Gobierno Brasileño

Comité Ejecutivo de Gobierno Electrónico

e-PING
Estándares de Interoperabilidad de Gobierno Electrónico

Documento de Referencia

Versión 2.0.1

05 de diciembre de 2006

GOVERNO FEDERAL

SUMARIO

Documento de Referencia de la e-PING – Versión 2.0.1

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 alcanzadas por la e-PING están segmentadas en:

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

Para cada uno de esos segmentos fueron especificados componentes, para los cuales son establecidos estándares.

Todo el contenido de este documento de referencia está en consonancia con las directrices del Comité Ejecutivo de Gobierno Electrónico, creado por el Decreto de 18 de octubre de 2000, y está publicado en sitio 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 está comprometido en asegurar que estas políticas y especificaciones permanezcan aliñadas 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, difusión y orientación para capacitación;
- las políticas y las especificaciones técnicas establecidas para todos los componentes de cada uno de los segmentos de la e-PING;
- glosario de términos técnicos referenciados;
- créditos – relación de los colaboradores de la presente versión de este documento.

Parte I – Visión General de la e-PING

1. Introducción

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

En ese contexto, la interoperabilidad de tecnología, procesos, información y datos es condición vital para el aprovisionamiento de servicios de calidad, volviéndose en premisa para gobiernos en todo el mundo, como fundamento para los conceptos de gobierno electrónico, el *e-gov*. La interoperabilidad permite racionalizar inversiones en TIC, por medio del compartimiento, 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 viene consolidando la arquitectura e-PING – "Estándares de Interoperabilidad de Gobierno Electrónico", que tiene como propósito ser el paradigma para el establecimiento de políticas y especificaciones técnicas que permitan la prestación de servicios electrónicos de calidad a la sociedad.

¿Lo que es Interoperabilidad?

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

"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 comprometimiento de las funcionalidades del sistema." (gobierno del Reino Unido);

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

"Habilidad de dos o más sistemas (computadores, medios de comunicación, redes, software y otros componentes de tecnología de información) de interaccionar y de intercambiar datos de acuerdo con un método definido, de forma a obtener los resultados esperados." (ISO);

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

Interoperabilidad no es solamente Integración de Sistemas, no es solamente Integración de Redes. No hace referencia únicamente a intercambio de datos entre sistemas. No contempla simplemente la definición de tecnología.

Es, en la verdad, 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 diversos de proveedores distintos. Tiene por objetivo la consideración de todos los factores para que los sistemas puedan actuar cooperativamente, fijando las normas, las políticas y los estándares necesarios para consecución de esos 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 administrados y direccionados para maximizar oportunidades de intercambio y reutilización de informaciones.

2. Descripción

Políticas y especificaciones claramente definidas para interoperabilidad y administración de informaciones son fundamentales para 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 actuantes 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 abarca 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, Judicial) y Ministerio Público Federal;
- Organismos Internacionales;
- Gobiernos de otros países;
- Empresas (en Brasil y en el mundo);
- Tercero Sector.

La figura a seguir representa esa relación.

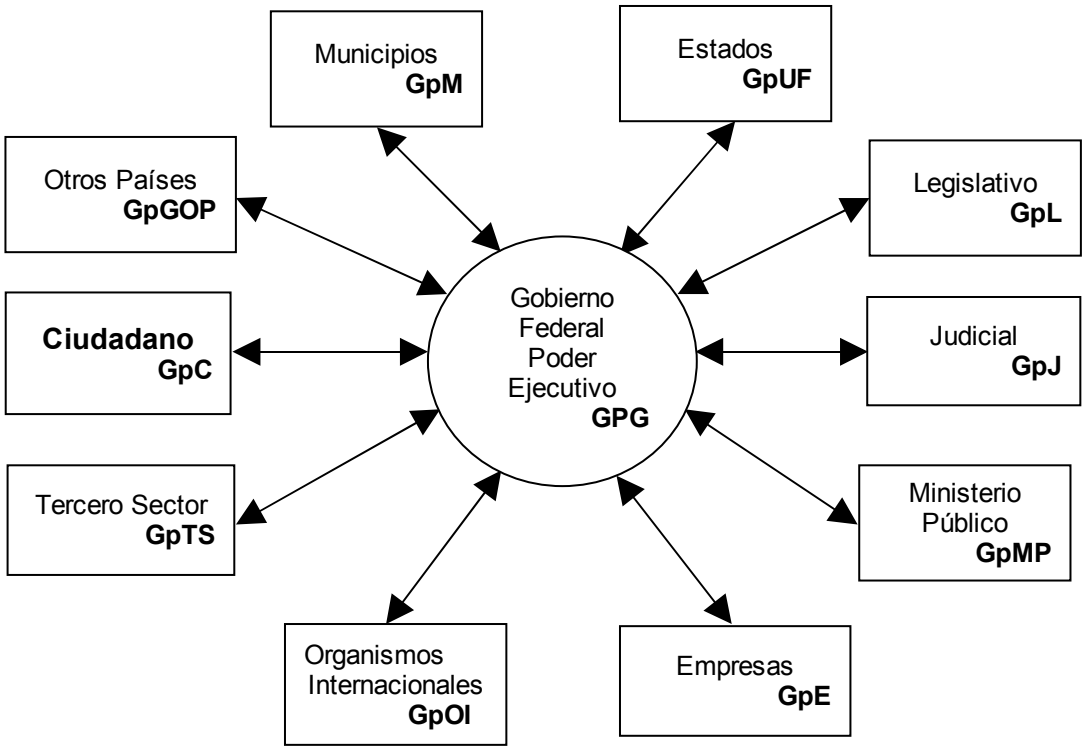

Figura 1 – Relaciones del gobierno federal.

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 diversas instancias del gobierno, dentro y fuera del país. El gobierno brasileño, entretanto, establece esas especificaciones como el estándar por el seleccionado y aceptado, o sea, estos son los estándares en que desea interoperar con las entidades fuera del gobierno federal –

Poder Ejecutivo brasileño. La adhesión de esas entidades se dará de manera voluntaria y sin cualquier 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 misma naturaleza jurídica, ligados directa o indirectamente a la Presidencia de la República de Brasil;
- las Autarquías y fundaciones.

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

- todos los nuevos sistemas de información que vengan a ser desarrollados e implantados en el gobierno federal y que se encuadran en la descripción de interacción, adentro del gobierno federal y con la sociedad en general;
- sistemas de información legados que sean objeto de implementaciones que involucren aprovisionamiento de servicios de gobierno electrónico o interacción entre sistemas;
- otros sistemas que hagan parte de los objetivos de disponibilizar los servicios de gobierno electrónico.

La adhesión sucederá de manera gradual, de acuerdo con el plan de implementación, que considerará la situación de cada una de esas instituciones con relación a la posibilidad de adecuarse a las especificaciones y recomendaciones de la e-PING.

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

Todas las compras y contrataciones del gobierno federal – Poder Ejecutivo direccionadas para 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 administradores de la e-PING y la sociedad.

2.2. Foco en la interoperabilidad

La e-PING no tendrá como foco de trabajo todos los asuntos del área de Tecnología de 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 administración de contenido. La e-PING involucra los asuntos comprendidos en la segmentación, descrita en el ítem 4 de este documento.

2.3. Asuntos no abordados

La e-PING no tiene por objetivo 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.

3. Políticas Generales

Cada uno de los segmentos de la e-PING contiene un conjunto de políticas técnicas que guía el establecimiento de las especificaciones de sus componentes. Esos conjuntos específicos de cada segmento están fundamentados 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, preferencialmente, por medio de tecnología fundamentada en *browser*; otras interfaces son permitidas en situaciones específicas, como en rutinas de actualización y captación de datos adonde no haya alternativa tecnológica disponible fundamentada 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, Fundamentado en estándares internacionalmente aceptos (http://www.eping.e.gov.br).

Desarrollo y manutención de la Lista de Asuntos del Gobierno: Taxonomía de Navegación (LAG), que contemple, en una estructura de directorio, los asuntos 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 alcanzado es la reducción de los costos y de los riesgos en la concepción y producción de servicios en los sistemas de informaciones gubernamentales.

Escalabilidad: las especificaciones seleccionadas deberán tener la capacidad de atender alteraciones de demanda en el sistema, tales como, cambios en volúmenes de datos, cantidad de transacciones o cantidad de usuarios. Los estándares establecidos no podrán ser factor restrictivo, debiendo ser capaz de fundamentar el desarrollo de servicios que atiendan desde necesidades más localizadas, envolviendo pequeños volúmenes de transacciones y de usuarios, hasta demandas de alcance nacional, con tratamiento de gran cantidad de informaciones y envolvimiento de un elevado contingente de usuarios.

Transparencia: los documentos de la e-PING estarán a la disposición de la sociedad, vía Internet, siendo previstos mecanismos de difusión, recibimiento y evaluación de sugestiones. En ese sentido, serán definidos – y difundidos para amplio conocimiento – plazos y compromisos para implantación y gestión de sitio dedicado en la Internet (http://www.eping.e.gov.br).

Adopción Preferencial de Estándares Abiertos: la e-PING define que, siempre que posible, serán adoptados estándares abiertos en las especificaciones técnicas. Estándares propietarios son aceptados, de forma transitoria, manteniendo las perspectivas de sustitución así que haya condiciones de migración. Sin perjuicio de esas metas, serán respetadas las situaciones en que haya necesidad de consideración de requisitos de seguridad e integridad de informaciones. Cuando disponibles, soluciones en Software Libre son consideradas preferenciales, conforme 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 a ser mencionado es el Guía de Migración de Software Libre del Gobierno Brasileño (http://www.governoeletronico.gov.br).

Garantía a la privacidad de información: todos los órganos responsables por el ofrecimiento de servicios de e-gov 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 difusión.

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 actuantes en órganos de los gobiernos federal, estadual y municipal, especialistas en cada asunto. Esos grupos fueron responsables por la elaboración de esta versión de la arquitectura, base para el establecimiento de los estándares de interoperabilidad del gobierno brasileño.

Los cinco segmentos – "Interconexión", "Seguridad", "Medios de Acceso", "Organización e Intercambio de Informaciones" y "Áreas de Integración para 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 seguir están 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 interoperacción entre el gobierno y la sociedad.

En este segmento, son establecidas las especificaciones para:

- Protocolo de Transferencia de Hipertexto;
- Transporte de Mensaje Electrónica;
- Seguridad de Contenido de Mensaje Electrónica;
- Acceso a la Caja Postal;
- Acceso Seguro a la Caja Postal;
- Directorio;
- Servicios de Nombramiento de Dominio;
- Direcciones de Caja Postal Electrónica;
- Protocolo de Transferencia de Archivos;
- Intercomunicación LAN / WAN;
- Transporte;
- *Web Services*: SOAP, UDDI y WSDL.

4.2. Seguridad

Este segmento trata de 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;
- Coleta y archivamiento de evidencias.

4.3. Medios de Acceso

En el segmento "Medios de Acceso", son expuestos las cuestiones relativas a los estándares de los dispositivos de acceso a los servicios de gobierno electrónico. En esta versión son abordadas, solamente, las políticas y las especificaciones para estaciones de trabajo, tarjetas inteligentes (*smart cards*), *tokens* y otras tarjetas. En versiones futuras, serán tratados otros dispositivos, tales como teléfono celular, *hand-helds* y televisión digital. Es formado por dos subgrupos, con 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 Banco de Datos para Estaciones de Trabajo;
- Especificación de Intercambio de Informaciones Gráficas e Imágenes Estáticas;
- Gráficos Vectoriales;
- Especificación de Estándares de Animación;
- Archivos del Tipo Audio y del Tipo Vídeo;
- Compactación de Archivos de Uso General;
- Archivos para georreferencia.

Tarjetas Inteligentes / *Tokens* / Otros:

- Definición de Datos;
- Aplicaciones (incluso multi-aplicaciones);
- Componentes Eléctricos;
- Protocolos de Comunicación;
- Estándares de Interface Físico;
- Seguridad;
- Infraestructura del Terminal.

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, comprendiendo los siguientes componentes:

- Lenguaje para intercambio de datos;
- Lenguaje para transformación de datos;
- Definición de los datos para intercambio;
- Catálogo de Estándares de Datos (CPD);
- Lista de Asuntos del Gobierno: Taxonomía para Navegación (LAG);
- Estándar de Metadatos del Gobierno (e-PMG).

4.5. Áreas de Integración para Gobierno Electrónico

Las metas de análisis y proposición de este segmento son:

- XML *Schemas* referentes a aplicaciones direccionadas a Áreas de Actuación de Gobierno, que serán organizados en forma de Catálogo, disponible en el sitio de la e-PING, y presentado con los contenidos actuales en el tópico siguiente;
- Componentes relacionados a temas transversales a Áreas de Actuación de Gobierno, cuya estandarización sea relevante para la interoperabilidad de servicios de Gobierno Electrónico, tales como Procesos e Informaciones Geográficas.

5. Gestión de la e-PING

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

5.1. Histórico

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

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

Esos tres órganos organizaron un Seminario, con participación de entidades del gobierno federal, en el ámbito del Poder Ejecutivo, teniendo como objetivo la formación de un comité interórganos – denominado Comité Constituyente – para conducir los trabajos iniciales de elaboración de la arquitectura.

Tras su institucionalización, por intermedio de la Portería Normativa nº 5, de 14 de julio de 2005, este se pasó a denominar Coordinación de la e-PING. Además de los tres organizadores, participan de ese grupo los siguientes órganos: DATAPREV, Banco do Brasil, Caixa Econômica Federal, DATASUS y ABEP - Associação Brasileira de Empresas Estaduais de Processamento de Dados.

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 abordados por la e-PING;
- creación de cinco grupos de trabajo responsables por las definiciones iniciales de políticas y especificaciones técnicas para cada uno de los segmentos;
- establecimiento de un cronograma de trabajo con el objetivo de construcción y difusión de la versión inicial de la arquitectura, denominada versión 0;
- realización de consulta pública y audiencias públicas en RS, SP, DF, RJ, MG y PE, de manera a recaudar contribuciones, de la sociedad en general, sobre el contenido propuesto en la versión 0;
- publicación de la versión 1, juntamente con la resolución de institucionalización de la e-PING en el ámbito de la APF – Poder Ejecutivo;
- publicación de la versión 1.5, conteniendo las actualizaciones y revisión de las especificaciones técnicas y de la visión general de la e-PING. Las versiones 1.1 hasta 1.4 quedaron en discusión interna a los grupos de trabajo y a la coordinación de la e-PING;
- realización de consulta pública y audiencias públicas de manera a recaudar contribuciones, de la sociedad en general, sobre el contenido propuesto en la versión 1.9;
- publicación de la versión 2.0, conteniendo las actualizaciones y revisiones de las especificaciones técnicas y de la visión general de la e-PING.

