Gobierno Brasileño

Comité Ejecutivo de Gobierno Electrónico

e-PING
Estándares de Interoperabilidad de Gobierno Electrónico

Documento de Referencia

Versión 4.0

16 de diciembre del 2008

ÍNDICE

Presentación

La arquitectura e-PING – Estándares de Interoperabilidad de Gobierno Electrónico – define un conjunto mínimo de premisas, políticas y especificaciones técnicas que reglamentan la utilización de la Tecnología de 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 abarcadas por la e-PING están segmentadas en:

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

En cada uno de esos sectores fueron especificados componentes, para los cuales son establecidos estándares.

Todo el contenido de este documento de Referencia está en consonancia con los lineamientos del Comité Ejecutivo de Gobierno Electrónico, creado por el Decreto del 18 de octubre del 2000, y está publicado en website específico en la Internet (http://www.eping.e.gov.br), garantizando acceso público a las informaciones de interés general y transparencia intrínseca a la iniciativa. El gobierno brasileño asume el compromiso de asegurar que estas políticas y especificaciones permanezcan alineadas con las necesidades de la sociedad y con la evolución del mercado y de la tecnología.

El documento de referencia de la e-PING contiene:

- los fundamentos de concepción, implantación y administración 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, discriminando responsabilidades, criterios de verificación de conformidad, gestión de cambios, divulgación y orientación para capacitación;
- las políticas y las especificaciones técnicas establecidas para todos los componentes de cada uno de los sectores de la e-PING;
- glosario de términos técnicos referenciados;
- lista 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 prestación de mejores servicios, adecuados a las necesidades de los ciudadanos y de los negocios, con menores costos, es la existencia de una infraestructura de Tecnología de la Información y Comunicación (TIC) que sirva como base para a creación de dichos servicios. Un gobierno moderno, integrado y eficiente, exige sistemas igualmente modernos, integrados e interoperables, trabajando de forma íntegra, segura y coherente en todo el sector público.

En este contexto, la interoperabilidad de tecnología, procesos, información y datos es condición vital para el suministro de servicios de calidad, siendo una premisa para gobiernos de todo el mundo, como fundamento para los conceptos de gobierno electrónico, o *e-gob*. La interoperabilidad permite racionalizar inversiones en TIC, mediante el uso compartido, reutilización e intercambio de recursos tecnológicos.

Gobiernos como el norteamericano, el canadiense, el británico, el australiano y el neozelandés invierten fuertemente en el desarrollo de políticas y procesos y en el establecimiento de estándares en TIC, montando estructuras dedicadas a obtener la interoperabilidad, con el objetivo de proveer servicios de mejor calidad a costos reducidos.

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

¿Qué es Interoperabilidad?

Para el establecimiento de los objetivos de la e-PING, es fundamental que se defina claramente el concepto de *Interoperabilidad*. A continuación son presentados cuatro conceptos que fundamentaron el entendimiento del gobierno brasileño a respecto del tema:

"Intercambio coherente de informaciones y servicios entre sistemas. Debe posibilitar la sustitución de cualquier componente o producto usado en los puntos de interconexión por otro de especificación similar, sin afectar las funcionalidades del sistema." (gobierno del Reino Unido);

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

"Habilidad de dos o más sistemas (computadoras, medios de comunicación, redes, software y otros componentes de tecnología de información) de interactuar y de intercambiar datos de acuerdo con un método definido, para 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 Talleres);

Interoperabilidad no es solamente Integración de Sistemas, no es solamente Integración de Redes. No se refiere únicamente al intercambio de datos entre sistemas. No contempla simplemente 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 la utilización de productos diferentes de proveedores diferentes. Su objetivo es la consideración de todos los factores para que los sistemas puedan actuar cooperativamente, fijando las normas, las políticas y los estándares necesarios para la consecución de dichos objetivos.

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

2. Alcance

Políticas y especificaciones claramente definidas para interoperabilidad y gestión de informaciones son fundamentales para propiciar la conexión del gobierno, tanto en el ámbito interno como en el contacto con la sociedad y, en mayor nivel de alcance, 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 al gobierno federal – Poder Ejecutivo, no restringiendo la participación, por adhesión voluntaria, de otros poderes y esferas de gobierno.

Los recursos de información del gobierno constituyen 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 auxilia en el aprovechamiento máximo de este activo, impulsando y estimulando la economía del país.

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 (estadual y municipal);
- Otros Poderes (Legislativo, Poder judicial) y Ministerio Público Federal;
- Organismos Internacionales;
- Gobiernos de otros países;
- Empresas (en Brasil y en el mundo);
- Tercer Sector.

La siguiente figura representa esa relación.

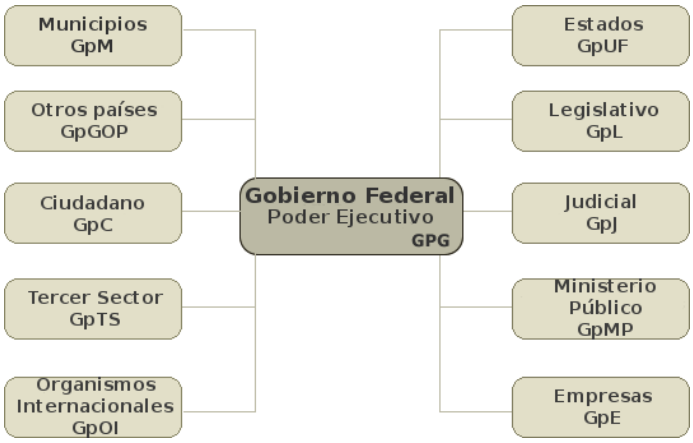

Figura 1 – Relaciones del gobierno federal.

2.1. Adhesión a la e-PING

La adopción de los estándares y políticas contenidos en la e-PING no puede ser impuesta a los ciudadanos y a las diferentes instancias de gobierno, dentro y fuera del país. El gobierno brasileño, sin embargo, establece esas especificaciones como el estándar seleccionado y aceptado por él, o sea, éstos son los estándares con que se desea interoperar con las entidades fuera del gobierno federal – Poder Ejecutivo brasileño. La adhesión de esas entidades se realizará de forma voluntaria y sin ninguna ingerencia por parte 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, vinculados directa o indirectamente a la Presidencia de la República de Brasil;
- las autarquías y fundaciones.

En el ámbito de las entidades anteriormente mencionadas, son obligatorias las especificaciones contenidas en la e-PING para:

- todos los nuevos sistemas de información que sean desarrollados e implantado en el gobierno federal y que se enmarcan en el alcance de interacción, dentro del gobierno federal y con la sociedad en general;
- sistemas de información legados que sean objeto de implementaciones que involucren suministro 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 ocurrirá de manera gradual, de acuerdo con plan de implementación elaborado por el propio órgano, que considerará la situación de la institución con relación a las condiciones para adecuarse a las especificaciones y recomendaciones de la e-PING.

Para los sistemas de información de gobierno que estén fuera del alcance de obligatoriedad delimitado, es recomendable que los responsables consideren la adecuación a los estándares de la e-PING siempre y cuando sean realizados 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 estar en consonancia con las especificaciones y políticas contenidas en este documento.

La e-PING incentiva la participación de todas las partes interesadas en el desarrollo y actualización continua de las especificaciones y recomendaciones integrantes de la arquitectura. La gestión de la e-PING prevé esa participación, con utilización de la Internet (http://www.eping.e.gov.br) como medio preferencial para el contacto entre los 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 temas del área de Tecnología de la Información y Comunicación (TIC). Serán tratadas solamente especificaciones que sean relevantes para garantizar la interconectividad de sistemas, integración de datos, acceso a servicio de gobierno electrónico y gestión de contenido. La e-PING involucra los temas comprendidos en la segmentación, descrita en el punto 4 de este documento.

2.3. Asuntos no abordados

La e-PING no tiene el objetivo de estandarizar la forma de presentación de las informaciones de los servicios de gobierno electrónico, restringiéndose 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 lineamientos y políticas sobre la presentación y accesibilidad de los portales y locales de gobierno electrónico están disponibles en el portal del gobierno electrónico brasileño (http://www.governoeletronico.gov.br).

3. Políticas Generales

Cada uno de los sectores de la e-PING contiene un conjunto de políticas técnicas que orienta el establecimiento de las especificaciones de sus componentes. Los conjuntos específicos de cada segmento están basados en las siguientes políticas generales:

Alineamiento con la INTERNET: todos los sistemas de información de la administración pública deberán estar alineados con las principales especificaciones usadas en la Internet y con la *World Wide Web*.

Adopción del XML como estándar primario de intercambio de datos para todos los sistemas del sector público.

Adopción de navegadores (*browsers*) como principal medio de acceso: todos los sistemas de información de gobierno deberán ser accesibles, preferentemente, a través 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 disponible basada en navegadores.

Adopción de metadatos para los recursos de información del gobierno.

Desarrollo y adopción de un Estándar de Metadatos del Gobierno Electrónico – e-PMG, basado en estándares internacionalmente aceptados (http://www.eping.e.gov.br).

Desarrollo y mantenimiento de la Lista de Asuntos del Gobierno: Taxonomía de Navegación (LAG), que contemple, en una estructura de directorio, los temas relacionados con la actuación de gobierno (http://www.eping.e.gov.br).

Soporte de mercado: todas las especificaciones contenidas en la e-PING contemplan soluciones ampliamente apoyadas por el mercado. El objetivo a ser logrado es la reducción de los costos y de los riesgos en materia de la concepción y producción de servicios en los sistemas de informaciones gubernamentales.

Escalabilidad: las especificaciones seleccionadas deberán tener capacidad de atender modificaciones de demanda en el sistema, tales como, cambios de los volúmenes de datos, cantidad de transacciones o cantidad de usuarios. Los estándares establecidos no podrán ser un factor restrictivo, debiendo ser capaces de fundamentar el desarrollo de servicios que satisfagan desde necesidades claramente localizadas, involucrando pequeños volúmenes de transacciones y de usuarios, hasta demandas de alcance nacional, con tratamiento de gran cantidad de informaciones y participación de un elevado contingente de usuarios.

Transparencia: los documentos de la e-PING estarán a disposición de la sociedad, vía Internet, siendo previstos mecanismos de divulgación, recepción y evaluación de sugerencias. En este sentido, serán definidos – y divulgados para amplio conocimiento – plazos y compromisos para implantación y gestión de website dedicado en la Internet (http://www.eping.e.gov.br).

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 transitoria, manteniéndose las perspectivas de sustitución cuando haya condiciones de migración. Sin dejar de lado esas metas, serán respetadas las situaciones en que haya necesidad de consideración de requisitos de seguridad e integridad de informaciones. Cuando estén disponibles, soluciones en Software Libre son consideradas preferenciales, de acuerdo con política definida por el Comité Ejecutivo de Gobierno Electrónico (CEGE).

La e-PING mantiene total compatibilidad con las iniciativas de gobierno en el área de TIC. Un ejemplo que puede ser mencionado es la Guía de Migración de Software Libre del Gobierno Brasileño (http://www.governoeletronico.gov.br).

Garantía de la privacidad de información: todos los órganos responsables de la oferta de servicios de e-gob deben garantizar las condiciones de preservación de la privacidad de las informaciones del ciudadano, empresas y órganos de gobierno, respetando y cumpliendo la legislación que define las restricciones de acceso y divulgación.

4. Segmentación

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

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

4.1. Interconexión

El segmento "Interconexión" establece las condiciones para que los órganos de gobierno 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 federal debe considerar. Son tratados los estándares para:

- Seguridad de IP;
- Seguridad de Correo Electrónico;
- Criptografía;
- Desarrollo de Sistemas;
- Servicios de Red;
- Redes Inalámbricas;
- Obtención, Tratamiento y Archivo de Evidencias.

4.3. Medios de Acceso

En el segmento "Medios de Acceso", son explicitadas las cuestiones sobre los estándares de los dispositivos de acceso a los servicios de gobierno electrónico. En esta versión son abordadas las políticas y las especificaciones para estaciones de trabajo, tarjetas inteligentes (*smart-cards*), *tokens* y otras tarjetas, televisión digital y movilidad. En versiones futuras, serán tratados otros dispositivos. Es formado por cuatro subgrupos contemplando los siguientes componentes:

Estándares para acceso vía estaciones de trabajo:

- Navegadores (*browsers*);
- Conjunto de Caracteres y Alfabetos;
- Formato de Intercambio de Hipertexto;
- Archivos del Tipo Documento;
- Archivos del Tipo Planilla;
- Archivos del Tipo Presentación;
- Archivos del Tipo base 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 georreferenciación.

Tarjetas Inteligentes / *Tokens* / Otros:

- Definición de Datos;
- Aplicaciones (inclusive multi-aplicaciones);
- Componentes Eléctricos;
- Protocolos de Comunicación;
- Estándares de Interfaz Física;
- Seguridad;
- Infraestructura de la Terminal.

Movilidad:

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

TV Digital:

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

4.4. Organización e Intercambio de Informaciones

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

- Lenguaje para intercambio de datos;
- Lenguaje para transformación de datos;
- Definición de los datos para intercambio;
- Lista de Asuntos del Gobierno: Taxonomía para Navegación (LAG);
- 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 apoyar 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 punto son tratados los aspectos de gestión de la arquitectura e-PING, especificando la forma en que el gobierno brasileño pretende consolidar la implantación de las políticas y especificaciones técnicas como estándares efectivos adoptados tanto internamente, por los órganos que integran 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. Historial

La finalidad de la arquitectura e-PING es ser el paradigma de interoperabilidad para el gobierno federal, inicialmente en el ámbito del Poder Ejecutivo. La iniciativa de montaje de la arquitectura correspondió a tres órganos de la esfera federal:

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

Esos tres órganos organizaron un Seminario, con participación de entidades del gobierno federal, en el ámbito del Poder Ejecutivo, con el objetivo de formar un comité inter-órganos – denominado Comité Constituyente – para conducir los trabajos iniciales de montaje de la arquitectura.

Después de su institucionalización, por intermedio de la Disposición Ministerial Normativa nº 5, del 14 de julio del 2005, éste pasó a denominarse Coordinación de la e-PING. Además de los tres organizadores, participan en ese grupo los siguientes órganos: Presidencia de la República, Ministerio de Relaciones Exteriores, , Ministerio de Salud, Banco do Brasil, Caixa Econômica Federal, DATAPREV y Asociación Brasileña de Entidades Estaduales de Tecnología de la Información y Comunicación (ABEP).

El Comité estableció el siguiente programa de trabajo:

- Definición de la forma inicial de elaboración y gestión de la arquitectura e-PING;
- Definición de la segmentación de los asuntos a ser cubiertos por la e-PING;
- Creación de cinco grupos de trabajo responsables de las definiciones iniciales de políticas y especificaciones técnicas para cada uno de los segmentos;
- Definición 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, con miras a recoger aportaciones de la sociedad en general, sobre el contenido propuesto en la versión 0;
- Publicación de la versión 1, conjuntamente 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 fueron discutidas internamente en los grupos de trabajo y la coordinación de la e-PING;
- Realización de consulta pública y audiencias públicas con miras a recoger contribuciones de la sociedad en general, a cada nueva versión del documento de referencia;
- Publicación de 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 la construcción de la arquitectura de interoperabilidad del gobierno brasileño. La Gestión de la e-PING está basada en la forma implementada por el gobierno del Reino Unido, en operación desde el año 2000. Su grado de madurez es actualmente reconocido como referencia en el ámbito internacional.

