets y en cualquier lugar. El XML es extensible porque, a diferencia del HTML, los símbolos markup son limitados y se autodefinen.

XML *Schemas*: Son documentos XML, encontrados también en una página de Internet, que especifican la estructura, número de ocurrencias de cada elemento, valores permitidos, unidades, etc., o sea, la sintaxis del documento. Los esquemas de un conjunto de documentos XML, de un mismo tipo, quedan disponibles públicamente en una página de Internet, para que programas puedan tener acceso a ellos y validar los documentos XML de este conjunto. http://www.uff.br/gdo/htm/tsld106.htm.

XMPP – *eXtensible Messaging and Presence Protocol* (Protocolo de Mensajería en Tiempo Real): Protocolo abierto, con base en XML, para mensajes en tiempo real.

XSL – *eXtensible Stylesheet Language*: Lenguaje de creación de planillas que describe cómo un dato es mandado por medio de la *web*, utilizando el XML, y es presentado al usuario. El XSL es un lenguaje para formatear un documento XML.

XSLT – *eXtensible Stylesheet Language Transformations*: Forma estándar de describir como cambiar la estructura de un documento XML en otro documento XML con estructura diferente. El

XSL puede definirse como una extensión del XSL. El XSLT muestra cómo el documento XSL debe reorganizarse en otra estructura de datos (que puede ser presentada siguiendo una planilla del XSL).

12. Integrantes

Coordinación de la e-PING

Agencia Nacional de Aguas (ANA)
Sérgio Augusto Barbosa

Agencia Nacional de Cine (ANCINE)
Sérgio Augusto S. de Morais

Associação Brasileira de Entidades Estaduais de Tecnologia da Informação e Comunicação (ABEP)
Dayse Vianna

Banco do Brasil (BB)
Ulisses de Sousa Penna

Caixa Econômica Federal (CAIXA)
Ângela B. Baylo
Paulo Maia da Costa
Rúbia Scrócaro

Empresa de Tecnologia e Informações da Previdência Social (DATAPREV)
Humberto Degrazia Campedelli

Ministerio de Defensa – Comando del Ejército (MD/CEX)
Emerson Magnus de A. Xavier
Jefferson Adelino Lemos Pita

Ministerio de Justicia (MJ)
Jorilson da Silva Rodrigues

Ministerio de la Salud (MS)
Fábio Lima Cordeiro

Ministerio de Relaciones Exteriores (MRE)
Filipe Carneiro Guimarães

Ministerio del Desarrollo, de la Industria y del Comercio Exterior (MDIC)
José Luismar de Campos Larcher

Ministerio del Medio Ambiente (MMA)
Maurício Dayriell
Paulo Henrique de Assis Santana

Ministerio de Planificación, Presupuesto y Gestión – Secretaría de Logística y Tecnología de la Información (MP/SLTI)
Nazaré Lopes Bretas (Coordinadora General)
Cláudio Muniz Machado Cavalcanti
Cristiano Rocha Heckert
Jorge Arruda
José Ney de Oliveira Lima
Leonardo Boselli da Motta
Lilian Barbara Bender Portugal
Marcelo Martins Villar
Mário Henrique Paes Vieira
Rogério Santanna dos Santos
Yuri Fontes de Oliveira

Nuclebrás Equipamentos Pesados S/A (NUCLEP)
Adilson Custódio
Elizabeth Rodrigues Cunha

Presidencia de la República (PR)
Macarino Bento Garcia de Freitas

Presidencia de la República – Instituto Nacional de Tecnología de la Información (ITI)

Mauricio Augusto Coelho
Renato da Silveira Martini

Secretaria da Receita Federal do Brasil (RFB)
Edna Pereira Pinto Fernandes

Secretaría de la Administración del Estado de Bahia (SAEB)
Ernani Marques dos Santos

Servicio Federal de Procesamiento de Datos (SERPRO)
Bruno Pacheco de Paes
Elói Juniti Yamaoka

