

**Gobierno Brasileño  
Comité Ejecutivo de Gobierno Electrónico**



**e-PING  
ESTÁNDARES DE  
INTEROPERABILIDAD  
DE GOBIERNO ELECTRÓNICO**

**Documento de Referencia  
Versión 3.0  
14 de diciembre de 2007**

## SUMARIO

|  |    |
|--|----|
| Presentación.....  | 4  |
| Parte I – Visión General de e-PING .....   | 5  |
| 1. Introducción.....   | 6  |
| 2. Ámbito.....   | 7  |
| 2.1. Adhesión a e-PING.....  | 7  |
| 2.2. Enfoque sobre la interoperabilidad.....   | 8  |
| 2.3. Temas no tratados.....  | 8  |
| 3. Políticas Generales.....  | 9  |
| 4. Segmentación.....   | 10 |
| 4.1. Interconexión .....   | 10 |
| 4.2. Seguridad.....  | 10 |
| 4.3. Medios de Acceso.....   | 10 |
| 4.4. Organización e Intercambio de Informaciones.....  | 11 |
| 4.5. Áreas de Integración para Gobierno Electrónico.....   | 11 |
| 5. Gestión de e-PING.....  | 12 |
| 5.1. Histórico.....  | 12 |
| 5.2. Estrategia de Implantación.....   | 13 |
| 5.3. Modelo de Gestión.....  | 13 |
| 5.3.1. Atribuciones .....  | 13 |
| 5.3.2. Responsabilidades.....  | 14 |
| 5.4. Actividades adicionales.....  | 15 |
| 5.4.1. Selección y Homologación de Estándares Tecnológicos.....  | 15 |
| 5.4.2. Auditoría de Conformidad.....   | 16 |
| 5.4.3. Creación y Mantenimiento del Sitio.....   | 16 |
| 5.4.4. Acompañamiento Legal e Institucional.....   | 17 |
| 5.4.5. Divulgación.....  | 17 |
| 5.4.6. Capacitación.....   | 17 |
| 5.5. Relación con Gobierno y Sociedad.....   | 17 |
| 5.5.1. Organismos del Gobierno Federal – Poder Ejecutivo.....  | 17 |
| 5.5.2. Otras Instancias de Gobierno (otros Poderes Federales, Gobiernos Estaduales y Municipales)..... | 18 |
| 5.5.3. Organizaciones del Sector Privado y del Tercer Sector.....                                      | 18 |
| 5.5.4. Ciudadano.....  | 18 |

|  |    |
|--|----|
| Parte II – Especificación Técnica de los Componentes de e-PING.....  | 20 |
| 6. Interconexión.....  | 21 |
| 6.1. Interconexión: Políticas Técnicas.....  | 21 |
| 6.2. Interconexión: Especificaciones Técnicas.....   | 21 |
| 6.3. Web Services.....   | 23 |
| 6.4. Mensaje Electrónico (E-mail).....   | 25 |
| 6.5. VPN.....  | 26 |
| 6.6. Redes peer-to-peer.....   | 26 |
| 7. Seguridad.....  | 27 |
| 7.1. Seguridad: Políticas Técnicas.....  | 27 |
| 7.2. Seguridad: Especificaciones Técnicas.....   | 28 |
| 8. Medios de Acceso.....   | 34 |
| 8.1. Medios de Acceso: Políticas Técnicas.....   | 34 |
| 8.2. Medios de Acceso: Especificaciones Técnicas para Estaciones de Trabajo.....                               | 35 |
| 8.3. Medios de Acceso: Especificaciones Técnicas para tokens, Tarjetas Inteligentes y Tarjetas en General..... | 40 |
| 9. Organización e Intercambio de Informaciones.....  | 49 |
| 9.1. Organización e Intercambio de informaciones: Políticas Técnicas.....                                      | 49 |
| 9.2. Organización e Intercambio de Informaciones: Especificaciones Técnicas.....                               | 49 |
| 9.3. Comentarios sobre XML y Middleware.....   | 50 |
| 10. Áreas de Integración para Gobierno Electrónico.....  | 51 |
| 10.1. Áreas de Integración para Gobierno Electrónico: Políticas Técnicas.....                                  | 51 |
| 10.2. Áreas de Integración para Gobierno Electrónico: Comentarios sobre Catálogo de XML Schemas.....           | 51 |
| 10.2.1. Consideraciones Iniciales.....   | 51 |
| 10.2.2. Objetivo.....  | 51 |
| 10.2.3. Ámbito.....  | 51 |
| 10.2.4. Propiedad y Responsabilidad.....   | 52 |
| 10.2.5. Mecanismos de Gestión del Catálogo de XML Schemas.....   | 52 |
| 10.2.6. Plantilla de XML Schemas.....  | 52 |
| 10.2.7. Clasificación del Catálogo de XML Schemas.....   | 53 |
| 10.3. Áreas de Integración para Gobierno Electrónico: Especificaciones Técnicas.....                           | 54 |
| 11. Glosario de siglas y Términos Técnicos.....  | 59 |
| 12. Integrantes.....   | 66 |

### Presentación

La arquitectura e-PING – Padrones 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 de cobertura de e-PING se circunscriben a:

- Interconexión;
- Seguridad;
- Medios de acceso;
- Organización e intercambio de informaciones;
- Áreas de Integración para Gobierno Electrónico.

Para cada uno de esos segmentos, se especificaron componentes, para los cuales se establecieron 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 un sitio específico en Internet (<http://www.eping.e.gov.br>), garantizando el acceso público a las informaciones de interés general y la transparencia intrínseca a la iniciativa. El gobierno brasileño se compromete a asegurar que estas políticas y especificaciones estén en línea con las necesidades de la sociedad y con la evolución del mercado y de la tecnología.

El documento de referencia de e-PING contiene:

- Los fundamentos de concepción, implantación y administración de e-PING, relacionando los beneficios esperados con el trabajo, definiendo los límites del ámbito de la arquitectura e-PING y subrayando las premisas consideradas y las políticas establecidas;
- El modelo de gestión de e-PING, que discrimina responsabilidades, criterios de verificación de conformidad, gestión de cambios, divulgación y orientación para capacitación;
- Las políticas y las especificaciones técnicas establecidas para todos los componentes de cada uno de los segmentos de e-PING;
- Glosario de términos técnicos referenciados;
- Rol de los integrantes y colaboradores de la presente versión de este documento.

El contenido de este documento es de dominio público y no hay restricciones sobre su reproducción ni tampoco respecto a la utilización de las informaciones que contiene. La reproducción es permitida para todos los medios, sin que haya necesidad de autorización específica. El uso inadecuado del material, con fines de depreciación, será considerado objeto de tratamiento jurídico apropiado de parte del gobierno brasileño, que detiene los derechos de autoría.

Se prohíbe la utilización del todo o de parte del contenido de este documento con fines comerciales.

## **Parte I – Visión General de e-PING**

## 1. Introducción

La base para el suministro de mejores servicios, adecuados a las necesidades de los ciudadanos y de los negocios con costes reducidos, es la existencia de una infraestructura de Tecnología de la Información y Comunicación (TIC) que se presta a la función de cimiento para la creación de este servicio. Un gobierno moderno, integrado y eficiente, exige sistemas igualmente modernos, integrados y que operen con interoperabilidad, trabajando de manera íntegra, segura y coherente en todo el sector público.

En este contexto, la interoperabilidad de tecnología, procesos, información y datos es condición vital para el suministro de servicios de calidad, y se torna premisa para gobiernos en todo el mundo, como fundamento para conceptos de gobierno electrónico, o e-gov. La interoperabilidad posibilita racionalizar inversiones en TIC, compartiendo, reutilizando e intercambiando recursos tecnológicos.

Gobiernos, como el de Norteamérica, el de Canadá, el de Inglaterra, el de Australia y de Nueva Zelanda, invierten, fuertemente, en el desarrollo de políticas y procesos y en el establecimiento de estándares en TIC, montando estructuras dedicadas a la obtención de la interoperabilidad con el objetivo de ofrecer servicios de mejor calidad con costes reducidos.

El gobierno de Brasil viene consolidando la arquitectura e-PING – “Estándares de Interoperabilidad de Gobierno Electrónico”, que tiene el propósito de ser el paradigma para el establecimiento de políticas y especificaciones técnicas que permitan la prestación de servicios electrónicos de calidad a la sociedad.

### ¿Qué es interoperabilidad?

Para que se de el establecimiento de los objetivos de e-PING, es fundamental que se defina claramente lo que se entiende por *interoperabilidad*. A continuación se presentan cuatro conceptos que fundamentarán el entendimiento del gobierno brasileño sobre el tema:

“Intercambio coherente de informaciones y servicios entre sistemas. Debe posibilitar la sustitución de cualquier componente o producto utilizado en los puntos de interconexión por otro de especificación semejante, sin que ello comprometa la funcionalidad 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 de Australia);

“Habilidad de dos o más sistemas (ordenadores, medios de comunicación, redes, software y otros componentes de tecnología de la información) de interactuar y de intercambiar datos según un método definido, para obtener los resultados esperados.” (ISO);

“Interoperabilidad define si dos componentes de un sistema, desarrollados con herramientas distintas, con surtidores distintos, 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 es referencia de intercambio de datos entre sistemas. No contempla, simplemente, definición de tecnología.

Es, en realidad, la suma de todos estos elementos, considerando también, la existencia de una herencia de sistemas, de plataformas de Hardware y Software instaladas. Parte de principios que consideran la diversidad de componentes con la utilización de productos diversos de surtidores distintos. Tiene el objetivo considerar todos los factores para que los sistemas puedan actuar cooperativamente, estableciendo las normas, las políticas y los estándares necesarios para la consecución de esos objetivos.

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

## 2. Ámbito

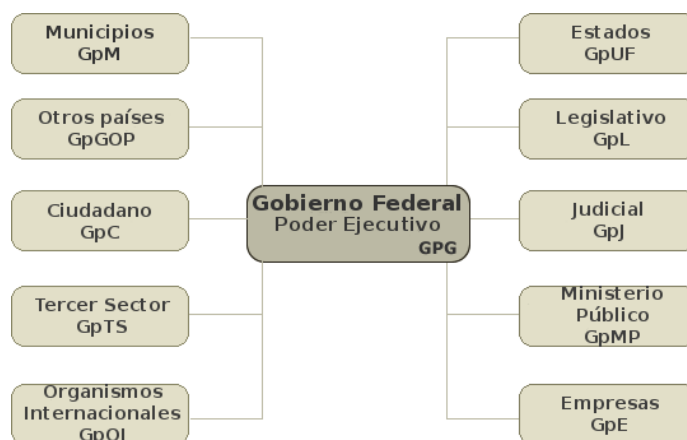
Políticas y especificaciones claramente definidas para la interoperabilidad y gestión de informaciones son fundamentales para propiciar la conexión del gobierno, tanto en el ámbito interno como en el contacto con la sociedad y, en mayor nivel de aprehensión, con el resto del mundo – otros gobiernos y empresas en actuación en el mercado mundial. E-PING se concibe como una estructura básica para la estrategia de gobierno electrónico, aplicada inicialmente al gobierno federal – Poder Ejecutivo, sin restringir la participación, por adhesión voluntaria de otros poderes y esferas de gobierno.

Los recursos de información del gobierno constituyen valerosos activos económicos. Al garantizar que la información gubernamental pueda rápidamente ser localizada e intercambiada entre el sector público y la sociedad, salvaguardadas 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 e 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);
- Tercer Sector.

La figura a continuación representa esa relación.



**Figura 1 – Relaciones del gobierno federal.**

### 2.1. Adhesión a e-PING

La adopción de los estándares y políticas contenidos en e-PING no puede ser impuesta a los ciudadanos y a las diversas instancias de gobierno, dentro y fuera del país. El gobierno brasileño, sin embargo, establece estas especificaciones como el estándar seleccionado y aceptado por él, es decir, estos son los estándares en los 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 de parte de la Coordinación de e-PING.

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

El “gobierno federal – Poder Ejecutivo” brasileño abarca:

- Los organismos de Administración Directa: Ministerios, Secretarías y otras entidades gubernamentales de igual naturaleza jurídica, conectados directa o indirectamente a la Presidencia de la República de Brasil;

- Las Autarquías y Fundaciones.

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

- Todos los nuevos sistemas de información que vengán a desarrollarse e implantarse en el gobierno federal y que se encuadren en el espacio de interacción, dentro del gobierno federal y con la sociedad en general;
- Sistemas de información legados que sean objeto de implementaciones que encuentren relación con el surtimiento de servicios de gobierno electrónico o interacción entre sistemas;
- Otros sistemas que compartan de los objetivos de disponibilizar los servicios de gobierno electrónico.

La adhesión se dará de manera gradual, según el plan de implementación, que considerará la situación de cada una de esas instituciones respecto a la posibilidad de adecuarse a las especificaciones y recomendaciones de e-PING.

Para los sistemas de información de gobierno que estén fuera del ámbito de obligatoriedad delimitado, se recomienda que los responsables consideren la adecuación a los estándares de e-PING, siempre que esfuerzos significativos de actualización sean planeados.

Todas las compras y contrataciones del gobierno federal – Poder Ejecutivo direccionadas hacia el 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.

E-PING fomenta 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 e-PING prevé esta participación, con utilización de la Internet (<http://www.eping.e.gov.br>) como medio preferencial para el contacto entre los gestores de e-PING y la sociedad.