5.2. Estrategia de Implantación

A 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, cada vez que haya modificaciones significativas.

A presente versión consolidó el trabajo de los grupos creados para los cinco segmentos definidos. Todo su contenido fue colocado a disposición para Consulta Pública, con el objetivo de obtener contribuciones a las propuestas de estándares publicadas en la versión 3.9.

5.3. Modelo de Gestión

En este punto son especificadas las formas de gestión de la arquitectura e-PING, siendo relacionadas las principales atribuciones y la forma de implementación de dichas 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**, se destacan:

- Definir los objetivos estratégicos y de gestión de gobierno para el establecimiento de los estándares;
- Administrar la arquitectura de interoperabilidad del gobierno brasileño, ofreciendo la infraestructura gerencial requerida 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 alinear los esfuerzos de interoperabilidad, asegurando 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 punto 2 - Alcance;
- Gerenciar y operacionalizar la divulgación de los estándares de la e-PING, considerando:
  - Creación y administración de un website en la Internet para la e-PING (http://www.eping.e.gov.br);
  - Coordinación del proceso de consultas públicas;
  - Coordinación del proceso de recepción y evaluación de propuestas de alteración y complementación;
  - Coordinación del proceso de solicitud de sugerencias para la e-PING;
  - Publicación de las versiones actualizadas de la e-PING y de las actualizaciones intermedias;
- Gerenciar la interacción con iniciativas de mismo propósito, conducidas por otros gobiernos, en el país y en el exterior;
- Incentivar la capacitación de los equipos del gobierno federal, actuando en conjunto con los órganos, tanto en la consideración de la e-PING en los planes específicos de entrenamiento de cada uno de ellos como en la realización de eventos corporativos dirigidos a la diseminación de los Patrones e-PING;
- Establecer, implantar y divulgar indicadores de seguimiento de los resultados obtenidos mediante la implantación de la e-PING;
- Gerenciar 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 escogidos a criterio de la coordinación de la e-PING tomando en cuenta su notorio reconocimiento internacional, competencia en su área de actuación y el establecimiento de estándares abiertos.
- Gerenciar la interacción con órganos de fomento nacionales e internacionales, para canalizar recursos, con miras a atender las necesidades de creación de infraestructura de la e-PING y promover la investigación y el desarrollo;

- Viabilizar la puesta en marcha y gerenciar el proceso de homologación de los estándares a ser establecidos para el gobierno;
- Viabilizar la puesta en marcha y gerenciar 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 adecuación a los Patrones e-PING; evaluar la posibilidad de auspiciar programas abarcadores que promuevan la utilización intensiva de los estándares propuestos.

Entre las **atribuciones de carácter técnico**, se destacan:

- Establecer las formas de elaboración y de mantenimiento de las políticas y especificaciones técnicas que integran la e-PING, considerando:
  - Identificación, creación y gestión de grupos de trabajo específicos;
  - Establecimiento de convenios y definición de instituciones de gobierno como responsables de las políticas y especificaciones técnicas de componentes específicos de los segmentos de interoperabilidad;
  - Identificación e implementación para alternativas de gestión técnica de los asuntos incluidos dentro del alcance de actuación de la e-PING;

- Coordinar el desarrollo y mantenimiento, en el ámbito del gobierno federal – Poder Ejecutivo, de:
  - Estándar de Metadatos de Gobierno (e-PMG);
  - Lista de Asuntos del Gobierno: Taxonomía para Navegación (LAG);
  - Catálogo de Estándares de Datos (CPD);
  - Catálogo de Referencia de los XML *Schemas*;
  - Demás estándares de Organización e Intercambio de Informaciones;
  - Estándares de Interconexión;
  - Estándares de Seguridad;
  - Estándares de Medios de Acceso a servicios electrónicos de gobierno;
  - Estándares de uso 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 de los segmentos técnicos definidos para la e-PING.

5.3.2. Responsabilidades

La estructura de gobierno creada para administración de la e-PING es presentada en el siguiente esquema simplificado.

Figura 2 – Administración de la e-PING.

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

e-PING.

La actuación de la Coordinación de la e-PING estará pautada por los siguientes puntos:

- Implantación de la arquitectura e-PING, realizando las actividades necesarias para la 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 diferentes 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 intermedias;
- Creación de un sello e-PING y administración de proceso que certifique la adhesión de determinado servicio o producto a la e-PING;
- Suministro de criterios y subsidios para la elaboración de la Ley Presupuestal 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 la consolidación de los estándares, como, por ejemplo, evaluación de propuestas de proyectos de e-gob orientados a la Administración Pública Federal, homologación de estándares y verificación de conformidad;
- Establecimiento de los puntos de contacto con los diferentes órganos de la Administración Pública Federal;
- Administración de los Grupos de Trabajo – GT, definiendo su composición y determinando los lineamientos de trabajo, basados en las políticas técnicas, generales y específicas, en las necesidades de gobierno y en el monitoreo del escenario tecnológico.

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

- Tratar los asuntos que integran los segmentos de la e-PING;
- Monitorear sistemáticamente el mercado, específicamente 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 el desempeño de sus atribuciones administrativas y técnicas.

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

5.4. Actividades adicionales

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

5.4.1. Selección y Homologación de Estándares Tecnológicos

Las políticas técnicas contenidas en este documento fundamentan los estándares de la e-PING, siendo como referencia en la selección de los componentes para los cuales son establecidas las especificaciones técnicas.

La e-PING prevé un proceso de análisis de los estándares aspirantes 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):** punto adoptado por el gobierno como estándar en la arquitectura e-PING, habiendo sido sometido a un proceso formal de homologación realizado por parte de una

institución del gobierno o por una otra institución con delegación formal para realizar el proceso. También es considerado homologado cuando está basado en una propuesta debidamente fundamentada por la coordinación del segmento, publicada en el website y aprobado por la Coordinación de la e-PING;

- **Recomendado (R):** punto que cumple con las políticas técnicas de la e-PING, es reconocido como un punto que debe ser utilizado en el ámbito de las instituciones de gobierno, pero que todavía no fue sometido a un proceso formal de homologación;
- **En Transición (T):** punto 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 en función de su uso significativo en instituciones de gobierno, tendiendo a ser desactivado cuando algún otro componente, en una de las dos situaciones anteriores, presente condiciones totales de substituirlo. Puede llegar a ser considerado un componente "recomendado" en el caso de que se adecue a todas las políticas técnicas establecidas. Cabe subrayar que el desarrollo de nuevo servicios o la reconstrucción de partes significativas de los ya existentes debe evitar el uso de componentes clasificados como transitorios;
- **En Estudio (E):** componente que está en evaluación y será encuadrado en una de las situaciones anteriores, cuando el proceso de evaluación esté concluido;
- **Estudio Futuro (F):** componente todavía no evaluado y que será objeto de estudio posterior.

El proceso de selección de los componentes adoptados por la e-PING y su consiguiente clasificación en las situaciones anteriormente señaladas, es de responsabilidad de los Grupos de Trabajo integrados por profesionales especialistas con actuación en el gobierno y en instituciones con las cuales sea establecido algún tipo de convenio o contrato específicamente con dicha finalidad.

La selección es hecha a partir de sugerencias formalizadas, demandas internas de los órganos del gobierno federal, Poder Ejecutivo, e investigaciones realizadas por los Grupos de Trabajo.

La homologación deberá ser objeto de un estudio más profundo por parte de los gestores de la e-PING. En virtud de la gran variedad de componentes tratados por la arquitectura, será necesario elaborar un sistema de homologación que contemple desde procesos en que será 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 convenios o acreditar instituciones para la elaboración de tests de conformidad, siempre definiendo cuales son los componentes que deben ser sometidos a procesos de homologación, cuales son los criterios de evaluación de los resultados y cuales son las condiciones de realización de los procedimientos.

La definición completa del proceso de selección y homologación, tomando en cuenta las especificidades de los segmentos, estará a cargo 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 un factor crítico de éxito de 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 creados con dicha finalidad, integrados por técnicos de gobierno con experiencia en procedimientos de esta naturaleza.

La forma preferencial de realización de ese tipo de procedimiento, entretanto, será la utilización de las estructuras propias en los órganos responsables de auditoría de sistemas. La Coordinación de la e-PING actuará en el sentido de sugerir los criterios básicos que deberán ser seguidos por los órganos. Con ese objetivo, fue constituido, por intermedio de la Disposición Ministerial nº 8, del 31

de octubre del 2008, de la SLTI/MP, un Grupo de Trabajo para estudiar, analizar y proponer modelo de auditoría en lo que atañe a la adhesión a los estándares de la e-PING. Dicha propuesta también contemplará el modelo de madurez de la e-PING (M-PING).

Otro tema que debe ser considerado será la colaboración de órganos de gobierno que actúan en el área, previéndose contactos con instituciones de otros Poderes y esferas de gobierno.

5.4.3. Creación y Mantenimiento del Website

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

- Divulgación completa de la documentación relativa a la arquitectura: versiones oficiales y respectivas actualizaciones de la arquitectura, versiones para consultas públicas, documentación técnica de apoyo, documentación legal e institucional conexa;
- Disponibilidad de las recomendaciones, determinaciones, especificaciones técnicas y políticas para validación, homologación y recepción de comentarios y sugerencias por parte de la sociedad;
- Publicación de solicitud de comentarios relativos a la especificación de componentes para la arquitectura;
- Disponibilidad de medio electrónico para recepción de sugerencias;
- Disponibilidad de links para documentos, estándares, normas o cualquier otro tipo de referencia que conste en la e-PING.

5.4.4. Seguimiento Legal e Institucional

La e-PING tendrá apoyo constante del equipo de Asesoramiento Jurídico del Ministerio de Planeamiento, Presupuesto y Gestión para garantizar la adhesión del contenido de los documentos que integran la arquitectura a las normas e instrumentos legales vigentes en el país.

Además, ese Asesoramiento tendrá también la responsabilidad de preparar toda la parte institucional necesaria para garantizar que las adecuaciones y recomendaciones de la e-PING integren el conjunto de instrumentos legales de TIC en el país.

La Coordinación de la e-PING podrá actuar para establecer una forma de colaboración con algún otro órgano de gobierno que tenga condiciones de proporcionar su estructura de apoyo jurídico para la realización de esta actividad.

5.4.5. Divulgación

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

- Realización de eventos específicos de divulgación, tales como Seminarios, *Talleres* y presentaciones en general;
- Participación en eventos gubernativas en el área de TIC y conexas;
- Participación en eventos dirigidos a públicos específicos;
- Publicación de todas las versiones de la e-PING y de las actualizaciones intermedias;
- Intercambio con otras esferas y otros Poderes de gobierno, con instituciones públicas, privadas y del tercer sector y con gobiernos de otros países.

5.4.6. Capacitación

Formarán parte de la agenda de puesta en marcha y Gestión de la e-PING eventos de capacitación. También está previsto el uso intensivo de Enseñanza a Distancia (EAD).

La Coordinación de la e-PING elaborará y publicará una programación mínima de entrenamiento, para que cada órgano de la APF tenga subsidios para planificar y estimar inversiones necesarias para capacitación de los profesionales involucrados en el proceso de adecuación a las recomendaciones de la e-PING.

Cada órgano de gobierno deberá observar las definiciones de estándar de la e-PING en la elaboración de sus planes particulares de capacitación, garantizando el entrenamiento adecuado para los componentes de sus equipos técnicos.

5.5. Relación con Gobierno y Sociedad

En este punto 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 el fomento y consolidación de la interoperabilidad en el sector público.

Aunque los lineamientos generales sean elaborados 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 esta naturaleza, se destacan:

- Contribuir al desarrollo y mejoramiento 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 adecuados a las recomendaciones de la e-PING;
- Disponer de un plan de implementación y adecuación de la infraestructura de TIC de la organización a la arquitectura e-PING;
- Asegurar que sean de dominio de los equipos de la institución, las habilidades para definir y utilizar las especificaciones requeridas para la interoperabilidad, suministrando soporte de entrenamiento cuando sea necesario;
- Establecer punto de contacto en las instituciones, para intercambio de informaciones y de necesidades con la Coordinación de la e-PING;
- Asignar y proporcionar recursos para dar soporte a sus procesos de adecuación a la e-PING;
- Aprovechar la oportunidad para racionalizar procesos (como resultado del aumento de la interoperabilidad) con miras a mejorar a calidad y reducir costos de prestación de los servicios de e-gob.

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 (Poder judicial, Legislativo) y otras esferas de gobierno (estadual y municipal), la adopción es facultativa

La coordinación de la e-PING actúa proactivamente con miras a la adopción de la e-PING por los entes integrantes de otras esferas y poderes, dada la relevancia 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, en especial, 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 en colaboración con la coordinación de la e-PING en la construcción de una matriz de intereses federativos para 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 por medio de los mecanismos de Consulta Pública, Solicitud de Comentarios y Recepción de Sugerencias.

Todas las entidades de esta naturaleza que participen en procesos de licitación para suministro de productos y servicios para el Poder Ejecutivo Federal deberán cumplir con a las especificaciones y recomendaciones de la e-PING.

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

5.5.4. Ciudadano

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

El gobierno debe incentivar a la sociedad a opinar, comentar, y contribuir con sugerencias de innovaciones que puedan ayudarlo a mejorar el acceso a 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

1. Interconexión

1.1. Interconexiones: Políticas Técnicas

Las Políticas Técnicas para interconexión son:

6.1.1. Los órganos de la APF deberán interconectarse utilizando IPv4 y planificar su futura migración para 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 e-mail deben utilizar SMTP/MIME para el transporte de mensajes. Para acceso a los mensajes, deben ser utilizados los protocolos POP3 y/o IMAP, siendo incentivado el uso de interfaces *web* para correo electrónico, observados, cuando sea necesario, los aspectos de seguridad.

6.1.3. Los órganos de la APF deben obedecer a la política de nombramiento de dominios del gobierno federal, establecida en la Resolución nº 7, que puede ser vista en la dirección electrónica

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

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

6.1.5. Los protocolos FTP y/o HTTP deben ser utilizados para transferencia de archivos, observando sus funcionalidades para recuperación de interrupciones y seguridad, cuando sea necesario. El HTTP debe tener prioridad para transferencias de archivos originarios de páginas de locales de la Internet.

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

6.1.7. A tecnología de *Web Services* es recomendada como estándar de interoperabilidad de la e-PING. Para tanto es adoptado el protocolo *Simple Object Access Protocol* (SOAP) para interconexión en arquitecturas descentralizadas y/o distribuidas.

1.2. Interconexiones: Especificaciones Técnicas

Tabela 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 buzón electrónico	Las reglas para definición de los nombres de los buzones postales de correo electrónico deberán seguir lo establecido en el documento “Buzones Individuales-Funcionales en el gobierno federal”, disponible en la dirección electrónica http://www.e.gov.br/correos/cp_individ.htm	**A**	

[1] Existen productos que pueden proporcionar acceso por el *browser* a los sistemas legados, sin necesidad de cambiar esos sistemas; típicamente estos productos pueden proporcionar acceso directo a las pantallas de legado o ser substituidos por interfaces gráficas (GUIs). Se debe prestar atención a cualquier implicación de seguridad con relación a su uso.