Grupo de Trabajo Interconexión

Cristiano Rocha Heckert (MP/SLTI) – Coordinador
Carlos Bellone Neto (RFB)
Dijasmo Martins Gomes Junior (ECT)
Filipe Carneiro Guimarães (MRE)
Helio de Araujo Castro (NUCLEP)
Juscelino Kilian (PR/GSI)
Leonardo Boselli da Motta (MP/SLTI)
Luiz Gustavo Lustosa Colombo (IPHAN)
Odilon de Freitas Militao Neto (CAIXA)
Paulo Guilherme Lanzillotti Jannuzzi (MPS)
Vanderlei de Jesus dos Santos Marques (ANVISA)
Wellington Luiz Barbosa (MP/SLTI)

Colaboradores
Hermógenes Batista Correia (MP/SLTI)

Grupo de Trabajo Seguridad

Jorilson da Silva Rodrigues (MJ) – Coordinador
Antônio Acras Filho (SERPRO)
Artur Nobre Mendes (FUNAI)
André Machado Caricatti (ITI)
Cláudio Muniz Machado Cavalcanti (MP/SLTI)
Cristiano Rocha Heckert (MP/SLTI)
Dante de Matos Gomes (PRODEB)
Filipe Carneiro Guimarães (MRE)
Gilberto de Oliveira Netto (SERPRO)
Humberto Degrazia Campedelli (DATAPREV)
Jean Carlo Rodrigues (ITI)
Joel Corrêa (DATAPREV)
José Eduardo Malta de Sá Brandão (IPEA)
José Luiz Povill de Souza (MJ/DPF)
Luiz Gustavo Lustosa Colombo (IPHAN)
Marcos Gomes Figueira (BB)
Marcos J.C. Euzébio (BACEN)
Mario Henrique Paes Vieira (MP/SLTI)
Nazaré Lopes Bretas (MP/SLTI)
Paulo Coelho Ventura Pinto (ANS)

Colaboradores
Anderson Claiton Fernandes (MJ)
Cláudia do Socorro Ferreira Mesquita (MP/SLTI)
Ronaldo Íon Miranda do Nascimento (MJ)

Grupo de Trabajo Medios de Acceso

Paulo Maia da Costa (CAIXA) – Coordinador
Artur Emilio de Rezende (MF)
Bruno Pacheco de Assis (SERPRO)
Carlos Bellone Neto (RFB)
Cláudio Muniz Machado Cavalcanti (MP/SLTI)
Danielle de Menezes Maciel Silva (ANVISA)
Denise Barros de Sousa (MEC)
Eliane Aristóteles Moreira (DATAPREV)
Frederico Cabral de Menezes (CONAB)
Geancarlo Noronha Vinhal (SERPRO)
Jacob Batista de Castro Junior (PR/GSI)
Jorge Arruda (MP/CGTI)
Juscelino Kilian (PR/GSI)
Márcio F. Viana M. (ME)
Márcio Humberto M. Cammarota (SERPRO)
Marconi Pereira Sodate (RFB)
Mauro Lemes da Silva (CAIXA)
Pedro Paulo Lemes Machado (ITI)
Reinaldo Silva Simão (PR)
Rubia Scrocaro (CAIXA)
Sonia Regina Rodrigues Motta (MEC)
Viviane Regina Lemos Bertol (ITI)
Wagner Ferreira Carneiro Junior (MF)

Colaboradores
André Luís da Silva Gonçalves (MP/SLTI)