Experiencias semejantes desarrolladas por gobiernos de otros países son constantemente pesquisadas. 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 apoyada en la forma implementada por el gobierno del Reino Unido, en operación desde el año 2000, y, actualmente, está en un grado de madurez internacionalmente reconocido como referencia.

5.2. Estrategia de Implantación

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

La presente versión consolidó el trabajo de los grupos elaborados para los cinco segmentos definidos. Todo su contenido fue puesto a disposición para Consulta Pública, con el objetivo de obtener contribuciones a las propuestas de estándares publicados en la versión 1.9.

5.3. Modelo de Gestión

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

5.3.1. Atribuciones

La Gestión de la e-PING comprende el desempeño de atribuciones de orden administrativa y de orden técnica.

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 necesaria para su correcta utilización y garantizando su actualización, considerando: las prioridades y metas de gobierno, las necesidades de la sociedad y la disponibilidad de nuevas tecnologías maduras y soportadas por el mercado de TIC;
- actuar como centro de coordinación de la arquitectura e-PING, buscando alineamiento de los esfuerzos de interoperabilidad, 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 ítem 2 - Descripción;
- administrar y operacionalizar la difusión de los estándares de la e-PING, considerando:
  - creación y administración de un sitio en la Internet para la e-PING (http://www.eping.e.gov.br);
  - coordinación del proceso de consultas públicas;
  - coordinación del proceso de recibimiento y evaluación de proposiciones de alteración y complementación;
  - coordinación del proceso de solicitación de sugestiones para la e-PING;
  - publicación de las versiones actualizadas de la e-PING y de las actualizaciones intermediarias;
- administrar la interacción con iniciativas de mismo propósito, conducidas por otros gobiernos, en el país y en el exterior;
- incentivar la capacitación de los equipos de 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 direccionados para diseminación de los estándares e-PING;
- establecer, implantar y difundir indicadores de acompañamiento de los resultados obtenidos con la implantación de la e-PING;
- administrar la interacción con organismos de especificación (W3C, IEEE, BSI, OMG, OGC, OASIS, IETF, Institutos Normativos de segmentos específicos, como ABNT, INMETRO, ISO, NIST, etc). Estos organismos serán elegidos a criterio de la coordinación de la e-PING llevando en consideración su notorio reconocimiento internacional, competencia en su área de actuación y el establecimiento de estándares abiertos.
- administrar la interacción con órganos de fomento nacionales e internacionales, para canalizar recursos, visando atender las necesidades de creación de infraestructura de la e-PING y promover la pesquisa y desarrollo;
- viabilizar la implantación y administrar el proceso de homologación de los estándares a ser

establecidos para el gobierno;

- viabilizar la implantación y administrar procesos de auditoría realizados con la finalidad de verificar el nivel de adhesión a las recomendaciones y especificaciones de la e-PING;
- actuar cooperativamente, como apoyo a los órganos de gobierno, en la realización de los procesos necesarios para adecuación a los estándares e-PING; evaluar la posibilidad de patrocinar programas de alcance que promuevan la utilización intensiva de los estándares propuestos.

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

- establecer las formas de elaboración y de manutención de las políticas y especificaciones técnicas que componen la e-PING, considerando:
  - identificación, creación y gestión de grupos de trabajo específicos;
  - establecimiento de convenios y definición de instituciones de gobierno como responsables por las políticas y especificaciones técnicas de componentes específicos de los segmentos de interoperabilidad;
  - identificación y implementación de formas alternativas de Administración técnica de los asuntos contemplados en el alcance de actuación de la e-PING;

- coordinar el desarrollo y manutención, en el ámbito del gobierno federal – Poder Ejecutivo, de:
  - estándar de Metadatos de Gobierno (e-PMG);
  - lista de Asuntos de 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 por 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 esquema simplificado a seguir.

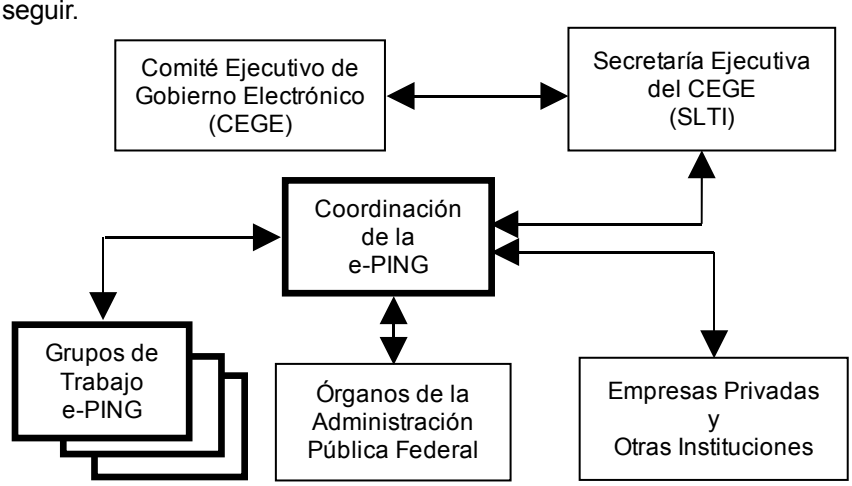

Figura 2 – Administración de la e-PING.

La Secretaría de Logística y Tecnología de Información del Ministerio de la Planificación, Presupuesto y Gestión, a través del instrumento del Sistema de Administración de los Recursos de Información e Informática (SISP), instituido por el Decreto 1.048, de 21 de enero de 1994, es el responsable por la institucionalización y por la definición del formato jurídico de la Coordinación de la e-PING.

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

- implantación de la arquitectura e-PING, providenciando las actividades necesarias para consolidación de la versión actual y dinámica de su evolución;
- gestión de la arquitectura e-PING;
- establecimiento y gestión de las normas y de los instrumentos institucionales y legales que garanticen la efectividad de las recomendaciones y especificaciones de la e-PING;
- administración de los estándares considerados en la e-PING;
- garantía de manutención de la actualización de los diversos catálogos de la e-PING;
- gestión de los procesos de Comunicación y Difusión de los estándares, de las decisiones y de las actividades de la e-PING, incluyendo la publicación de nuevas versiones y de las actualizaciones intermediarias;
- creación de un sello e-PING y administración de proceso que certifique la adherencia de determinado servicio o producto a la e-PING;
- proveer criterios y subsidios para la elaboración de la Ley Presupuestaria Anual del Gobierno Federal;
- gestión de los procesos de contratación de los servicios y de establecimiento de convenios para realización de las atribuciones necesarias para consolidación de los estándares, como, por ejemplo, evaluación de propuestas de proyectos de e-gov direccionados para la Administración Pública Federal, homologación de estándares y verificación de conformidad;
- establecimiento de los puntos de contacto con los diversos órganos de la Administración Pública Federal;
- administración de los Grupos de Trabajo – GT, definiendo su composición y determinando las directrices de trabajo, fundamentadas en las políticas técnicas, generales y específicas, en las necesidades de gobierno y en la monitorización del escenario tecnológico.

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

- tratar los asuntos que componen los segmentos de la e-PING;
- monitorizar sistemáticamente el mercado, específicamente para los segmentos bajo su responsabilidad, con el objetivo de detectar las necesidades de actualización tecnológica de las políticas y especificaciones técnicas;
- subsidiar la actuación de la Coordinación de la e-PING, en el desempeño de sus atribuciones administrativas y técnicas.

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

5.4. Actividades adicionales

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

5.4.1. Selección y Homologación de Estándares Tecnológicos

Las políticas técnicas contenidas en este documento fundamentan los estándares de la e-PING, actuando 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 candidatos a integrar la arquitectura. Ese proceso abarca la selección, la homologación y la clasificación de las especificaciones seleccionadas en cinco niveles de situaciones, que caracterizan el grado de adherencia a las políticas técnicas generales y específicas de cada segmento.

Esos cinco niveles son los siguientes:

- **Adoptado (A):** ítem adoptado por el gobierno como estándar en la arquitectura e-PING, 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 basado en una proposición debidamente fundamentada por la coordinación del segmento, publicada en el sitio y aprobado por la Coordinación de la e-PING;

- **Recomendado (R):** ítem que atiende a las políticas técnicas de la e-PING, es reconocido como un ítem que debe ser utilizado en el ámbito de las instituciones de gobierno, pero todavía no fue sometido a un proceso formal de homologación;
- **En Transición (T):** ítem que el gobierno no recomienda, por no atender a uno o más requisitos establecidos en **las** políticas generales y técnicas de la arquitectura; es incluido en la e-PING en razón de su uso significativo en instituciones de gobierno, tendiendo a ser desactivado así que algún otro componente, en una de las dos situaciones anteriores venga a presentar condiciones totales de sustituirlo. Puede venir a ser considerado un componente "recomendado" caso venga a adecuarse a todas las políticas técnicas establecidas. Conviene resaltar que el desarrollo de nuevos servicios o la reconstrucción de partes significativas de los ya existentes debe evitar el uso de componentes clasificados como transitorios;
- **En Estudio (E):** componente que está en evaluación y será encuadrado en una de las situaciones arriba citada, así que 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 consecuente clasificación en las situaciones arriba indicadas, es de responsabilidad de los Grupos de Trabajo compuestos por profesionales especialistas con actuación en el gobierno y en instituciones con las cuales sea establecido algún tipo de convenio o contrato específicamente para esa finalidad.

La selección es hecha a partir de sugestiones formalizadas, demandas internas de los órganos del gobierno federal, Poder Ejecutivo, y pesquisas realizadas por los Grupos de Trabajo.

Ya la homologación deberá ser objeto de estudio más detallado por parte de los administradores de la e-PING. En virtud de la grande variedad de componentes tratados por la arquitectura, habrá necesidad de elaboración de una sistemática de homologación que contemple desde procesos en que será necesaria la evaluación de características físicas de determinados componentes (Tarjetas Inteligentes, por ejemplo) hasta otros en que haya la necesidad de estudio de aspectos que implican el uso del componente en el desarrollo y construcción de servicios (organización y intercambio de informaciones y seguridad, por ejemplo).

En ese caso, el gobierno deberá establecer convenios o catastrar instituciones para elaboración de exámenes de conformidad, siempre definiendo cuales componentes deben ser sometidos a procesos de homologación, cuales los criterios de evaluación de los resultados y cuales las condiciones de realización de los procedimientos.

La definición completa del proceso de selección y homologación, llevando en consideración las especificidades de los segmentos, quedará 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 factor crítico de éxito en la implantación y consolidación de la e-PING. Los administradores de la e-PING recomendarán la realización de procesos de auditoría para verificación del atendimiento a las especificaciones y políticas de la arquitectura.

Podrá haber delegación de responsabilidad para equipos especialmente elaborados para esa finalidad, compuestas por técnicos de gobierno con experiencia en procedimientos de esa naturaleza.

La forma preferencial de realización de ese tipo de procedimiento, entretanto, será la utilización de las estructuras propias en los órganos responsables por auditoría de sistemas. La Coordinación de la e-PING actuará en el sentido de sugerir los criterios básicos a ser seguidos por los órganos.

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

5.4.3. Creación y Manutención del Sitio

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

funcionalidades:

- difusión 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 correlacionada;
- disponibilidad de las recomendaciones, determinaciones, especificaciones técnicas y políticas para validación, homologación y recibimiento de comentarios y sugestiones por parte de la sociedad;
- publicación de solicitación de comentarios relativos a la especificación de componentes para la arquitectura;
- disponibilidad de medio electrónico para recibimiento de sugestiones;
- disponibilidad de links para documentos, estándares, normas o cualquier otro tipo de referencia constante en la e-PING.

5.4.4. Acompañamiento Legal e Institucional

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

Además, esa Asesoría tendrá todavía la responsabilidad de preparar toda la parte institucional necesaria para garantizar que las adecuaciones y recomendaciones de la e-PING vengan a componer el conjunto de instrumentos legales de TIC en el país.

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

5.4.5. Difusión

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

- realización de eventos específicos de difusión, como Seminarios, *Workshops* y presentaciones en general;
- participación en eventos gubernamentales en el área de TIC y correlacionadas;
- participación en eventos direccionados a públicos específicos;
- publicación de todas las versiones de la e-PING y de las actualizaciones intermediarias;
- intercambio con otras esferas y otros Poderes de gobierno, con instituciones públicas, privadas y del tercero sector y con gobiernos de otros países.

5.4.6. Capacitación

Harán parte de la agenda de implantación y gestión de la e-PING eventos direccionados para capacitación. También es previsto el uso intensivo de Enseñanza a Distancia (EAD).

La Coordinación de la e-PING elaborará y publicará una tabla mínima de entrenamiento, de modo que cada órgano de la APF tenga subsidios para planear 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 abastecimiento de entrenamiento adecuado para los componentes de sus equipos técnicos.

5.5. Relación con Gobierno y Sociedad

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

5.5.1. Organizaciones del Gobierno Federal – Poder Ejecutivo

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

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

- contribuir para el desarrollo y mejoría continua de la e-PING;
- garantizar que sus estrategias organizacionales de TIC consideren que los sistemas integrantes de servicios de gobierno electrónico bajo su responsabilidad estean 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 interoperabilidad, dando soporte de entrenamiento cuando necesario;
- establecer punto de contacto en las instituciones, para intercambio de informaciones y de necesidades con la Coordinación de la e-PING;
- alquilar y suplir 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) de manera a mejorar la calidad y reducir costos de aprovisionamiento de los servicios de e-gov.

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

En su fase inicial, la e-PING se direcciona, básicamente, para el gobierno federal, Poder Ejecutivo. Otros Poderes (Judicial, Legislativo y Ministerio Público Federal) y otras esferas de gobierno (estadual y municipal) serán considerados como entidades externas.

En este caso, vale la orientación de que el gobierno federal – Poder Ejecutivo no determina la forma como las demás entidades de la sociedad deben actuar. Solamente específica la forma preferencial como pretende interoperar con esas entidades.

La adhesión de otras instancias de gobierno es incentivada y reconocida como una buena estrategia para perfeccionar el establecimiento de estándares y consolidar la e-PING como una arquitectura de estándares de interoperabilidad del gobierno brasileño.