[2] Es posible tener acceso a las RFCs en http://www.ietf.org/rfc.html

Componente	Especificación	SIT	Observaciones
Transporte de mensaje electrónico	Utilizar productos de mensajería electrónica que soportan interfaces de acuerdo con SMTP/MIME para transferencia 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.	**R**	
Acceso a Buzón	A menos que las exigencias de seguridad lo determinen de otra forma, programas de correo que ofrecen facilidades de acceso a correspondencia deberán, como mínimo, estar de acuerdo con POP3 para acceso remoto a buzón postal. RFC correlacionada: RFC 1939 (actualizada por la RFC 1957 y RFC 2449).	**T**	
	Donde facilidades adicionales fueren necesarias, a menos que requisitos de seguridad lo determinen de forma contraria, los programas de correo que proveen facilidades avanzadas de acceso a correspondencia, deberán estar de acuerdo con IMAP para acceso remoto al buzón. 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) están definidos por la RFC 2778 y RFC 2779.	**T**	
	El modelo y requisitos para *Extensible Messaging and Presence Protocol* (XMPP) están definidos por la RFC 3920 y RFC 3921.	**R**	
Servicio de Mensajes Curtos	El Servicio de Mensajes Curtos (SMS) deberá utilizar el protocolo SMPP, como definido por el SMS *Foro* http://www.smsforum.net	**R**	

Tabela 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, supeditado a las limitaciones de seguridad.	**A**	
Intercomunicación LAN/WAN	IPv4 (RFC 791)	**A**	
	IPv6 (RFC 2460)	**E**	
Tráfico avanzado	Cuando sea necesario, el tráfico de red puede ser optimizado por el uso del MPLS (RFC 3031), debiendo éste poseer, como mínimo, cuatro clases de servicio.	**A**	
Calidad de servicio	Adopción de una arquitectura para servicios	**F**	

Componente	Especificación	SIT	Observaciones
	diferenciados por el uso del Diffserv (RFC 2475).		
Red metropolitana Inalámbrica	IEEE 802.16, de acuerdo con las determinaciones del *WiMax Foro* (http://www.wimaxforum.org) y con las normas de la Anatel (http://www.anatel.gov.br).	**E**	
Red local Inalámbrica	IEEE 802.11 B/G, de acuerdo con las determinaciones del *Wi-Fi Alliance* (http://www.wi-fi.org) y con las normas de la Anatel (http://www.anatel.gov.br).	**R**	

Tabela 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 traspaso de hipertexto	Utilizar HTTP/1.1 (RFC 2616).	**A**	
Protocolos de traspaso de archivos	FTP (RFC 959 y RFC 2228) (con re-inicialización y recuperación) y HTTP (RFC 2616) para traspaso de archivos.	**R**	
Directorio	LDAP v3 deberá ser utilizado para acceso general al directorio, de acuerdo con RFC 4510.	**A**	
Sincronismo de tiempo	RFC 1305 IETF - *Network Time Protocol* - NTP version 3.0. RFC 4330 IETF - *Simple Network Time Protocol* - SNTP version 4.0.	**R**	
Servicios de Nombramiento de Dominio	El DNS debe ser utilizado para resolución de nombres de dominios Internet, de acuerdo con la RFC 1035. Por su parte, las directrices de nombramiento de dominio del gobierno brasileño se encuentran en la Resolución Nº 7 del Comité Ejecutivo del Gobierno Electrónico, en la dirección electrónica https://www.planalto.gov.br/ccivil_03/Resolución/2002/RES07-02web.htm Además de dichas directrices, por decisión del Comité Gestor de la Internet en Brasil, el nombramiento de dominios obedece a las orientaciones del Ministerio de Planeamiento, Presupuesto y Gestión, a quien le compete gerenciar los dominios .GOV.BR. Las peculiaridades 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 los direcciones, son abordadas 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	**R**	

Componente	Especificación	SIT	Observaciones
	en la capa de aplicación (señalización) para crear, modificar y terminar sesiones con uno o más participantes.		
Protocolos de gestión de red	Uso del protocolo SNMP, definido por las RFCs 3411 y 3418, como protocolo de gerencia de red.	**F**	
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**	

1.3. Mensaje Electrónico (E-mail)

A efectos de claridad, la e-PING utilizará los siguientes conceptos:

Transporte de mensaje electrónico

El Transporte de mensaje electrónico es definido como la interfaz entre dos sistemas de correo.

Acceso a buzón

Acceso a buzón es definido como la interfaz entre un cliente de correo y un sistema de correo.

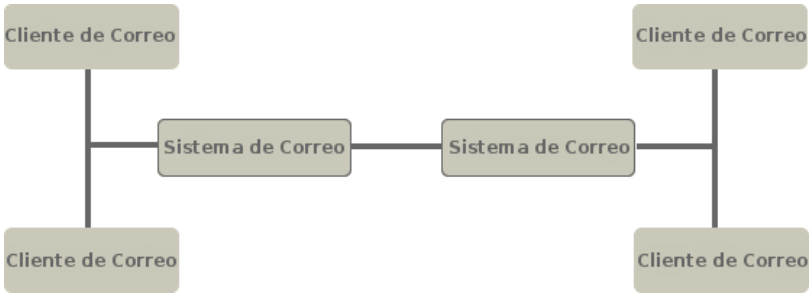

Figura 3 – Interfaces entre sistemas y clientes de Correo.

1.4. 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 lugar de utilizar circuitos dedicados o redes de paquetes para conectar redes remotas, se utiliza generalmente la infraestructura de la 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, porque los datos en tránsito pueden ser leídos por cualquier equipo, siendo necesario el uso de VPN.

Los túneles virtuales trafican datos criptografiados sobre redes públicas o privadas, formando un canal virtual seguro a través de dichas redes. Para tanto, son utilizados protocolos de circulación en túnel.

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

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

1.5. Redes *peer-to-peer*

Sistemas *Peer-to-Peer* (P2P) son sistemas distribuidos que consisten de nodos interconectados, con capacidad de organizarse a sí mismos en topologías de red, con el objetivo de compartir recursos tales como procesamiento, almacenamiento y ancho de banda, capaces de adaptarse a fallas y acomodar poblaciones transitorias de nodos, mientras mantienen conectividad y performance aceptables, sin depender de la intermediación o soporte de una autoridad (servidor) central.

Aunque sistemas P2P puedan contribuir al uso compartido de recursos y colaboración en gran escala, con control descentralizado y bajo acoplamiento, también están susceptibles a diversos problemas de seguridad, imposibilitando el uso sistemático de redes P2P. Este tema será abordado más adelante.

2. Seguridad

2.1. Seguridad: Políticas Técnicas

7.1.1. Los datos, informaciones y sistemas de información del gobierno deben ser protegidos contra amenazas para reducir riesgos y asegurar la integridad, confidencialidad y disponibilidad.

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

7.1.3. Las informaciones sensibles que transitan en redes inseguras, incluyendo las redes inalámbricas, deben ser criptografiadas, de modo adecuado, 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 de acuerdo con la clasificación de la información, niveles de servicio definidos y resultado del análisis de riesgos.

7.1.5. La seguridad debe ser tratada de forma preventiva. Para los sistemas que apoyan procesos críticos deben ser elaborados planes de continuidad, en los cuales serán tratados los riesgos residuales con miras a atender los niveles mínimos de producción.

7.1.6. La seguridad es un proceso que debe estar insertado 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 forenses, siendo imprescindible la adopción de un sistema de sincronismo de tiempo centralizado. También deben utilizarse mecanismos que garanticen la autenticidad de los registros almacenados, si fuera posible con firma digital.

7.1.8. Los servicios de seguridad de XML deben estar de acuerdo con las especificaciones del W3C.

7.1.9. En las redes inalámbricas metropolitanas se recomienda la adopción de valores randómicos en las asociaciones de seguridad, diferentes identificadores para cada servicio y la limitación del tiempo de vida de las claves de autorización.

7.1.10. El uso de criptografía y certificación digital, para la protección del tráfico, almacenamiento de datos, control de acceso, firma digital y firma de código, debe estar de acuerdo con las reglas de la 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.

7.1.12. Los usuarios deben conocer sus responsabilidades con relación a la seguridad y deben estar capacitados para la realización de sus faenas y utilización correcta de los medios de acceso.

7.1.13. Los Órganos de la APF, con miras al mejoramiento 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 ISO/IEC 15999-1:2007 y 15999-2:2008 – gestión de continuidad de negocios y NBR ISO/IEC 27005:2008 – gestión de riesgos de seguridad de la información.

2.2. Seguridad: Especificaciones Técnicas

Tabela 4 – Especificaciones para Seguridad – IP

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Transferencia de datos en redes inseguras por los protocolos HTTP, LDAP, IMAP, POP3, Telnet.	TLS – *Transport Layer Security*, RFC 2246 (http://www.ietf.org/rfc/rfc2246.txt). En el caso de que sea necesario el protocolo TLS v1 puede emular el SSL v3. HTTP sobre TLS, RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt) Pudiendo aplicar los siguientes algoritmos criptográficos: - algoritmos para cambio de claves de sesión, durante el *handshake*: RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA; - algoritmos para definición de clave de cifrado: RC4, IDEA, 3DES, 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/rfc4835.txt) para autenticación de encabezamiento del IP. IKE – *Internet Key Exchange*, RFC 4306 (http://www.ietf.org/rfc/rfc4306.txt), debe ser utilizado siempre que sea necesario para negociación de la asociación de seguridad entre dos entidades para intercambio de material de clave. 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 ser utilizado cuando sea apropiado para seguridad de mensajes generales de gobierno.	**A**	

Componente	Especificación	SIT	Observaciones
Seguridad de redes IPv6 en la capa 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 encabezamiento AH (*Authentication Header*) RFC 4302 (http://www.ietf.org/rfc/rfc4302.txt) o autenticación IP, y la seguridad del encapsulación IP, ESP. (*Encrypted Security Payload*) RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt).	**R**	

Tabela 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 buzones	El Acceso a buzón deberá ocurrir a través del cliente del software de correo electrónico utilizado, considerando las facilidades de seguridad nativas del cliente. Cuando no sea posible utilizar el cliente específico o sea necesario tener acceso a un buzón a través de redes no seguras (por ejemplo: Internet) se debe utilizar HTTPS de acuerdo con los estándares de seguridad de transporte descriptos en la RFC 2595 (http://www.ietf.org/rfc/rfc2595.txt), que aborda la utilización del TLS con IMAP, POP3 y ACAP.	**A**	
Contenido de e-mail	El S/MIME V3 deberá ser utilizado cuando sea apropiado para seguridad de mensajes generales de gobierno. Eso incluye 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**	
Transporte de e-mail	Utilizar SPF (*Sender Policy Framework*) en los términos de la RFC 4408 (http://www.ietf.org/rfc/rfc4408.txt).	**R**	
Firma	Utilizar certificado estándar ICP-Brasil para firma de e-mail, cuando sea exigido. De acuerdo con lo dispuesto en el Decreto 3.996 del 31 de octubre del 2001.	**A**	

Tabela 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, sin embargo, todavía no se transformaron en norma en la Administración Pública Federal.
Algoritmo para transporte de clave criptográfica de contenido/sesión	RSA	**A**	
algoritmos criptográficos basados en curvas elípticas	ECMQV y ECDH, ambos para acuerdo de claves, ECDSA, para firmas digitales, y ECIES para cifrado y transporte seguro de claves criptográficas. El uso de estos algoritmos está supeditado a reglamentación y normatización por la ICP-Brasil en lo que se refiere a los requisitos de seguridad.	**E**	
Requisitos de seguridad para módulos criptográficos	FIPS 140-2 – requisitos mínimos para las soluciones de almacenamiento de claves privadas y certificados digitales emitidos en el ámbito de la ICP – Brasil, que usan dispositivos tanto de *software* como de *hardware* tipo *token* o *smart card*. Adhesión al estándar: a. Seguir, como mínimo, las reglas establecidas para el nivel 1 o 2 de seguridad del estándar; b. Seguir, como mínimo, las reglas establecidas para el nivel 2 de seguridad del estándar FIPS 140-1 o 2, para verificación de violación en el *hardware* (*Tamper Evidence*).	**R**	

Tabela 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) de acuerdo con definido por el W3C http://www.w3.org/TR/xmldsig-core/	**A**	
Cifrado XML	Sintaxis y Procesamiento de Cifrado XML (XMLenc) de acuerdo con definido por el W3C http://www.w3.org/TR/xmlenc-core/	**R**	
Firma y cifrado XML	Transformación de desciframiento para firma XML de acuerdo con definido por el W3C http://www.w3.org/TR/xmlenc-decrypt	**R**	
Principales gerenciamientos XML cuando un ambiente PKI es utilizado	XML – *Key Management Specification* (XKMS 2.0) (Especificaciones de Gestión de Clave XML) de acuerdo con definido por el W3C http://www.w3.org/TR/xkms2/	**R**	
Autenticación y autorización de acceso XML	SAML – de acuerdo con lo definido por el OASIS cuando un ambiente ICP es utilizado http://www.oasis-open.org/committees/security/index.shtml	**R**	
Intermediación o Federación de Identidades	WS-Security 1.1 - esquema 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 se unirse a este componente después de estudios.
Navegadores	Solamente utilizar testigos de conexión de carácter permanente (*cookies*) con la concordancia del usuario. Resolución n. 7 del Comité Ejecutivo del Gobierno Electrónico (CAPÍTULO II, Art.7º).	**A**	

Tabela 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	Disposición Ministerial Normativa nº 2, del 3 de octubre del 2002 - Publicada en el Diario Oficial. del día 4 de octubre del 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 del 29/07/2002 – Comité Ejecutivo del Gobierno Electrónico Prácticas de Seguridad para Administradores de Redes Internet 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 1.2, 16 de mayo del 2003.	**R**	
Transferencia de archivos de forma segura	HTTPS RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt).	**R**	
Transferencia de archivos de forma segura	SSH FTP	**E**	Los documentos todavía están en el formato de borrador.
Transferencia de archivos de forma segura	Securing FTP with TLS, RFC 4217 http://www.faqs.org/rfcs/rfc4217.html y RFC 2246 http://www.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 *version* 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 de acuerdo con las resoluciones y demás normas de la ICP-Brasil.

Tabela 9 – Especificaciones para Seguridad – Redes Inalámbricas

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

Tabela 10 – Especificaciones para Seguridad – Obtención, Tratamiento y Archivo de Evidencias

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**	
Respuesta a incidentes	*Expectations for Computer Security Incident Response*, RFC 2350 (http://www.ietf.org/rfc/rfc2350.txt).	**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] 0 802.16 es definido por el IEEE como uma interfaz tecnológica para redes de acceso inalámbrico 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.

3. Medios de Acceso

3.1. Medios de Acceso: Políticas Técnicas

Las Políticas Técnicas para permitir el acceso a los servicios electrónicos del gobierno federal para la sociedad en general – ciudadanos, otras esferas de gobierno, otros Poderes, servidores públicos, empresas privadas y otras instituciones – son:

8.1.1. Los sistemas de información del gobierno deben ser proyectados de manera tal que la legislación brasileña sea respetada, suministrando recursos de accesibilidad a los ciudadanos portadores de necesidades especiales, a grupos étnicos minoritarios y los que están en riesgo de marginación social o digital. La atención en el mostrador de prestación de servicios debe ser considerada en todo su alcance, para posibilitar que los beneficios derivados del uso de los servicios de gobierno electrónico sean extendidos a los sectores de la población que no pueden tener acceso directo a dichos servicios por medio de los dispositivos previstos.