### **2.2. Enfoque sobre la interoperabilidad**

E-PING no tendrá como enfoque de trabajo todos los temas del campo de Tecnología de la Información y Comunicación (TIC). Serán tratadas solamente, las especificaciones que sean relevantes para garantizar la interconexión de sistemas, integración de datos, acceso a servicio y gobierno electrónico y gestión de contenido. E-PING incorpora los temas comprendidos en la segmentación descrita en el tópico 4 de este documento.

### **2.3. Temas no tratados**

E-PING no tiene el objetivo de estandarizar la forma de presentación de las informaciones de los servicios de gobierno electrónico y se restringe a la definición de los requisitos de intercambio de datos y de las condiciones de disponibilidad de estos datos para los dispositivos de acceso.

### 3. Políticas Generales

Cada uno de los segmentos de e-PING contiene un conjunto de políticas técnicas que orienta el establecimiento de las especificaciones de sus componentes. Esos conjuntos específicos de cada segmento están fundamentados en las siguientes políticas generales.

**Alineación con INTERNET:** todos los sistemas de información de administración pública deberán estar alineados con las principales especificaciones utilizadas en 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, de modo preferencial, por intermedio de tecnología basada en *browser*, otras interfaces se permiten en situaciones específicas, como en rutinas de actualización y captación de datos donde no exista alternativa tecnológica disponible basada en navegadores.

**Adopción de metadatos** para recursos de información del gobierno.

**Desarrollo y adopción de un Estándar de Metadatos del Gobierno Electrónico – e-PMG<sup>1</sup>**, basado en estándares internacionalmente aceptados (<http://www.eping.e.gov.br>).

**Desarrollo y mantenimiento de la Lista de Temas del Gobierno:** taxonomía de navegación (LAG), que contemple en una estructura de directorio, los temas relacionados a la actuación del gobierno (<http://www.eping.e.gov.br>).

**Soporte de mercado:** todas las especificaciones contenidas en e-PING contemplan soluciones ampliamente apoyadas por el mercado. El objetivo que se busca es la reducción de los costes y de los riesgos en la concepción y producción de servicios en el sistema de informaciones gubernamentales.

**Escalabilidad:** las especificaciones seleccionadas deberán tener la capacidad de atender a cambios de demanda en el sistema, tales como, alteración en volúmenes de datos, cantidad de transacciones o cantidad de usuarios. Los estándares establecidos no podrán ser factor restrictivo, debiendo ser capaces de fundamentar el desarrollo de servicios que atiendan tanto a necesidades más específicas, que tengan relación con un pequeño volumen de transacciones y de usuarios, como demandas de escala nacional, con trámite de gran cantidad de informaciones y la participación de un elevado contingente de usuarios.

**Transparencia:** los documentos de e-PING estarán al alcance de la sociedad, en Internet, y para tal son previstos mecanismos de promoción, recibimiento y evaluación de sugerencias. En este sentido se definirán – y divulgarán para amplio conocimiento – plazos y compromisos para la implantación y gestión de sitio dedicado en Internet (<http://www.eping.e.gov.br>).

**Adopción preferencial de estándares abiertos:** e-PING define que, siempre que posible, serán adoptados estándares abiertos en las especificaciones técnicas. Estándares propietarios son aceptados de manera transitoria, manteniéndose las perspectivas de sustitución tan pronto como haya condición de migración. Sin perjuicio de estas metas, serán respetadas las situaciones en que haya necesidad de consideración de requisitos de seguridad e integridad de informaciones. Cuando existan soluciones en Software Libre disponibles, serán consideradas como preferenciales, según política definida por el Comité Ejecutivo de Gobierno Electrónico (CEGE).

E-PING mantiene total compatibilidad con las iniciativas de gobierno en el área de TIC. Un ejemplo que debe ser nombrado es el Catálogo de Migración de Software Libre del Gobierno Brasileño (<http://www.governoeletronico.gov.br>).

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

---

<sup>1</sup> Padrão de Metadados de Governo Eletrônico - en portugués. N. del Trad.

### 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 organismos de gobierno federal, estadual y municipal, expertos en cada asunto. Esos grupos han sido 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 se establecieron las políticas y las especificaciones técnicas que serán adoptadas por el gobierno federal. A continuación se relacionan los componentes que constituyen cada uno de los cinco segmentos.

#### 4.1. Interconexión

El segmento “Interconexión” establece las conexiones para que los organismos de gobierno se interconecten, además de establecer las condiciones de interoperación entre el gobierno y la sociedad.

En este segmento, se establecen las especificaciones para:

- Protocolo de Transferencia de Hipertexto;
- Transporte de Mensaje Electrónico;
- Seguridad de Contenido de Mensaje Electrónico;
- Acceso al Apartado Postal;
- Acceso Seguro al Apartado Postal;
- Directorio;
- Servicios de Nombramiento de Dominio;
- Direcciones de Apartado Postal Electrónico;
- 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;
- Colecta y Archivo de Evidencias.

#### 4.3. Medios de Acceso

En el segmento “Medios de Acceso”, son explicitadas las cuestiones referentes a los estándares de los dispositivos de acceso a los servicios del gobierno electrónico. En esta versión se tratan, 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 teléfonos móviles, *hand-helds* y televisión digital. Es formado por dos subgrupos, con los siguientes componentes:

Padrones 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 par Estaciones de Trabajo;
- Especificación de Intercambio de Informaciones Gráficas e Imágenes Estáticas;
- Gráficos Vectoriales;
- Especificación de Estándares de Animación;
- Archivos del Tipo Audio y del Tipo Video;
- Compactación de Archivos de Uso General;
- Archivos para Georreferenciamento.

### Tarjetas Inteligentes/Tokens/Otros:

- Definición de Datos;
- Aplicaciones (incluso multiaplicaciones);
- Componentes eléctricos;
- Protocolos de Comunicación;
- Padrones de Interfaz Física;
- Seguridad;
- Infraestructura del Terminal.

#### **4.4. Organización e Intercambio de Informaciones**

Trata de los aspectos relativos al tratamiento y a la transferencia de informaciones en los servicios de gobierno electrónico. Incluye estándar de estructura de temas de gobierno y de metadatos, y comprende los componentes a continuación:

- Lenguaje para Intercambio de Datos;
- Lenguaje para Transformación de Datos;
- Transformación de los Datos para intercambio;
- Catálogo de Estándares de Datos (CPD)<sup>2</sup>;
- Lista de Temas 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 orientadas hacia Áreas de Actuación de Gobierno, que serán organizados bajo la forma de catálogo facilitado en el sitio de e-PING, y presentado con contenidos actuales en tópico explicitado a continuación;
- Componentes relacionados a temas transversales a Áreas de Actuación de Gobierno, cuya estandarización sea relevante para la interoperabilidad de los servicios de Gobierno Electrónico, tales como Procesos e Informaciones Geográficas.

---

<sup>2</sup> Catálogo de Padrões de Dados en português. N. del Trad.

### 5. Gestión de e-PING

En este tópico 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 organismos que componen la Administración Pública Federal, como en la interoperabilidad con las entidades externas, representadas por otras instancias de gobierno, por la iniciativa privada, por instituciones actuantes en el tercer sector y por el ciudadano.

#### 5.1. Histórico

La arquitectura e-PING tiene la finalidad de establecerse como el paradigma de interoperabilidad para el gobierno federal, inicialmente en el ámbito del Poder Ejecutivo. La iniciativa de preparación de la arquitectura estuvo bajo la responsabilidad de tres organismos de la esfera federal:

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

Esos tres organismos organizaron un Seminario, con participación de entidades del gobierno federal, en el ámbito del Poder Ejecutivo, que tenía el objetivo de formar un comité interorganismos – nombrado Comité Constituyente – para conducir los trabajos iniciales de arreglo de la arquitectura.

Tras su institucionalización, por intermedio de la Portaria Normativa no. 5, de 14 de julio de 2005, este pasó a denominarse coordinación de e-PING. Además de los tres organizadores, participan de este grupo los siguientes organismos: Presidencia de la República, Ministerio de las Relaciones Exteriores, Ministerio de la Salud, Banco do Brasil, Caixa Econômica Federal, DATAPREVI y ABEP – Asociación Brasileña de Empresas Estaduales de Procesamiento de Datos.

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 que serán involucrados por 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 promoción de la versión inicial de la arquitectura, nombrada versión 0;
- Realización de consulta pública y audiencias públicas en RS, SP, DF, RJ, MG y PE, de modo a recoger contribuciones de la sociedad en general sobre el contenido propuesto en la versión 0;
- Publicación de la versión 1 junto con la resolución de institucionalización de e-PING, en el ámbito APF – Poder Ejecutivo;
- Publicación de la versión 1.5 conteniendo las actualizaciones y revisión de las especificaciones técnicas y de la visión general de e-PING. Las versiones 1.1. hasta 1.4. fueron mantenidas en discusión interna en los grupos de trabajo y en la coordinación de e-PING;
- Realización de consulta pública y de audiencias públicas de modo a recoger contribuciones de la sociedad en general, a cada nueva versión del documento de referencia;
- Publicación de versión anual que contenga las actualizaciones y revisiones de las especificaciones técnicas y de la visión general de e-PING.

Experiencias semejantes desarrolladas por gobiernos de otros países son a menudo investigadas. 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 e-PING está apoyada en la forma implementada por el gobierno del Reino Unido en operación desde el año 2000 y que, actualmente, se encuentra en un nivel de madurez reconocido internacionalmente como referencia.

### 5.2. Estrategia de Implantación

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

La presente versión consolidó el trabajo de los grupos montados para los cinco segmentos definidos. Su contenido se ha hecho disponible en la totalidad para Consulta Pública, con el objetivo de obtener contribuciones para las propuestas de estándares publicados en la versión 2.9.

### 5.3. Modelo de Gestión

En este tópico, se especifican las formas de gestión de la arquitectura e-PING, siendo relacionadas las principales atribuciones y la forma de implementación de estas actividades en la organización estructural del gobierno.

#### 5.3.1. Atribuciones

La gestión de e-PING comprende el desempeño de atribuciones de orden administrativo y de orden técnico.

Respecto a las **atribuciones de carácter administrativo** se encuentran:

- La definición de los objetivos estratégicos y de gestión de gobierno para el establecimiento de los estándares;
- La administración de la arquitectura de interoperabilidad del gobierno brasileño suministrando la infraestructura inicial 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 apoyadas por el mercado de TIC;
- La actuación como centro de coordinación de la arquitectura e-PING, buscando aunar los esfuerzos de interoperabilidad, asegurando la coherencia de las iniciativas emprendidas por los organismos del gobierno;
- Específicamente para los segmentos de interoperabilidad, la administración de la relación entre el gobierno federal – Poder Ejecutivo – y las demás instancias definidas en el tópico 2 – Ámbito;
- La gestión y la puesta en marcha de la divulgación de los estándares de e-PING, considerando:
  - La creación y administración de un sitio en Internet para e-PING (<http://www.eping.e.gov.br>);
  - La coordinación del proceso de consultas públicas;
  - La coordinación del proceso de recibimiento y evaluación de proposiciones de cambio o complementación;
  - La coordinación del proceso de solicitud de sugerencias para e-PING;
  - La publicación de las versiones actualizadas de e-PING y de las actualizaciones intermedias;
- La gestión de la interacción con iniciativas de igual propósito, conducidas por otros gobiernos, en el país y en el exterior;
- El fomento de la capacitación de los equipos del gobierno federal, procediendo en conjunto con los organismos, tanto en la consideración de e-PING en los planes específicos de entrenamiento, de cada uno de ellos, como en la realización de eventos corporativos direccionados para la diseminación de los estándares e-PING;
- El establecimiento, implantación y divulgación de indicadores de acompañamiento de los resultados obtenidos con la implantación de e-PING;
- La gestión de la interacción con organismos de especificación (W3C, IEEE, BSI, OMG, OGC, OASIS, IETF, Institutos Normativos de segmentos específicos como ABNT, INMETRO, ISO, NIST, etc.). Estos organismos serán escogidos bajo criterio de la coordinación de e-PING, teniendo en cuenta su notorio reconocimiento internacional, competencia en su campo de actuación y el establecimiento de estándares abiertos.
- La gestión de la interacción con organismos de fomento nacionales e internacionales, para

encauzar recursos, visando atender las necesidades de creación, infraestructura de e-PING y el fomento de la investigación y el desarrollo;

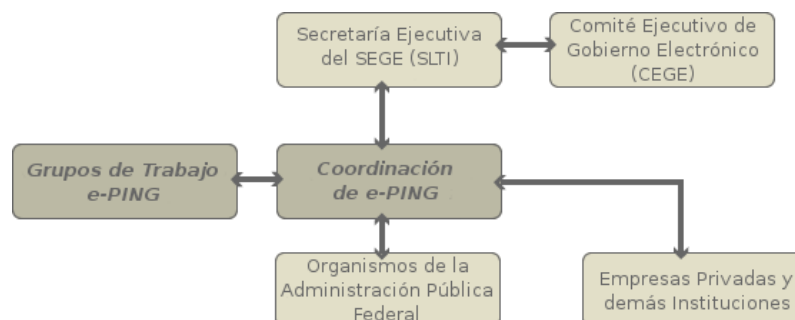
- Tornar viable la implantación y la gestión del proceso de homologación de los estándares que serán establecidos para el gobierno;
- Tornar viable la implantación y gestión de procesos de auditoría realizados con la finalidad de verificar el nivel de alineamiento con las recomendaciones y especificaciones de e-PING;
- La actuación cooperativa con apoyo a los organismos de gobierno para la realización de los procesos necesarios para adecuación a los estándares e-PING; la evaluación de la posibilidad de patrocinar programas ampliados que promuevan la utilización intensiva de los estándares propuestos.