En el plan de gestión de la e-PING los demás Poderes federales y los gobiernos estaduales y municipales son considerados prioritarios. Es meta a ser alcanzada, tan pronto sean establecidos y firmados los estándares en el ámbito del Poder Ejecutivo Federal, la extensión de las discusiones a los órganos e instituciones que componen esas áreas de gobierno.

5.5.3. Organizaciones del Sector Privado y del Tercero Sector

La e-PING prevé la interacción con el Sector Privado y con el Tercero Sector por medio de los mecanismos de Consulta Pública, Solicitación de Comentarios y Recibimiento de Sugerencias.

Todas las entidades de esa naturaleza que participen de procesos de licitación para proveer productos y servicios para el Poder Ejecutivo Federal deberán atender a las especificaciones y recomendaciones de la e-PING.

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

5.5.4. Ciudadano

Gobierno electrónico significa, esencialmente, el gobierno servir mejor a las necesidades del

ciudadano utilizando los recursos de Tecnología, Información y Comunicación. La arquitectura e-PING posibilita la integración y disponibiliza servicios de forma integral, segura y coherente, permitiendo obtener mejores niveles de eficiencia en el gobierno.

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

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

6. Interconexión

6.1. Interconexión: Políticas Técnicas

Las políticas técnicas para interconexión son:

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

6.1.3. Los órganos de la APF deben usar esquema de Directorio compatible con el del Servicio de Directorio del gobierno federal, disponible en la dirección electrónica http://www.e.gov.br/correios/dir_redegoverno.htm.

6.1.4. Los órganos de la APF deben obedecer a la política de nombramiento de dominios del gobierno federal, establecida en la Resolución n.º 7, que puede ser obtenida en la dirección electrónica

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

6.1.5. El DNS debe ser utilizado para resolución de nombres de dominios Internet, convirtiéndolos en direcciones IP y, en sentido inverso, convirtiendo IPs en nombres de dominios, a través de la manutención de los mapas directo y reverso, respectivamente.

6.1.6. Los protocolos FTP y/o HTTP deben ser utilizados para transferencia de archivos, observando sus funcionalidades para recuperación de interrupciones y seguridad, cuando necesario. El HTTP debe ser priorizado para transferencias de archivos originarios de páginas de sitios de la Internet.

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

6.1.8. La tecnología de *Web Services* es recomendada como estándar de interoperabilidad de la e-PING.

6.1.9. Los *Web Services* deberán ser registrados y estar localizados en estructuras de directorio compatibles con el estándar UDDI. El protocolo de acceso a esa estructura deberá ser el HTTP.

6.1.10. El protocolo SOAP es recomendado para comunicación entre los clientes y los *Web Services* y la especificación del servicio deberá utilizar el lenguaje WSDL. Vea nota sobre *Web Services*, ítem 6.3.

6.2. Interconexión: Especificaciones Técnicas

Tabla 1 – Especificaciones para Interconectividad[2]

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		

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

[2] Las RFCs pueden ser accesadas en el sitio http://www.ietf.org/rfc.html

Componente	Especificación	SIT	Observaciones
Protocolo de transferencia de hipertexto	Utilizar HTTP/1.1 (RFC 2616) y/o HTTPS (RFC 2660).	**R**	
Transporte de mensaje electrónica	Utilizar productos de mensajería electrónica que soportan interfaces en conformidad con SMTP/MIME para transferencia de mensajes. RFCs correlacionadas: RFC 2821; RFC 2822; RFC 2045; RFC 2046; RFC 2646; RFC 2047; RFC 2231; RFC 2048; RFC 3023; RFC 2049.	**R**	
Seguridad de contenido de mensaje electrónica	El S/MIME v3.1 deberá ser utilizado cuando sea apropiado para seguridad de contenido de mensajes generales del gobierno, a menos que los requisitos de seguridad determinen otra forma. RFCs correlacionadas: RFC 3852, RFC 2631, RFC 3850 y RFC 3851.	**R**	
Acceso a la Caja Postal	A menos que las exigencias de seguridad determinen de otra forma, programas de correo que proveen facilidades de acceso a la correspondencia deberán, como mínimo, estar de acuerdo con POP3 para acceso remoto a la caja postal. RFCs correlacionadas: RFC 1939, RFC 1957 y RFC 2449. Adonde facilidades adicionales sean necesarias, a menos que requisitos de seguridad establescán de forma contraria, los programas de correo que proveen facilidades avanzadas de acceso a la correspondencia, deberán estar de acuerdo con IMAP para acceso remoto a la caja postal. RFCs correlacionadas: RFC 3501, RFC 2342, RFC 2971, RFC 3502, RFC 3503 y RFC 3510.	**R**	
Acceso seguro a la caja postal	El acceso a la caja postal, a través de redes no seguras, deberá usar HTTPS, de acuerdo con los estándares de seguridad en el transporte. Cuando sea necesario usar IMAP o POP, usarlo a través de TLS, conforme RFC 2595.	**R**	
Directorio	Usar el esquema del directorio central, conforme definido en la dirección electrónica http://www.e.gov.br/correios/dir_redegoverno.htm LDAP v3 deberá ser utilizado para acceso general al directorio.	**R**	
Servicios de Nombramiento de Dominio	El DNS debe ser utilizado para resolución de nombres de dominios Internet, conforme la RFC 1035. Por su vez, las directivas de nombramiento de dominio del gobierno brasileño son encontradas en la Resolución Nº 7 del Comité Ejecutivo del Gobierno Electrónico, en la dirección electrónica https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm Además de esas directivas, por decisión del Comité Gestor de Internet en Brasil, el nombramiento de dominios obedece a las orientaciones del Ministerio de la Planificación, a quien compite administrar los dominios .GOV.BR. Las particularidades de otros niveles de gobierno, como por ejemplo, los dominios de los gobiernos de las Unidades de la Federación, que incluyen la sigla de la UF en la composición de las direcciones, son abordadas en la dirección electrónica	**R**	

Componente	Especificación	SIT	Observaciones
	http://registro.br/faq/faq1.html#12		
Direcciones de caja postal electrónica	Las reglas para definición de los nombres de las cajas postales de correo electrónico deberán seguir lo establecido en el documento “Cajas Postales Individuales-Funcionales en el Gobierno Federal”, disponible en la dirección electrónica http://www.e.gov.br/correios/cp_individ.htm	**R**	
Protocolos de transferencia de archivos	FTP (RFC 959 y RFC 2228) (con re-inicialización y recuperación) y HTTP (RFC 2616) para transferencia de archivos.	**R**	
Protocolos de Señalización	Uso del Protocolo de Inicialización de Sesión (SIP), definido por la RFC 3261, como protocolo de control en la camada de aplicación (señalización) para crear, modificar y terminar sesiones con uno o más participantes.	**R**	
Mensajería en Tiempo Real	El modelo y requisitos para Mensajería Instantánea y Protocolo de Presencia (IMPP) son definidos por la RFC 2778 y RFC 2779.	**R**	
Servicio de Mensajes Cortas	El Servicio de Mensajes Cortas (SMS) deberá utilizar el protocolo SMPP, como definido por el SMS *Forum* http://www.smsforum.net	**R**	
Intercomunicación LAN/WAN	IPv4 (RFC 791)	**R**	La especificación del IPv6 se encuentra como un “borrador/proyecto” (*Draft Standard* RFC 2460).
Transporte	TCP (RFC 793) UDP (RFC 768) cuando necesario, sujeto a las limitaciones de seguridad.	**R**	
Tráfico Avanzado	Cuando necesario, el tráfico de red puede ser optimizado por el uso del MPLS (RFC 3031).	**R**	

6.3. Web Services

Los *Web Services* son aplicaciones de software, identificadas por una URI (*Uniform Resource Identifier*), cuyas interfaces y conexiones son capaces de ser definidas, descritas y descubiertas por artefactos basados en XML. Además de eso, posee soporte para integración directa con otras aplicaciones de software, utilizando, como estándar de interoperabilidad, mensajes escritas en XML y encapsuladas en protocolos de aplicación estándar de Internet.

La necesidad de integración entre los diversos sistemas de información de gobierno, implementados en diferentes tecnologías, a veces de forma simultánea y en tiempo real, implica en la adopción de un estándar de interoperabilidad que garantice escalabilidad y facilidad de uso.

La tecnología de *Web Services* es adecuada para atender tales necesidades, además de ser independiente con relación a los Sistemas Operacionales y a los Lenguajes de Programación.

Una de sus características más relevantes se refiere al nivel de abstracción, superior al concepto de componentes de software. Desde un formulario perteneciente a una página *web*, hasta un componente de software, que encapsula una compleja regla de negocio, pueden ser transformados en *Web Services*, lo que vuelve su uso bastante flexible.

El uso de *Web Services* contempla tanto transferencias de documentos entre Instituciones, como solicitaciones para ejecución de servicios remotos.

Las estructuras de documentos XML serán descritas a través de XML *Schemas*, como forma de

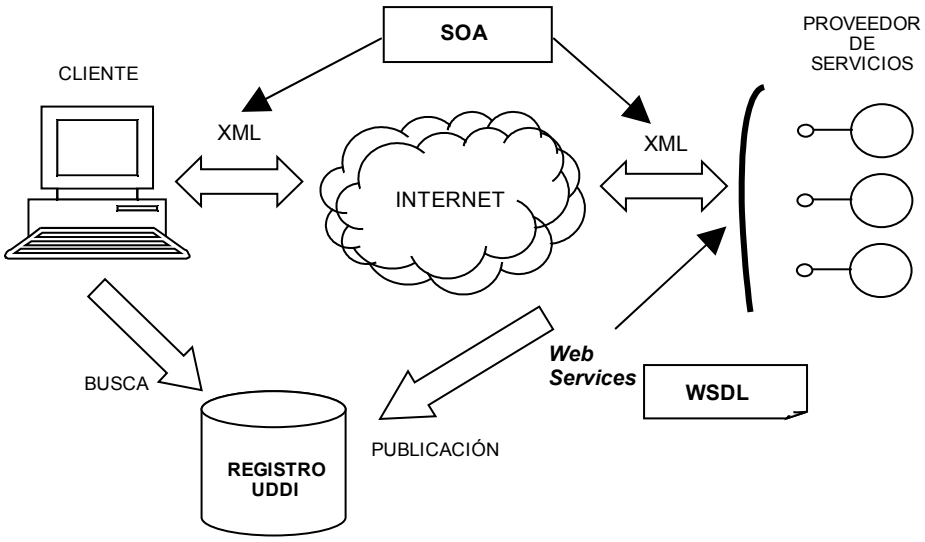

Figura 3 – Visión general de funcionamiento de *Web Services.*

Tabla 2 – Especificaciones para *Web Services*[3]

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Protocolo de cambio de informaciones	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/	**R**	
Infraestructura de registro	Especificación UDDI v3.0.2 (*Universal Description, Discovery and Integration*) definida por la OASIS http://uddi.org/pubs/uddi_v3.htm	**R**	
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	**R**	La especificación del WSDL 2.0 está como "borrador/proyecto" (*Working Draft*) en http://www.w3.org/TR/wsdl20/
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	**F**	
Portlets remotos	WSRP 1.0 (Web Services for Remote Portlets) como definido por la OASIS http://www.oasis-open.org/committees/wsrp	**E**	

[3] Las cuestiones de seguridad relativas a *Web Services* son abordadas en el capítulo 7.

6.4. Mensaje Electrónica (E-mail)

Para efecto de clareza, la e-PING utilizará los siguientes conceptos:

Transporte de Mensaje Electrónica

El transporte de mensaje electrónica es definido como la interface entre dos sistemas de correo.

Acceso a la caja postal

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

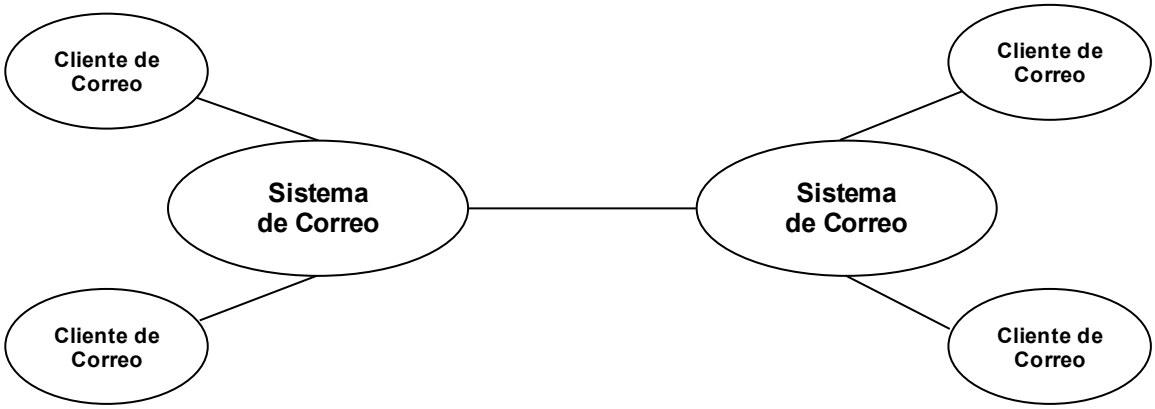

Figura 4 – Interfaces entre sistemas y clientes de Correo.

6.5. LAN Sin Cable

Existe una creciente necesidad de computación móvil adentro del gobierno para permitir estándares de trabajo más flexibles. Las soluciones LAN sin cable, basadas en las series de estándar IEEE 802.11, son bien aceptas por el mercado. Se recomienda observar las especificaciones sobre seguridad, contenidas en el capítulo 7 de este documento.

6.6. VPN

Virtual Private Network (VPN), o Red Privada Virtual, es una red privada construida sobre la infraestructura de una red pública, normalmente la Internet. En vez de utilizarse *links* dedicados o redes de paquetes para conectar redes remotas, se utiliza la infraestructura de la Internet.

La utilización de la Internet, como infraestructura de conexión entre *hosts* de la red privada, es una buena solución en términos de costos, pero no en términos de privacidad, pues la Internet es una red pública, adonde los datos en tránsito pueden ser leídos por cualquier equipamiento.

Los túneles virtuales habilitan el tráfico de datos criptografados por la Internet y esos dispositivos son capaces de entender los datos criptografados, formando una red virtual segura sobre la Internet.