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

- cuando utilicen la Internet como medio de comunicación y estaciones de trabajo como dispositivo de acceso, serán preferentemente proyectados para proporcionar acceso a su informaciones con uso de tecnologías y protocolos de comunicación de la *web* basados en navegadores(*browsers*);
- cuando utilicen otros dispositivos de acceso, como, por ejemplo, teléfonos móviles celulares, televisión digital y tarjetas inteligentes (*smart cards*), podrán hacer uso de otras interfaces además de los navegadores *web*;
- deberán ser proyectados para colocar a disposición de los usuarios servicios de gobierno electrónico por intermedio de varios medios de acceso;
- deben prever la sustitución gradual de la sistemática de "login/seña" por autenticación de usuarios con utilización de certificado digital, preferentemente embarcados en tarjetas inteligentes o *tokens*, de acuerdo con estándares preconizados por la ICP – Brasil (referencia: http://w.ww.icpbrasil.gov.br/);
- nuevos servicios deberán ser creados ya con soporte a la autenticación de usuarios por medio de certificados digitales ICP-Brasil;
- en esta versión, la e-PING trata de los siguientes medios de acceso:
  - Estaciones de Trabajo;
  - Tarjetas Inteligentes, *Tokens* y otras Tarjetas;
  - Movilidad;
  - TV Digital.

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

8.1.4. Todos los sistemas de información del gobierno que suministren servicios electrónicos deben ser capaces de utilizar la Internet como medio de comunicación, directamente o por medio de servicios de terceros.

8.1.5. El desarrollo de los servicios de gobierno electrónico debe ser dirigido con miras a proveer atención a los usuarios que no tengan acceso a las tecnologías más recientes disponibles en el mercado. Por otro lado, también debe ser considerada la necesidad de atención a los usuarios portadores de necesidades especiales, requisito que incluye la utilización de recursos más sofisticados y de uso específico. Con miras a conciliar estas necesidades, deberán ser observadas las recomendaciones del Modelo de Accesibilidad de Gobierno Electrónico (e-MAG)[9].

8.1.6. Cuando la Internet sea usada como medio de comunicación, los sistemas de información del gobierno deben ser proyectados de manera tal que el máximo de informaciones pueda ser trabajado a partir de navegadores que satisfagan al estándar mínimo expresado por el soporte a las Especificaciones Técnicas pertinentes previstas en la sección 8.2. Complementariamente, la e-

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

PING recomienda que todo servicio de gobierno electrónico especifique, con claridad y, de preferencia, en su página inicial, las versiones mínimas de navegadores que soportan las funcionalidades solicitadas por el servicio asociado.

En la atención al estándar mínimo anteriormente mencionado, deben ser consideradas las excepciones que involucren temas de seguridad en el tratamiento de informaciones.

8.1.7. Cuando la Internet sea utilizada como medio de comunicación, *middleware* o *plug-ins* adicionales podrán ser utilizados, si no hubiera alternativa técnicamente viable, para optimizar a funcionalidad del navegador en las Estaciones de Trabajo. En este caso, ese software adicional deberá ser ofrecido sin el pago de tasa de licencia y deberá estar de acuerdo con 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 de la aplicación.

8.1.8. Los servicios de gobierno electrónico deben ser proyectados con miras a garantizar a los usuarios la autenticidad del contenido por medio de emisión de certificado digital, de acuerdo con estándares preconizados por la ICP – Brasil. Referencias: http://www.icpbrasil.gov.br/. En este sentido, todos los sitios *web* deberán obligatoriamente utilizar “https” en vez de “http”.

8.1.9. La necesidad de la sociedad, conjuntamente con la posibilidad del gobierno de desarrollar e implantar servicios electrónicos fundamentará la definición de las Especificaciones Técnicas exigidas por los medios de acceso disponibles. Técnicas de gestión de contenido y tecnologías que posibiliten adaptación de los dispositivos para soportar los servicios de gobierno electrónico podrán ser usadas para facilitar el acceso por medio del estándar mínimo de navegador w*eb* (de acuerdo con el punto 3. Políticas Generales) y para que sea viable el uso de quioscos públicos, de mostradores de atención 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 cuando sea técnica y económicamente viable, la construcción de adaptadores que permitan el acceso a las informaciones de los servicios electrónicos en *web* para una diversidad de ambientes, presentando tiempos de respuesta aceptables y costos reducidos.

Esos adaptadores pueden ser utilizados para filtrar, convertir y reformatear, dinámicamente, el contenido *web*, con miras a adaptarse a las exigencias y a las capacidades de exhibición del dispositivo de acceso. Pueden, también, posibilitar la modificación del contenido de una PÁGINA *web*, en base a protocolos de datos, XML, XSL, preferencias de usuario y parametrización de red y de dispositivos de acceso.

Esos adaptadores también podrán ser utilizados como forma alternativa para posibilitar el acceso a minorías étnicas, a portadores de deficiencia visual (por ejemplo: por la utilización de traductores de textos, fuentes y gráficos mayores, audio, etc.). Dichos aspectos son abordados por la Resolución nº 7 del Comité Ejecutivo de Gobierno Electrónico. Referencia:

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

8.1.11. Serán considerados preferenciales los tipos de archivo que tienen como estándar de empacotamiento el “xml”, para facilitar la interoperabilidad entre los servicios de gobierno electrónico.

8.1.12. Los servicios de gobierno electrónico que coloquen a disposición documentos a sus usuarios deberán hacerlo empleando en el propio enlace de acceso al documento información clara en lo que se refiere su proveniencia, versión, fecha de publicación y formato. Por fecha de publicación se entiende la fecha en que el documento fue publicado en diario oficial, para los casos en que esta medida fuera exigida, o la fecha de la puesta a disposición en el website, para los demás casos. Otras informaciones sobre el documento, tales como autor, redactor, emisor, fecha tópica o otras relevantes para su exacta caracterización, deberán constar en el campo propiedades del propio documento.

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

Para elaboración de borradores de documentos o trabajos que necesiten ser creados colaborativamente por más de una persona y/o órgano, pueden ser utilizados los formatos

previstos en el Cuadro 11.

Para la elaboración de la versión final de documentos, debe ser enviada a otros órganos o incluso archivada digitalmente, 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 firmados digitalmente por su autor, utilizando certificado ICP-Brasil.

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

Tabela 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*)	Ver punto 3. Políticas Generales.	**E**	
Conjunto de Caracteres 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), generado de acuerdo con especificaciones del W3C[10].	**A**	
	XHTML versiones 1.0 o 1.1 (.xhtml), generado de acuerdo con especificaciones del W3C[11].	**A**	
	XML versiones 1.0 o 1.1 (.xml), generado de acuerdo con especificaciones del W3C[12].	**A**	
	SHTML (.shtml).	**R**	
	MHTML (.mhtl o .mht)[13].	**T**	

[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 empacotamento de arquivos *web* de la Microsoft (*Mime Enscapsulation of Aggregate HTML Documents*).

Componente	Especificación	SIT	Observaciones
Archivos del Tipo Documento	XML versiones 1.0 o 1.1 (.xml), o con formatación (opcional) XSL (.xsl), generado de acuerdo con especificaciones del W3C[14].	**R**	
	Open Document (.odt), generado de acuerdo con especificaciones del estándar ISO/IEC 26300[15].	**A**	
	OpenOffice.org XML (.sxw), generado en el formato del OpenOffice versión 1.0.	**T**	
	Rich Text Format (.rtf).	**T**	
	PDF (.pdf) generado en formato hasta versión 1.3.	**T**	
	PDF versión abierta PDF/A[16].	**R**	
	Texto puro (.txt).	**A**	
	HTML versión 4.01 (.html o .htm), generado de acuerdo con especificaciones del W3C.	**R**	
	Microsoft Word document (.doc), generado en el formato del MS Office hasta versión 2000.	**T**	
Archivos del Tipo Planilla	Open Document (.ods), generado de acuerdo con especificaciones del estándar ISO/IEC 26300.	**A**	
	OpenOffice.org XML (.sxc). generado en el formato del Open Office versión 1.0.	**T**	
	Planilla MS Excel (.xls), generada en el formato del MS Office hasta versión 2000.	**T**	
Archivos del tipo presentación	Open Document (.odp), generado de acuerdo con especificaciones del estándar ISO/IEC 26300.	**A**	
	OpenOffice.org XML (.sxi), generado en el formato del Open Office versión 1.0.	**T**	
	HTML (.html o .htm), generado de acuerdo con especificaciones del W3C.	**R**	
	Presentación MS Power Point (.ppt), generado en el formato del MS Office hasta versión 2000.	**T**	

[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
Archivos del tipo "base de datos" para estaciones de trabajo	XML versiones 1.0 o 1.1 (.xml)	**R**	En las opciones texto plan (txt) y csv, debe ser incluido obligatoriamente el lay-out de los campos, para posibilitar su tratamiento.
	MySQL Database (.myd, .myi), generados en los formatos del MySQL, versión 4.0 o superior.	**R**	
	Texto puro (.txt)	**A**	
	Texto Puro (.csv) – comma-separated values	**A**	
	Archivo del Base (.odb), generado en el formato del BrOffice.org (o OpenOffice.org) versión 2.0 o posterior.	**R**	
	Archivo MS Access (.mdb), generado en el formato del MS Office, hasta versión 2000.	**T**	
Intercambio de informaciones gráficas e imágenes estáticas	PNG (.png), generado de acuerdo con especificaciones del W3C[17] – ISO/IEC 15948:2003 (E).	**A**	
	TIFF (.tif)[18].	**R**	
	SVG (.svg), generado de acuerdo con especificaciones del W3C[19].	**R**	
	JPEG File Interchange Format (.jpeg, .jpg o .jfif) [20].	**R**	
	Open Document (.odg), generado de acuerdo con especificaciones del estándar ISO/IEC 26300.	**A**	
	OpenOffice.org XML (.sxd), generado en el formato del Open Office versión 1.0.	**T**	
	XCF (.xcf), generado en el formato del GIMP versión 1.0 o superior.	**R**	
	BMP (.bmp).	**T**	
	GIF (.gif), generado de acuerdo con las especificaciones GIF87a y GIF89a[21].	**T**	
	Imagen Colores Photo-Panel (.cpt), generada en el formato de la suíte Corel Draw hasta versión 7.	**T**	
	Imagen Photoshop (.psd), generada en el formato del Adobe Photoshop hasta versión 4.	**T**	

[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/. Acceso el 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/. Acceso el 7 dic. 2005.

[20] *JPEG File Interchange Format (version 1.02) 1 September 1992. Disponible en:* http://www.jpeg.org/public/jfif.pdf. Acceso en: 7 dic. 2005.

[21] *Graphics Interchange Format (CompuServe/America Online, Inc.).*

Componente	Especificación	SIT	Observaciones
Gráficos vectoriales	SVG (.svg), generado de acuerdo con especificaciones del W3C.	**R**	
	Open Document (.odg), generado de acuerdo con especificaciones del estándar ISO/IEC 26300.	**R**	
	OpenOffice.org XML (.sxd), generado en el formato del Open Office versión 1.0.	**T**	
	Gráfico Corel Draw (.cdr), generado en el formato hasta versión 7.	**T**	
	MSX (.msx), generado en el formato de la suíte Corel Draw hasta versión 7.	**T**	
	Gráfico MS Vision (.vss o .vsd), generados en el formato hasta versión 2000.	**T**	
	Windows Metafile (.wmf).	**T**	
Especificación de Estándares de Animación	SVG (.svg), generado de acuerdo con especificaciones del W3C.	**R**	
	GIF (.gif), generado de acuerdo con la especificación GIF89a.	**T**	
	Shockwave Flash (.swf), generado en el formato del Macromedia Flash hasta versión 4, del Macromedia Shockwave versión 1.	**T**	

Componente	Especificación	SIT	Observaciones
Archivos del tipo audio y del tipo video	.mpg	**R**	
	Audio y video MPEG-4, Part.14 (.mp4)[22]	**R**	
	MIDI (.mid)[23]	**R**	
	Audio Ogg Vorbis I (.ogg)[24]	**R**	
	Audio-Ver Interleaved (.avi), con codificación Xvid.	**R**	
	Audio-Ver Interleaved (.avi), con codificación divX.	**T**	
	Audio MPEG-1, Audio Layer 3 (.mp3)[25]	**T**	
	Real Media (.rm o .rmm), generado en el formato de los aplicativos Real Audio Media Player, hasta versión 8.	**T**	
	Real Audio (.ra o .ram), generado en el formato de los aplicativos Real Audio Media Player, hasta versión 8.	**T**	
	WAVE (.wav)	**T**	
	Shockwave Flash (.swf), generado en el formato del Macromedia Flash, hasta versión 4 o por el Macromedia Shockwave, versión 1.	**T**	
	Windows Media Ver (.wmv), generado en el formato del Windows Media Player, hasta versión 6.4.	**T**	
	Windows Medí Audio (.wma), generado en el formato del Windows Media Player, hasta versión 6.4.	**T**	
	QuickTime (.mov), generado en el formato del Apple Quicktime, hasta versión 6.	**T**	
	QuickTime (.QT), generado en el formato del Apple Quicktime, hasta versión 6.	**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**	

[22] *ISO/IEC 14496-14:2003 - Information Technology - Coding of audio-visual objects - Part 14: MP4 file format.*
[23] Musical Instrument Digital Interface, conforme a especificação *The Complete MIDI 1.0 Detailed Specification*. Version 96.1, 2.ed., nov. 2001. Disponible en: http://www.midi.org/about-midi/specinfo.shtml. Acceso el 30 Mayo. 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/Color 1:1996.

Componente	Especificación	SIT	Observaciones
Informaciones georreferenciadas – estándares de archivos para intercambio entre estaciones de trabajo	GML versión 1.0 o superior[26].	**A**	Indicado para estructuras vectoriales complejas, involucrando primitivas geográficas como polígonos, puntos, líneas, superficies, colecciones y atributos numéricos o textuales sin límites de cantidad de caracteres.
	ShapeFile[27].	**A**	Indicado para estructuras vectoriales limitadas a líneas, puntos y polígonos, cuyos atributos textuales no superen los 256 caracteres. Puede almacenar también las dimensiones M y Z.
	GeoTIFF[28].	**A**	Indicado para estructuras matriciales limitadas a matrices de pixel.
	SFS.	**E**	SFS (*Sencillas Features Interfaz Standard*) es un estándar OGC (http://www.opengeospatial.org/standards/sfa) que define la forma en que las aplicaciones almacenarán (crear, actualizar y excluir) y tener acceso a facciones geográficas en sistemas gerenciadores de base de datos objetos-relacionales. OpenGIS *Sencillas Features* (facciones simples) son facciones espaciales descriptas utilizando elementos de datos como puntos, líneas y polígonos.
Programación Extendida (Plug-ins)	Asunto para consideración futura.	**F**	

3.3. Medios de Acceso: Especificaciones Técnicas para *Tokens,* Tarjetas Inteligentes y Tarjetas en General

Las especificaciones iniciales sobre tarjetas inteligentes y *tokens* recibieron como aumento las conclusiones del Grupo de Trabajo de la ICP-Brasil (Disposición ministerial nº 33, del 08 de abril del 2003) que usó como líneas básicas la familia ISO/IEC (7816 partes 1 a 6).