Respecto a las **atribuciones de carácter técnico**, pueden subrayarse:

- El establecimiento de las formas de composición y mantenimiento de las políticas y especificaciones técnicas que componen e-PING, considerando:
  - La identificación, creación y gestión de grupos de trabajo específicos;
  - El establecimiento de convenios y definición de instituciones de gobierno como responsables por las políticas y especificaciones técnicas de componentes específicos del segmentos de interoperabilidad;
  - Identificación e implementación de formas alternativas de gestión técnica de los temas contemplados en el campo de actuación de e-PING;
- La coordinación del desarrollo y mantenimiento, en el ámbito del gobierno federal – Poder Ejecutivo, de:
  - Estándar de Metadatos de Gobierno (e-PMG);
  - Lista de Temas de Gobierno: Taxonomía para Navegación (LAG);
  - Catálogo de Estándares de Datos (CPD);
  - Catálogo de Referencia de los XML *Schemas*;
  - Otros padrones de Organización e Intercambio de Informaciones;
  - Padrones de Interconexión;
  - Padrones de Seguridad;
  - Padrones de Medios de Acceso a servicios electrónicos de gobierno;
  - Padrones de utilización de Tarjetas Inteligentes, *Tokens* y otros tipos de tarjeta;
- La garantía de la unicidad de concepción, conceptos, definiciones y establecimiento de estándares de parte de los responsables por los segmentos técnicos definidos para e-PING.

### 5.3.2. Responsabilidades

La estructura de gobierno creada para la administración de e-PING se presenta en el esquema simplificado a continuación:



**Figura 2 – Administración de e-PING**

La Secretaría de Logística y Tecnología de la Información del Ministerio de Planeamiento, Presupuesto y Gestión, por intermedio 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

## Documento de Referencia de e-PING – Versión 3.0

1994, es la responsable por la institucionalización y por la definición del formato jurídico de la Coordinación de e-PING.

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

- Implantación de la arquitectura de e-PING, haciéndose cargo de las actividades necesarias para la consolidación de la versión actual y dinámica de su evolución;
- Gestión de la arquitectura e-PING;
- Establecimiento y gestión de las normas y de los instrumentos institucionales y legales que garanticen la efectividad de las recomendaciones y especificaciones de e-PING;
- Administración de los padrones considerados en e-PING;
- Garantía de mantenimiento de los distintos catálogos de e-PING;
- Gestión de los Procesos de Comunicación y Divulgación de los padrones, de las decisiones y de las actividades de e-PING, incluso la publicación de nuevas versiones y de las actualizaciones intermedias;
- Creación de un sello e-PING y administración de proceso que certifique la adherencia de determinado servicio o producto a e-PING;
- Suministro de criterios y subsidios a 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 las propuestas de proyectos de e-gov volcados hacia la Administración Pública Federal, homologación de estándares y verificación de conformidad;
- Establecimiento de los puntos de enlace con los distintos organismos de la Administración Pública Federal;
- Administración de los Grupos de Trabajo – GT, definiendo su composición y determinando las directrices de trabajo, basadas en las políticas técnicas, generales y específicas, en las necesidades de gobierno y en el monitoreo del escenario tecnológico.

Los Grupos de Trabajo de e-PING, constituidos por representantes señalados por distintos organismos de la APF y por representantes de instituciones de otras esferas de gobiernos, son responsables por:

- Tratar los temas que componen los segmentos de e-PING;
- Monitorear sistemáticamente el mercado, específicamente en los segmentos bajo su responsabilidad, con el objetivo de detectar las necesidades de actualización tecnológica de las políticas y especificaciones técnicas;
- Ofrecer subsidios a la actuación de la Coordinación de e-PING en el desarrollar de sus atribuciones administrativas y técnicas.

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

### 5.4. Actividades adicionales

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

#### 5.4.1. Selección y Homologación de Estándares Tecnológicos

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

E-PING estipula 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):** tópico 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 otra institución acreditada 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 e-PING;

- **Recomendado (R):** tópico que se refiere a las políticas técnicas de e-PING, es reconocido como un tópico que se debe utilizar en el ámbito de las instituciones de gobierno, pero que aún no ha sido sometido a un proceso formal de homologación;
- **En transición (T):** tópico que el gobierno no recomienda, porque no atiende a uno o más requisitos establecidos en las políticas generales y técnicas de la arquitectura; su inclusión en e-PING se debe a su significativa utilización en instituciones del gobierno. Tiende a ser descartado tan pronto como otro componente, en una de las dos situaciones anteriores, venga a presentar condiciones absolutas para sustituirlo. Puede llegar a ser considerado un componente “recomendado” en el caso de adecuarse a todas las políticas técnicas establecidas. Conviene subrayar que el desarrollo de nuevos servicios o la reconstrucción de partes significativas de los que ya existan 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 descritas arriba, tan pronto como el proceso de evaluación esté concluido;
- **Estudio Futuro (F):** componente aún no evaluado y que será objeto de estudio posterior.

El proceso de selección de los componentes adoptados por e-PING y su consecuente clasificación en las situaciones señaladas arriba es de responsabilidad de los Grupos de Trabajo compuestos por profesionales expertos con actuación en el gobierno y en instituciones con las que se haya establecido algún tipo de convenio o contrato específicamente para esa finalidad.

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

La homologación, por su parte, deberá ser objeto de estudio más hondo, conducido por los gestores de e-PING. En virtud de la gran variedad de componentes considerados por la arquitectura, habrá necesidad de construcción de una sistemática de homologación que contemple tanto a procesos, en que será necesaria la evaluación de características físicas de determinados componentes (Tarjetas Inteligentes, por ejemplo) como a otros en que se presente la necesidad de estudio de aspectos que abarquen el uso del componente en el desarrollo y construcción de servicios (organización e intercambio de informaciones y seguridad, por ejemplo).

En este caso, el gobierno deberá establecer convenios o acreditar instituciones para la construcción de evaluación de conformidad, definiendo siempre cuáles componentes deben ser sometidos a procesos de homologación, cuáles son los criterios de evaluación de los resultados y cuales son las condiciones de realización de los procedimientos.

La definición completa del proceso de selección y homologación, llevando en cuenta las especificidades de los segmentos, quedará a cargo de la Coordinación de e-PING.

### 5.4.2. Auditoría de Conformidad

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

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

La forma preferencial de realización de ese tipo de procedimiento, sin embargo, será la utilización de las estructuras propias en los organismos responsables por auditoría de sistemas. La Coordinación de e-PING actuará en el sentido de proponer los criterios básicos que se deben seguir por los organismos.

Otra cuestión que se debe considerar será la colaboración de organismos de gobierno actuantes en el campo, siendo posibles los contactos con instituciones de otros Poderes y esferas de gobierno.

### 5.4.3. Creación y Mantenimiento del Sitio

Todo el proceso de intercambio de informaciones sobre e-PING con usuarios, colaboradores e interesados es realizado, de forma preferencial, por Internet, en la dirección <http://www.eping.e.gov.br>. En su estadio más avanzado de funcionamiento, el sitio de e-PING tendrá, como principales funcionalidades:

- Divulgación completa de la documentación referente 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 sugerencias de parte de la sociedad;
- Publicación de solicitud de comentarios referentes a la especificación de componentes para la arquitectura;
- Disponibilidad de medio electrónico para recibir las sugerencias;
- Disponibilidad de enlaces para documentos, estándares, normas o cualquier otro tipo de referencia constante en e-PING.

### 5.4.4. Acompañamiento Legal e Institucional

E-PING tendrá constante apoyo del equipo de la Asesoría Jurídica del Ministerio del Planeamiento, presupuesto y Gestión para garantizar la adherencia del contenido de los documentos que componen la arquitectura a las normas e instrumentos legales en vigor en el país.

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

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

### 5.4.5. Divulgación

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

- Realización de eventos específicos de divulgación, como Seminarios, *Workshops* y presentaciones en general;
- Participación en eventos gubernamentales en el área de TIC y correlacionados;
- Publicación de todas las versiones de e-PING y de las actualizaciones intermedias;
- Intercambio con otras esferas y otros Poderes de gobierno, con instituciones públicas, privadas y del tercer sector y con gobiernos de otros países.

### 5.4.6. Capacitación

Harán parte de la agenda de implantación y gestión de e-PING eventos orientados hacia la capacitación. También está prevista la utilización intensiva de la enseñanza a distancia (EAD).

La Coordinación de e-PING elaborará y publicará un guión mínimo de entrenamiento, de modo que cada organismo de la APF tenga los subsidios para planear y estimar las inversiones necesarias para la capacitación de los profesionales involucrados en el proceso de adecuación a las recomendaciones de e-PING.

Cada organismo de gobierno deberá observar las definiciones de estándar de e-PING a la hora de montar sus planes particulares de capacitación, garantizando el entrenamiento adecuado para los componentes de sus equipos técnicos.

## 5.5. Relación con Gobierno y Sociedad

En este tópico se consideran las formas de relación de e-PING con las entidades que componen el gobierno y la sociedad.

### 5.5.1. Organismos 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 e-PING, cada institución en particular tendrá su responsabilidad en la gestión y salvaguardia del uso de los estándares e-PING. De entre las atribuciones de esa naturaleza cabe subrayar las siguientes:

- Contribuir para el desarrollo y mejoría continua de e-PING;
- Asegurar que sus estrategias organizacionales de TIC consideren que los sistemas integrantes de servicios de gobierno electrónico bajo su responsabilidad estén adecuados a las recomendaciones de e-PING;
- Disponer de un plan de implementación y adecuación de la infraestructura de TIC de la organización a la arquitectura e-PING;
- Asegurar el hecho de que los equipos de la institución dominen las habilidades para definir y utilizar las especificaciones requeridas para interoperabilidad, ofreciendo el soporte de entrenamiento cuando necesario;
- Establecer punto de contacto en las instituciones, para intercambio de informaciones y de necesidades con la Coordinación de e-PING;
- Alocar y suplir recursos para dar soporte a sus procesos (como resultado del aumento de la interoperabilidad) de forma a mejorar la calidad reducir costes de provisión de los servicios de e-gov.

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

En su estadio inicial, e-PING se orienta, básicamente, para el gobierno federal, Poder Ejecutivo. Otros Poderes (Judicial, Legislativo y Ministerio Público Federal) y demás 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 proceder. Solamente especifica la forma preferencial como pretende interoperar con esas entidades.

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

En el plan de gestión de e-PING, los demás Poderes federales y los gobiernos estaduales y municipales son considerados prioritarios. El objetivo a alcanzarse, tan pronto como se establezcan y firmen los estándares en el ámbito del poder Ejecutivo Federal, es la extensión de las discusiones a los organismos e instituciones que componen esas áreas de gobierno.

### 5.5.3. Organizaciones del Sector Privado y del Tercer Sector

E-PING contempla la interacción con el Sector Privado y con el Tercer Sector por medio de los mecanismos de Consulta Pública, Solicitud de Comentarios y Recibimiento de Sugerencias.

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

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

### 5.5.4. Ciudadano

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

## Documento de Referencia de e-PING – Versión 3.0



El gobierno debe estimular en la sociedad la opinión, el comentario y la contribución con sugerencias de innovaciones que puedan ayudarlo a mejorar el acceso a la información y a la prestación de sus servicios. Todos los procesos de divulgación y de interrelación de e-PING contemplan 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 e-PING

## 6. Interconexión

### 6.1. Interconexión: Políticas Técnicas

Las políticas técnicas para interconexión son:

**6.1.1.** Los organismos de la APF deberán interconectarse utilizando IPv4 y planeando su futura migración para IPv6. Nuevas contrataciones y actualizaciones de redes deben contemplar soporte a la coexistencia de los protocolos IPv4 y IPv6 y a productos que comporten a ambos protocolos.

**6.1.2.** Los sistemas de e-mail deben utilizar SMTP/MIME para el transporte de mensajes. Para acceso a los mensajes, se deben utilizar protocolos POP3 y/o IMAP, y se alienta el uso de interfaces *web* para correo electrónico, observados, cuando haga falta, los aspectos de seguridad.

**6.1.3.** Los organismos 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](http://www.e.gov.br/correios/dir_redegoverno.htm).

**6.1.4.** Los organismos de la APF deben obedecer a la política de nombramiento de dominios del gobierno federal, establecida en la Resolución n.º 7, que puede visualizarse en la dirección electrónica [https://www.planalto.gov.br/ccivil\\_03/Resolucao/2002/RES07-02web.htm](https://www.planalto.gov.br/ccivil_03/Resolucao/2002/RES07-02web.htm).

**6.1.5.** El DNS se debe utilizar para resolución de nombres de dominios Internet, convirtiéndolos en direcciones IP e, inversamente, convirtiendo IPs en nombres de dominios, a través del mantenimiento de los verso 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. HTTP debe ser priorizado para transferencias de archivos oriundos de páginas de sitios de Internet.

**6.1.7.** Siempre que posible<sup>3</sup>, se debe emplear tecnología basada en la *web* en aplicaciones que utilizaron Emulación de Terminal anteriormente.

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

**6.1.9.** Los *Web Services* deberán ser registrados y ubicarse 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. Ver acotación sobre *Web Services*, tópico 6.3.