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

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

6.7. Redes peer-to-peer

Sistemas Peer-to-Peer (P2P) son sistemas distribuidos que consisten de nodos interconectados, con capacidad de auto organizarse en topologías de red, con el objetivo de compartir recursos como procesamiento, almacenamiento y anchura de banda, capaces de se adaptar a fallas y acomodar poblaciones transientes de nodos, mientras mantiene conectividad y actuaciones aceptables, sin

depender de la intermediación o soporte de una autoridad (servidor) central.

Debido al hecho de diversas cuestiones de seguridad que todavía imposibilitan el uso sistemático de redes Peer-to-Peer, este asunto será abordado en momento futuro.

7. Seguridad

7.1. Seguridad: Políticas Técnicas

7.1.1. Los datos, informaciones y sistemas de información del gobierno deben ser protegidos contra amenazas de forma a reducir riesgos y garantizar 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 transitando.

7.1.3. Las informaciones que transitan en redes inseguras, incluyendo aquellas sin cable, deben adoptar los controles de seguridad disponibles en la camada de transporte (IPv4). En el caso de LAN sin cable los protocolos de seguridad específicos de esta tecnología deben ser usados, cuando necesario. Los sistemas de información del gobierno deben ser protegidos contra riesgos de seguridad en la conexión con esas redes.

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 adonde serán tratados los riesgos residuales visando atender los niveles mínimos de producción.

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

7.1.7. Los sistemas deben poseer registros históricos (*logs*) para permitir auditorias y exámenes forenses, siendo imprescindible la adopción de un sistema de sincronismo de tiempo centralizado, bien como se debe utilizar mecanismos que garanticen la autenticidad de los registros almacenados, si posible con firma digital.

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

7.1.9. 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 en conformidad con las reglas de la ICP-Brasil.

7.1.10. La documentación de los sistemas, de los controles de seguridad y de las topologías de los ambientes debe ser mantenida actualizada y protegida.

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

7.1.12. Los Órganos de la APF, visando la mejora de la seguridad, deben tener como referencia la norma NBR ISO/IEC 17799:2005 código de práctica para la gestión de la seguridad de la información, editada por la ABNT.

7.2. Seguridad: Especificaciones Técnicas

Tabla 3 – Especificaciones Técnicas para Seguridad de IP

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		

Componente	Especificación	SIT	Observaciones
Transferencia de datos en redes inseguras por los protocolos HTTP, LDAP, IMAP, POP3, Telnet siempre que posible. – Seguridad de redes IPv4 en la camada de transporte	TLS – *Transport Layer Security*, RFC2246 (http://www.ietf.org/rfc/rfc2246.txt). Caso sea necesario el protocolo TLS v1 puede emular el SSL v3. HTTP sobre TLS, RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt) Podiendo implementar los siguientes algoritmos criptográficos: - Algoritmos para cambio de llaves de sesión, durante el *handshake*: RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA - Algoritmos para definición de llave de cifracción: RC4, IDEA, 3DES - Algoritmos que implementan la función de *hash* para definición del MAC: SHA-1, SHA-256 ou 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 2402 e RFC 2404 para autenticación de cabezal del IP. http://www.ietf.org/rfc/rfc2402.txt http://www.ietf.org/rfc/rfc2404.txt IKE – *Internet Key Exchange*, RFC 2409 (http://www.ietf.org/rfc/rfc2409.txt), debe ser utilizado siempre que necesario para negociación de la asociación de seguridad entre dos entidades para cambio de material de llaveamiento. ESP – *Encapsulating Security Payload,* RFC 2406 (http://www.ietf.org/rfc/rfc2406.txt) Requisito para VPN – Virtual Private Network.	**R**	
Seguridad de redes IPv4 para protocolos de aplicación	El S/MIME v3 ,RFC2633 (http://www.ietf.org/rfc/rfc2633.txt) deberá ser utilizado cuando sea apropiado para seguridad de mensajes generales de gobierno.	**R**	
Seguridad de redes IPv6 en la camada de red	El IPv6 definido en la RFC2460 (http://www.ietf.org/rfc/rfc2460.txt) presenta implementaciones de seguridad nativas en el protocolo. Las especificaciones del IPv6 definirán dos mecanismos de seguridad: la autenticación de cabezal AH (*Authentication Header*) RFC2402 (http://www.ietf.org/rfc/rfc2402.txt) o autenticación IP, y la seguridad del encapsulamiento IP, ESP (*Encrypted Security Payload*) RFC2406 (http://www.ietf.org/rfc/rfc2406.txt).	**R**	

Componente	Especificación	SIT	Observaciones
LAN sin cable 802.11 g	El uso de la especificación WPA (*Wi-Fi Protect Access*) con el estándar 802.11g debe ser incentivado, una vez que la protección ofrecida por el estándar WEP (*Wired Equivalent Privacy*) presenta vulnerabilidades.	**R**	

Tabla 4 – Especificaciones Técnicas para Seguridad de Correo Electrónico

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Acceso a cajas postales	El acceso a la caja postal deberá 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 acceder la caja postal a través de redes no seguras (por ejemplo: Internet) se debe utilizar HTTPS de acuerdo con los estándares de seguridad de transporte descritos en la RFC 2595 (http://www.ietf.org/rfc/rfc2595.txt), que trata de la utilización del TLS con IMAP, POP3 y ACAP.	**R**	
Contenido de e-mail	El S/MIME V3 deberá ser utilizado cuando sea apropiado para seguridad de mensajes generales de gobierno. Eso induye 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) y RFC 3851 (http://www.ietf.org/rfc/rfc3851.txt).	**R**	
Transporte de e-mail	Verificar si el reverso está de acuerdo con el nombre en el HELO, para garantía del origen del mensaje y minimizar SPAM.	**F**[4]	
Firma	Utilizar estándar ICP-Brasil para la firma de e-mail, cuando exigido. En conformidad con lo dispuesto en el Decreto 3.996 de 31 de octubre de 2001.	**R**	

Tabla 5 – Especificaciones Técnicas para Seguridad – Criptografía

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Algoritmo de cifracción	3DES, AES	**R**	

[4]Posible implicación en la actuación; posible descarte de mensajes válidas; imposibilidad de tratar múltiplos dominios.

Componente	Especificación	SIT	Observaciones
Algoritmo para firma	SHA-1, SHA-256 o SHA-512 con RSA y SHA-1, SHA-256 o SHA-512 con DSA	**R**	Los sistemas deben tener soporte para el algoritmo de *hash* MD5 con RSA, para garantizar compatibilidad con implementaciones anteriores.
Algoritmo para *hashing*	SHA-1, SHA-256 o SHA-512	**R**	Los sistemas deben tener soporte para el algoritmo de *hash* MD5, para garantizar compatibilidad con implementaciones anteriores.
Algoritmo para transporte de llave criptográfica de contenido/sesión	RSA	**R**	
Algoritmos criptográficos basados en curvas elípticas	ECMQV y ECDH, ambos para acuerdo de llaves, ECDSA, para firmas digitales, y ECIES para cifracción y transporte seguro de llaves criptográficas. El uso de estos algoritmos está sujeto a reglamentación y normatización por la ICP-Brasil con relación a los requisitos de seguridad.	**E**	
Requisitos de seguridad para módulos criptográficos	FIPS 140-2 – requisitos mínimos para las soluciones de almacenamiento de llaves 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*. Adherencia al estándar: a. Seguir, por lo menos, las reglas establecidas para el nivel 1 o 2 de seguridad del estándar; b. Seguir, por lo menos, 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**	

Tabla 6 – Especificaciones Técnicas 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) conforme definido por el W3C http://www.w3.org/TR/xmldsig-core/	**R**	
Cifracción XML	Sintaxis y Procesamiento de Cifración XML (XMLenc) conforme definido por el W3C http://www.w3.org/TR/xmlenc-core/	**R**	

Componente	Especificación	SIT	Observaciones
Firma y cifracción XML	Transformación descifracción para firma XML conforme 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 Gerenciamiento de llave XML) conforme definido por el W3C http://www.w3.org/TR/xkms2/	**R**	
Autenticación y autorización de acceso XML	SAML – conforme 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 - estructura de estándares para garantizar 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).	**E**	El componente anterior (SAML) podrá juntarse 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**	

Tabla 7 – Especificaciones Técnicas para Seguridad – Servicios de Red

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Directorio	Portería Normativa Nº 2, de 3 de octubre de 2002 - Publicada en el D.O. del día 4 de octubre de 2002. Sección 1, página 85. LDAPv3 RFC 2251 (http://www.ietf.org/rfc/rfc2251.txt) LDAP v3 extensión para TLS RFC2830 (http://www.ietf.org/rfc/rfc2830.txt)	**R**	
DNS	Resolución nº. 7 de 29/07/2002 – Comité Ejecutivo del Gobierno Electrónico Prácticas de Seguridad para Administradores de Redes Internet NIC BR Security Office http://www.nbso.nic.br/docs/seg-adm-redes/seg-adm-chklist.pdf Versión 1.2 16 de mayo de 2003 Securing an internet name server, CERT – ago/2002.	**R**	

Componente	Especificación	SIT	Observaciones
Transferencia de archivos de forma segura	FTP RFC 959 (http://www.ietf.org/rfc/rfc959.txt) e RFC 2228 (http://www.ietf.org/rfc/rfc2228.txt) HTTPS RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt)	**R**	El SFTP - *Secure File Transfer Protocol* – se encuentra como "borrador", razón por la cual será abordado posteriormente http://www.ietf.org/internet-drafts/draft-ietf-secsh-scp-sftp-ssh-uri-04.txt
Newsgroup		**F**	
Mensaje instantánea	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 1305 IETF-*Network Time Protocol* – NTP *version* 3.0 (http://www.ietf.org/rfc/rfc1305.txt). RFC 2030 IETF- *Simple Network Time Protocol* - SNTP *version* 4.0 (http://www.ietf.org/rfc/rfc2030.txt)	**R**	
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.

Tabla 8 – Especificaciones Técnicas para Seguridad – Colecta y Archivamiento 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)	**E**	
Respuesta a incidentes	*Expectations for Computer Security Incident Response*, RFC 2350 (http://www.ietf.org/rfc/rfc2350.txt)	**E**	

8. Medios de Acceso

8.1. 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, funcionarios públicos, empresas privadas y otras instituciones – son:

8.1.1. Los sistemas de información del gobierno deben ser proyectados de manera a respectar la legislación brasileña, disponibilizando recursos de accesibilidad a los ciudadanos portadores de necesidades especiales, a grupos étnicos minoritarios y a aquellos bajo riesgo de exclusión social o digital. El atendimiento vía mostrador de prestación de servicios debe ser considerado en toda su alcance, de forma a posibilitar que los beneficios decurrentes del uso de los servicios de gobierno electrónico vengan a ser extendidos a la camada de la población que no puede tener acceso directo a esos servicios por medio de los dispositivos previstos.

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

- cuando utilizaren la Internet como medio de comunicación y estaciones de trabajo como dispositivo de acceso, serán preferencialmente proyectados para proveer acceso a sus informaciones con uso de tecnologías y protocolos de comunicación de la *web* basados en navegadores (*browsers*);
- cuando utilizaren otros dispositivos de acceso, como, por ejemplo, teléfonos celulares, televisión digital y tarjetas inteligentes (*smart cards*), podrán hacer uso de otras interfaces además de los navegadores *web*;
- deberán ser proyectados para disponibilizar a 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, preferencialmente con tarjetas inteligentes o *tokens*, conforme estándares preconizados por la ICP – Brasil (referencia: http://www.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, considerando acceso a los usuarios de forma directa o indirecta, por medio de la prestación de servicios vía mostrador de atendimiento;
  - tarjetas inteligentes, *tokens* y otras tarjetas;
  - otros medios de acceso, como teléfonos celulares, *hand-helds* y televisión digital serán objeto de estudio futuro para determinación de los estándares aceptos por el gobierno federal.

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 aquel dispositivo.

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

8.1.5. El desarrollo de los servicios de gobierno electrónico debe ser direccionado de manera a proveer atendimiento 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 atendimiento a aquellos usuarios portadores de necesidades especiales, requisito que envulve la utilización de recursos más sofisticados y de uso específico. De modo a conciliar esas necesidades, deberán ser observadas las recomendaciones del Modelo de Accesibilidad de Gobierno Electrónico (e-MAG)[5].

8.1.6. Cuando la Internet sea usada como medio de comunicación, los sistemas de información del gobierno deben ser proyectados de manera que lo máximo de informaciones pueda ser trabajado a partir de navegadores que atiendan al estándar mínimo expreso por el soporte a las especificaciones

[5] BRASIL. Ministerio de la Planificación, 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. Brasília, 2005. Disponible en: (http://www.governoeletronico.gov.br/emag/). Accesado en: 13/07/2006.

técnicas pertinentes previstas en la sección 8.2. Complementarmente, la e-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 requeridas por el servicio asociado.

En el atendimiento al estándar mínimo citado, deben ser consideradas las excepciones que envuelvan cuestiones 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 exista alternativa técnicamente viable, para optimizar la funcionalidad del navegador en las estaciones de trabajo. En este caso, ese software adicional deberá ser ofrecido sin pagamiento de tasa de licencia y deberá estar en conformidad con todas las especificaciones técnicas correspondientes discriminadas en la e-PING. Además de eso, deberá ser disponibilizado en repositorio seguro mantenido por el órgano gubernamental responsable por la aplicación.

8.1.8. Los servicios de gobierno electrónico deben ser proyectados de manera a garantizar a los usuarios la autenticidad del contenido por medio de emisión de certificado digital, conforme estándares preconizados por la ICP – Brasil. Referencia: http://www.icpbrasil.gov.br/. En ese sentido, todos los sitios *web* deberán obligatoriamente utilizar “https” al revés de “http”.

8.1.9. La necesidad de la sociedad aliada a 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 Administración 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* (conforme ítem 3. Políticas Generales) y para tornar viable el uso de quioscos públicos, de mostradores de atendimiento y de Centrales de Atendimiento al ciudadano (como, por ejemplo, Telecentros).

8.1.10. Los sistemas de información del gobierno federal deben prever, cuando necesario y cuando 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 reformatar, dinámicamente, el contenido *web*, de manera a adaptarse a las exigencias y a las capacidades de exhibición del dispositivo de acceso. Pueden, todavía, posibilitar la modificación del contenido de una página *web*, con base en protocolos de datos, XML, XSL, preferencias de usuario y parametrizacción de red y de dispositivos de acceso.