Las conclusiones de ese grupo también fueron utilizadas para la elaboración de los Manuales de Conductas Técnicas del ITI, documentos que establecen los requisitos técnicos a ser observados en los procesos de homologación de tarjetas inteligentes y *tokens* criptográficos en el ámbito de la

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

ICP-Brasil. Las especificaciones que constan en esos manuales también fueron utilizadas para la elaboración de este documento de referencia, específicamente para dispositivos criptográficos.

La homologación de sistemas y equipos de certificación digital en el ámbito de la ICP-Brasil fue instituida por la Resolución 36 del Comité Gestor de la ICP-Brasil, del 21/10/2004, siendo el Instituto Nacional de Tecnología de la Información (ITI), responsable de la conducción del proceso, mientras los Laboratorios de Estudios y Auditoría (LEA), creados por la Resolución 36, son responsables de los ensayos de conformidad.

Según aquella Resolución, los medios que almacenan los certificados digitales y respectivos lectores, además de los sistemas y equipos necesarios para la realización de la certificación digital, deberán obedecer a estándares y especificaciones técnicas mínimas, con el objetivo de garantizar su interoperabilidad y la confiabilidad de los recursos de seguridad de la información utilizados por ellos.

Por el reglamento, son pasibles de homologación medios tales como *tokens* criptográficos y *smart cards*, sistemas de firma electrónica, de autenticación de firma, de autoridades certificados y de registro, y equipos como los de HSM, sincronismo y sello de tiempo, entre otros. Los productos homologados por dicho proceso tendrán un laudo de conformidad emitido y utilizarán el sello de homologación y su correspondiente número de identificación.

Importante observar que los datos almacenados en un determinado tarjeta inteligente o *token* no podrán estar protegidos por cualquier tipo de licenciamiento que prohíba su lectura por cualquier otro software que no sea el del proveedor de aquella tarjeta inteligente o *token*.

La estandarización de esos dispositivos facilitará la inserción de Brasil en acuerdos internacionales relativos a la certificación digital, además de mantener la adhesión a los Estándares de Interoperabilidad de Gobierno Electrónico – e-PING y ayudar a masificar el uso de la certificación, porque entre otros aspectos podrá contribuir a baratear esta solución tecnológica.

En el contexto de la e-PING, fueron considerados, también: la ISO/IEC 7810, que define las propiedades físicas tales como flexibilidad, resistencia a la temperatura y dimensiones para tres distintos tipos de formato de tarjeta (ID-1, ID-2 y ID-3), el estándar PC/SC *Workgroup* y la estandarización para seguridad de dispositivos FIPS-140, del *National Institute of Standards and Technology* (http://www.nist.gov). Esos estándares fundamentales fueron utilizados en el Grupo de Trabajo de la ICP-Brasil con el objetivo de obtener mejor interoperabilidad en el universo de dispositivos de acceso del tipo tarjetas inteligentes y *tokens*, es decir, dispositivos que manejan certificados digitales. También fueron incorporadas las normas ISO para tarjetas magnéticas y tarjetas ópticas, los tradicionales y de bajo costo, éstos más audaces y de alto costo.

Para las versiones futuras de la e-PING, será establecida una agenda mínima que deberá revisar todo el cuadro de especificaciones e identificar, en el ámbito del gobierno federal, las acciones y planes de gobierno que usan algún tipo de tarjeta inteligente y que, consiguientemente, deben ser contemplados. Deberá ser ejecutada una investigación exhaustiva que suministre subsidios para la inclusión o no, en la e-PING, de los estándares de tarjetas efectivamente usados por los órganos de gobierno. Como ejemplo de esta situación, pueden ser mencionados los llamados *embossed smart cards* (ISO/IEC 7811), tarjetas grabadas en relieve, que no están contemplados en esta versión. En el caso de que fuera constatada, en esta investigación, el uso intensivo de ese tipo de dispositivo, será analizada la viabilidad de su inclusión en el conjunto de especificaciones tratadas por la e-PING.

También para las versiones futuras, serán analizados en profundidad los estándares típicamente orientados hacia la Comunidad Europea. Es el caso del eEurope, el *Open Smart Card Infrastructure for Europe* – versión 2" que asimila la tecnología de tarjetas sin contacto, presente en la ISO/IEC 14443. Lo mismo se aplica al estándar CALYPSO (*Fourth European Research and Technological Devepment Framework Program*) para sistemas de tarjetas (o tickets) sin contacto, orientados a sistemas de transportes públicos. Deberán ser evaluadas las estandarizaciones, sistemas de patentes y licenciamientos que puedan existan.

Tabela 12 – Especificaciones para Medios de Acceso – Tarjetas Inteligentes, *Tokens* y Tarjetas en General

Componente	Especificación	SIT	Aplicable a	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro			
Definición de Datos	Manuales de Conductas Técnicas del ITI – Volumen 1 (http://www.lea.gov.br/).	**A**	Todas las tarjetas y *tokens* que manejan certificados digitales.	
	Tarjetas de identificación **ISO/IEC 7816-6** Tarjetas de Circuito(S) Integrado(S) con contactos Parte 6: Elementos de datos intersectoriales.	**A**	Todos.	De acuerdo con opción del GT de la ICP-Brasil.
	Tarjetas de identificación **ISO/IEC 7812-1** Identificación de los emisores Parte 1: Sistema de Numeración.	**R**	Todos.	
	Tarjetas de transacciones financieras **ISO 9992-2**. Mensajes entre la tarjeta de circuito integrado y el dispositivo de aceptación de la tarjeta Parte 2: Funciones, mensajes (comandos y respuestas), elementos y estructuras de datos.	**F**	Todos.	
	Sistemas de tarjeta de identificación **BS EN 1546-3** – *Inter-sector electronic purse* - Parte 3: Elementos e intercambio de datos Sistemas de tarjeta de identificación **BS EN 1546-4** – *Inter-sector electronic purse* - Parte 4: Objetos de datos.	**F**	Todos.	La edición actual fue publicada en julio de 1999. La edición actual fue publicada en agosto de 1999.

Componente	Especificación	SIT	Aplicable a	Observaciones
Aplicaciones incluyendo multi-aplicaciones	Tarjetas de identificación **ISO/IEC 7816-4** Parte 4: Comandos intersectoriales para intercambio.	**A**	Tarjetas de Circuito(S) Integrado(S) con contactos.	Establece las estructuras de los archivos, asegura mensajes para tener acceso a archivos, inicialización de aplicativos de tarjeta, y canales lógicos para utilización cuando la tarjeta tenga más de un canal virtual de comunicación activo.
	Tarjetas de identificación **ISO/IEC 7816-5** Parte 5: Sistema de numeración y procedimiento de registro para identificadores de aplicación.	**R**		Comandos específicos de aplicación no son descriptos y de esta forma, el estándar trata los códigos de comando como aplicaciones específicas cuando no son definidas en esta parte.
	ISO/IEC 7816-7 Parte 7: Comandos intersectoriales para *Structured Card Query Language* (SCQL);	**R**		De acuerdo con opción del GT de la ICP-Brasil. La actual edición fue publicada en junio de 1994. Existe también una alteración ISO/IEC 7816-5/AM1 *Registered Application Provider Identifiers* (RDIs) (Identificadores de Proveedores de Aplicaciones Registradas) que fue publicada en diciembre de 1996.
	ISO/IEC 7816-11 Parte 11: Estructura para el manejo dinámico de aplicaciones múltiples en tarjetas de circuitos integrados.			
	Tarjetas de identificación **ISO/IEC 7813** – Tarjetas de transacciones financieras.	**R**	Tarjetas financieras.	
	Tarjetas de identificación de los emisores **ISO/IEC 7812-2** Parte 2: Procedimientos de aplicación y registro.	**R**	Todos.	
	Tarjetas de identificación **ISO/IEC 15693-4** – Tarjetas de circuito(s) integrado(s) sin contacto, Tarjetas de proximidad {*Vicinity Integrated Circuit(s) Cards* (VICC) (Tarjetas de Circuito(s) Integrado(s) de Proximidad} Parte 4: Registro de aplicaciones/emisores.	**R**	Tarjetas de circuito integrado de proximidad.	
	Sistemas de tarjeta de identificación **EN 1332-1**:1999 – Interfaz hombre-máquina – Parte 1: Principios de proyecto para interfaz de usuario Sistemas de tarjeta de identificación **EN 1332-4:**1999 – Interfaz Hombre-máquina – Parte 4: Codificación de	**R**	Todos.	

Componente	Especificación	SIT	Aplicable a	Observaciones
	exigencias de usuario para personas con necesidades especiales.			
Eléctrico	Tarjetas de identificación **ISO/IEC 7816-10** – Tarjetas de circuito(s) Integrado(s) con contactos – Parte 10: Señales electrónicos y respuesta para reinicialización para tarjetas síncronas. **ISO/IEC 7816—12** Parte 12: Interfaz USB.	**R**	Tarjetas de Circuito(s) Integrado(s) con contactos.	
	Tarjetas de identificación **ISO/IEC 14443-2** – Tarjetas de circuito(s) Integrado(s) sin contacto – Tarjetas de proximidad – Parte 2: Interfaz de potencia y señal de frecuencia de radio.	**R**	Tarjetas de circuito integrado de proximidad.	Esta parte define la interfaz de frecuencia de radio, y contiene dos técnicas de modulación muy diferentes (Tipos A y B) para la comunicación de datos entre tarjeta y terminal. El tipo A está basado en la tecnología Philips Mifare (ampliamente licenciada para otros fabricantes). El tipo B es un nuevo concepto. Estos dos tipos son procesados en paralelo en esta parte del estándar y de la parte 3. Además, algunos ítems específicos del Tipo A aparecen en la parte 4.
	Tarjetas de identificación **ISO/IEC 10536-3** Tarjetas de circuito(s) integrado(s) sin contacto {*Close Coupling Integrated Circuit(s) Cards* (CICC) (Tarjetas de Circuito(s) Integrado(s) de Acoplamiento Fuerte)} Parte 3: Procedimiento de señales electrónicos y reinicialización.	**F**	Tarjetas de circuito(s) integrado(s) de acoplamiento fuerte.	
	Tarjetas de identificación **ISO/IEC 15693-2** Tarjetas de circuito(s) integrado(s) sin contacto. Tarjetas de Proximidad {*Vicinity Integrated Circuit(s)* Cards (VICC) (Tarjetas de Circuito(s) Integrado(s) de Proximidad)}: Parte 2: Interfaz y inicialización por el aire;	**R**	Tarjetas de circuito(s) integrado(s) de proximidad sin contacto.	
Protocolos de comunicaciones	Tarjetas de identificación **ISO/IEC 7816-3** Parte 3: Protocolos de señales y transmisiones electrónicas.	**R**	Tarjetas de circuito(s) integrado(s) con contactos.	De acuerdo con opción del GT de la ICP-Brasil
	Tarjetas de identificación **ISO/IEC 14443-3** - Tarjetas de	**R**	Tarjetas de circuito(s)	Esta parte da continuidad al duopolio de los Tipos A y B,

Componente	Especificación	SIT	Aplicable a	Observaciones
	circuito(s) integrado(s) sin contacto – Tarjetas de proximidad – Parte 3: Inicialización y anticolisión. Tarjetas de identificación **ISO/IEC 14443-4** – Tarjetas de circuito(s) Integrado(s) sin contacto – Tarjetas de proximidad – Parte 4: Protocolos de transmisión.		integrado(s) de proximidad.	definiendo procedimientos de inicialización y anticolisión. de tarjetas y protocolos básicos de comunicaciones. Los procedimientos de anticolisión son métodos utilizados para identificar y seleccionar una tarjeta cuando varias tarjetas estuvieran activas dentro del campo RF de la Terminal. Éste contiene informaciones de alto nivel (nivel de mensaje) de protocolo de transmisión de datos, equivalentes al protocolo T=1 del ISO/IEC 7816, y es un puente sobre el ISO 7816-4. Solamente para tarjetas Tipo A el ISO/IEC 14443-4 incluye un procedimiento de inicialización de protocolo.
	Tarjetas de identificación **ISO/IEC 15693-3** – Tarjetas de circuito(s) Integrado(s) sin contacto – Tarjetas de proximidad – Parte 3: Protocolo de anticolisión y transmisión.	**R**	Tarjetas de circuito integrado de proximidad. sin contacto.	
	Mensaje originado en tarjeta de transacción financiera **ISO 8583** – especificación de mensaje de intercambio.	**F**	Todos.	
	Tarjetas de transacciones financieras **ISO 9992-1** – Mensajes entre la tarjeta de circuito integrado y el dispositivo de aceptación de la tarjeta – Parte 1: Conceptos y estructuras; ISO 9992-2 Parte 2: Funciones, mensajes (comandos y respuestas), elementos y estructuras de datos.	**F**	Todos.	
	Tarjetas de transacciones financieras **ISO 10202-2** Arquitectura de seguridad de sistemas de transacción financiera utilizando tarjetas de circuito integrado. Parte 2: Proceso de transacción; ISO 10202-6 **Parte 6: Verificación del portador de la tarjeta.**	**R**	Todos.	
	Tarjetas de identificación **ISO/IEC 10536-4** tarjetas de	**F**	Tarjetas de circuito(s)	

Componente	Especificación	SIT	Aplicable a	Observaciones
	circuito(s) integrado(s) sin contacto {*Close Coupling Integrated Circuit(s) Cards* (CCIC) (Tarjetas de Circuito(s) Integrado(s) de Acoplamiento Fuerte)}. Parte 4: Respuesta a protocolos de reinicialización y transmisión.		integrado(s) de acoplamiento fuerte.	
Los Estándares de físico/físico y de interfaz cubren las dimensiones de la tarjeta; localidad y *lay-out* de contactos.	**Características físicas** Tarjetas de identificación **ISO/IEC 7810**	**R**	Todas los tarjetas de contacto y combinación	Para asegurar que puedan ser leídos en lectora estándar, todas los tarjetas deben seguir el formato ID-1 de acuerdo con lo definido en este estándar.
	Tarjeta Magnética **ISO/IEC 7811**, partes 2, 4 y 5: definen las propiedades, posicionamiento y codificación (*coding*) de la banda magnética de la tarjeta.	**R**	Todas las tarjetas con banda magnética.	
	Tarjeta de memoria óptica **ISO/IEC 11693** y **11694.**	**F**	Tarjetas ópticas.	Tarjetas que soportan el almacenamiento de muchos *megabytes*.
	Tarjetas de identificación **ISO/IEC 7816-1** Parte 1: Características físicas Tarjetas de identificación **ISO/IEC 15693-1** - Tarjetas de circuito(s) integrado(s) sin contacto – Tarjetas de proximidad - Parte 1: Características físicas. Tarjetas de identificación **ISO/IEC 7816-2** – Tarjetas de circuito(s) integrado(s) con contactos Parte 2: Dimensiones y localización de los contactos.	**A**	Tarjetas de circuito(s) integrado(s) con contactos.	Esta parte suplementa el ISO/IEC 7810, estableciendo las características físicas particulares de las tarjetas de CI / con contactos. De acuerdo con la opción del GT de la ICP-Brasil y Manual de Conductas Técnicas del ITI – Volumen I.
	Tarjetas de identificación **ISO/IEC 14443-1** – Tarjetas de circuito(s) integrado(s) sin contactos – Tarjetas de proximidad - Parte 1: Características físicas.	**R**	Tarjetas de circuito integrado de proximidad.	Esta parte suplementa las características físicas definidas en el ISO/IEC 7810.
	Tarjetas de identificación **ISO/IEC 15693-1** – Tarjetas de circuito(s) integrado(s) sin contacto – Tarjetas de proximidad - Parte 1: Características físicas. Esta parte del **ISO/IEC 15693** fue publicada el 15-07-2000.	**R**	Tarjetas de circuito(s) integrado(s) de proximidad sin contacto.	Esta parte del **ISO/IEC 15693** fue publicada el 15-07-2000.
	Tarjetas de identificación **ISO/IEC 10536-1** – Tarjetas de circuito(s) integrado(s) sin	**F**	Tarjetas de circuito(s) integrado(s) de	