### 6.2. Interconexión: Especificaciones Técnicas

Tabla 1 – Especificaciones para Interconectividad<sup>4</sup>

| Componente                               | Especificación   | SIT      | Observaciones |
|--|--|----------|---------------|
|  | A = Adoptado<br>R = Recomendado<br>T = En Transición<br>E = En Estudio<br>F = Estudio Futuro |          |               |
| Protocolo de transferencia de hipertexto | Utilizar HTTP/1.1 (RFC 2616) y/o HTTPS (RFC 2660).   | <b>A</b> |               |

<sup>3</sup> Existen productos que pueden propiciar acceso por el *browser* a los sistemas legados, sin necesidad de cambiarlos; típicamente estos productos pueden facilitar el acceso directo a las pantallas de legado o mismo sustituirse por interfaces gráficas (GUIs). Hay que poner atención a toda y cualquier implicación de seguridad referente a su utilización.

<sup>4</sup> Las RFCs pueden ser accedidas en <http://www.ietf.org/rfc.html>

## Documento de Referencia de e-PING – Versión 3.0

| Componente                                    | Especificación  | SIT | Observaciones |
|---|---|-----|---------------|
| Transporte de mensaje electrónico             | Utilizar productos de mensajería electrónica que soporten 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 2183; RFC 2048; RFC 3023 e RFC 2049.  | R   |               |
| Seguridad de contenido de mensaje electrónico | El S/MIME v3.1 deberá utilizarse 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 e RFC 3851.   | R   |               |
| Acceso al apartado postal                     | A excepción de que las exigencias de seguridad determinen de otra manera, programas de correo que ofrecen facilidades de acceso a la correspondencia deberán, como mínimo, estar de acuerdo con POP3 para acceso remoto al apartado postal. RFCs correlacionadas: RFC 1939; RFC 1957 e RFC 2449. Donde facilidades adicionales sean necesarias, a menos que requisitos de seguridad dispongan en contrario, los programas de correo que ofrecen facilidades avanzadas de acceso a la correspondencia, deberán estar de acuerdo con IMAP para acceso remoto al apartado postal. RFCs correlacionadas: RFC 3501; RFC 2342; RFC 2971; RFC 3502; RFC 3503; RFC 3510 e RFC 2910.   | R   |               |
| Acceso seguro al apartado postal              | El acceso al apartado postal, por medio de redes no seguras, deberá usar HTTPS, de acuerdo con los padrones de seguridad en el transporte. Cuando sea necesario usar IMAP o POP, usarlo a través de TLS, según RFC 2595.  | R   |               |
| Directorio                                    | Usar el esquema del directorio central, conforme definido en la dirección electrónica <a href="http://www.e.gov.br/correios/dir_redegoverno.htm">http://www.e.gov.br/correios/dir_redegoverno.htm</a> 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. A su vez, las directivas de nombramiento de dominio del gobierno brasileño son encontradas en la Resolución No7 del Comité Ejecutivo del Gobierno Electrónico, en la dirección electrónica <a href="https://www.planalto.gov.br/ccivil_03/Resolucao/2002/RES07-02web.htm">https://www.planalto.gov.br/ccivil_03/Resolucao/2002/RES07-02web.htm</a> . Además de esas directivas, por decisión del Comité Gestor de la Internet en Brasil, el nombramiento de dominios obedece a las orientaciones del Ministerio del Planeamiento, Presupuesto y Gestión, a quien corresponde administrar los dominios .GOV.BR. Las particularidades de otros niveles de gobierno, como por ejemplo, los dominios de los gobiernos de las Unidades de la Federación, que incluyen la sigla de la UF en la composición de las direcciones, son abordadas en la dirección electrónica <a href="http://registro.br/faq/faq1.html#1">http://registro.br/faq/faq1.html#1</a> | A   |               |

| Componente                                 | Especificación   | SIT | Observaciones |
|--|--|-----|---------------|
| Direcciones de apartado postal electrónico | Las reglas para definición de los nombres de los apartados postales de correo electrónico deberán seguir lo establecido en el documento “Apartados Postales Individuales-Funcionales en el Gobierno Federal”, disponible en la dirección electrónica <a href="http://www.e.gov.br/correios/cp_individ.htm">http://www.e.gov.br/correios/cp_individ.htm</a> | A   |               |
| Protocolos de transferencia de archivos    | FTP (RFC 959 e RFC 2228) (con reinicio 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 un o más participantes.   | R   |               |
| Mensajería en Tiempo Real                  | El modelo y requisitos para <i>Instant Messaging and Presence Protocol</i> (IMPP) son definidos por la RFC 2778 y RFC 2779.  | T   |               |
|  | El modelo y requisitos para <i>Extensible Messaging and Presence Protocol</i> (XMPP) son definidos por la RFC 3920 y RFC 3921.   | R   |               |
| Servicio de Mensajes Cortos                | El Servicio de Mensajes Cortos (SMS) deberá utilizar el protocolo SMPP, como definido por el <i>SMS Forum</i> <a href="http://www.smsforum.net">http://www.smsforum.net</a>  | R   |               |
| Intercomunicación LAN/WAN                  | IPv4 (RFC 791)   | A   |               |
|  | IPv6 (RFC 2460)  | E   |               |
| Transporte                                 | TCP (RFC 793)<br>UDP (RFC 768) cuando necesario, sometido a las limitaciones de seguridad.   | R   |               |
| Tráfico avanzado                           | Cuando necesario, el tráfico de red puede ser optimizado por el uso del MPLS (RFC 3031), debiendo este poseer, como mínimo, cuatro formas de servicio.   | R   |               |
| Red local inalámbrica                      | IEEE 802.11 b/g, en conformidad con las determinaciones del <i>Wi-Fi Alliance</i> ( <a href="http://www.wi-fi.org">http://www.wi-fi.org</a> ) y con las normas de la Anatel ( <a href="http://www.anatel.gov.br">http://www.anatel.gov.br</a> ).   | R   |               |
| Red metropolitana inalámbrica              | IEEE 802.16, en conformidad con las determinaciones del <i>WiMax Forum</i> ( <a href="http://www.wimaxforum.org">http://www.wimaxforum.org</a> ) y con las normas de la Anatel ( <a href="http://www.anatel.gov.br">http://www.anatel.gov.br</a> ).  | E   |               |

### 6.3. Web Services

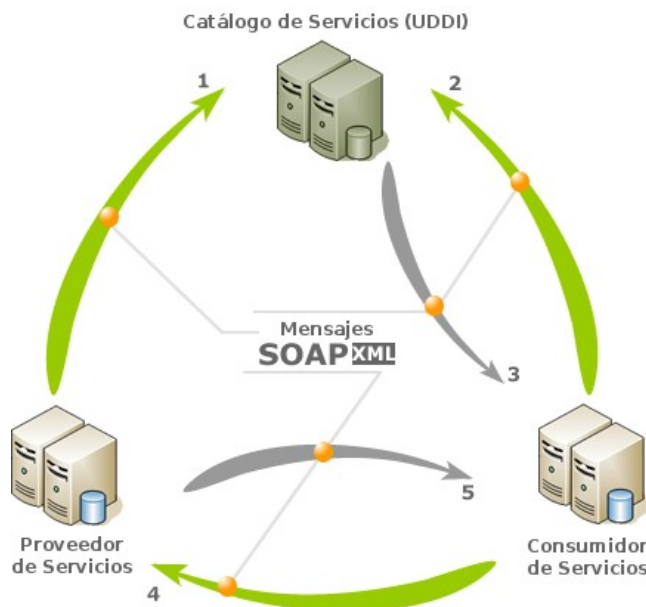
Se puede definir el término *Web Services*<sup>5</sup> como un servicio disponible en la red (Internet o Intranet) que utilice un sistema estándar – XML – para cambiar mensajes, independiente de sistema operacional o lenguaje de programación, con dos propiedades básicas:

(a) posibilitar su descubierta: al crear un *Web Service*, su publicación debe ser hecha mediante registro en un catálogo de servicios para que potenciales usuarios puedan encontrarlo. El catálogo puede usar UDDI. Otras formas de repositorios pueden ser usadas, entre ellas la ebXML – actualmente se encuentra en estudio por e-PING;

<sup>5</sup> La definición de Web Services fue adaptada del libro de Ethan Cerami - *Web Services Essentials - Distributed Applications with XML-RPC, SOAP, UDDI & WSDL*, 2002. O' Reilly & Associates Inc., Sebastol, CA.

(b) auto descripción: los *Web Services* ofrecen una descripción completa de sus servicios y de como los usuarios (desarrolladores) podrán crear aplicaciones para interactuar con ellos. Esa descripción es realizada a través de WSDL.

La Figura 1 presenta los pasos genéricos para suministrar y consumir un servicio a través de *Web Services*:



**Figura 3 – Visão geral do funcionamento de *Web Services*<sup>6</sup>.**

(1) el registro del servicio es hecho donde un proveedor de servicio describe su servicio usando WSDL. Se publica esa definición en un catálogo de servicios;

(2) el consumidor de servicio realiza una o más consultas al directorio de servicios para localizar un servicio y verificar cual forma de comunicación con ese servicio;

(3) informaciones sobre los servicios localizados son enviadas al consumidor de servicio. Esas informaciones son parte del WSDL facilitado por el proveedor de servicios, como, por ejemplo, la dirección donde está localizado el servicio solicitado;

(4) y (5) se refieren al consumo del servicio. Proveedor y consumidor cambian mensajes (XML) entre si. Al recibir un mensaje, el *Web Service* la valida de acuerdo con las informaciones contenidas en el WSDL. A partir de ese momento, el *Web Service* sabe como tratar el mensaje, como procesarlo (quizás enviándolo para otro programa) y sabe como montar la respuesta para el consumidor del servicio.

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

En ese contexto, se entiende que el uso de *Web Services* es adecuado para esas necesidades. *Web Services* ofrecen un tratamiento dinámico para integración, en el cual los servicios son localizados, determinados y utilizados de forma automática. La tecnología de *Web Services* aporta una forma estándar de interoperación entre diferentes aplicaciones de softwares. Además, un *Web Service* puede presentar diferentes niveles de granularidad. Tanto un formulario perteneciente a una página *web*, como un componente de software, que involucra una regla de negocio compleja, pueden ser transformados en *Web Services*, lo que torna su uso bastante flexible.

El soporte de *Web Services* para integración directa con otras aplicaciones de software utiliza

<sup>6</sup> La figura 1 es una adaptación de la figura presentada por el W3C Working Group - <http://www.w3.org/TR/wsarch/#whatis>.

mensajes escritos en XML como estándar de interoperabilidad. Esos mensajes son involucrados en protocolos de aplicación estándar de Internet – SOAP. Es importante subrayar que las estructuras de documentos XML serán descritas por medio de XML Schemas, como forma de validación de los tipos de datos pertenecientes a las líneas de negocio.

**Tabla 2 – Especificaciones para Web Services<sup>7</sup>**

| Componente                                | Especificación  | SIT | Observaciones   |
|---|---|-----|---|
|   | A = Adoptado<br>R = Recomendado<br>T = En Transición<br>E = En Estudio<br>F = Estudio Futuro  |     |   |
| Protocolo de intercambio de informaciones | SOAP v1.2, como definido por el W3C<br><a href="http://www.w3.org/TR/soap12-part1/">http://www.w3.org/TR/soap12-part1/</a><br><a href="http://www.w3.org/TR/soap12-part2/">http://www.w3.org/TR/soap12-part2/</a> Especificaciones del protocolo SOAP pueden ser encontradas en <a href="http://www.w3.org/TR/soap12-part0/">http://www.w3.org/TR/soap12-part0/</a> | R   |   |
| Infraestructura de registro               | Especificación UDDI v3.0.2 ( <i>Universal Description, Discovery and Integration</i> ) definida por la OASIS<br><a href="http://uddi.org/pubs/uddi_v3.htm">http://uddi.org/pubs/uddi_v3.htm</a>   | R   |   |
|   | ebXML (Electronic Business using eXtensible Markup Language). La especificación puede ser encontrada en <a href="http://www.ebxml.org/specs/index.htm">http://www.ebxml.org/specs/index.htm</a>   | E   |   |
| Lenguaje de definición del servicio       | WSDL 1.1 ( <i>Web Service Description Language</i> ) como definido por el W3C.<br><br>La especificación puede ser encontrada en <a href="http://www.w3.org/TR/wsdl">http://www.w3.org/TR/wsdl</a>   | R   |   |
|   | WSDL 2.0 ( <i>Web Service Description Language</i> ) como definido por el W3C.<br><br>La especificación puede ser encontrada en <a href="http://www.w3.org/TR/wsdl20/">http://www.w3.org/TR/wsdl20/</a>   | E   |   |
| Perfil básico de interoperabilidad        | <i>Basic Profile 1.1 Second Edition</i> , como definido por la WS-I<br><a href="http://www.ws-i.org/Profiles/BasicProfile-1.1.html">http://www.ws-i.org/Profiles/BasicProfile-1.1.html</a>  | E   | La versión 1.2 del Basic Profile se encuentra como borrador ( <i>Working Draft</i> ) en <a href="http://www.wsi.org/Profiles/BasicProfile-1.2.html">http://www.wsi.org/Profiles/BasicProfile-1.2.html</a> |
| Portlets remotos                          | WSRP 1.0 (Web Services for Remote Portlets) como definido por la OASIS<br><a href="http://www.oasis-open.org/committees/wsrp">http://www.oasis-open.org/committees/wsrp</a>   | E   |   |

#### 6.4. Mensaje Electrónico (E-mail)

Para que quede claro, e-PING utilizará los siguientes conceptos:

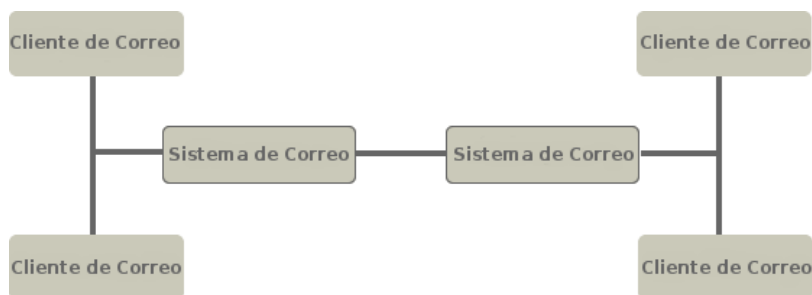
#### Transporte de Mensaje Electrónico

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

<sup>7</sup> Las cuestiones de seguridad referentes a Web Services son tratadas en el capítulo 7.