Esos adaptadores también podrán ser utilizados como forma alternativa de 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.). Tales aspectos son abordados por la Resolución n.º 7 del Comité Ejecutivo de Gobierno Electrónico. Referencia:

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

8.1.11. Serán considerados preferenciales aquellos tipos de archivos que tienen como estándar de empaquetamiento el “xml”, de forma a facilitar la interoperabilidad entre los servicios de gobierno electrónico.

8.1.12. Los servicios de gobierno electrónico que disponibilizen documentos a sus usuarios deberán hacerlo empleando en el propio link de acceso al documento información clara a respecto de su procedencia, versión, fecha de publicación y formato. Por fecha de publicación se entiende aquella en que el documento fue publicado en diario oficial, para los casos en que esta medida sea exigida, o la fecha de la disponibilización en el sitio, para los demás casos. Otras informaciones sobre el documento, tales como, actor, redactor, emisor, fecha tópica o otras relevantes para su precisa caracterización, deberán estar en el campo propiedades del propio documento.

8.1 Medios de Acceso: Especificaciones Técnicas para Estaciones de Trabajo

Para elaboración de minutas 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 ítem 8.1.

Ya para la elaboración de la versión final de documentos, la cual debe ser enviada a otros órganos o

mismo archivada digitalmente, se recomienda la utilización del formato pdf/a. Documentos que necesiten de garantía de integridad y/o autoría, además de estaren en formato pdf/a, deben ser firmados digitalmente por su actor, utilizando certificado ICP-Brasil.

La mención a los productos que generan los formatos de archivos citados en el ítem 8.1 tiene como objetivo único la identificación de una **referencia mínima** a partir de la cual los servicios de e-gov deben intercambiar informaciones, estando aptos a recibir o enviar archivos en **versiones iguales o posteriores** a las mencionadas.

Tabla 9 – Especificaciones Técnicas – Estaciones de Trabajo

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Navegadores (*browsers*)	Ver ítem 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 .html), generado conforme especificaciones del W3C[6].	**R**	
	XHTML versiones 1.0 o 1.1 (.xhtml), generado conforme especificaciones del W3C[7].	**R**	
	XML versiones 1.0 o 1.1 (.xml), generado conforme especificaciones del W3C[8].	**R**	
	SHTML (.shtml).	**R**	
	MHTML (.mhtl o .mht)[9].	**T**	

[6] *HTML 4.01 Specification - W3C Recommendation 24 December 1999*. Disponible en: http://www.w3.org/TR/html4/

[7] *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/

[8] *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/

[9] Formato de empaquetamiento de archivos *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 conforme especificaciones del W3C[10].	**R**	
	Open Document (.odt), generado conforme especificaciones del estándar ISO/IEC 26300[11].	**R**	
	OpenOffice.org XML (.sxw), generado en el formato del OpenOffice versión 1.0.	**T**	
	Rich Text Format (.rtf).	**R**	
	PDF (.pdf) generado en formato hasta versión 1.3.	**T**	
	PDF versión abierta PDF/A[12].	**R**	
	Texto puro (.txt).	**R**	
	HTML versión 4.01 (.html o .htm), generado conforme especificaciones del W3C.	**R**	
	Microsoft Word document (.doc), generado en el formato del MS Office hasta versión 2000.	**T**	
	Star Office document (.sdw), generado en el formato del Star Office hasta versión 5.2.	**T**	
Archivos del tipo planilla	Open Document (.ods), generado conforme especificaciones del estándar ISO/IEC 26300.	**R**	
	OpenOffice.org XML (.sxc). generado en el formato del Open Office versión 1.0.	**T**	
	Planilla StarCalc (.sdc) generado en el formato del Star Office hasta versión 5.2.	**T**	
	Planilla MS Excel (.xls), generado en el formato del MS Office hasta versión 2000.	**T**	
Archivos del tipo presentación	Open Document (.odp), generado conforme especificaciones del estándar ISO/IEC 26300.	**R**	
	OpenOffice.org XML (.sxi), generado en el formato del Open Office versión 1.0.	**T**	
	HTML (.html o .htm), generado conforme especificaciones del W3C.	**R**	
	Presentación MS Power Point (.ppt), generado en el formato del MS Office hasta versión 2000.	**T**	
	Presentación StarImpress (.sdd), generado en el formato del Star Office hasta versión 5.2.	**T**	

[10] *Extensible Stylesheet Language (XSL) Version 1.0 - W3C Recommendation 15 October 2001*. Disponible en: http://www.w3.org/TR/xsl/

[11] *Open Document Format for Office Applications (OpenDocument)* v1.0 – estándar ISO/IEC 26300. Disponible en: http://www.iso.org/

[12] *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 "banco de datos" para estaciones de trabajo	.xml	**R**	En las opciones texto plan (txt) y csv, debe ser incluido obligatoriamente el esbozo de los campos, de forma a posibilitar su tratamiento.
	.myd, .myi, generados en los formatos del MySQL, versión 4.0 o superior.	**R**	
	.txt	**R**	
	.csv	**R**	
	OpenDocument (.odb), generado conforme especificaciones del estándar ISO/IEC 26300.	**R**	
	sdb, generado en el formato del Star Office, hasta versión 5.2.	**T**	
	.mdb, generado en el formato del MS Office, hasta versión 2000.	**T**	
Intercambio de informaciones gráficas e imágenes estáticas	PNG (.png), generado conforme especificaciones del W3C[13] – ISO/IEC 15948:2003 (E).	**R**	
	TIFF (.tif)[14].	**R**	
	SVG (.svg), generado conforme especificaciones del W3C[15].	**R**	
	JPEG File Interchange Format (.jpeg, .jpg o .jfif)[16].	**R**	
	Open Document (.odg), generado conforme especificaciones del estándar ISO/IEC 26300.	**R**	
	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 conforme las especificaciones GIF87a y GIF89a[17].	**T**	
	Imagen Corel Photo-Paint (.cpt), generado en el formato del suíte Corel Draw hasta versión 7.	**T**	
	Imagen Photoshop (.psd), generado en el formato del Adobe Photoshop hasta versión 4.	**T**	

[13] *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 en: 7 diciembre de 2005.

[14] *Tagged Image File Format (Adobe Systems).*

[15] *Scalable Vector Graphics (SVG) 1.1 Specification. W3C Recommendation 14 January 2003. Disponível em:* http://www.w3.org/TR/2003/REC-SVG11-20030114/. Acesso em: 7 dez. 2005.

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

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

Componente	Especificación	SIT	Observaciones
Gráficos vectoriales	SVG (.svg), generado conforme especificaciones del W3C.	**R**	
	Open Document (.odg), generado conforme 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 Visio (.vss o .vsd), generados en el formato hasta versión 2000.	**T**	
	Windows Metafile (.wmf).	**T**	
Especificación de estándares de animación	SVG (.svg), generado conforme especificaciones del W3C.	**R**	
	GIF (.gif), generado conforme 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 vídeo	.mpg	**R**	
	.mp4	**R**	
	.mid	**R**	
	.ogg	**R**	
	.avi, con codificación Xvid.	**R**	
	.avi, con codificación divX.	**T**	
	.mp3	**T**	
	.rm, generado en el formato de los aplicativos Real Audio Media Player, hasta versión 8.	**T**	
	.ra, generado en el formato de los aplicativos Real Audio Media Player, hasta versión 8.	**T**	
	.ram, generado en el formato de los aplicativos Real Audio Media Player, hasta versión 8.	**T**	
	.rmm, generado en el formato de los aplicativos Real Audio Media Player, hasta versión 8.	**T**	
	.avi	**T**	
	.wav	**T**	
	.swf, generado en el formato del Macromedia Flash, hasta versión 4 o por el Macromedia Shockwave, versión 1.	**T**	
	.wmv, generado en el formato del Windows Media Player, hasta versión 6.4.	**T**	
	.wma, generado en el formato del Windows Media Player, hasta versión 6.4.	**T**	
	.mov, generado en el formato del Apple Quicktime, hasta versión 6.	**T**	
	.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**	
	MS Cabinet (.cab).	**T**	
Georreferencia- - estándares de archivos para estaciones de trabajo	Asunto en estudio.	**E**	
Programación Extendida (Plug-ins)	Asunto para consideración futura.	**F**	

8.2. Medios de Acceso: Especificaciones Técnicas para *tokens, Tarjeta*s Inteligentes y Tarjetas en General

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

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

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

Según aquella Resolución, los medios de comunicación que almacenan los certificados digitales y respectivas lectoras, además de los sistemas y equipamientos necesarios a la realización de la certificación digital, deberán obedecer a estándares y especificaciones técnicas mínimas, para garantizar su interoperabilidad y la confiabilidad de los recursos de seguridad de información por ellos utilizados.

Por el reglamento son pasibles de homologación medios de comunicación como *tokens* criptográficos y *smart cards*, sistemas como de firma electrónica, de autenticación de firma, de autoridades certificadoras y de registro, y equipamientos como los de HSM, sincronismo y sello de tiempo, entre otros. Los productos homologados por ese 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 una determinada tarjeta inteligente o *token* no podrán estar protegidos por cualquier tipo de licenciamiento que prohíba su lectura por cualquier otro software que no el del proveedor de aquella tarjeta inteligente o *token*.

La estandarización de esos dispositivos facilitará la inserción de Brasil en acuerdos internacionales relativos a certificación digital, además de mantener la adherencia a los Estándares de Interoperabilidad de Gobierno Electrónico – e-PING y ayudar a masificar el uso de la certificación, pues entre otros aspectos podrá contribuir para el barateamiento de esa 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 diferentes 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*, a saber, dispositivos que manejan certificados digitales. Todavía fueron incorporadas las normas ISO para tarjetas magnéticas y tarjetas ópticas, aquellas tradicionales y de bajo costo, estos más innovadores 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 y mapear, en el ámbito del gobierno federal, las acciones y planes de gobierno que usan algún tipo de tarjeta inteligente y que, por consiguiente, deben ser contemplados. Deberá ser ejecutada una pesquisa exhaustiva que dé subsidios para la inclusión o no, en la e-PING, de los estándares de tarjetas efectivamente usadas por los órganos de gobierno. Como ejemplo de esa situación, pueden ser citados los llamados *embossed smart cards* (ISO/IEC 7811), tarjetas gravadas en relieve, que no son contemplados en esta versión. Caso sea constatada, en esa pesquisa, 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.

Todavía para las versiones futuras, serán analizados profundamente los estándares típicamente direccionados para 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 ticketes) sin contacto,

direccionados para sistemas de transportes públicos. Se deberán evaluar las estandarizaciones, sistemas de patentes y licenciamientos que por ventura puedan existir.

Tabla 10 – 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**	Todos 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 intersectorial.	**A**	Todos.	Conforme elección 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 actual edición fue publicada en julio de 1999. La actual edición fue publicada en agosto de 1999.

Componente	Especificación	SIT	Aplicable a	Observaciones
Aplicaciones incluyendo múltiplas 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 accesar archivos, inicialización de aplicativos de tarjeta, y canales lógicos para utilización cuando la tarjeta pueda tener 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 descritos, y de esta forma el estándar trata los códigos de comando como aplicaciones específicas cuando no definidas en esta parte.
	ISO/IEC 7816-7 Parte 7: Comandos intersectoriales para *Structured Card Query Language* (SCQL);	**R**		Conforme elección 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 manoseo dinámico de aplicaciones múltiples en tarjetas de circuitos integrados.	**R**		
	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 – Interface hombre-máquina – Parte 1: Principios de proyecto para interface de usuario Sistemas de tarjeta de identificación **EN 1332-4:**1999 – Interface Hombre-máquina – Parte 4: Codificación de exigencias de usuario para personas con necesidades especiales.	**R**	Todos.	

Componente	Especificación	SIT	Aplicable a	Observaciones
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 síncronos. **ISO/IEC 7816—12** Parte 12: Interface 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: Interface de potencia y señal de frecuencia de radio.	**R**	Tarjetas de circuito integrado de proximidad.	Esta parte define la interface de frecuencia de radio, y contiene dos técnicas de modulación bien diferentes (Tipos A y B) para la comunicación de datos entre tarjeta y terminal. El tipo A es 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 de eso, 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: Interface e inicialización por el aire;	**R**	Tarjetas de circuito(s) integrado(s) de proximidad sin contacto.	

Componente	Especificación	SIT	Aplicable a	Observaciones
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.	Conforme elección del GT de la ICP-Brasil
	Tarjetas de identificación **ISO/IEC 14443-3** - Tarjetas de circuito(s) integrado(s) sin contacto – Tarjetas de proximidad – Parte 3: Inicialización y anticolisión.	**R**	Tarjetas de circuito(s) integrado(s) de proximidad.	Esta parte dá continuidad al duopolio de los Tipos A y B, 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 estén activas dentro del campo RF del terminal.
	Tarjetas de identificación **ISO/IEC 14443-4** – Tarjetas de circuito(s) integrado(s) sin contacto – tarjetas de proximidad – Parte 4: Protocolos de transmisión.			Este contiene informaciones de alto nivel (nivel de mensaje) de protocolo de transmisión de datos, equivalentes al protocolo T=1 do ISO/IEC 7816, y es un puente sobre el ISO 7816-4. Solamente para tarjetas Tipo A o 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 originada de 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.	

Componente	Especificación	SIT	Aplicable a	Observaciones
	Tarjetas de transacciones financieras **ISO 10202-2** Arquitectura de seguridad de sistemas transacción financiera usando 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 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.	**F**	Tarjetas de circuito(s) integrado(s) de acoplamiento fuerte.	
Los Estándares de físico/físico y de interface cubren las dimensiones de la tarjeta; localidad y *layout* de contactos.	**Características físicas** Tarjetas de identificación **ISO/IEC 7810**	**R**	Todos las tarjetas de contacto y combinación	Para asegurar que puedan ser leídos en lectora estándar, todas las tarjetas deben seguir el formato ID-1 conforme 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. Conforme elección del GT de la ICP-Brasil y Manual de Conductas Técnicas del ITI – Volumen I.