Grupo de Trabajo Organización e Intercambio de Informaciones

Eloi Juniti Yamaoka (SERPRO) – Coordinador
Alisson de Oliveira Rodrigues (MI)
Ângela B. Baylo (CAIXA)
Antonio Celso Xavier de Oliveira (MRE)
Aurélia Dolores Gonçalves Bruner (ELETROBRÁS)
Beatriz Barreto Brasileiro Lanza (CELEPAR)
Brenda Couto de Brito Rocco (AN-CC)
Cintia de Souza Cinquini (PR)
Cláudia Carvalho Masset Lacombe Rocha (AN-CC)
Dayse Vianna (PRODERJ)
Dilma de Fátima Avellar Cabral da Costa (AN-CC)
Eduardo Rafael Miranda Feitoza (MI)
Eliane Pereira dos Santos (MS)
Elizabeth da Silva Maçulo (AN-CC)
Fernanda Hoffmann Lobato (MP/SLTI)
Hilda Pimentel (ANCINE)
João Alberto Lima (Senado Federal)
Ligia Leindorf Bartz Kraemer (UFPR)
Luciana Ferreira Pinto da Silva (INEP)
Márcia Helena Gonçalves Rollemberg (MS)
Márcia Izabel Fugizawa Souza (EMBRAPA)
Márcio Imamura (IBGE)
Margareth da Silva (AN-CC)
Maria Valéria Lins Tenório (Gobierno de Pernambuco / ATI)
Neuza Arantes Silva (MAPA)
Sérgio Silva dos Santos (MAPA)
Siomara Zgiet (MS)
Sylmara Campos Pinho Garcia (ANCINE)
Vicente de Paula Teixeira (CGU)

Virgilio Dantas Lins Filho (ME)
Vivianne Muniz Veras Barrozo (SERPRO)

Colaboradores
Dalva Clementina Luca (MJ)

Grupo de Trabajo Áreas de Integración para Gobierno Electrónico

Cláudio Muniz Machado Cavalcanti (MP/SLTI) – Coordinador
Adelino Fernando Correia (DATASUS)
Aliomar Mariano Rego (EMBRAPA)
Ananda de Medeiros Macias (SERPRO)
Antônio Campos Monteiro (ANEEL)
Bruno Palvarini (MP/SEGES)
Carlos Bellone Neto (RFB)
Carlos Maranhão (ANS)
Ceres Albuquerque (ANS)
Cláudio Manoel Cordeiro (SERPRO)
Ewerton Luciano Martins (ANVISA)
Frederico Duarte Guerra de Macedo (ME)
José Glaucy Rocha (RFB)
Hesley Py (IBGE)
Maurício Dayrell (MMA)
Marcelo Bastos Brandão (ABIN)
Márcio Humberto M. Cammarota (SERPRO)
Márcio Lúcio Vasconcelos Donato (MEC)
Mônica Maria Lucatelli Dória de Araújo (DATAPREV)
Paulo Henrique Santana (MMA)
Pedro Paulo Cirineo (BB)
Ricardo de Lima (INCRA)
Rogério Werneck (PR/DIRTI)
Tatiana Giachini (SERPRO)
Werangge Custódio (ANVISA)
Wilson de Morais Coelho (DATASUS)

Colaboradores
Cláudia do Socorro Ferreira Mesquita (MP/SLTI)
Luís Carlos Ramos (DATASUS)

Subgrupo: ABEP
Dayse Vianna (Gobierno de Rio de Janeiro / PRODERJ) – Coordinadora
Tarcísio Quirino Falcao (Gobierno de Pernambuco / ATI)

Subgrupo: Guía de Interoperabilidad de Servicios de Gobierno
Cláudia do Socorro Ferreira Mesquita (MP/SLTI) – Coordinadora
Lucio Ribeiro (Gobierno de Pernambuco / ATI)
Tarcísio Quirino Falcão (Gobierno de Pernambuco / ATI)
Rodrigo Henriques Medeiros (SERPRO)

Subgrupo: Estándares para Intercambio de Informaciones Espaciales
Emerson Magnus de A. Xavier (MD/CEX/CIGEx) – Coordinador
Cristiane Vaz Domingues (DATAPREV)
Jedson F. Passos (CAIXA)
Linda Soraya Issmael (MD/CEX/DSG)
Marcelo Martins Villar (MP/SLTI)
Moema Augusto (IBGE)
Yoshihisa Kawano (ABIN)
Yuri Fontes de Oliveira (MP/SLTI)

Ilustraciones
Hezrai de Souza Cruz (MP/SLTI)