### Acceso al apartado postal

Acceso al apartado postal es definido como la interfaz entre un cliente de correo y un sistema de correo.



**Figura 4 – Interfaces entre sistemas y clientes de Correo**

### 6.5. VPN

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

Dicha utilización, como infraestructura de conexión entre hosts de la red privada, es una buena solución en términos de costes, pero no en lo que se refiere a la privacidad, pues los datos en tránsito pueden ser leídos por cualquier equipo, siendo necesario el uso de VPN.

Los túneles virtuales trafican datos encriptados sobre redes pública o privada, formando un canal virtual seguro a través de esas redes. Para tanto, se utilizan protocolos de túneles virtuales.

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.

### 6.6. Redes peer-to-peer

Sistemas Peer-to-Peer (P2P) son sistemas distribuidos que consisten en nodos interconectados, con capacidad de auto organización en topologías de red, con el objetivo de compartir recursos como procesamiento, almacenamiento y anchura de banda, capaces de adaptación a fallos y acomodar poblaciones transientes de nodos, mientras mantienen conectividad y resultados aceptables, sin depender de la intermediación o soporte de una autoridad (servidor) central.

Aunque sistemas P2P puedan contribuir para compartir recursos y colaboración en amplia escala, con control descentralizado y bajo acoplamiento, aún están susceptibles a diversos problemas de seguridad, imposibilitando el uso sistemático de redes P2P. Este asunto será tratado en un 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 sean procesados, almacenados o en tránsito.

**7.1.3.** Las informaciones que transitan en redes inseguras, incluyendo aquellas inalámbricas, deben adoptar los controles de seguridad disponibles en la camada de transporte (IPv4). En el caso de LAN inalámbrico 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 riesgo.

**7.1.5.** La seguridad debe ser tratada de forma preventiva. Para los sistemas que dan soporte a procesos críticos se deben elaborar planes de continuidad, en los cuales serán tratados los riesgos residuales tratando de atender los niveles mínimos de producción.

**7.1.6.** A segurança é um processo que deve estar inserido em todas as etapas do ciclo de desenvolvimento de um sistema.

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

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

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

**7.1.10.** El uso de criptografía y certificación digital, para la protección del tráfico, almacenamiento de datos, control de acceso, firma digital y firma de código, debe estar en conformidad con las reglas de la ICP-Brasil.

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

**7.1.12.** Los usuarios deben conocer sus responsabilidades respecto a la seguridad y deben estar capacitados para la realización de sus tareas y utilización correcta de los medios de acceso.

**7.1.13.** Los Organismos de la APF, objetivando la mejora de la seguridad, deben tener como referencia la norma NBR ISO/IEC 27002:2005 código de práctica para la gestión de la seguridad de la información y NBR ISO/IEC 27001:2006 sistemas de gestión de seguridad de la información, editadas por la ABNT.

7.2. Seguridad: Especificaciones Técnicas

Tabla 3 – Especificaciones Técnicas para Seguridad de IP

| Componente  | Especificación  | SIT | Observaciones |
|---|---|-----|---------------|
|   | A = Adoptado<br>R = Recomendado<br>T = En Transición<br>E = En Estudio<br>F = Estudio Futuro  |     |               |
| 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 – <i>Transport Layer Security</i> , RFC2246 ( <a href="http://www.ietf.org/rfc/rfc2246.txt">http://www.ietf.org/rfc/rfc2246.txt</a> ). Si es necesario el protocolo TLS v1 puede emular el SSL v3.<br><br>HTTP sobre TLS, RFC 2818 ( <a href="http://www.ietf.org/rfc/rfc2818.txt">http://www.ietf.org/rfc/rfc2818.txt</a> )<br>Pudiendo implementar los siguientes algoritmos criptográficos:<br><br>- Algoritmos para cambio de llaves de sesión, durante el <i>handshake</i> :<br>RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA;<br><br>- Algoritmos para definición de llave de cifra:<br>RC4, IDEA, 3DES, AES;<br><br>- Algoritmos que implementan la función de <i>hash</i> para definición del MAC:<br>SHA-256 ou SHA-512.<br><br>- Tipo de Certificado Digital - X.509 v3 - ICP-Brasil, <a href="http://www.iti.gov.br">http://www.iti.gov.br</a><br>SASL - <i>Simple Authentication and Security Layer</i> , RFC 4422 ( <a href="http://www.ietf.org/rfc/rfc4422.txt">http://www.ietf.org/rfc/rfc4422.txt</a> ). | R   |               |
| Seguridad de redes IPv4   | IPSec <i>Authentication Header</i> RFC 2402 e RFC 2404 para autenticación de cabecera del IP.<br><a href="http://www.ietf.org/rfc/rfc2402.txt">http://www.ietf.org/rfc/rfc2402.txt</a><br><a href="http://www.ietf.org/rfc/rfc2404.txt">http://www.ietf.org/rfc/rfc2404.txt</a><br><br>IKE – <i>Internet Key Exchange</i> , RFC 2409 ( <a href="http://www.ietf.org/rfc/rfc2409.txt">http://www.ietf.org/rfc/rfc2409.txt</a> ), debe ser utilizado siempre que necesario para negociación de la asociación de seguridad entre dos entidades para cambio de material de cierre.<br><br>ESP – <i>Encapsulating Security Payload</i> , RFC 2406 ( <a href="http://www.ietf.org/rfc/rfc2406.txt">http://www.ietf.org/rfc/rfc2406.txt</a> ) Requisito para VPN – Virtual Private Network.  | R   |               |
| Seguridad de redes IPv4 para protocolos de aplicación   | El S/MIME v3 ,RFC2633 ( <a href="http://www.ietf.org/rfc/rfc2633.txt">http://www.ietf.org/rfc/rfc2633.txt</a> ) 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 ( <a href="http://www.ietf.org/rfc/rfc2460.txt">http://www.ietf.org/rfc/rfc2460.txt</a> ) presenta implementaciones de seguridad nativas en el protocolo. Las especificaciones del IPv6 definieron dos mecanismos de seguridad: la autenticación de  | R   |               |

| Componente | Especificación   | SIT | Observaciones |
|------------|--|-----|---------------|
|            | encabezamiento AH ( <i>Authentication Header</i> ) RFC2402<br>( <a href="http://www.ietf.org/rfc/rfc2402.txt">http://www.ietf.org/rfc/rfc2402.txt</a> ) o autenticación IP, y la seguridad del ambiente IP, ESP ( <i>Encrypted Security Payload</i> ) RFC2406 ( <a href="http://www.ietf.org/rfc/rfc2406.txt">http://www.ietf.org/rfc/rfc2406.txt</a> ). |     |               |

**Tabla 4 – Especificações Técnicas para Segurança de Correio Eletrônico**

| Componente                  | Especificación   | SIT            | Observaciones |
|-----------------------------|--|----------------|---------------|
|                             | A = Adoptado<br>R = Recomendado<br>T = En Transición<br>E = En Estudio<br>F = Estudio Futuro   |                |               |
| Acceso a apartados postales | El acceso al apartado postal deberá suceder por intermedio 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 al apartado postal a través de redes no seguras (por ejemplo: Internet) se debe utilizar HTTPS de acuerdo con los padrones de seguridad de transporte descritos en la RFC 2595 ( <a href="http://www.ietf.org/rfc/rfc2595.txt">http://www.ietf.org/rfc/rfc2595.txt</a> ), 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 adecuado para seguridad de mensajes generales de gobierno. Eso incluye RFC 3369 ( <a href="http://www.ietf.org/rfc/rfc3369.txt">http://www.ietf.org/rfc/rfc3369.txt</a> ), RFC 3370 ( <a href="http://www.ietf.org/rfc/rfc3370.txt">http://www.ietf.org/rfc/rfc3370.txt</a> ), RFC 2631 ( <a href="http://www.ietf.org/rfc/rfc2631.txt">http://www.ietf.org/rfc/rfc2631.txt</a> ), RFC 3850 ( <a href="http://www.ietf.org/rfc/rfc3850.txt">http://www.ietf.org/rfc/rfc3850.txt</a> ) y RFC 3851 ( <a href="http://www.ietf.org/rfc/rfc3851.txt">http://www.ietf.org/rfc/rfc3851.txt</a> ). | R              |               |
| Transporte de e-mail        | Verificar se el reverso confiere con el nombre en el HELO, para garantía del origen del mensaje y minimizar SPAM.  | F <sup>8</sup> |               |
| 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<br>R = Recomendado<br>T = En Transición<br>E = En Estudio<br>F = Estudio Futuro |     |               |
| Algoritmo de cifra | 3DES o AES   | R   |               |

<sup>8</sup> Posible implicación en el resultado de la actuación; posible descarte de mensajes válidos; imposibilidad de tratar múltiples dominios.

## Documento de Referencia de e-PING – Versión 3.0

| Componente   | Especificación  | SIT | Observaciones  |
|--|---|-----|--|
| Algoritmo para firma/hashting  | SHA-256 o SHA-512   | R   | Los sistemas deben tener soporte para el algoritmo de <i>hash</i> MD5 con RSA, para alcanzar compatibilidad con implementadores anteriores.  |
| Algoritmos para firma/hashting                                       | SHA-224 o SHA-238   | E   | Considerando que fueron incluidas en el Reporte Final del Grupo de Trabajo de Criptografía I, instituido por la Oficina de Seguridad Institucional de la Presidencia de la República, aunque, aún no se transformaron en norma en la Administración Pública Federal. |
| Algoritmo para transporte de llave criptografada de contenido/sesión | RSA   | R   |  |
| Algoritmos criptográficos basados en curvas elípticas                | ECMQV e ECDH, ambos para acuerdo de llaves, ECDSA, para firmas digitales, y ECIES para cifración y transporte seguro de llaves criptográficas. El uso de estos algoritmos está sometido a reglamentación y normatización por la ICP-Brasil respecto 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 utilizan dispositivos tanto de <i>software</i> como de <i>hardware</i> tipo <i>token</i> o <i>smart card</i> .<br>Adherencia al estándar:<br>a. Seguir, como mínimo, las reglas establecidas para el nivel 1 o 2 de seguridad del estándar;<br>b. Seguir, como mínimo, las reglas establecidas para el nivel 2 de seguridad del estándar FIPS 140-1 o 2, para verificación de violación en el <i>hardware</i> ( <i>Tamper Evidence</i> ). | R   |  |

Tabla 6 – Especificaciones Técnicas para Seguridad – Desarrollo de Sistemas

| Componente  | Especificación   | SIT | Observaciones   |
|---|--|-----|---|
|   | A = Adoptado<br>R = Recomendado<br>T = En Transición<br>E = En Estudio<br>F = Estudio Futuro   |     |   |
| Firmas XML  | Sintaxis y Procesamiento de firma XML (XMLsig) conforme definido por el W3C<br><a href="http://www.w3.org/TR/xmlsig-core/">http://www.w3.org/TR/xmlsig-core/</a>   | R   |   |
| Cifra XML   | Sintaxis y Procesamiento de Cifra XML (XMLenc) conforme definido por el W3C<br><a href="http://www.w3.org/TR/xmlenc-core/">http://www.w3.org/TR/xmlenc-core/</a>   | R   |   |
| Firma y cifra XML   | Transformación de decodificación para firma XML conforme definido por el W3C<br><a href="http://www.w3.org/TR/xmlenc-decrypt">http://www.w3.org/TR/xmlenc-decrypt</a>  | R   |   |
| Principales gestiones XML cuando un ambiente PKI es utilizado | XML – <i>Key Management Specification</i> (XKMS 2.0) (Especificaciones de Gestión de Llave XML) conforme definido por el W3C<br><a href="http://www.w3.org/TR/xkms2/">http://www.w3.org/TR/xkms2/</a>  | R   |   |
| Autenticación y autorización de acceso XML                    | SAML – conforme definido por el OASIS cuando un ambiente ICP es utilizado<br><a href="http://www.oasisopen.org/committees/security/index.shtml">http://www.oasisopen.org/committees/security/index.shtml</a>   | R   |   |
| Intermediación o Federación de Identidades                    | WS-Security 1.1 - conjunto de estándares para garantizar integridad y confidencialidad en mensajes SOAP.<br>( <a href="http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-soapmessage-security-1.0.pdf">http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-soapmessage-security-1.0.pdf</a> ).<br><br>WS-Trust 1.3 – extensiones para el estándar WSSecurity, definiendo el uso de credenciales de seguridad y gestión de confianza distribuida.<br>( <a href="http://docs.oasis-open.org/ws-sx/ws-trust/200512">http://docs.oasis-open.org/ws-sx/ws-trust/200512</a> ). | E   | El componente anterior (SAML) podrá juntarse a este componente después de estudios. |
| Navegadores   | Solamente utilizar testimonios de conexión de carácter permanente ( <i>cookies</i> ) 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<br>R = Recomendado<br>T = En Transición<br>E = En Estudio<br>F = Estudio Futuro   |     |               |
| Directorio | Portaría 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.<br>LDAPv3 RFC 2251<br>( <a href="http://www.ietf.org/rfc/rfc2251.txt">http://www.ietf.org/rfc/rfc2251.txt</a> ). | R   |               |