Componente	Especificación	SIT	Aplicable a	Observaciones
	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 en 15-07-2000.	**R**	Tarjetas de circuito(s) integrado(s) de proximidad sin contacto.	Esta parte del **ISO/IEC 15693** fue publicada en 15-07-2000.
	Tarjetas de identificación **ISO/IEC 10536-1** – *Tarjeta*s de circuito(s) integrado(s) sin contacto Parte 1: Características físicas; **ISO/IEC 10536-2** Parte 2: Dimensiones y localización de las áreas de acoplamiento.	**F**	Tarjetas de circuito(s) integrado(s) de acoplamiento fuerte.	
	Identificadores táctiles. Sistemas de Tarjetas de identificación **BS EN 1332-2** – Interface 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 dado como auxilio a los deficientes visuales.	Algunos equipamientos de personalización de tarjetas, a menos que modificados, podrán tener dificultad en el procesamiento de tarjetas con identificadores táctiles del tipo '*notch*' ('relieve'). Un acuerdo, portanto, debe ser realizado junto al proveedor del servicio de personalización para la utilización de tales tarjetas.

Componente	Especificación	SIT	Aplicable a	Observaciones
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 Parte 1: Ciclo de vida de la tarjeta; Parte 2: Principios y resumen general; Parte 3: Relacionamientos de llave criptográfica; Parte 4: Módulos seguros de aplicación; Parte 5: Utilización de algoritmos; Parte 6: Verificación del portador de la tarjeta; Parte 7: Administración de llave.	**F**	Todos.	

Componente	Especificación	SIT	Aplicable a	Observaciones
Infraestructura del terminal	Sistemas de tarjetas de identificación EN 1332-3:1999 – Interface 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 Computador Personal Parte 1. Introducción y Visión General de la Arquitectura Parte 2. Requisitos de Interface para Tarjetas Compatibles con CI y Dispositivos de Interface Parte 3. Requisitos para Dispositivos de Interface Conectados a PC Parte 4. Consideraciones del proyecto IFD e Información de Referencia del Proyecto Parte 5. Definición del Administrador de Recursos ICC Parte 6. Definición de la Interface 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 gerenciamiento de certificados digitales.	
	Estándar FIPS-140-2.	**A**	Todos.	Según el ítem 1 del GT de la ICP-Brasil: seguir por lo mínimo las reglas establecidas para el nivel 1 de seguridad del FIPS-140-2. Seguir por lo mínimo las reglas establecidas para el nivel 2 de seguridad para verificación de violación del hardware.

Componente	Especificación	SIT	Aplicable a	Observaciones
Tarjetas tipo **Java Card®**	API (*Application Programming Interface*) para la plataforma de tarjetas Java Card.	**A**	Esta API define un conjunto de clases a partir de las cuales la tecnología Java Card basada en *applets* puede ser construida.	Versión general para la tecnología Java Card es 2.2.1 (octubre de 2003), http://java.sun.com/products/javacard/
	Especificación para el ambiente de ejecución (*runtime environment*) para la plataforma Java Card.	**A**	Esta especificación describe el ambiente requerido para la ejecución de *applets* basado en tarjetas Java Card.	
	Especificación para la máquina virtual para la plataforma Java Card.	**A**	Esta especificación define la configuración requerida para la máquina virtual de la tarjeta.	

9. Organización e Intercambio de Informaciones

9.1. Organización e Intercambio de informaciones: Políticas Técnicas

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

9.1.1. Uso de XML para intercambio de datos.

9.1.2. Uso de 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.

9.2. Organización e Intercambio de Informaciones: Especificaciones Técnicas

Tabla 11 – 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	**R**	
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	**R**	
Definición de los datos para intercambio	XML *Schema* como definido por el W3C: -XML *Schema Part 0: Primer* http://www.w3.org/TR/2004/REC-xmlschema-0-20041028/ -XML *Schema Part 1: Structures* http://www.w3.org/TR/xmlschema-1/structures -XML *Schema Part 2: Datatypes* http://www.w3.org/TR/xmlschema-2/datatypes UML (*Unified Modeling Language*) como definido por el OMG http://www.omg.org/gettingstarted/specsandprods.htm/	**R**	
Descripción de datos	RDF (*Resource Description Framework*) Como definido por el W3C.	**F**	
Elementos de Metadatos para gestión de contenidos	e-PMG – Estándar de Metadatos para el Gobierno Electrónico conforme definición en el sitio http://www.eping.e.gov.br	**E**	
Taxonomía para navegación	LAG - Lista de Asuntos del Gobierno, conforme definición en el sitio http://www.eping.e.gov.br	**E**	
Definición de datos	Catálogo de Estándares de Datos según definición en http://www.eping.e.gov.br	**E**	

9.3. Notas sobre XML y *Middleware*

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

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

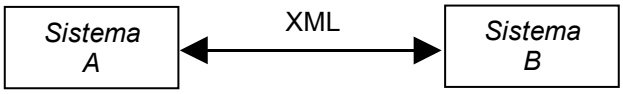

Figura 5 – Modelo XML Directo – Intercambio Directo.

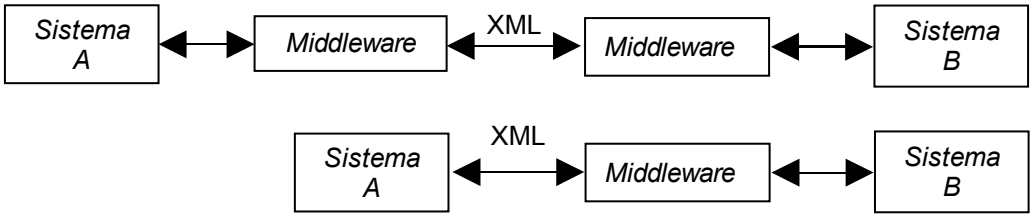

Figura 6 – Intercambios vía *middleware.*

9.4. Notas sobre Asuntos en Estudio y Elaboración

Lista de Asuntos de Gobierno: Taxonomía para Navegación (LAG)

Órganos de gobierno disponibilizan informaciones y servicios en portales y sitios de la *web*, pero la complejidad de la estructura gubernamental puede hacer de la localización de la información una tarea ardua.

La Lista de Asuntos del Gobierno: Taxonomía para Navegación (LAG), está siendo creada para ayudar personas a encontrar informaciones independiente del conocimiento de la estructura del gobierno o de cual órgano es responsable por el asunto.

Los mecanismos utilizados en los populares directorios de la Internet son los más conocidos ejemplos de listas de categorías.

La versión cero de la LAG está en fase final de elaboración.

Estándar de Metadatos para el Gobierno Electrónico (e-PMG)

La simplificación de la busca por informaciones debe ser una meta primordial de los gobiernos de esta era de la información. Esa constatación estimula la creación de un Estándar de Metadatos para el Gobierno Electrónico (e-PMG), en elaboración.

Metadatos son datos relativos a otros datos, o sea, datos estructurados y/o codificados que describen y permiten encontrar, administrar, comprender y preservar otros datos al largo del tiempo.

El e-PMG será basado en el estándar de metadatos Dublin Core (DCMI – *Dublin Core Metadata Iniciative*).

10. Áreas de Integración para Gobierno Electrónico

10.1. Áreas de Integración para Gobierno Electrónico: Políticas Técnicas

Las directrices para el segmento son:

- Las especificaciones técnicas bajo responsabilidad del segmento incluyen:
  - XML *Schemas* referentes a aplicaciones direccionadas para Áreas de Actuación de Gobierno, organizados en la forma de Catálogo, disponible en el sitio de la e-PING y presentado con los contenidos actuales en el tópico a seguir;
  - Componentes relacionados a temas transversales a las Áreas de Actuación de Gobierno, cuya estandarización sea relevante para la interoperabilidad de servicios de Gobierno Electrónico, tales como Procesos e Informaciones Geográficas.
- En lo que se refiere a XML *Schemas* referentes a aplicaciones direccionadas para Áreas de Actuación de Gobierno, el segmento actuará buscando la identificación, acompañamiento 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 las instancias competentes en lo que se refiere a la priorización;
- Las especificaciones técnicas referentes a XML *Schemas* constantes del Segmento Organización e Intercambio de Informaciones deben ser atendidas por los proponentes;
- A partir del entendimiento de que la materialización del uso de XML *Schemas* se dá a través de servicios interoperables:
- Se Recomienda que la Arquitectura Orientada a Servicios (SOA) y a políticas técnicas relacionadas al Segmento Interconexión sean observadas en el proyecto e implementación de aplicaciones basadas en los XML *Schemas* referidos;
  - El segmento pasa a referenciar la iniciativa “Arquitectura Referencial de Interoperacción de los Sistemas Informatizados de Gobierno (AR)”, que es un modelo de Arquitectura Orientada para Servicios, adaptado a la realidad de los Sistemas Informatizados de Gobierno y que, puede ser accesada en http://i3gov.cos.ufrj.br/igov/;
- Existe fuerte interligación entre el Catálogo de Estándares de Datos y el Catálogo de XML *Schemas* y, consideradas las especificidades de los contenidos, se busca mantener los principios generales y mecanismos de gestión compatibles.

10.2. Áreas de Integración para Gobierno Electrónico: Notas sobre Catálogo de XML *Schemas*

10.2.1. Consideraciones Iniciales

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. En este sentido, la constitución de repositorio que permita a administradores y proyectistas de aplicaciones de Gobierno Electrónico consultar XML *Schemas* consolidados, bien como proponer la catalogación de esquemas bajo su responsabilidad, tiene innegable contribución para consolidar buenas prácticas de interoperabilidad en el ámbito gubernamental.

10.2.2. Objetivo

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

10.2.3. Descripción

El Catálogo contiene los estándares aceptos, en la forma de XML *Schemas* para intercambio de datos envolviendo el sector público. Tales estándares tanto pueden constituirse en un único esquema, como en un conjunto de XML *Schemas*, desde que el conjunto se refiera a una misma temática dentro del Área de Integración asociada.

La publicación de XML *Schemas* no implica automáticamente en garantía de acceso a los contenidos

correspondientes o servicios asociados, para lo que pueden ser definidas reglas específicas por el respectivo administrador.

10.2.4. Propiedad y Responsabilidad

La Coordinación de la e-PING es responsable por este Catálogo, en especial por el gerenciamiento de los procesos de cambios y por fomentar que los estándares sean usados en desarrollos futuros.

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

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

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

Las entradas en el Catálogo de XML pueden darse a través de las siguientes situaciones:

a) proposición seguida de acepte de propuesta de contenido para el Catálogo de Estándares de Datos (CPD);

b) sumisión seguida de acepte de propuesta de contenido a la Arquitectura Referencial de Interoperacción de los Sistemas Informatizados de Gobierno (AR);

c) sumisión, por profesional vinculado al sector público, de contenido directamente al Catálogo de XML *Schemas*, a través de formulario electrónico disponible a partir del sitio de la e-PING.

En las situaciones descritas en los ítems (b) y (c) los contenidos serán encaminados para análisis de los integrantes del Grupo Organización e Intercambio de Informaciones, de forma a evaluar la pertinencia de publicar Estándar(es) de Dato(s) asociado(s).

La proposición de catastro de XML *Schemas* será sometida a análisis de los integrantes del Grupo Áreas de Integración para Gobierno Electrónico por medio de formulario electrónico específico, disponible en el sitio de la e-PING (www.e-ping.e.gov.br). Serán mantenidas en el Catálogo solamente las proposiciones aceptadas, siendo que las que todavía estén en estudio, las rechazadas, así como las versiones anteriores de XML *Schemas* aceptadas serán mantenidas en ambiente “de trabajo” a ser oportunamente concebido e implementado.

Los criterios de evaluación empleados incluirán:

- reconocimiento por la comunidad usuaria;
- acuerdo del administrador del área/subárea (en el caso de no ser el, el proponente); y
- adherencia a los estándares de la e-PING.

O sea, la ocurrencia de sumisiones en que el proponente de determinado XML *Schemas* no sea el administrador del área está prevista, pero tendrá como condición adicional de acepte la concordancia del administrador, a partir de interlocución realizada por el propio proponente y/o por el Grupo Áreas de Integración para Gobierno Electrónico.

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

La carga inicial del Catálogo, presentada a seguir, fue constituida por conjuntos de XML *Schemas* relacionados a iniciativas ya mapeadas por los integrantes del Grupo Áreas de Integración para Gobierno Electrónico. El objetivo de publicar estos contenidos es el de dar visibilidad a casos de uso efectivos de XML *Schemas* por parte de la Administración Pública Federal y órganos socios.

Los contenidos consolidados en la carga inicial y las actualizaciones pueden ser consultados en la página de la e-PING (www.e-ping.e.gov.br).

10.2.6. Clave de XML *Schemas*

Cada XML *Schema*, o agrupamiento de XML *Schemas* correlativos, debe ser documentado de acuerdo con el siguiente gabarito:

ÓRGANO PROPONENTE: Nombre del Órgano superior proponente del XML *Schema*. Ej.: Ministerio de la Agricultura, Ministerio de la Educación, Ministerio del Medio Ambiente etc;

RESPONSABLE: Nombre del profesional responsable por la proposición del XML *Schema*;

CPF: CPF del profesional responsable por la proposición del XML *Schema*;

UNIDAD DE LOTEO: Unidad de loteo del responsable por la propuesta de catastro. Indicar la secuencia de unidades hasta el Órgano superior, por ejemplo, GIS/DSI/SLTI/MP;

E-MAIL: Dirección electrónica del profesional responsable por la proposición del XML *Schema*;

TELÉFONO 1: Número del teléfono de contacto con profesional responsable por la proposición del XML *Schema*;

TELÉFONO 2: Número del teléfono de contacto alternativo con profesional responsable por la proposición del XML *Schema*. Campo de relleno opcional;

INDICADOR DE GESTIÓN: Indicación de la situación del proponente en relación a la gestión del área/subárea la que se refiere el XML *Schema*. Debe ser relleno a través de la elección de una de las opciones (Si o No);

ÓRGANO ADMINISTRADOR: Aquel órgano con atribuciones para administrar el área/subárea a la cual se refiere el XML *Schema*. Debe ser relleno solamente cuando el indicador de gestión sea “No” y el órgano administrador sea de conocimiento del proponente;

NOMBRE DEL XML *SCHEMA*: Denominación usual del agrupamiento o del único XML *Schema* que se propone catalogar;

VERSIÓN: Versión del XML *Schema* que se propone catalogar;

URL DEL XML SCHEMA: URL en que será encontrado archivo XSD (Definición de XML *Schema*) e informaciones detalladas sobre el (conjunto de) XML *Schema*;

DESCRIPCIÓN: Breve descripción sobre el (conjunto de) XML *Schema*. Y consideraciones que el proponente considerar pertinente.