Componente	Especificación	SIT	Aplicable a	Observaciones
	contacto Parte 1: Características físicas; **ISO/IEC 10536-2** Parte 2: Dimensiones y localización de las áreas de acoplamiento.		acoplamiento fuerte.	
	Identificadores táctiles. Sistemas de Tarjetas de identificación **BS EN 1332-2** – Interfaz hombre-máquina Parte 2: Dimensiones y localización - un identificador táctil para tarjetas ID-1.	**F**	Cuando la grabación en relieve no es utilizada y existe, es solicitado al usuario que introduzca la tarjeta en un determinado sentido, un identificador táctil deberá ser suministrado como auxilio para los portadores de deficiencias visuales.	Algunos equipos de personalización de tarjetas, a menos que sean modificados, podrán tener dificultad en el procesamiento de tarjetas con identificadores táctiles del tipo '*notch*' ('relieve'). Un acuerdo, por lo tanto, debe ser realizado con el proveedor del servicio de personalización para la utilización de dichas tarjetas.
Seguridad	Tarjetas de identificación **ISO/IEC 7816-8** – Tarjetas de circuito(s) integrado(s) con contactos. Parte 8: Comandos de seguridad intersectoriales ISO/IEC 7816-9 Parte 9: Comandos adicionales intersectoriales y atributos de Seguridad. Tarjetas de identificación **ISO/IEC 7816-11** – Tarjetas de circuito(s) integrado(s) con contactos - Parte 11: Verificación personal a través de métodos biométricos. Tarjetas de identificación **ISO/IEC 7816-15** – Tarjetas de circuito(s) integrado(s) con contactos - Parte 15: Información de dispositivo Criptográfico en tarjetas CI.	**A**	Tarjetas de circuito(s) integrado(s) con contactos.	
	Tarjetas de transacción financiera **ISO 10202** Arquitectura de seguridad de sistemas de transacción financiera utilizando tarjetas de circuito integrado	**F**	Todos.	

Componente	Especificación	SIT	Aplicable a	Observaciones
	Parte 1: Ciclo de vida de la tarjeta; Parte 2: Principios y resumen general; Parte 3: Listas de clave criptográfica; Parte 4: Módulos seguros de aplicación; Parte 5: Utilización de algoritmos; Parte 6: Verificación del portador de la tarjeta; Parte 7: Gestión de clave.			
Infraestructura de la Terminal	Sistemas de tarjetas de identificación EN 1332-3:1999 – Interfaz Hombre-máquina – Parte 3: Teclados.	**R**	Todos.	
	Estándares PC/SC. Estándares del Consorcio Grupo de Trabajo PC/SC Especificación de Interoperabilidad para ICCs y Sistemas de Computadora Personal Parte 1. Introducción y Visión General de la Arquitectura Parte 2. Requisitos de Interfaz para Tarjetas Compatibles con CI / y Dispositivos de Interfaz Parte 3. Requisitos para Dispositivos de Interfaz Conectados a PC Parte 4. Consideraciones del proyecto IFD e Información de Referencia del Proyecto Parte 5. Definición del Gerenciados de Recursos ICC Parte 6. Definición de la Interfaz del Proveedor de Servicio ICC Parte 7. Consideraciones del Proyecto de Dominio / Desarrollador de la Aplicación Parte 8. Recomendación para la Implementación de Dispositivos de Seguridad y Privacidad ICC.	**A**	Todos.	Para uso general en PCS.
	Manual de Conductas Técnicas del ITI – Volumen I.	**A**	Tarjetas con capacidad de gestión de certificados digitales.	
	Estándar FIPS-140-2.	**A**	Todos.	Según el punto 1 del GT de la ICP-Brasil: seguir como mínimo las reglas establecidas para el nivel 1 de seguridad del FIPS-140-2. Seguir como

Componente	Especificación	SIT	Aplicable a	Observaciones
				mínimo las reglas establecidas para el nivel 2 de seguridad para verificación de violación del hardware.

3.4. Medios de Acceso: Especificaciones Técnicas para Movilidad

El número de aparatos de telefonía móvil ya es mayor que el de los aparatos de la telefonía fija, convirtiéndose así en un amplio canal de comunicación con el ciudadano. Además, la oferta de computadoras personales con recursos de movilidad, a precios más accesibles para el ciudadano, está creciendo cada día que pasa, motivada por incentivos gubernamentales y reducción del costo de producción. Así, es un gran reto para el gobierno posibilitar el acceso de la sociedad a los productos y servicios del gobierno electrónico, a partir de dispositivos móviles, en general portátiles, como *notebooks*, teléfonos móviles celulares, *smartphones* y similares.

Tabela 13 – 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		**F**	
Navegación		**F**	
Estándar Hipertexto		**F**	
Programación extendida		**F**	
Mensajería		**F**	
Archivos de Video y Sonido		**F**	
Archivos de Imagen		**F**	
Archivos de Oficina		**F**	
Lector PDF		**F**	

3.5. Medios de Acceso: Especificaciones Técnicas para TV Digital

Tomando en cuenta el alto nivel de la presencia de aparatos receptores de señales de televisión en los hogares brasileños y la eminente puesta en marcha del Sistema Brasileño de TV Digital, que permite la interacción con los telespectadores, éste se convierte en un canal de gran potencial para la relación entre gobierno y sociedad. Así, surgen nuevas posibilidades de acceso a los productos y servicios del gobierno electrónico, a partir de los nuevos aparatos de TV Digital.

Su utilización ofrece mucho más que una señal de calidad, ofrece interactividad y accesibilidad con Servicios Comerciales tales como: compras, juegos y acceso a bancos, y también Servicios Sociales, tales como: consultas al FGTS, PIS/, Programas Sociales del gobierno, tele-educación entre otros, haciendo que los ciudadanos pasen de una actividad esencialmente pasiva a una actividad participativa.

La TV Digital. se convierte en un estándar de comunicación en diferentes perspectivas como: la perspectiva tecnológica, con la migración del sistema analógico al digital; la perspectiva económica, con la migración de nuevas posibilidades de servicios y negocios; la perspectiva social, con oferta de diversidad de contenidos e inclusión digital al utilizar la internet a través del aparato de TV; la política, con la posibilidad de incentivar la discusión de un nuevo hito regulatorio y la perspectiva comportamental, con la posibilidad de participación activa de los telespectadores mediante el uso de diferentes niveles de interactividad en la TV Digital.

Para ajustarse a los temas técnicos, la Asociación Brasileña de Normas Técnicas – ABNT, elaboró diversas normas, tal como son presentadas en el siguiente cuadro:

Tabela 14 – Normas ABNT sobre TV Digital

Referencia	Título
ABNT NBR15601	Televisión digital terrestre – Sistema de transmisión.
ABNT NBR 15602-1	Televisión digital terrestre – Codificación de video, audio y multiplexación – Parte 1: Codificación de video.
ABNT NBR 15602-2	Televisión digital terrestre – Codificación de video, audio y multiplexación – Parte 2: Codificación de audio.
ABNT NBR 15602-3	Televisión digital terrestre – Codificación de video, audio y multiplexación – Parte 3: Sistema de Multiplexación de señales.
ABNT NBR 15603-1	Televisión digital terrestre – Multiplexación y servicios de información (SI) – Parte 1: Servicios de información del sistema de radiodifusión.
ABNT NBR 15603-2	Televisión digital terrestre – Multiplexación y servicios de información (SI) – Parte 2: Sintaxis y definiciones de la información básica de SI.
ABNT NBR 15603-3	Televisión digital terrestre – Multiplexación y servicios de información (SI) – Parte 3: Sintaxis y definición de la información extendida del SI.
ABNT NBR 15604	Televisión digital terrestre – Receptores.
ABNT NBR 15605	Televisión digital terrestre – Tópicos de seguridad.
ABNT NBR 15606-1	Televisión digital terrestre – Codificación de datos y especificaciones de transmisión para radiodifusión digital – Parte 1: Codificación de datos.
ABNT NBR 15606-2	Televisión digital terrestre – Codificación de datos y especificaciones de transmisión para radiodifusión digital – Parte 2: Ginga-NCL para receptores fijos y móviles – Lenguaje de aplicación XML para codificación de aplicaciones.
ABNT NBR 15606-3	Televisión digital terrestre – Codificación de datos y especificaciones de transmisión para radiodifusión digital – Parte 3: Especificación de transmisión de datos.
ABNT NBR 15606-5	Televisión digital terrestre – Codificación de datos y especificaciones de transmisión para radiodifusión digital – Parte 5: Ginga-NCL para receptores portátiles – Lenguaje de aplicación XML para codificación de aplicaciones.
ABNT NBR 15607-1	Televisión digital terrestre – Canal de interactividad – Parte 1: Protocolos, interfaces físicas e interfaces de software.
ABNT NBR 15608	Televisión digital terrestre – Guía de elaboración.
ABNT NBR 15609	Televisión digital terrestre – Suíte de tests (en elaboración).
ABNT NBR 15610	Televisión digital terrestre – Ensayos para receptores (en elaboración).

Tabela 15 – Especificaciones para Medios de Acceso – TV Digital

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Middleware		**F**	
Codificación de audio		**F**	
Codificación de video		**F**	
Capa de Transporte		**F**	
Transmisión		**F**	

4. Organización e Intercambio de Informaciones

4.1. 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 XML *Schema* 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.

4.2. Organización e Intercambio de Informaciones: Especificaciones Técnicas

Tabela 16 – 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 intercambio	XML *Schema* tal como es 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*) Tal como es definido por la W3C.	**F**	
Elementos de Metadatos para gestión de contenidos	e-PMG – Estándar de Metadatos para el Gobierno Electrónico.	**E**	
Taxonomía para navegación	LAG - Lista de Asuntos del Gobierno, Versión 1.0. De acuerdo con definición en http://www.eping.e.gov.br	**A**	

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

4.3. Notas sobre XML y Middleware

Ni todos los sistemas necesitan tener capacidad de comunicarse directamente en XML, tal como es representado en la Figura 5. Cuando fuera apropiado, es aceptable la utilización de *Middleware* de acuerdo con la ilustración de la Figura 6.

Aunque las siguientes configuraciones presenten soluciones potenciales, el modelo XML directo (Figura 5) es preferencial, siendo posible la utilización del modelo indirecto, presentado en la Figura 6, en los casos en que existan razones fundamentales que justifiquen su uso.

Figura 4 – Modelo XML Directo – Intercambio Directo.

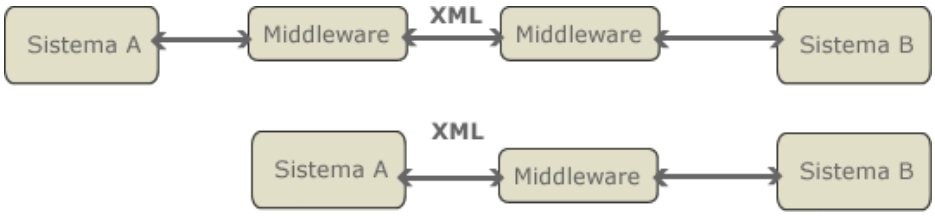

Figura 5 – Intercambios vía *Middleware.*

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

4.4. Nota sobre el uso de UML

Para la descripción de datos complejos con miras a mejor explicitación es recomendado, cuando corresponda, el uso del diagrama de clases de la UML.

5. Áreas de Integración para Gobierno Electrónico

5.1. Áreas de Integración para Gobierno Electrónico: Políticas Técnicas

10.1.1. Como directriz técnica para integración de sistemas de información se recomienda la gradual adopción de la Arquitectura Orientada a Servicios (SOA), teniendo como referencia para implementación, la iniciativa "**Arquitectura Referencial de Interoperabilidad de los Sistemas Informatizados de Gobierno (AIRE)**", que es un modelo de Arquitectura Orientada a Servicios, adaptado a la realidad de los Sistemas Informatizados del Gobierno Federal, que está disponible en el portal: http://i3gov.softwarepublico.gov.br/i3gov/.

10.1.2. La arquitectura e-PING - Estándares de Interoperabilidad de Gobierno Electrónico preconiza la adopción del XML y el desarrollo de XML *Schemas* como fundamentos para la integración e interoperabilidad electrónica del gobierno.

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

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

10.1.5. Con relación a los datos esenciales y XML *Schemas* referentes a aplicaciones dirigidas al área de Actuación de Gobierno, el segmento actuará buscando la identificación, seguimiento de la producción y análisis de contenidos de interés de la Administración Pública, en articulación con grupos representativos del gobierno y de la sociedad, reportándose a instancias competentes en lo que atañe a la priorización.

10.1.6. El Catálogo de Estándares de Datos y el Catálogo de XML *Schemas* tienen fuerte interconexión. Así, se debe observar la compatibilidad entre sus ítems. No se recomienda la inclusión de un componente, aisladamente, en apenas uno de los catálogos;

10.1.7. Los Catálogos Estándar de Datos, XML *Schemas* y Servicios Interoperables (*Web Services*) estarán disponibles en el website de la e-PING.

10.1.8. Datos de interés amplio del gobierno deben ser colocados a disposición en los Catálogos Estándar de Datos y XML *Schemas*, de acuerdo con las reglas de utilización de estas herramientas.

10.1.9. El Catálogo Estándar de Datos y el Catálogo XML *Schemas* son elementos centrales del ambiente de interoperabilidad del Gobierno Federal. Su utilización es considerada equivalente a la situación Adoptado (A).

10.1.10. Las Especificaciones Técnicas referentes a XML *Schemas* que constan en el Segmento Organización e Intercambio de Informaciones deben ser atendidas por los proponentes.

10.1.11. Los Servicios Interoperables (*Web Services*) de interés general deben ser colocados a disposición en el Catálogo de Servicios, sin embargo, es necesario observar reglas de utilización de los servicios de acceso restricto definidas por los respectivos órganos;

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

5.2. Áreas de Integración para Gobierno Electrónico: Nota explicativa sobre los Catálogos Estándar de Datos y XML *Schemas*

5.2.1. Consideraciones Iniciales

Los Catálogos Estándar de Datos y XML *Schemas* están disponibles en el portal del Gobierno Electrónico en el website http://www.governoeletronico.gov.br/.

El Catálogo Estándar de Datos tiene el objetivo de establecer estándares de tipos e ítems de datos que se aplican a las interfaces de los sistemas que forman parte del sector público, estando dividiendo en dos documentos:

- Volumen 1, que establece los principios generales, es decir, las razones, abordaje y reglas para la aplicación de los estándares de Tipo y Ítems de Datos; y
- Volumen 2, que presenta los Tipos e Ítem de Datos estandarizados.