| Componente                                | Especificación   | SIT | Observaciones  |
|---|--|-----|--|
|   | LDAP v3 extensión para TLS RFC2830 ( <a href="http://www.ietf.org/rfc/rfc2830.txt">http://www.ietf.org/rfc/rfc2830.txt</a> ).  |     |  |
| 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 <a href="http://www.nbso.nic.br/docs/seg-adm-redes/seg-admchclist.pdf">http://www.nbso.nic.br/docs/seg-adm-redes/seg-admchclist.pdf</a><br><br>Versión 1.2<br>16 de mayo de 2003<br>Securing an internet name server, CERT – ago/2002.   | R   |  |
| Transferencia de archivos de forma segura | HTTPS RFC 2818 ( <a href="http://www.ietf.org/rfc/rfc2818.txt">http://www.ietf.org/rfc/rfc2818.txt</a> ).  | R   |  |
| Transferencia de archivos de forma segura | SSH FTP  | F   | Los documentos aún están en el formato de borrador.  |
| Transferencia de archivos de forma segura | Securing FTP with TLS, RFC 4217 <a href="http://www.faqs.org/rfcs/rfc4217.html">http://www.faqs.org/rfcs/rfc4217.html</a> y RFC 2246 <a href="http://www.faqs.org/rfcs/rfc2246.html">http://www.faqs.org/rfcs/rfc2246.html</a>   | E   |  |
| Newsgroup                                 |  | F   |  |
| Mensaje instantáneo                       | RFC 2778 ( <a href="http://www.ietf.org/rfc/rfc2778.txt">http://www.ietf.org/rfc/rfc2778.txt</a> ), RFC 3261 ( <a href="http://www.ietf.org/rfc/rfc3261.txt">http://www.ietf.org/rfc/rfc3261.txt</a> ), RFC 3262 ( <a href="http://www.ietf.org/rfc/rfc3262.txt">http://www.ietf.org/rfc/rfc3262.txt</a> ), RFC 3263 ( <a href="http://www.ietf.org/rfc/rfc3263.txt">http://www.ietf.org/rfc/rfc3263.txt</a> ), RFC 3264 ( <a href="http://www.ietf.org/rfc/rfc3264.txt">http://www.ietf.org/rfc/rfc3264.txt</a> ) y RFC (3265. <a href="http://www.ietf.org/rfc/rfc3265.txt">http://www.ietf.org/rfc/rfc3265.txt</a> ). | E   |  |
| Sincronismo de tiempo                     | RFC 1305 IETF- <i>Network Time Protocol</i> – NTP version 3.0 ( <a href="http://www.ietf.org/rfc/rfc1305.txt">http://www.ietf.org/rfc/rfc1305.txt</a> ).<br>RFC 2030 IETF- <i>Simple Network Time Protocol</i> - SNTP version 4.0 ( <a href="http://www.ietf.org/rfc/rfc2030.txt">http://www.ietf.org/rfc/rfc2030.txt</a> ).   | R   |  |
| Sello de tiempo                           | RFC 3628 TSAs - <i>Policy Requirements for Time-Stamping Authorities</i> ( <a href="http://www.ietf.org/rfc/rfc3628.txt">http://www.ietf.org/rfc/rfc3628.txt</a> ), <i>Time-Stamp Protocol</i> ,<br>RFC 3161 ETSI TS101861 ( <i>Time-Stamping Profile</i> ) ( <a href="http://www.ietf.org/rfc/rfc3161.txt">http://www.ietf.org/rfc/rfc3161.txt</a> ).   | 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 de Redes Inalámbricas**

| Componente  | Especificación   | SIT | Observaciones |
|---|--|-----|---------------|
|   | A = Adoptado<br>R = Recomendado<br>T = En Transición<br>E = En Estudio<br>F = Estudio Futuro                         |     |               |
| MAN <sup>9</sup> inalámbrico 802.16-2004 <sup>10</sup><br>802.16.2-2004 <sup>11</sup> | Utilizar PKM-EAP ( <i>Privacy Key Management - Extensible Authentication Protocol</i> ) com:<br>• EAP – TLS ou TTLS; | E   |               |

<sup>9</sup> El 802.16 es definido por el IEEE como una interfaz tecnológica para redes de acceso inalámbrico metropolitanas o WMAN (Wireless Metropolitan Access Network).

<sup>10</sup> <http://standards.ieee.org/getieee802/download/802.16-2004.pdf>.

| Componente                                       | Especificación  | SIT      | Observaciones |
|--|---|----------|---------------|
| 802.16e <sup>12</sup> e<br>802.16f <sup>13</sup> | • AES <sup>14</sup> (Advanced Encryption Standard).             |          |               |
| LAN inalámbrico<br>802.11                        | Utilizar la especificación WPA2 (Wi-Fi <i>Protect Access</i> ). | <b>R</b> |               |

**Tabla 9 – Especificaciones Técnicas para Seguridad – Colecta, Tratamiento y Archivo de Evidencias**

| Componente                | Especificación  | SIT      | Observaciones |
|---------------------------|---|----------|---------------|
|                           | A = Adoptado<br>R = Recomendado<br>T = En Transición<br>E = En Estudio<br>F = Estudio Futuro  |          |               |
| Preservación de registros | <i>Guidelines for Evidence Collection and Archiving</i> , RFC 3227 ( <a href="http://www.ietf.org/rfc/rfc3227.txt">http://www.ietf.org/rfc/rfc3227.txt</a> ).   | <b>R</b> |               |
| Respuesta a incidentes    | <i>Expectations for Computer Security Incident Response</i> , RFC 2350 ( <a href="http://www.ietf.org/rfc/rfc2350.txt">http://www.ietf.org/rfc/rfc2350.txt</a> ).   | <b>R</b> |               |
| Informática Forense       | <i>Guide to Integrating Forensic Techniques into Incident Response – NIST - Special Publication 800-86 (Draft) –</i> ( <a href="http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf">http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf</a> ). | <b>R</b> |               |

<sup>11</sup> <http://standards.ieee.org/getieee802/download/802.16.2-2004.pdf>.

<sup>12</sup> <http://standards.ieee.org/getieee802/download/802.16e-2005.pdf>.

<sup>13</sup> <http://standards.ieee.org/getieee802/download/802.16f-2005.pdf>.

<sup>14</sup> <http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf>.

## 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, demás esferas de gobierno, demás Poderes, servidores públicos, empresas privadas y otras instituciones – son:

**8.1.1.** Los sistemas de información del gobierno deben ser proyectados de forma a respetar la

legislación brasileña, facilitando recursos de accesibilidad a los ciudadanos portadores de necesidades especiales, a grupos étnicos minoritarios y a aquellos cuyo riesgo de exclusión social o digital sea elevado. La atención en la barra de prestación de servicios debe ser considerada en toda su amplitud, de forma a posibilitar que los beneficios decurrentes del uso de los servicios de gobierno electrónico sean extendidos a la camada de la población que no puede tener acceso directo a esos servicios por medio de los dispositivos previstos.

**8.1.2.** Sistemas de información del gobierno que ofrecen servicios de gobierno electrónico:

- cuando utilicen la Internet como medio de comunicación y estaciones de trabajo como dispositivo de acceso, serán proyectados objetivando facilitar el acceso a sus informaciones con uso de tecnologías y protocolos de comunicación de la *web* basados en navegadores (*browsers*);
- cuando utilicen otros dispositivos de acceso, como, por ejemplo, teléfonos móviles, televisión digital y tarjetas inteligentes (*smart cards*), podrán servirse de otras interfaces además de los navegadores *web*;
- deberán ser proyectados para disponibilizar a los usuarios servicios de gobierno electrónico por intermedio de varios vehículos de acceso;
- deben estipular la sustitución gradual de la sistemática de “login/seña” por autenticación de usuarios con utilización de certificado digital, de modo preferencial embarcados en 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, 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 en la barra de recepción;
  - tarjetas inteligentes, *tokens* y otras tarjetas;
  - otros mecanismos de acceso, como teléfonos móviles, *hand-helds* y televisión digital serán objeto de estudio futuro para determinación de los padrones aceptados por el gobierno federal.

**8.1.3.** Los sistemas de información del gobierno, contruidos para dar soporte a un determinado dispositivo de acceso, deben seguir, obligatoriamente, las especificaciones publicadas en e-PING para aquél dispositivo.

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

**8.1.5.** El desarrollo de los servicios de gobierno electrónico debe ser orientado de modo a ofrecer atención a los usuarios que no dispongan de acceso a las tecnologías más recientes disponibles en el mercado. Por otra parte, también se debe llevar en cuenta la necesidad de atención con aquellos usuarios portadores de necesidades especiales, requisito que involucra la utilización de recursos más sofisticados y de uso específico. De modo a conciliar esas necesidades, se deberán observar las recomendaciones del Modelo de Accesibilidad de Gobierno Electrónico (e-MAG)(13).

**8.1.6.** Cuando la Internet sea utilizada como medio de comunicación, los sistemas de información del gobierno deben proyectarse de manera que se pueda trabajar una cantidad máxima de informaciones a partir de navegadores que atiendan al estándar mínimo explicitado por el soporte a las especificaciones técnicas pertinentes previstas en la sección 8.2. A título complementario, e-PING recomienda que cualquier servicio de gobierno electrónico especifique, de forma clara y, de ser posible, en su página inicial, las 13 BRASIL. Ministerio del Planeamiento, Presupuesto y Gestión. Recomendaciones de Accesibilidad para la construcción y adaptación de contenidos del Gobierno

Brasileño en Internet: modelo de accesibilidad. Versión 2.0. Brasilia, 2005. Disponible en: (<http://www.governoeletronico.gov.br/emag/>). Accedido en: 13/07/2006. versiones mínimas de navegadores que soportan las funcionalidades requeridas por el servicio asociado.

En atención al estándar mínimo referido arriba, deben ser consideradas las excepciones que involucren cuestiones de seguridad en el trato de informaciones.

**8.1.7.** Cuando la Internet sea utilizada como medio de comunicación, *middleware* o *plug-ins* adicionales podrán utilizarse, si no hay alternativa técnicamente posible, para optimizar la funcionalidad del navegador en las estaciones de trabajo. En este caso, ese software adicional deberá ser ofrecido sin el pago de tasa de licencia y deberá estar en conformidad con todas las especificaciones técnicas correspondientes discriminadas en e-PING. Además, deberá ser presentado en repositorio seguro mantenido por el organismo gubernamental responsable por la aplicación.

**8.1.8.** Los servicios de gobierno electrónico deben ser proyectados de manera que garanticen a los usuarios la autenticidad del contenido por medio de emisión de certificado digital, conforme padrones preconizados por la ICP – Brasil. Referencia: <http://www.icpbrasil.gov.br/>. En ese sentido, todos los sitios *web* deberán, de modo obligatorio, utilizar “https” en vez de “http”.

**8.1.9.** La necesidad de la sociedad aunada a la posibilidad del gobierno de desarrollar e implementar 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 *web* (conforme tópico 3. Políticas Generales) y para tornar viable el uso de quioscos públicos, de barras de atención y de Centrales de Atención al ciudadano (como, por ejemplo, Telecentros).

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

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

Esos adaptadores también podrán ser utilizados como forma alternativa 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/Resolucao/2002/RES07-02web.htm](https://www.planalto.gov.br/ccivil_03/Resolucao/2002/RES07-02web.htm)

**8.1.11.** Serán considerados preferenciales aquellos tipos de archivo 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 faciliten documentos a sus usuarios deberán hacerlo empleando en el propio enlace de acceso al documento información clara respecto a proveniencia, 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 se exija, o la fecha de la disposición en el sitio, para los otros casos. Otras informaciones sobre el documento, tales como, autor, redactor, emisor, fecha tónica u otras relevantes para su precisa caracterización, deberán constar en el campo propiedades del propio documento.

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

Para la construcción de minutas de documentos o trabajos que necesiten ser creados en colaboración por más de una persona y/u organismo, pueden ser utilizados los formatos previstos en la Tabla 9.

Ya para la construcción de la versión final de documentos, la cual debe ser enviada a otros organismos o incluso archivada digitalmente, se recomienda la utilización del formato pdf/a.

## Documento de Referencia de e-PING – Versión 3.0

Documentos que necesiten de garantía de integridad y/o autoría, además de que estén en formato pdf/a, deben ser firmados digitalmente por su autor, utilizando certificado ICP-Brasil.

La mención a los productos que generan los formatos de archivos referidos en la Tabla 9 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 10 – Especificaciones Técnicas – Estaciones de Trabajo**

| Componente                           | Especificación  | SIT | Observaciones |
|--------------------------------------|---|-----|---------------|
|                                      | A = Adoptado<br>R = Recomendado<br>T = En Transición<br>E = En Estudio<br>F = Estudio Futuro  |     |               |
| Navegadores ( <i>browsers</i> )      | Ver tópico 3. Políticas Generales.  | E   |               |
| Conjunto de caracteres y alfabetos   | UNICODE <i>standard</i> versión 4.0, latin-1, UTF8, ISBN 0-321-18578-1.   | R   |               |
| Formato de intercambio de hipertexto | HTML versión 4.01 (.html ou .htm), generado conforme especificaciones del W3C <sup>15</sup>   | A   |               |
|                                      | XHTML versiones 1.0 o 1.1 (.xhtml), generado conforme especificaciones del W3C <sup>16</sup>  | A   |               |
|                                      | XML versiones 1.0 o 1.1 (.xml), generado conforme especificaciones del W3C <sup>17</sup>  | A   |               |
|                                      | SHTML (.shtml).   | R   |               |
|                                      | MHTML (.mhtml ou .mht) <sup>18</sup> .  | T   |               |
| Archivos del tipo documento          | XML versiones 1.0 o 1.1 (.xml), o con formatación (opcional) XSL (.xsl), generado conforme especificaciones del W3C <sup>19</sup> . | R   |               |
|                                      | Open Document (.odt), generado conforme especificaciones del estándar ISO/IEC 26300 <sup>20</sup> .                                 | R   |               |
|                                      | OpenOffice.org XML (.sxw), generado en el formato del OpenOffice version 1.0.   | T   |               |
|                                      | Rich Text Format (.rtf).  | T   |               |
|                                      | PDF (.pdf) generado en formato hasta versión 1.3.   | T   |               |

<sup>15</sup> HTML 4.01 Specification - W3C Recommendation 24 December 1999. Disponible en: <http://www.w3.org/TR/html4/>.