SUBÁREA: Denominación usual adentro del área de actuación de gobierno la cual el conjunto de XML *Schema* se refiere, debe ser informada solamente cuando el área no sea suficiente para calificar la temática contemplada por el XML *Schema*;

XML *SCHEMAS* COMPONENTES: Nombre de los XML *Schemas* que componen aquel que está siendo catastrado.

10.2.7. Clasificación del Catálogo de XML *Schemas*

El Catálogo de XML *Schemas* será organizado por Áreas Temáticas de Actuación de Gobierno, en el cual serán relacionados XML *Schemas* organizados según clasificación de 1º nivel dada por la Lista de Áreas de Actuación de Gobierno, que tiene como referencia el Plan Plurianual (PPA), y es presentada a seguir:

Lista de Áreas de Actuación de Gobierno, basada en el Plan Plurianual – PPA:

1. Asistencia Social;
2. Salud;
3. Seguridad Pública;
4. Educación;
5. Administración;
6. Administración Tributaria;
7. Habitación;
8. Ciencia y Tecnología;

9. Comercio y Servicios;
10. Relaciones Exteriores;
11. Defensa Nacional;
12. Encargos Especiales;
13. Cultura;
14. Gestión Ambiental;
15. Seguridad Social;
16. Trabajo;
17. Transporte;
18. Energía;
19. Agricultura;
20. Organización Agraria;
21. Comunicaciones;
22. Judicial;
23. Legislativa;
24. Esencial a la Justicia;
25. Derechos de la Ciudadanía;
26. Deporte y Ocio;
27. Indústria;
28. Saneamiento;
29. Urbanismo.

La versión electrónica del Catálogo de XML *Schemas* dará como opción de búsqueda alternativa a la clasificación por Lista de Áreas de Actuación de Gobierno, lista alfabética de los XML *Schemas* catalogados.

10.3. Áreas de Integración para Gobierno Electrónico: Especificaciones Técnicas

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

Tabla 12 – Especificaciones para Áreas de Integración para Gobierno Electrónico – Temas Transversales a Áreas 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, conforme 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 orquestración de procesos y coreografía serán futuramente conducidos por el grupo.
PROCESOS – Notación de Modelado de Procesos	BPMN 1.0, conforme definido por el OMG: http://www.bpmn.org/Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf	**R**	

Temas	Especificación	ST	Observaciones
GEOPROCESAMIENTO – Interoperabilidad entre sistemas de información geográfica	WMS, WFS, WCS e GML, conforme definido por el OGC: http://schemas.opengis.net/gml/3.1.1/ http://schemas.opengis.net/wcs/1.0.0/ http://schemas.opengis.net/wfs/1.1.0/ http://schemas.opengis.net/wms/1.3.0/	**R**	
	SFS, conforme definido por el OGC.	**E**	

Tabla 13 – Especificaciones para Áreas de Integración para Gobierno Electrónico – Catálogo de XML *Schemas* referentes a Áreas de Actuación de Gobierno

Área/Subárea	Especificación	Observaciones
ADMINISTRACIÓN – Compras Gubernamentales	https://www.comprasnet.gov.br/xml/aviso.xsd https://www.comprasnet.gov.br/xml/consultamatserv.xsd https://www.comprasnet.gov.br/xml/dispinex.xsd https://www.comprasnet.gov.br/xml/contratoent.xsd https://www.comprasnet.gov.br/xml/empenho.xsd https://www.comprasnet.gov.br/xml/resultado.xsd	XML *Schemas* por el sistema ComprasNet referentes a Encerramiento de Resultado de Licitación, Empeño, Dispensa / Inexigibilidad de Licitación, Consulta de Material vía CATMAT, Contrato de entidades en el SISG y Aviso de Licitación.
ADMINISTRACIÓN – Estructuras de Gobierno	http://guialivre.governoeletronico.gov.br/igov/	Conjunto de XML *Schemas* relacionados a los sistemas de gestión administrativa de la Administración Pública Federal.
ADMINISTRACIÓN – Gestión de Redes Locales/CACIC	http://guialivre.governoeletronico.gov.br/cacic/sisp2/invent/Invent.html	Estos *Schemas* hacen parte de la solución CACIC, que fue desarrollada por Dataprev, y son utilizados para transmisión de datos de inventario de *hardware* e de sus componentes conectados en ambiente de red. La implementación de estos *Schemas* ocurrió en sociedad con el Ministerio del Medio Ambiente (MMA).
ADMINISTRACIÓN TRIBUTARIA – Nota de Gastos Electrónica	http://200.198.224.29/portal/info/Schemas.htm	*Schema* XML utilizado para emisión de la nota de gastos electrónica, en sustitución a la de papel y con validad jurídica para todos los fines. Este proyecto es coordinado por el Encuentro Nacional de los Administradores y Coordinadores Tributarios Estaduales (ENCAT) y desarrollado en sociedad con

Área/Subárea	Especificación	Observaciones
		la Secretaría de la Receita Federal.
DERECHOS DE LA CIUDADANÍA – Registros	http://www.mj.gov.br/Schemas/Cartorio/ConsultaCartorio.xsd	Corresponde al Ministerio de la Justicia mantener el Catastro Nacional de Registros Civiles. Este esquema, a partir de un filtro generado por la unidad de la federación y/o el municipio y/o barrio y/o la atribución de la oficina de registros civiles, consulta el catastro de oficinas registros civiles de Brasil devolviendo una lista de las oficinas de registros civiles que atienden al filtro. El esquema permite, además, entregar el detallamiento de cada oficina de registros civiles listada.
DERECHOS DE LA CIUDADANÍA – Defensa del Consumidor	http://www.mj.gov.br/Schemas/DireitoConsumidor/SINDEC.xsd	Este esquema permite la consulta a la estadística consolidada sobre atendimiento en los Procons asociados al Sistema Nacional de Informaciones de Defensa del Consumidor (SINDEC) por unidad de la federación o nombre del proveedor o por el CNPJ, devolviendo las estadísticas de atendimiento adherentes a los criterios pesquisados.
DERECHOS DE LA CIUDADANÍA – Defensa del Consumidor	http://www.mj.gov.br/Schemas/Recall/ConsultaRecall.xsd	Corresponde al Ministerio de la Justicia formular, promover, supervisionar y coordinar la política de protección de la orden económica, en las áreas de concurrencia y defensa del consumidor. El procedimiento por el cual el proveedor informa al público sobre los defectos detectados en los productos o servicios que pondrá en el mercado es llamado de *recall*. Los objetivos esenciales de ese tipo de procedimiento son el de proteger y preservar la vida, salud, integridad y seguridad del consumidor, bien como de evitar o minimizar cualquier especie de perjuicio, sea de orden material, o sea de orden moral. Este esquema permite consultar la base de banco de

Área/Subárea	Especificación	Observaciones
		datos de *recall* del Departamento de Protección y Defensa del Consumidor para conferir si un determinado producto está siendo objeto de *recall.* Para eso, el esquema al ser accionado retorna a la lista de proveedores/modelos que hicieron *recall*, posibilitando verificar detalles del *recall* a partir de la elección del producto o número de serie, chasis, modelo entre otros.
DERECHOS DE LA CIUDADANÍA	http://www.mj.gov.br/Schemas/ClassificacaoIndicativa/ConsultaClassindFilmes.xsd	Corresponde al Ministerio de la Justicia ejercer la clasificación, para efecto indicativo, de diversiones públicas y de programas de radio y televisión. A partir del nombre de película o programa, este esquema consulta el banco de datos de Clasificación Indicativa y devuelve una lista de coincidentes para los cuales pueden ser exhibidos detalles de la clasificación indicativa y la justificativa.
GESTIÓN AMBIENTAL – Licenciamiento Ambiental/PNLA	http://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_completo.xsd http://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_simples.xsd http://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_totalizadores.xsd	Los *Schemas* se aplican al ámbito del licenciamiento ambiental y son adoptados por la plataforma del Portal Nacional de Licenciamiento Ambiental (PNLA) del MMA que consolida las informaciones sobre licencias ambientales de varios estados por medio de *Web Services*. Sigue abajo la descripción del propósito de cada esquema: •licenciamiento_ambiental_completo.xsd – provee el esquema de las informaciones pertinentes a una licencia ambiental, llevando en consideración los datos frecuentes en los diversos órganos licenciadores investigados; •licenciamiento_ambiental_simples.xsd – provee el esquema para la composición de un informe conteniendo un

Área/Subárea	Especificación	Observaciones
		conjunto de licencias con los datos mínimos de su identificación. Es útil para la navegación preliminar sobre las licencias para un posterior detallamiento que es hecho por medio del primer esquema; •licenciamiento_ambiental_ totalizadores.xsd – consolida el cuantitativo de licencias basado en un tema arbitrario.
JUDICIAL – Servicios de Oficinas de Registro Extrajudiciales	www.anoregsp.org.br/arquivos	Los XML *Schemas* se refieren a la estandarización de las consultas a los servicios de oficinas de registro extrajudiciales

11. Glosario de Siglas y Términos Técnicos

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 compilación de referencias de material utilizado para la producción de documentos y para inclusión en bibliografías, resumen, reseñas, recensiones y otros.

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

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

BPM - *Business Process Management*: Visión de los procesos de negocio de una organización como flujo de servicios utilizando estándares de representación de notación, ejecución y coordinación en XML, cuyo rigor semántico permite su interoperabilidad entre sistemas de plataformas diferentes, siendo de esa forma un fundamento para la implementación 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, intraorganización, es denominada esa coordinación como Orquestración. Cuando, la coordinación se dá sin la subordinación a un proceso maestro, en general, interorganización, se denomina Coreografía.

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

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

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

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

DNS – *Domain Name System* (Sistema de Nombres de Dominio): forma como los nombres de dominio son encontrados y traducidos en la dirección de protocolo de la Internet. Un nombre de dominio es un recurso fácil de ser recordado cuando 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 simples de cambiar archivos entre computadores en la Internet.

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

***Hand-helds*:** Computador de mano, también conocido como PDA, pocket PC o palm top. Equipamiento portátil desarrollado para servir como dispositivo de acceso.

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

***Hashing*:** es la transformación de una cadena de caracteres en un valor de tamaño fijo normalmente menor o en una llave que representa la cadena original. Es utilizada para indexar y recuperar ítems en un banco de datos, porque es más rápido encontrar el ítem utilizando la menor llave transformada de 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, vídeo y otros archivos multimídia) 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 criptoanalisa solicitaciones y retornos de páginas retornadas por el servidor *web*. El HTTPS es solamente el uso del SSL (*Secure Sockets Layer*) del Netscape como una subcamada bajo la organización normal de los programas de las aplicaciones HTTP.

ICP – Brasil: conjunto de técnicas, prácticas y procedimientos, a ser implementado 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 llave 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 vuelven 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 a Mensaje en la Internet): protocolo estándar para accesar 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): método o protocolo a través de los cuales los datos son enviados de un computador a otro en la Internet. Cada computador, en la Internet, posee por lo menos una dirección IP que lo identifica únicamente en relación a todos los otros computadores de la Internet.

IPSec – *Internet Protocol Security* (Seguridad de Protocolo de Internet): estándar de desarrollo relativo a la seguridad en la camada de la red o del procesamiento de paquetes de la comunicación en red. Una grande ventaja del IPsec es que las disposiciones de seguridad pueden ser manipuladas sin exigir cambios en los computadores de usuarios individuales. El IPsec provee dos opciones de servicios de seguridad: *Authentication Header* (AH), que esencialmente permite la autenticación del remitente de datos, y *Encapsulating Security Payload* (ESP), que soporta tanto la autenticación del remitente cuanto a la codificación criptográfica de datos.

IPv4 – *Internet Protocol Version* 4 (Protocolo de Internet Versión 4): ver “IPv6”.

IPv6 – *Internet Protocol Version* 6 (Protocolo de Internet Versión 6): último nivel del IP, hoy ya incluido como parte del soporte IP en muchos productos, incluso los principales sistemas operacionales de computadores. Formalmente, IPv6 es un conjunto de especificaciones de la IETF. El IPv6 fue proyectado como un conjunto evolutivo de perfeccionamientos hechos al IPv4. El perfeccionamiento más significativo del IPv6 en relación al IPv4 es que las direcciones IP son aumentadas de 32 bits para 128 bits.

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

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

Medio de acceso: conjunto de componentes físicos (dispositivos de acceso) y de no físicos (software básico, aplicativos, etc.) que permite al usuario el acceso a un servicio de gobierno electrónico.

Mensajería en Tiempo Real o Mensaje Instantánea: Es un tipo de comunicación que permite que un usuario mande y reciba mensajes en tiempo real con otro usuario también conectado a la red.

Metadatos: son informaciones adicionales necesarias para que los datos se vuelvan útiles. Es información esencial para que se pueda hacer uso de los datos. En suma, metadatos son un conjunto de características sobre los datos que no están normalmente incluidas en los datos propiamente dichos. http://www.isa.utl.pt/dm/sig/sig20002001/TemaMetadados/trabalho.htm.

***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 asunto que consiste en mensajes enviadas a un sitio central en la Internet y redistribuidas por la Usenet, una red global de grupos de discusión de noticias. Los usuarios pueden enviar mensajes a grupos de noticias existentes, responder a mensajes anteriores y crear nuevos grupos de noticias.

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

Estándar abierto: todo el estándar tecnológico establecido por órganos internacionales o por consorcios de empresas del mercado que desarrollan especificaciones que se encuentran públicamente disponibles. El PC (computador personal) fue lanzado y es desarrollado con estándar abierto. Las especificaciones de la Internet y su desarrollo también. La grande mayoría de los lenguajes de programación también.

Estándar de Metadatos: Un conjunto de metadatos es un estándar, definido por una comunidad de usuarios, que incluye un Vocabulario de elementos descriptivos y un Esquema o reglas de codificación de estos elementos en un medio legible por computador. http://www.uff.br/gdo/htm/tsld013.htm.

***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: Sitio en la Internet que agrega servicios, noticias y grande 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 sitios 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 monitoramiento, de la gestión de los elementos interactivos, del modelo organizacional, de la identidad visual y de la seguridad de los sitios gubernamentales en la red mundial de computadores. http://www.governoeletronico.e.gov.br.