El Catálogo XML *Schemas* tiene el objetivo de establecer estándares de XML *Schemas* que se aplican a las interfaces de sistemas que apoyen la oferta de servicios de Gobierno Electrónico.

El Catálogo XML *Schemas* contiene los estándares aceptados, en la forma de XML *Schemas* para intercambio de datos involucrando al sector público. Dichos estándares tanto pueden constituir un único esquema, como un conjunto de XML *Schemas*, siempre y cuando el conjunto se refiera a una misma temática dentro del área de Integración asociada.

La publicación de XML *Schemas* no implica automáticamente garantía de acceso a los contenidos correspondientes o servicios asociados, para el que pueden ser definidas reglas específicas por el respectivo gestor.

5.2.2. Propiedad y Responsabilidad

La Coordinación de la e-PING es responsable de estos Catálogos, en especial de la definición de las reglas para la gestión de los procesos de cambios y de fomentar que los estándares sean usados en desarrollo futuros.

En este sentido, se recomienda que el desarrollo o mantenimiento de sistemas que apoyen la oferta de servicios de Gobierno Electrónico conexos con área/subáreas de actuación de gobierno contempladas en el Catálogo consideren los XML *Schemas* publicados.

El desarrollo y mantenimiento de estos Catálogos son responsabilidad del Grupo Áreas de Integración para Gobierno Electrónico que tiene la participación de diferentes segmentos del gobierno en las esferas federal y estadual.

5.2.3. Mecanismos de Gestión del Catálogo de XML *Schemas*

Las entradas al Catálogo de XML pueden ocurrir a través de las siguientes situaciones:

a) Propuesta seguida de aceptación de propuesta de contenido para el Catálogo de Estándares de Datos (CPD);

b) Sometimiento a la consideración, seguida de aceptación de propuesta de contenido, de la Arquitectura Referencial de Interoperación de los Sistemas Informatizados de Gobierno (AR);

c) Sometimiento, por profesional vinculado al sector público, de contenido, directamente al Catálogo de XML *Schemas*, a través de formulario electrónico disponible en el website de la e-PING.

La propuesta de registro de XML *Schemas* será sometida al análisis de los integrantes del Grupo Áreas de Integración para Gobierno Electrónico por medio de formulario electrónico específico, disponible en el website de la e-PING (www.e-PING.e.gov.br). Serán mantenidas en el Catálogo solamente las propuestas aceptadas, siendo que las que todavía estuvieran en estudio, las rechazadas, así como las versiones anteriores de XML *Schemas* aceptadas serán mantenidas en ambiente “de tests” que será oportunamente concebido e implementado.

Los criterios de evaluación empleados incluirán:

- reconocimiento por la comunidad usuaria;
- acuerdo del gestor del área/subárea (en el caso de que él no sea el ofertante); y
- adhesión a los estándares de la e-PING.

O sea, está previsto el sometimiento a consideración en que el ofertante de determinado XML

Schemas no sea el gestor del área, pero tendrá como condición adicional de aceptación la concordancia del gestor, a partir de interlocución realizada por el propio ofertante y/o por el Grupo Áreas de Integración para Gobierno Electrónico.

Solicitudes de alteración para XML *Schemas* ya publicados serán analizadas preliminarmente por los integrantes del Grupo Áreas de Integración para Gobierno Electrónico. La decisión de aceptación le corresponderá a la Coordinación Central de la e-PING, que podrá adoptar los cambios propuestos de acuerdo con su alcance e impacto o someterlas a consulta pública, a través del website http://www.governoeletronico.gov.br.

Para esta versión del documento e-PING, se optó por colocar a disposición el contenido del Catálogo XML *Schemas* apenas en la herramienta desarrollada para la gestión de éste, siendo suprimida la publicación en el documento de las referencias a los mismos. Esta opción está basada en el objetivo de incentivar el uso y mantenimiento de los XML *Schemas* en la herramienta apropiada y permitir más flexibilidad de la gestión de los XML *Schemas*.

5.3. Áreas de Integración para Gobierno Electrónico: Especificaciones Técnicas

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

Tabela 17 – Especificaciones para Áreas de Integración para Gobierno Electrónico – Temas Transversales el área de Actuación de Gobierno

Temas	Especificación	ST	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
PROCESOS – Lenguaje para Ejecución de Procesos	BPEL4WS V1.1, de acuerdo con definido por el 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 BPEL4WS versión 2.0. Estudios referentes a la orquestación de procesos y coreografía serán futuramente conducidos por el grupo.
PROCESOS – Notación de Modelo de Procesos	BPMN 1.0, de acuerdo con lo definido por el OMG http://www.bpmn.org/Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf	**R**	
Intercambio de Informaciones Financieras	XBRL - *eXtensible Business Reporting Language* http://www.xbrl.org/SpecRecommendations/	**F**	www.xbrl.org
Legislación, Jurisprudencia y Propuestas Legislativas	LexML v. 1.0 http://proyecto.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 GEORREFERENCI	WMS versión 1.0 o posterior http://www.opengeospatial.org/standards	**A**	

Temas	Especificación	ST	Observaciones
ADAS – Interoperabilidad entre sistemas de información geográfica	WFS versión 1.0 o posterior http://www.opengeospatial.org/standards	**A**	
	WCS versión 1.0 o posterior http://www.opengeospatial.org/standards	**A**	
	CAT	**R**	El estándar CAT/CSW - Catalogue Services for the Web - es un estándar OpenGIS para intercambio de metadatos por medio de XML. La utilización del CSW es fundamental en la implantación de redes de intercambio de metadatos, en total observancia de las recomendaciones del e-PING en lo que se refiere al uso de XML y disponibilidad de bibliotecas libres para su implantación.
	WFS-T	**E**	El estándar WFS-T (*Web Feature Service - Transaction*) se refiere a las operaciones opcionales Transaction y *Lockfeature* del servicio WFS, de la OpenGIS. La operación Transaction es utilizada para describir la edición de datos espacias (inserción, marginación y actualización) colocados a disposición vía *WEB* y la *Lockfeature* asegura la consistencia de las facciones geométricas en base de datos geográficos colocados a disposición vía WFS por medio de acceso serial.
	WKT/WKB	**E**	El WKT (*Well-Known Text* – texto estructurado de una forma estandarizada) o WKB (*Well-Kown Binary*) es un formato para representación de las coordenadas que componen una facción

Temas	Especificación	ST	Observaciones
			geográfica y utilizado en situaciones específicas de transporte de coordenadas. Puede representar geometrías del tipo punto, línea, polígono, TIN y poliedro.

Tabela 18 – 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 inscripción	Especificación UDDI v3.0.2 (*Universal Description, Discovery and Integration*) definida por la OASIS http://uddi.org/pubs/uddi_v3.htm	**R**	
	ebXML (*Electronic Business using eXtensible Markup Language*). La especificación puede ser encontrada en http://www.ebxml.org/specs/index.htm	**E**	
Lenguaje de definición del servicio	WSDL 1.1 (*Web Service Description Language*) como definido por el W3C. La especificación puede ser encontrada en http://www.w3.org/TR/wsdl	**A**	
	WSDL 2.0 (*Web Service Description Language*) como definido por el W3C. La especificación puede ser encontrada en http://www.w3.org/TR/wsdl20/	**E**	
Perfil básico de interoperabilidad	*Basic Profile 1.1 Second Edition*, como definido por la WS-I http://www.ws-i.org/Profiles/BasicProfile-1.1.html	**E**	La versión 1.2 del Basic Profile se encuentra 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 la OASIS http://www.oasis-open.org/committees/wsrp	**E**	

[29] As questões de segurança relativas a *Web Services* son abordadas en el capítulo 7.

6. Glosario de Siglas y Términos Técnicos[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 sobre la preparación y recopilación de referencias de material utilizado para la producción de documentos y para inclusión en bibliografías, resúmenes, reseñas, análisis críticos 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 la Internet.

APF – Administración Pública Federal: agrupa 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 así un fundamento para la puesta en marcha de soluciones basada en arquitectura orientada a servicios. Cuando la coordinación de la ejecución de los servicios es realizada con subordinación a un proceso maestro, en general, intra-organización, dicha coordinación recibe la denominación de Orquestación. Cuando, la coordinación se realiza sin la subordinación a un proceso maestro, en general, interorganización, se denomina Coreografía.

***Browser*:** Navegación de la *web* – Una aplicación cliente que permite que el usuario vea contenidos de la *World Wide Web* en otra red o en la computadora del usuario, acompañar los vínculos de hipertexto y transferir archivos.

Catálogo de XML *Schemas*: guía de informaciones sobre los XML *Schemas*.

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

CAT – *Catalog Service Implementation Specification*: especificación *OpenGIS* que define interfaces para publicar, tener acceso a, navegar y consultar *metadatos* sobre informaciones georreferenciadas. El término más utilizado actualmente para *Calatog Service* es CSW.

CSW – *Catalog Service Implementation Specification*: especificación *OpenGIS* que define interfaces para publicar, tener acceso a, navegar y consultar *metadatos* sobre informaciones georreferenciadas.

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 en que los nombres de dominio son encontrados y traducidos en la dirección de protocolo de la Internet. Un nombre de dominio es un recurso fácil de ser recordado cuando es referenciado como una dirección en la Internet.

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

[30] Microsoft Press. Diccionario de informática. Tradutor 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 Tecnología y Linguística y Texto Digital. São Paulo: Futura, 2003. ISBN 85-7413-138-5.

GML – *Geography Markup Language*: especificación OpenGIS basada en el XML desarrollada para permitir el transporte y almacenamiento 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.

***Handshake*:** en una comunicación por teléfono, intercambio de informaciones entre dos modems y el resultante acuerdo sobre qué 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 clave que representa a cadena original. Es utilizada para indexar y recuperar ítems en una base de datos, porque es más rápido encontrar el punto utilizando la menor clave transformada que el valor original. También es utilizada en algoritmos de criptografía.

HELO: parámetros que limitan la entrega de e-mail comercial no solicitado. http://www.postfix.org/uce.html.

HTTP – *Hyper Text Transfer Protocol* (Protocolo de Transferencia de hipertexto): conjunto de reglas para permuta de archivos (texto, imágenes gráficas, sonido, video y otros archivos multimedios) en la *World Wide Web*.

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

ICP – Brasil: conjunto de técnicas, prácticas y procedimientos, que será puesto en marcha por las organizaciones gubernamentales y privadas brasileñas con el objetivo de establecer los fundamentos técnicos y metodológicos de un sistema de certificación digital basado en clave pública. http://www.icpbrasil.gov.br.

IEEE – *Institute of Electrical and Electronics Engineers* (Instituto de Ingenieros Eléctricos y Electrónicos): fomenta el desarrollo de estándares y normas que frecuentemente se convierten en estándares nacionales e internacionales.

IETF – *Internet Engineering Task Force* (Fuerza Tarea de Ingeniería de la Internet): entidad que define protocolos operacionales estándar de la Internet, como el TCP/IP.

IMAP – *Internet Message Access Protocol* (Protocolo de Acceso el mensaje en la Internet): protocolo estándar para tener acceso a e-mail a partir del servidor local. IMAP es un protocolo cliente-servidor en que el e-mail 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 ser considerado como un conjunto de números que representa el local de un determinado equipo (normalmente computadoras) en una red privada o pública.

IPSec – *Internet Protocol Security* (Seguridad de Protocolo de Internet): estándar de desarrollo relativo a la seguridad en la capa de la red o del procesamiento de paquetes de la comunicación en red. Una gran ventaja del IPsec es que las provisiones de seguridad pueden ser manipuladas sin exigir transformaciones en las computadoras de usuarios individuales. El IPsec suministra dos opciones de servicios de seguridad: *Authentication Header* (AH), que esencialmente permite la autenticación del remitente de datos, y *Encapsulating Security Payload* (ESP), que apoyo tanto la autenticación del remitente como la codificación criptográfica de datos.

IPv4 – *Internet Protocol Version 4* (Protocolo de Internet Versión 4): es la versión del protocolo IP más utilizada actualmente. Es 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 inter-red y la segunda parte identifica un equipo (host) dentro de esa red.

IPv6 – *Internet Protocol Version 6* (Protocolo de Internet Versión 6): es la versión más actual del protocolo IP. Es 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. Él está siendo implantado gradualmente en la Internet y debe funcionar lado a lado con el IPv4, en una situación técnicamente llamada de "pila doble", durante

cierto tiempo. A largo plazo, el IPv6 tiene como objetivo sustituir al IPv4, que solamente soporta alrededor de 4 mil millones (4 x 109) de direcciones, en comparación con alrededor de 3,4 x 1038 direcciones del nuevo protocolo.

LAN – *Local Area Network* (Red Local): grupo de computadoras 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 tiene aplicaciones y almacenamiento de datos compartidos por varios usuarios en diferentes computadoras.

LDAP – *Lightweight Directory Access Protocol* (Protocolo Liviano 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, tanto en la Internet pública como en una intranet corporativa.

Medio de acceso: conjunto de componentes físicos (dispositivos de acceso) y de componentes 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 intercambie mensajes en tiempo real con otro usuario también conectado a la red.

Metadatos: conocido como “datos sobre datos” metadatos son utilizados para registrar atributos sobre un recurso de información con miras a facilitar la recuperación, la gestión, la interoperabilidad, dar soporte a la identificación digital y dar soporte al archivo y preservación.

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

Newsgroup (Grupo de Noticias): discusión sobre un determinado tema que consiste en mensajes enviados a un website central en la 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*): tiene la misión de “desarrollar especificaciones para interfaces espaciales que serán colocadas a disposición libremente para uso general”.

OWS - OGC *Web Services*: se refiere a todas las especificaciones *OpenGIS* que aplican geoprocesamiento por medio de la Web.

Estándar abierto:

I - posibilita la interoperabilidad entre diferentes aplicativos y plataformas, internas y externas;

II - permite la aplicación sin ninguna restricción o pago de royalties;

III - puede ser implementado plena e independientemente por múltiples proveedores de programas de computadora, en múltiples plataformas, sin ningún cargo relativo a la propiedad intelectual para la necesaria tecnología.

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 adiciona capacidades al programa principal. Normalmente, en aplicaciones *web*, son programas que pueden ser fácilmente instalados y usados 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 e-mails. El POP3 es un protocolo de cliente/servidor en el cual el e-mail es recibido y guardado por el servidor de Internet.

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

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

Resolución nº 7 del Gobierno Electrónico: establece reglas y directrices para los locales en la 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 identidad visual y de la seguridad de los locales gubernamentales en la red mundial de computadoras. http://www.governoeletronico.e.gov.br.