<sup>16</sup> 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/>

<sup>17</sup> 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/>.

<sup>18</sup> Formato de empaquetamiento de archivos web de Microsoft (*Mime Encapsulation of Aggregate HTML Documents*).

<sup>19</sup> Extensible Stylesheet Language (XSL) Version 1.0 - W3C Recommendation 15 October 2001. Disponible en: <http://www.w3.org/TR/xsl/>.

<sup>20</sup> Open Document Format for Office Applications (OpenDocument) v1.0 - estándar ISO/IEC 26300. Disponible em: <http://www.iso.org/>.

## Documento de Referencia de e-PING – Versión 3.0

| Componente  | Especificación   | SIT | Observaciones   |
|---|--|-----|---|
|   | PDF versión abierta PDF/A <sup>21</sup> .  | R   |   |
|   | Texto puro (.txt).   | A   |   |
|   | HTML versión 4.01 (.html ou .htm), generado conforme especificaciones del W3C.                               | R   |   |
|   | Microsoft Word document (.doc), generado en el formato del MS Office hasta versión 2000.                     | T   |   |
| Archivos del tipo planilla                                    | Open Document (.ods), generado conforme especificaciones del estándar ISO/IEC 26300.                         | R   |   |
|   | OpenOffice.org XML (.sxc), generado en el formato del Open Office versión 1.0.                               | 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   |   |
| Archivos del tipo “banco de datos” para estaciones de trabajo | XML versiones 1.0 o 1.1 (.xml)   | R   | En las opciones texto plano (txt) y csv, se debe incluir, de modo obligatorio, el lay-out de los campos, de forma a posibilitar su tratamiento. |
|   | MySQL Database (.myd, .myi), generados en los formatos del MySQL, versión 4.0 o superior.                    | R   |   |
|   | Texto Puro (.txt)  | A   |   |
|   | Texto Puro (.csv) – comma-separated values   | A   |   |
|   | Archivo del Base (.odb), generado en el formato del BrOffice.org (u OpenOffice.org) versión 2.0 o posterior. | R   |   |
|   | Archivo MS Access (.mdb), generado en el formato del MS Office, hasta versión 2000.                          | T   |   |
| Intercambio de informaciones gráficas e imágenes estáticas    | PNG (.png), generado conforme especificaciones del W3C <sup>22</sup> – ISO/IEC 15948:2003 (E).               | A   |   |
|   | TIFF (.tif) <sup>23</sup>  | R   |   |
|   | SVG (.svg), generado conforme especificaciones del W3C <sup>24</sup> .                                       | R   |   |
|   | JPEG File Interchange Format (.jpeg, .jpg o .jfif) <sup>25</sup>   | R   |   |

<sup>21</sup> 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/>.

<sup>22</sup> 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/RECPNG-20031110/>. Acceso en: 7 dic 2005.

<sup>23</sup> Tagged Image File Format (Adobe Systems).

<sup>24</sup> Scalable Vector Graphics (SVG) 1.1 Specification. W3C Recommendation 14 January 2003. Disponible en: <http://www.w3.org/TR/2003/REC-SVG11-20030114/>. Acceso en: 7 dic. 2005.

<sup>25</sup> JPEG File Interchange Format (version 1.02) 1 September 1992. Disponible em: <http://www.jpeg.org/public/jfif.pdf>. Acceso en: 7 dic. 2005.

## Documento de Referencia de e-PING – Versión 3.0

| Componente                                | Especificación  | SIT | Observaciones |
|---|---|-----|---------------|
|   | 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 <sup>26</sup>                              | T   |               |
|   | Imagen Corel Photo-Paint (.cpt), generado en el formato de la suite Corel Draw hasta versión 7.               | T   |               |
|   | Imagen Photoshop (.psd), generado en el formato del Adobe Photoshop hasta versión 4.                          | T   |               |
| 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 suite Corel Draw hasta versión 7.                                    | T   |               |
|   | Gráfico MS Visio (.vss ou .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), gerado conforme a especificação GIF89a.   | T   |               |
|   | Shockwave Flash (.swf), gerado no formato do Macromedia Flash até versão 4, do Macromedia Shockwave versão 1. | T   |               |
| Archivos del tipo audio y del tipo video  | .mpg  | R   |               |
|   | Audio y video MPEG-4, Part 14 (.mp4) <sup>27</sup>  | R   |               |
|   | MIDI (.mid) <sup>28</sup>   | R   |               |
|   | Audio Ogg Vorbis I (.ogg) <sup>29</sup>   | R   |               |
|   | Audio-Video Interleaved (.avi), con codificación Xvid.  | R   |               |
|   | Audio-Video Interleaved (.avi), con codificación divX.  | T   |               |
|   | Audio MPEG-1, Audio Layer 3 (.mp3) <sup>30</sup>  | T   |               |

<sup>26</sup> Graphics Interchange Format (CompuServe/America Online, Inc.).

<sup>27</sup> ISO/IEC 14496-14:2003 - Information Technology - Coding of audio-visual objects - Part 14: MP4 file format.

<sup>28</sup> Musical Instrument Digital Interface, conforme la especificación *The Complete MIDI 1.0 Detailed Specification*. Version 96.1, 2.ed., nov. 2001. Disponible en:

<http://www.midi.org/aboutmidi/specinfos.shtml>. Acceso en: 30 mayo. 2007.

<sup>29</sup> Xiph.Org Foundation. Especificación disponible en: [http://xiph.org/vorbis/doc/Vorbis\\_I\\_spec.html](http://xiph.org/vorbis/doc/Vorbis_I_spec.html).

<sup>30</sup> ISO/IEC 11172-3:1993 - Information technology - Coding of moving pictures and associated audio for

| Componente   | Especificación  | SIT   | Observaciones  |
|--|---|---|--|
|  | <i>Real Media</i> (.rm ou .rmm), generado en el formato de los aplicativos Real Audio Media Player, hasta versión 8.                  | T   |  |
|  | <i>Real Audio</i> (.ra o .ram), generado en el formato de los aplicativos Real Audio Media Player, hasta versión 8.                   | T   |  |
|  | WAVE (.wav)   | T   |  |
|  | <i>Shockwave Flash</i> (.swf), generado em el formato del Macromedia Flash, hasta versión 4 o por el Macromedia Shockwave, versión 1. | T   |  |
|  | <i>Windows Media Video</i> (.wmv), generado en el formato del Windows Media Player, hasta versión 6.4.                                | T   |  |
|  | <i>Windows Media Audio</i> (.wma), generado en el formato del Windows Media Player, hasta versión 6.4.                                | T   |  |
|  | <i>QuickTime</i> (.mov), generado en el formato del Apple Quicktime, hasta versión 6.   | T   |  |
|  | <i>QuickTime</i> (.qt), generado en el formato del Apple Quicktime, hasta versión 6.  | T   |  |
| Compactación de archivos de uso general<br>Informaciones georreferenciadas – padrones de archivos para intercambio entre estaciones de trabajo | ZIP (.zip).   | R   |  |
|  | GNU ZIP (.gz).  | R   |  |
|  | Paquete TAR (.tar).   | R   |  |
|  | Paquete TAR compactado (.tgz ou .tar.gz).   | R   |  |
|  | BZIP2 (.bz2).   | R   |  |
|  | Paquete TAR compactado con BZIP2 (.tar.bz2).  | R   |  |
|  | MS Cabinet (.cab).  | T   |  |
|  | GML versión 1.0 o superior <sup>31</sup> .  | A   | Señalado para estructuras vectoriales complejas, abarcando primitivas geográficas como polígonos, puntos, líneas, superficies, colecciones, y atributos numéricos o textuales sin límites de número de caracteres. |
| ShapeFile <sup>32</sup> .  | A   | Señalado para estructuras vectoriales limitadas a líneas, puntos y polígonos, cuyos atributos textuales no sobrepasen 256 caracteres. Puede almacenar también las |  |

digital storage media at up to about 1,5Mbit/s - Part 3: Audio.  
ISO/IEC 11172-3:1993/Cor 1:1996.

<sup>31</sup> *Geography Markup Language*. Especificaciones disponibles en: <http://www.opengeospatial.org/standards>.

<sup>32</sup> *ESRI Shapefile Technical Description*. Disponible em: <http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf>.

| Componente                       | Especificación                  | SIT | Observaciones  |
|----------------------------------|---------------------------------|-----|--|
|                                  |                                 |     | dimensiones M y Z.   |
|                                  | GeoTIFF <sup>33</sup> .         | A   | Señalado para estructuras matriciales limitadas a matrices de pixel. |
|                                  | SFS.                            | E   |  |
| Programación Extendida (Plugins) | Tema para consideración futura. | F   |  |

### 8.3. Medios de Acceso: Especificaciones Técnicas para *tokens*, Tarjetas Inteligentes y Tarjetas en General

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

Las conclusiones de aquel grupo también fueron utilizadas para la construcción de los Manuales de Conductas Técnicas del ITI, documentos que establecen los requisitos técnicos que serán 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 equipos 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 la Información (ITI), como responsable por la conducción del proceso, mientras que los Laboratorios de Estudios y Auditoría (LEA), creados por la Resolución 36, quedaron responsables por los ensayos de conformidad.

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

Por el reglamento son pasibles de homologación medias como *tokens* criptográficos y *smart cards*, sistemas como el de firma electrónica, de autenticación de firma, de autoridades certificadoras y de registro, y equipos 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 que fornece 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 Padrones de Interoperabilidad de Gobierno Electrónico – e-PING y ayudar a masificar el uso de la certificación, pues entre otros aspectos podrá contribuir para la disminución del coste de esa solución tecnológica.

En el contexto de 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 e 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 padrones 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 trabajar con certificados digitales. Aún fueron incorporadas las normas ISO para tarjetas magnéticas y tarjetas

<sup>33</sup> *GeoTIFF Format Specification*. Disponible em: <http://remotesensing.org/geotiff/geotiff.html>.

## Documento de Referencia de e-PING – Versión 3.0

ópticas, aquellos tradicionales y de bajo coste, estos más arrojados y de alto coste.

Para las versiones futuras de e-PING, será establecida una agenda mínima que deberá revisar todo el cuadro de especificaciones y perfilar, 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 conducida una investigación exhaustiva que suministre subsidios para la inclusión o no, en e-PING, de los padrones de tarjetas efectivamente utilizados por los organismos de gobierno. Como ejemplo de esa situación, pueden ser nombrados los llamados *embossed smart cards* (ISO/IEC 7811), tarjetas gravadas en relieve, que no son contemplados en esta versión. Caso sea constatada, en esa investigación, el uso intensivo de ese tipo de dispositivo, será evaluada la viabilidad de su inclusión en el conjunto de especificaciones tratadas por e-PING.

Aún para las versiones futuras, serán evaluadas en profundidad los padrones característicamente orientados hacia la comunidad europea. Es el caso del eEurope, el *Open Smart Card Infrastructure for Europe – versión 2* que asimila la tecnología de tarjetas sin contacto, presente en la ISO/IEC 14443. Lo mismo será hecho en el estándar CALYPSO (*Fourth European Research and Technological Development Framework Program*) para sistemas de tarjetas (o billetes) sin contacto, orientadas para sistemas de transportes públicos. Será necesario evaluar los estándares, sistemas de patentes y licenciamientos que pudieran existir.