RFC – *Request for Comments* (Solicitación de Comentarios): documento formal de la IETF, resultante de modelos y revisiones de partes interesadas. La versión final del RFC se volvió un estándar en que ni comentarios ni alteraciones son permitidas. Las alteraciones pueden ocurrir, sin embargo, por medio de RFCs subsecuentes que sustituyen 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*: cifracción 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 disponibilidad de servicios del gobierno para 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 gobernabilidad, certificación y tributación;

3. prestación de cuentas públicas, transparencia y monitoramiento de la ejecución presupuestaria;

4. enseñanza a distancia, alfabetización digital y manutención de bibliotecas virtuales;

5. difusión cultural con énfasis en las identidades locales, fomento y preservación de culturas locales;

6. e-procurement, o sea, adquisición de bienes y servicios por medio de la Internet, como licitaciones públicas electrónicas, "*pregões*" electrónicos, bolsas 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 pequeñas y medianas empresas. http://www.governoeletronico.gov.br/r1.

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

- gestión de gobierno: Planeamiento, Presupuesto, Ejecución Presupuestaria, Administración Financiera, Administración de Recursos Humanos, Administración de Servicios Generales, Gestión de Documentación e Informaciones, Organización y Modernización Administrativa, Recursos de Información e Informática y Control Interno;

- actuación final de gobierno: actividades finalísticas de los 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/projetos/reg_gestao.asp.

SFS – *Simple Features Specification*: esta especificación define un formato, de acuerdo con el SQL (*Structured Query Language*) estándar para almacenamiento, lectura, análisis y actualización de "maneras simples" (datos geográficos) a través de una API (*Application Programming Interface*).

***Smart Cards*:** tarjeta de plástico, con aproximadamente el tamaño de una tarjeta de crédito, con un microchip embutido que puede ser cargado con datos, puede ser usado para efectuar llamadas telefónicas, pagamientos electrónicos en dinero y otras aplicaciones. Es periodicamente 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 cifracción RSA (Rivest-Shamir-Adleman). S/MIME describe como informaciones encriptadas y un certificado digital pueden ser incluidos como parte del contexto 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): Arquitectura propuesta para interoperabilidad de sistemas por medio de conjunto de interfaces de servicios débilmente acoplados (*loosely coupled*), adonde los servicios no necesitan de detalles técnicos de la plataforma de los otros servicios para el intercambio de informaciones a ser realizada.

SOAP – *Simple Object Access Protocol* (Protocolo Simples para Acceso a Objetos): describe un modelo para el empaquetamiento 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 computador disponible a través de su código-fuente y con la permisión para cualquier uno usarlo, copiarlo y distribuirlo, sea en su forma original o con modificaciones, sea gratuitamente o con costo. El software libre es necesariamente no propietario, pero es importante no confundir software libre con software gratis.

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

SSL – *Secure Sockets Layer* (Capa de Soquetes Segura): es un protocolo comúnmente utilizado

para administrar 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, objetivando facilitar a los usuarios de sitios y portales de internet a descubrir información a través de 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 computadores 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 accesar el computador de otra persona, asumiendo que le dieron permisión. Más técnicamente, Telnet es un comando de usuario y un protocolo subliminal TCP/IP para accesar computadores remotos.

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 obtener 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 por el cual los desarrolladores registran los *Web Services* disponibles que permiten a los clientes el descubrimiento y la utilización de los servicios situados en Extranets y Intranets.

UDP – *User Datagram Protocol* (Protocolo de Datagrama de Usuarios): protocolo de comunicación que ofrece una cantidad limitada de servicio cuando los mensajes son intercambiadas entre computadores 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 de un computador para otro. Diferentemente del TCP, el UDP no provee el servicio de dividir un mensaje en paquetes y remontarla en otra extremidad. El UDP no provee la secuencia de los paquetes en que los datos llegan. Eso significa que el programa de aplicativo que usa el UDP debe garantizar que el mensaje entero chegó y está en orden. Los aplicativos de red que quieren ahorrar el tiempo de procesamiento porque tienen unidades muy pequeñas de datos para cambiar pueden preferir el UDP en vez del TCP.

UML – *Unified Modeling Language* (Lenguaje de Modelado Unificado): anotación estándar de modelo de objetos del mundo real como el primer paso en el desarrollo de una metodología de design orientado a objetos.

URI - *Uniform Resource Identifier* (Identificador Único de Recurso): estándar de codificación de nombres y direcciones en la Internet. Una URI es compuesta por un nombre (ej.: file, http, ftp, news, mailto, gopher), seguido por dos puntos, y por fin, 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 sometidas 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 particular, que se utiliza de 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 dá 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 visa 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 Grande Área): Red de computadores que abarca extensas áreas geográficas como un estado, un país o un continente.

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

WFS – *Web Feature Service*: especificación OpenGIS que presenta una forma de acceso (inserción, actualización, exclusión y análisis) a la manera a través del ambiente *Web* (HTTP).

WMS – *Web Map Service*: especificación OpenGIS que define 4 protocolos (*GetCapabilities*, *GetMap*, *GetFeatureInfo* y *DescribeLayer*) que permiten la lectura de múltiplas capas de informaciones (*layers*) 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, bien como su localización y forma de acceso.

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

XML *Schemas*: son documentos XML, encontrados también en un sitio Internet, que especifican la estructura, número de ocurrencias de cada elemento, valores permitidos, unidades, etc, o sea, el 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 planillas que describe como un dato es mandado por medio de la *web*, usando el XML, y es presentado al usuario. El XSL es un lenguaje para formatar un documento XML.

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

12. Bibliografía Consultada

Cámara Técnica de Implementación del Software Libre. Planeamiento Estratégico 2003–2004 - Directrices, Objetivos y Acciones Prioritarias.

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

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

13. Créditos

Coordinación de la e-PING

Associação Brasileira de Empresas Estaduais de Processamento de Dados (ABEP)
Dayse Vianna
Paulo Cezar Coelho

Banco do Brasil (BB)
Ulisses de Sousa Penna

Caixa Econômica Federal (CAIXA)
Ângela B. Baylo

Empresa de Tecnologia e Informações da Previdência Social (DATAPREV)
Humberto Degrazia Campedelli
José Antônio Borba Soares

Ministério da Justiça (MJ)
Jorilson da Silva Rodrigues

Ministério do Planejamento – Secretaria de Logística e Tecnologia da Informação (MP/SLTI)
Leandro Corte (Coordinador General)
Antônio Carlos Alff
Eduardo Favero
José Ney de Oliveira Lima
Leonardo Boselli da Motta
Leonardo Lanna Guillén
Nazaré Lopes Bretas
Rogério Santanna dos Santos
Sylmara Garcia

Presidência da República – Instituto Nacional de Tecnologia da Informação (ITI)
Mauricio Augusto Coelho
Renato da Silveira Martini
Viviane Regina Lemos Bertol

Serviço Federal de Processamento de Dados (SERPRO)
Antônio Sérgio Borba Cangiano
Catia Gontijo Rezende
Elói Juniti Yamaoka
Geancarlo Noronha Vinhal
Wagner Junqueira Araújo

Grupo de Trabajo Interconexión

Leonardo Lanna Guillén (MP/SLTI) - Coordinador
Carlos Bellone Neto (SRF)
Eder Manoel de Abreu (EMBRAPA)
Flávio Arthur Leal Ferreira (PROCERGS-RS)
Júlio César Japiassu Lyra (MJ)
Leonardo Boselli da Motta (MP/SLTI)
Luiz Gonzaga Costa (SERPRO)
Odilon de Freitas Militão Neto (CAIXA)
Paulo Guilherme Lanzillotti Jannuzzi (DATAPREV)
Ruben César Macedo (CELEPAR-PR)
Sílvia Aparecida da Cunha (MP/CGTI)
Ulisses de Sousa Penna (BB)
Vicente Eduardo Costa de Paula Pessoa (SRF)
Webster's Gomes Fernandes (MI)

Grupo de Trabajo Seguridad

Jorilson da Silva Rodirgues (MJ) – Coordinador
Alerrandro Luís Augusto Caetano Corrêa (MEC)
Alexandre Almeida Lima (SEORI)
Alexandre Braga (CPqD)
Carlos Eduardo de Santos Souza (CENSIPAM)
Catarina da Matta (ELETROBRÁS)
Clari Dorça Stacciarini (CGU)
Cristiano Sakai (PR)
Daniel Bispo de Jesus (CODESP)
Eloi Juniti Yamaoka (SERPRO)
Ernandes Lopes Bezerra (MP/SLTI)
Etienne César Ribeiro de Oliveira (IBGE)
Humberto Degrazia Campedelli (DATAPREV)
Jailson Mario dos S. Pereira (CORREIOS)
Jean Carlo Rodrigues (ITI)
Joana D'arc Felipe dos Santos (MI)
João Carlos Levy Argel (FUNARTE)
José Ney de Oliveira Lima (MP/SLTI)
Jovino Francisco Filho (MC)
Leonice Tereza Vanni Rangel (CEPROMAT – MT)
Luiz Augusto Barbosa Mozzer (CGU)
Luiz Augusto Vieira de Melo (ANCINE)
Marco Antonio Goes de Oliveira (FNDE)
Marco Aurélio Bonato (CELEPAR)
Marcos Allemand Lopes (SERPRO)
Marcos José da Silva (DATAPREV)
Mônica Vieira Guimarães (MI)
Nilson Carlos de M. Pontes (IBGE)
Renato Navajas (MDIC)
Ronaldo Íon Miranda do Nascimento (MJ)
Ruy Siqueira de Moura (MRE)
Sérgio Carreira dos Santos (IPHAN)
Silvio Márcio Santos Nery (CGU)
Wagner Junqueira Araújo (SERPRO)

Grupo de Trabajo Medios de Acceso

Mauricio Augusto Coelho (ITI) – Coordinador
Renato da Silveira Martini (ITI) – Coordinador
Alessander Florindo da Silva (MS)
Eliane Aristóteles Moreira (DATAPREV)
Eliane Pereira dos Santos (MS)
Eloína Terezinha Domanski (MF)
Geancarlo Noronha Vinha (SERPRO)
Jean Carlo Rodrigues (ITI)
Jorilson da Silva Rodrigues (MJ)
José de Souza Rangel Filho (ATI-PE)
Juscelino Ney Carrico (SGI-MS)
Márcia Luiza Albertini (MS)
Paulo Édison de Souza (MEC)
Ricardo José Leal dos Santos (PRODERJ-RJ)
Silvio Melo de Souza (ITI)
Viviane Regina Lemos Bertol (ITI)

Grupo de Trabajo Organización e Intercambio de Informaciones

Eloi Juniti Yamaoka (SERPRO) – Coordinador
Ailton Luiz Gonçalves Feitosa (CLDF)
Aline Ramalho Bezerra (MJ)
Ana Lúcia de Medeiros (CORREIOS)

Documento de Referencia de la e-PING – Versión 2.0.1

Ana Maria Moura (PRODERJ)
Ângela B. Baylo (CAIXA)
Aurélia Dolores Gonçalves Bruner (ELETROBRAS)
Beatriz Barreto Brasileiro Lanza (CELEPAR)
Cláudia Carvalho Masset Lacombe Rocha (AN-CC)
Dalva Clementina Luca (MJ)
Dayse Vianna (PRODERJ)
Dilma de Fátima Avellar Cabral da Costa (AN-CC)
Diogo Arce Moreth (MT)
Eliane Pereira dos Santos (MS)
Elizabeth da Silva Maçulo (AN-CC)
Fernanda Hoffmann Lobato (MP/SLTI)
Flávia Lacerda Oliveira de Macedo (TCU)
João Alberto Lima (Senado Federal)
José Gabriel Medef Filho (CGU)
Luciana Ferreira Pinto da Silva (INEP)
Luiz Antônio Nery de Oliveira (DATAPREV)
Márcia Izabel Fugizawa Souza (EMBRAPA)
Márcia Luzia Albertini (MS)
Márcio Imamura (IBGE)
Marcos Augusto Francisco Borges (CPqD)
Margareth da Silva (AN-CC)
Maria Augusta de Oliveira Gomes (MF)
Maria Célia Pelisson Jacon (IBGE)
Maria das Graças Comaru de Oliveira (SERPRO)
Maria de Fátima Porcaro (IPT)
Maria Valéria Lins Tenório (ATI-PE)
Nádia Maria F. C. Abrantes Ferrão (MF)
Neuza Arantes Silva (MAPA)
Paulo César Pereira Soares (FUNARTE)
Ricardo Torres Lenzi (INEP)
Rosiane Fonseca (ANCINE)
Samuel Batista dos Santos (IPT)
Sérgio Silva dos Santos (MAPA)
Siomara Zgiet (MS)
Taciano Tres (BB)
Vicente de Paula Teixeira (CGU)
Vivianne Veras Barrozo (SERPRO)

Grupo de Trabajo Áreas de Integración para Gobierno Electrónico

Nazaré Lopes Bretas (MP/SLTI) – Coordinadora
Ana Lúcia Viçoso da Cruz Almeida (DATAPREV)
Alexandre Grossi (MD)
André Redivo (PR)
Antônio Carlos Alves Carvalho (MEC)
Caio Nakashima (MDS)
César Cardoso (CORREIOS)
Cláudio Machado (MS)
Dalva Clementina Luca (MJ)
Dayse Vianna (PRODERJ-RJ)
Edna Paulo Cirineo (SRF)
Edmar Morett (MMA)
Ednylton Maria Franzosi (MP/SLTI)
Eduardo Favero (MP/SLTI)
Efraim Soares dos Santos (CAIXA)
Elisa Torrido Lorensi (IBAMA)
Enos Josué Rose (MCIDADES)
Fábio Borges (DNPM)
Gabriel Mathias (IBICT)
João Lima (SENADO)
Jorge D.M. Cerqueira (PR/GSI)

Documento de Referencia de la e-PING – Versión 2.0.1

Jorge Luiz Salomão de Oliveira (CORREIOS)
José Eustáquio Nogueira Guimarães (PR/GSI)
José Ney de Oliveira Lima (MP/SLTI)
Karina Lima de Moura (MP/SEGES)
Leandro Corte (MP/SLTI)
Maria de Fátima (IPT)
Maria Rita Almeida (SRF)
Mauricio Dayrell (MMA)
Moema José de Carvalho Augusto (IBGE)
Mônica Lucatelli (DATAPREV)
Onivaldo Rosa Junior (MEC)
Paulo César Pereira Soares (FUNARTE)
Paulo Henrique Santana (MMA)
Pedro Paulo Cirineo (BB)
Ricardo Torres Lenzi (INEP)
Rodolfo Pinto da Luz (INEP)
Samuel Batista (IPT)
Sandro Araújo (ANA)
Silmara Ramos (PR/GSI)
Sylmara Garcia (MP/SLTI)
Valério Falcão (MP/SLTI)