RFC – *Request for Comments* (Solicitud de Comentarios): documento formal de la IETF, resultante de modelos y revisiones de partes interesadas. La versión final del RFC se convirtió en un estándar en que ni comentarios ni modificaciones son permitidos. Las modificaciones pueden ocurrir, sin embargo, por medio de RFCs subsiguientes que substituyen o elaboran en todas las partes de los RFCs anteriores. RFC también es la abreviación de 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 ser definido por el uso de la tecnología para aumentar el acceso y mejorar la prestación de servicios del gobierno a ciudadanos, proveedores y servidores. En líneas generales, las funciones características del gobierno electrónico son:

1. Prestación electrónica de informaciones y servicios.
2. Reglamentación de las redes de información, involucrando principalmente gobernanza, certificación y tributación.
3. Rendición de cuentas públicas, transparencia y monitoreo de la ejecución presupuestal.
4. Enseñanza a distancia, alfabetización digital y mantenimiento de bibliotecas virtuales.
5. Difusión cultural con énfasis en las identidades locales, fomento y preservación de culturas locales.
6. e-procurement, es decir, adquisición de bienes y servicios por medio de la Internet, como licitaciones públicas electrónicas, subastas electrónicos, conjuntos de compras públicas virtuales y otros tipos de mercados digitales para los bienes adquiridos por el gobierno.
7. Estímulo a los e-negocios, a través de la creación de ambientes de transacciones seguras, especialmente para empresas pequeñas y medianas. http://www.governoeletronico.gov.br/r1.

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

- gestión de gobierno: Planificación, Presupuesto, Ejecución Presupuestal, 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 diversos órganos de la estructura gubernamental, como infraestructura (transporte, comunicaciones, energía, administración de recursos naturales), Agricultura, Salud, Educación, etc.

referencia: http://www.redegoverno.gov.br/proyectos/reg_gestao.asp.

SFS. – *Simple Features Specification for* SQL: especificación *OpenGIS* que define la estandarización del esquema SQL que soporta almacenamiento, recuperación, consulta y actualización sobre informaciones georreferenciadas.

***Smart Cards*:** tarjeta de plástico, con aproximadamente el tamaño de un tarjeta de crédito, con un microchip embutido que puede ser cargado con datos, puede ser usado para efectuar llamadas telefónicas, pago electrónicos en dinero y otras aplicaciones. Es periódicamente actualizado para recibir usos adicionales.

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

SMTP/MIME – *Simple Mail Transfer Protocol/Multi-purpose Internet Mail Extensions* (Protocolo de Transferencia de Mensaje Simples/Extensiones de Correo de Internet Multipropósito): SMTP es un protocolo TCP/IP usado en el envío y recepción de e-mails. MIME es una extensión de protocolo de e-mail original de la Internet que posibilita el intercambio de diferentes tipos de archivos de datos por la Internet.

SOA - *Service Oriented Architecture* (Arquitectura Orientada a Servicios): es un paradigma para organización y utilización de competencias distribuidas que están bajo control de diferentes dominios propietarios. La arquitectura SOA es utilizada para interoperabilidad de sistemas por medio de conjunto de interfaces de servicios débilmente acoplados (*loosely coupled*), donde los servicios no necesitan detalles técnicos de la plataforma de los otros servicios para realizar el intercambio de informaciones.

SOAP – *Simple Object Access Protocol* (Protocolo Simple para Acceso a Objetos): describe un modelo para el empacotamiento de preguntas y respuestas XML. El envío de mensajes SOAP es utilizado 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 a través de su código-fuente y con el permiso para que cualquiera pueda usarlo, copiarlo y distribuirlo, tanto en su forma original como con modificaciones, gratuitamente o con costo. El software libre es necesariamente no propietario, pero es importante no confundir software libre con software gratuito.

SPAM: e-mail no solicitado en la Internet. Desde el punto de vista del remitente, esta es una forma de mensaje en masa, normalmente para una lista separada de personas inscritas a un grupo de discusión Usenet u obtenida por empresas especialistas en crear listas de distribución de e-mail. Para el destinatario, el *spam* normalmente es considerado como basura.

SSL – *Secure Sockets Layer* (Capa de Sockets Segura): es un protocolo comúnmente usado para gerenciar la seguridad de una transmisión de mensaje en la Internet.

Taxonomía para navegación: es un vocabulario controlado de términos y frases, organizado y estructurado jerárquicamente, de acuerdo con relaciones naturales o presumidas, con el objetivo de facilitar a los usuarios de locales y portales de la internet el descubrimiento de información mediante la navegación.

TCP – *Transmission Control Protocol* (Protocolo de Control de Transmisión): conjunto de reglas usadas con el IP para enviar datos en forma de unidades de mensaje entre computadoras por la Internet. Mientras el IP trabaja con la entrega real de los datos, el TCP controla las unidades individuales de los datos en que un mensaje es dividido para roteamiento eficiente a través de la Internet.

Telnet: la manera de tener acceso a la computadora de otra persona, asumiendo que le dieron permiso. Más técnicamente, Telnet es un comando de usuario y un protocolo subliminar TCP/IP para tener acceso a computadoras remotas.

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

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

UDDI – *Universal Description Discovery and Integration* (Descripción, Descubrimiento e Integración Universales): es el repositorio en el cual los responsables de desarrollo registran los *Web Services* disponibles que permiten a los clientes el descubrimiento y la utilización de los servicios asignados en Extranets 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 computadoras en una red que usa el IP. El UDP es una alternativa para el TCP y, con el IP, es referido como UDP/IP. Así como el TCP, el UDP usa el IP para llevar una unidad de datos desde una computadora hasta otra. A diferencia del TCP, el UDP no suministra el servicio de dividir un mensaje en paquetes y remontarlo en la otra extremidad. El UDP no suministra la secuencia de los paquetes en que los datos llegan. Esto significa que el programa de

aplicativo que usa el UDP debe garantizar que el mensaje entera llegó y está en orden. Los aplicativos de red que quieren ahorrar el tiempo de procesamiento porque tienen unidades muy pequeñas de datos para intercambiar pueden preferir el UDP en vez del TCP.

UML – *Unified Modeling Language* (Lenguaje de Modelación Unificada): La UML es mucho más que la estandarización de una notación, o sea, ella es un lenguaje-estándar para la elaboración de la estructura de proyectos de *software*, incluyendo aspectos conceptuales tales como procesos de negocios y funciones del sistema, además de ítems concretos como las clases escritas en determinado lenguaje de programación, esquemas de base de datos y componentes de *softwares* reutilizables. A UML puede ser empleada para la visualización, la especificación, la construcción y la documentación de artefactos de sistemas de *software,* también puede ser utilizada en la modelación de negocios y otros tipos de sistemas y no sólo de *software*.

URI - *Uniform Resource Identifier* (Identificador Único de Recurso): estándar de codificación de nombres y direcciones en la Internet. Una URI está compuesta por un nombre (ej.: file, http, ftp, news, mailto, gopher), seguido de 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 sometidos por usuarios sobre varios asuntos que son enviados 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 concreto, que utiliza la infraestructura de una red pública de telecomunicaciones, como la Internet, por ejemplo, para la transmisión de informaciones confidenciales. Los datos transmitidos son encriptados. Su implementación se realiza por medio de túneles virtuales, por los cuales transitan las informaciones, protegiéndolas del acceso de usuarios no autorizados.

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 computadoras que abarca extensas áreas geográficas como un estado, un país o un continente.

WCS – *Web Coverage Service Implementation Specification*: especificación *OpenGIS* que define interfaces para manipular y tener acceso a operaciones (*GetCapabilities, DescribeCoverage* y *GetCoverage*) sobre informaciones georreferenciadas en el formato Coverage.

***Web Services*:** Aplicación lógica, programable que vuelve compatibles entre sí la os más diferentes aplicativos, independientemente del sistema operacional, permitiendo la comunicación e intercambio de datos entre diferentes redes.

WFS – *Web Feature Service Implementation Specification*: especificación *OpenGIS* que define interfaces para manipular y tener acceso a operaciones (*GetCapabilities, DescribeFeaureType, GetFeature, Transaction* y *LockFeature*) sobre informaciones georreferenciadas, por medio del protocolo HTTP. Basado en dichas operaciones, dos clases de servicios pueden ser definidas:

- **WFS Básico (WFS):** es capaz de aplicar solamente las operaciones: *GetCapabilities, DescribeFeatureType* y *GetFeature*. Por eso, es considerado un servicio WMS solamente lectura.
- **WFS Transaccional (WFS-T):** es capaz de implementar todas las operaciones de un WFS básico y operaciones transaccionales. Opcionalmente, podría implementar también la operación *LockFeature*.

WMS – *Web Map Service Implementation Specification*: especificación OpenGIS que define interfaces para manipular y tener acceso a operaciones (*GetCapabilities, GetMap, GetFeatureInfo*) sobre múltiples capas (*layers*) de informaciones georreferenciadas, conteniendo vectores y/o imágenes.

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. Ella describe las funcionalidades de los servicios ofrecidos por el proveedor de servicios, así como su posición y forma de acceso.

XML – *eXtensible Markup Language* (Lenguaje Markup Extensible): manera flexible de crear

formatos de informaciones comunes y compartir ambos formatos y los 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 ilimitados y se autodefinen.

XML *Schemas*: están documentos XML, encontrados también en un sitio Internet, que especifican la estructura, número de ocurrencia 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 un sitio Internet, para que programas puedan tener acceso a ellos para 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, basado en XML para mensajes en tiempo real.

XSL – *eXtensible Stylesheet Language*: lenguaje de creación de hojas de cálculo que describe como 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*: modo estándar de describir cómo cambiar la estructura de un documento XML en otro documento XML con otra estructura. El XSLT puede ser pensado como una extensión del XSL. El XSLT muestra cómo el documento XSL debe ser reorganizado en otra estructura de datos (que puede ser presentado siguiendo una planilla del XSL).

7. Integrantes

Coordinación de la e-PING

Agencia Nacional de Aguas (ANA)
Sérgio Augusto Barbosa

Agencia Nacional de Petróleo (ANP)
Roberto Moreira Caldeira

Asociación Brasileña de Entidades Estaduales de Tecnología de la Información y Comunicación (ABEP)
Dayse Vianna

Banco do Brasil (BB)
Ulisses de Sousa Penna

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

Departamento de Informática del SUS (DATASUS)
Wilson Moraes Coelho

Empresa de Tecnología e Informaciones de la Previsión Social (DATAPREV)
Humberto Degrazia Campedelli

Instituto del Patrimonio Histórico y Artístico Nacional (IPHAN)
Carlos Augusto Pessoa Machado

Ministerio de Defensa – Comando del Ejército (MD/CEX)
Linda Soraya Issmael
Roberto Penido Duque Estrada

Ministerio de Justicia (MJ)
Jorilson da Silva Rodrigues

Ministerio de Salud (MS)
Eliane Pereira dos Santos
Ernani Bento Bandarra
Márcia Helena Gonçalves Rollemberg

Ministerio de Relaciones Exteriores (MRE)
Filipe Carneiro Guimarães

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

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

Ministerio do Planificación, Presupuesto y Gestión– Secretaría de Logística y Tecnología de la Información (MP/SLTI)
Nazaré Lopes Bretas (Coordinadora General)
Cláudio Muniz Machado Cavalcanti
Corinto Meffe
Ednylton Maria Franzosi
José Ney de Oliveira Lima
Leonardo Boselli da Motta
Leonardo Lanna Guillén
Rogério Santanna dos Santos

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

Marcelo André de Barros Oliveira
Roberto Montella Pimenta

Presidencia de la República – Instituto Nacional de Tecnología de la Información (ITI)
Mauricio Augusto Coelho
Renato da Silveira Martini

Secretaría de la Receita Federal de Brasil (RFB)
Edna Pereira Pinto Fernandes

Servicio Federal de Procesamiento de Datos (SERPRO)
Elói Juniti Yamaoka
Márcio Humberto M. Cammarota

Grupo de Trabajo Interconexión

Leonardo Lanna Guillén (MP/SLTI) – Coordinador
Carlos Bellone Neto (RFB)
Daniel Moreira Guilhon (CGU)
Filipe Carneiro Guimarães (MRE)
Hugo Góis Cordeiro (MinC)
Júlio César Japiassu Lyra (MJ)
Juscelino Kilian (PR/GSI)
Leonardo Boselli da Motta (MP/SLTI)
Luiz Carlos de Oliveira (ECT)
Marco Antonio Silva (ANA)
Marcos Martins Melo (SERPRO)
Nelson Soares de Rezende (IBGE)
Odilon de Freitas Militao Neto (CAIXA)
Paulo Guilherme Lanzillotti Jannuzzi (DATAPREV)
Roberto Moutella Pimenta (ITI)
Rogerio Alencar d´Araujo Couto (EMBRAPA)
Sumaid Andrade de Albuquerque (MTur)
Ulisses de Sousa Penna (BB)
Vanderlei de Jesus dos Santos Marques (ANVISA)

Colaboradores
Diogo da Fonseca Tabalipa (MP/SLTI)

Grupo de Trabajo Seguridad

Jorilson da Silva Rodirgues (MJ) – Coordinador
Emanuel Alamo Diogenes (ME)
Fábio Abdalla Afonso (CGU)
Filipe Carneiro Guimarães (MRE)
Georgia de Souza Assumpção (IBGE)
Gilberto de Oliveira Netto (SERPRO)
Humberto Degrazia Campedelli (DATAPREV)
Jean Carlo Rodrigues (ITI)
Joel Corrêa (DATAPREV)
Luiz Augusto Barbosa Mozzer (CGU)
Maisa Netto Leidemer (MC)
Márcio Vasconcelos Donato (MEC)
Marcos Gomes Figueira (BB)
Marcos J.C. Euzébio (BACEN)
Renato Navajas (MDIC)
Ricardo Campos dos Santos (SERPRO)
Roberta Rodrigues (ME)
Saulo Medeiros de Araújo (MDA)

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) – Coordenador
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 Aristoteles 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. VianaM. (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)
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 (Governo do Rio de Janeiro / PRODERJ) – Coordinadora
Aldecir Paz D´Avila Junior (Gobierno do Acre)
David William Honorio Araujo da Silva (Gobierno de Rio Grande do Norte)
Edinara Maria Ferreira Vale (Gobierno de Acre)
Marcos Ueda (Gobierno de Mato Grosso)
Tarcísio Quirino Falcao (Gobierno de Pernambuco / ATI)

Subgrupo: Guía de Interoperabilidad de Servicios de Gobierno
Cláudia del 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
Roberto Penido Duque Estrada (MD/CEX/DSG) – Coordinador
Alex Araújo (CAIXA)
Aramis Mota (PR/GSI)

Christian André H. Govastki (MME)
Dêner Lima F. Martins (ABIN)
Ellio Alves de O. Soares (CAIXA)
Eneias Roberto Shüller (CAIXA)
Fernando Gibotti (CAIXA)
Gerson Barrey (MEC)
Gilberto Ribeiro Queiroz (INPE)
Gustavo Araújo (MME)
Hisao Fujimoto (MME)
Jorge D. M. Cerqueira (PR/GSI)
Linda Soraya Issmael (MD/CEX/DSG)
Lúbia Vinhas (INPE)
Lúcia Helena Luz (CAIXA)
Moema José de Carvalho Augusto (IBGE)
Mosar Rabelo Júnior (MMA)
Silmara Ramos (PR/GSI)
Silvio Carlos Heitor Jorge (CAIXA)
Tálsia Garcia Meira (CC)
Valdevino S. Campos Neto (ANA)
Zandhor F. S. Cavalli Pradi (MS)

Colaboradores
Carlos Brasileiro (MDS)
Edmar Morett (MMA)
Enos Josué Rose (MCIDADES)
Rafael M. Sperb (UNIVALI)
Wilfredo Pacheco (ANA)
Werner Leyh (MS)

Ilustraciones
Hezrai de Souza Cruz (MP/SLTI)