**Tabla 11 – Especificaciones para Medios de Acceso – Tarjetas Inteligentes, *tokens* y Tarjetas en General**

| Componente          | Especificación  | SIT      | Aplicable a   | Observaciones                                     |
|---------------------|---|----------|---|---|
|                     | A = Adoptado<br>R = Recomendado<br>T = En Transición<br>E = En Estudio<br>F = Estudio Futuro  |          |   |   |
| Definición de datos | Manuales de Conductas Técnicas del ITI – Volumen 1 ( <a href="http://www.lea.gov.br/">http://www.lea.gov.br/</a> ).   | <b>A</b> | Todas las tarjetas y <i>tokens</i> que utilizan certificados digitales. |   |
|                     | Tarjetas de identificación <b>ISO/IEC 7816-6</b> Tarjetas de Circuito(s) Integrado(s) con contactos Parte 6: Elementos de datos Intersectorial.   | <b>A</b> | Todos   | Según opción del GT de la ICP-Brasil.             |
|                     | Tarjetas de identificación <b>ISO/IEC 7812-1</b> Identificación de los emisores Parte 1: Sistema de Numeración.   | <b>R</b> | Todos   |   |
|                     | Tarjetas de transacción financiera <b>ISO 9992-2</b> . 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. | <b>F</b> | Todos   |   |
|                     | Sistemas de tarjeta de identificación <b>BS EN 1546-3 – Inter-sector electronic purse -</b> Parte 3: Elementos e intercambio de datos   | <b>F</b> | Todos   | La actual edición fue publicada en julio de 1999. |

| Componente  | Especificación   | SIT   | Aplicable a   | Observaciones  |
|---|--|---|---|--|
|   | Sistemas de tarjeta de identificación <b>BS EN 1546-4</b> – <i>Inter-sector electronic purse</i> - Parte 4: Objetos de datos.                    |   |   | La actual edición fue publicada en agosto de 1999.   |
| Aplicaciones incluyendo multiaplicaciones   | Tarjetas de identificación <b>ISO/IEC 7816-4</b><br>Parte 4: Comandos intersectoriales para intercambio.   | <b>A</b>                                      | Tarjetas de Circuito(s) Integrado(s) con contactos. | Establece las estructuras de los archivos, asegura mensajes para el acceso a archivos, inicialización de aplicativos de tarjeta, y canales lógicos para el uso cuando la tarjeta pueda tener un canal virtual de comunicación activo más. 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.<br><br>Conforme opción del GT de la ICP-Brasil. La actual edición fue publicada en junio de 1994. Existe también una mudanza ISO/IEC 7816-5/AM1 <i>Registered Application Provider Identifiers</i> (RDIs) (Identificadores de Proveedores de Aplicaciones Registradas) que se publicó en diciembre de 1996. |
|   | Tarjetas de Identificación <b>ISO/IEC 7816-5</b><br>Parte 5: Sistema de numeración y tramitación de registro para identificadores de aplicación. | <b>R</b>                                      |   |  |
|   | <b>ISO/IEC 7816-7</b><br>Parte 7: Comandos intersectoriales para <i>Structured Card Query Language</i> (SCQL);                                   | <b>R</b>                                      |   |  |
|   | <b>ISO/IEC 7816-11</b><br>Parte 11: Estructura para el uso dinámico de aplicaciones múltiples en tarjetas de circuitos integrados.               | <b>R</b>                                      |   |  |
|   | Tarjetas de identificación <b>ISO/IEC 7813</b> – Tarjetas de transacciones financieras.  | <b>R</b>                                      | Tarjetas financieras.                               |  |
| Tarjetas de identificación de los emisores <b>ISO/IEC 7812-2</b><br>Parte 2: Procedimientos de aplicación y registro.   | <b>R</b>   | Todos   |   |  |
| Tarjetas de identificación <b>ISO/IEC 15693-4</b> – Tarjetas de circuito(s) integrado(s) sin contacto, Tarjetas de proximidad { <i>Vicinity Integrated Circuit(s) Cards</i> (VICC) (Tarjetas de Circuito(s) Integrado(s) de Proximidad)}<br>Parte 4: Registro de aplicaciones/emisores. | <b>R</b>   | Tarjetas de circuito integrado de proximidad. |   |  |
| Sistemas de tarjeta de identificación <b>EN 1332-1:1999</b> – Interfaz hombre/máquina – Parte 1: Principios de proyecto para interfaz de usuario  | <b>R</b>   | Todos   |   |  |

Documento de Referencia de e-PING – Versión 3.0

| Componente  | Especificación  | SIT  | Aplicable a  | Observaciones   |
|---|---|--|--|---|
|   | Sistemas de tarjeta de identificación <b>EN 1332-4:1999</b><br>–<br>Interfaz hombre/máquina –<br>Parte 4: Codificación de exigencias de usuario para personas con necesidades especiales.   |  |  |   |
| Eléctrico   | Tarjetas de identificación <b>ISO/IEC 7816-10</b> – Tarjetas de circuito(s) Integrado(s) con contactos – Parte 10: Señales electrónicos y respuesta para reinicio para tarjetas síncronas.<br><br><b>ISO/IEC 7816—12</b><br>Parte 12: Interfaz USB. | <b>R</b>   | Tarjetas de circuito(s) integrado(s) con contactos.          |   |
|   | Tarjetas de identificación <b>ISO/IEC 14443-2</b> – Tarjetas de circuito(s) Integrado(s) sin contacto – Tarjetas de proximidad – Parte 2: Interfaz de potencia y señal de frecuencia de radio.  | <b>R</b>   | Tarjetas de circuito integrado de proximidad.                | Esta parte define la interfaz de frecuencia de radio, y contiene dos técnicas de modulación bien distintas (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 aspectos específicos del Tipo A aparecen en la parte 4. |
|   | Tarjetas de identificación <b>ISO/IEC 10536-3</b> Tarjetas de circuito(s) integrado(s) sin contacto { <i>Close Coupling Integrated Circuit(s) Cards</i> (CICC) (Tarjetas de Circuito(s) Integrado(s) de Acoplamiento Fuerte)}                       | <b>F</b>   | Tarjetas de circuito(s) integrado(s) de acoplamiento fuerte. |   |
|   | Parte 3: Procedimiento de señales electrónicos y reinicialización.  |  |  |   |
| Tarjetas de identificación <b>ISO/IEC 15693-2</b> Tarjetas de circuito(s) integrado(s) sin contacto.<br>Tarjetas de Proximidad { <i>Vicinity Integrated Circuit(s) Cards</i> (VICC) (Tarjetas de Circuito(s) Integrado(s) de Proximidad)}:<br>Parte 2: Interfaz e | <b>R</b>  | Tarjetas de circuito(s) integrado(s) de proximidad sin contacto. |  |   |

## Documento de Referencia de e-PING – Versión 3.0

| Componente   | Especificación   | SIT    | Aplicable a  | Observaciones  |
|--|--|--------|--|--|
|  | inicialización Por el aire;  |        |  |  |
| Protocolos de Comunicaciones   | Tarjetas de identificación <b>ISO/IEC 7816-3</b> Parte 3: Protocolos de señales y transmisiones electrónicas.  | R      | Tarjetas de circuito(s) integrado(s) con contactos.        | Según opción del GT de la ICP-Brasil   |
|  | Tarjetas de identificación <b>ISO/IEC 14443-3</b> - 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 da 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 <b>ISO/IEC 14443-4</b> – 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 del ISO/IEC 7816, y es una puente sobre el ISO 7816-4. Solamente para tarjetas Tipo A el ISO/IEC 14443-4 incluye un procedimiento de inicialización de protocolo.   |
|  | Tarjetas de identificación <b>ISO/IEC 15693-3</b> – 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 <b>ISO 8583</b> – especificación de Mensaje de intercambio.   | F      | Todos.   |  |
|  | Tarjetas de transacciones financieras <b>ISO 9992-1</b> – Mensajes entre la tarjeta de circuito integrado y el dispositivo de aceptación de la tarjeta – Parte 1: Conceptos y estructuras; <b>ISO 9992-2</b> Parte 2: Funciones, mensajes (comandos y respuestas), elementos y estructuras de datos. | F      | Todos.   |  |
| Tarjetas de transacciones financieras <b>ISO 10202-2</b> Arquitectura de seguridad de sistemas transacción financiera usando tarjetas de circuito integrado. Parte 2: Proceso de | R  | Todos. |  |  |

| Componente   | Especificación  | SIT | Aplicable a  | Observaciones   |
|--|---|-----|--|---|
|  | transacción;<br>ISO 10202-6<br><b>Parte 6: Verificación del portador de la tarjeta.</b>   |     |  |   |
|  | Tarjetas de identificación <b>ISO/IEC 10536-4</b> tarjetas de circuito(s) integrado(s) sin contacto { <i>Close Coupling Integrated Circuit(s) Cards</i> (CCIC) (Tarjetas de Circuito(s) Integrado(s) de Acoplamiento Fuerte)}.<br>Parte 4: Respuesta a protocolos de reinicialización y transmisión.  | F   | Tarjetas de circuito(s) integrado(s) de acoplamiento fuerte.     |   |
| Los Padrones de físico/físico y de interfaz cubren las dimensiones de la tarjeta;<br><br>Localidad y <i>layout</i> de contactos. | <b>Características físicas</b><br>Tarjetas de identificación <b>ISO/IEC 7810</b>  | R   | Todas las tarjetas de contacto y combinación.                    | Para asegurar que puedan ser leídos en lectora estándar, todas las tarjetas deben seguir el formato ID-1 según definido en este estándar.   |
|  | <b>Tarjeta Magnética ISO/IEC 7811</b> , partes 2, 4 e 5: definen las propiedades, posicionamiento y codificación ( <i>coding</i> ) de la banda magnética de la tarjeta.   | R   | Todas las tarjetas con banda magnética.                          |   |
|  | <b>Tarjeta de memoria óptica ISO/IEC 11693 e 11694.</b>   | F   | Tarjetas ópticas   | Tarjetas que soportan el almacenamiento de muchos <i>megabytes</i> .  |
|  | Tarjetas de identificación <b>ISO/IEC 7816-1</b><br>Parte 1: Características físicas<br>Tarjetas de identificación <b>ISO/IEC 15693-1</b> - Tarjetas de circuito(s) integrado(s) sin contacto – Tarjetas de proximidad - Parte 1: Características físicas.<br>Tarjetas de identificación <b>ISO/IEC 7816-2</b> – Tarjetas de circuito(s) integrado(s) con contactos<br>Parte 2: Dimensiones y ubicación 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.<br><br>Conforme opción del GT de la ICP-Brasil y Manual de Conductas Técnicas del ITI – Volumen I. |
|  | Tarjetas de identificación <b>ISO/IEC 14443-1</b> – 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 <b>ISO/IEC 15693-1</b> – Tarjetas de circuito(s) integrado(s) sin contactos – Tarjetas de proximidad - Parte 1: Características físicas.   | R   | Tarjetas de circuito(s) integrado(s) de proximidad sin contacto. | Esta parte del <b>ISO/IEC 15693</b> se publicó en 15-07-2000.   |

| Componente | Especificación   | SIT | Aplicable a   | Observaciones  |
|------------|--|-----|---|--|
|            | Esta parte del <b>ISO/IEC 15693</b> se publicó en 15-07-2000.  |     |   |  |
|            | Tarjetas de identificación <b>ISO/IEC 10536-1</b> – Tarjetas de circuito(s) integrado(s) sin contacto<br>Parte 1: Características físicas;<br><b>ISO/IEC 10536-2</b><br>Parte 2: Dimensiones y ubicación de las áreas de acoplamiento.   | F   | Tarjetas de circuito(s) integrado(s) de acoplamiento fuerte.  |  |
|            | Identificadores táctiles. Sistemas de Tarjetas de identificación <b>BS EN 1332-2</b> – Interfaz hombre/máquina<br>Parte 2: Dimensiones y ubicación - un identificador táctil para tarjetas ID-1.   | F   | Cuando la grabación en relieve no es utilizada y existe, se solicita al usuario que introduzca la tarjeta en un determinado sentido, un identificador táctil deberá ser facilitado como auxilio a los deficientes visuales. | Algunos equipos de personalización de tarjetas, a excepción de que sean modificados podrán tener dificultad en el procesamiento de tarjetas con identificadores táctiles del tipo 'notch' ('relieve'). Un acuerdo, por lo tanto, debe ser realizado junto al facilitador del servicio de personalización para la utilización de dichas tarjetas. |
| Seguridad  | Tarjetas de identificación <b>ISO/IEC 7816-8</b> – Tarjetas de circuito(s) integrado(s) con contactos.<br>Parte 8: Comandos de seguridad intersectoriales ISO/IEC 7816-9<br>Parte 9: Comandos adicionales intersectoriales y atributos de Seguridad.<br>Tarjetas de identificación <b>ISO/IEC 7816-11</b> – Tarjetas de circuito(s) integrado(s) con contactos.<br>- Parte 11: Verificación personal<br>Por medio de métodos biométricos.<br>Tarjetas de identificación <b>ISO/IEC 7816-15</b> – Tarjetas de circuito(s) integrado(s) con contactos.<br>- Parte 15: Información de dispositivo Criptográfico en tarjetas CI. | A   | Tarjetas de circuito(s) integrado(s) con contactos.   |  |
|            | Tarjetas de transacción financiera <b>ISO 10202</b><br>Arquitectura de seguridad de  | F   | Todos.  |  |

Documento de Referencia de e-PING – Versión 3.0

| Componente                   | Especificación   | SIT      | Aplicable a                                       | Observaciones            |
|------------------------------|--|----------|---|--------------------------|
|                              | <p>sistemas de transacción financiera utilizando tarjetas de circuito integrado</p> <p>Parte 1: Ciclo de vida de la tarjeta;</p> <p>Parte 2: Principios y visión general;</p> <p>Parte 3: Relaciones de llave criptográfica;</p> <p>Parte 4: Módulos seguros de aplicación;</p> <p>Parte 5: Utilización de algoritmos;</p> <p>Parte 6: Verificación del portador De la tarjeta;</p> <p>Parte 7: Gestión de llave.</p>  |          |   |                          |
| Infraestructura del terminal | <p>Sistemas de tarjetas de identificación EN 1332-3:1999 – Interfaz Hombre/máquina – Parte 3: Teclados.</p>  | <b>R</b> | Todos.  |                          |
|                              | <p>Padrones PC/SC. Padrones del Consorcio Grupo de Trabajo PC/SC Especificación de Interoperabilidad para ICCs y Sistemas de Ordenador Personal</p> <p>Parte 1. Introducción y Visión General de la Arquitectura</p> <p>Parte 2. Requisitos de Interfaz para Tarjetas Compatibles con CI y Dispositivos de Interfaz</p> <p>Parte 3. Requisitos para Dispositivos de Interfaz Conectados a PC</p> <p>Parte 4. Consideraciones del proyecto IFD e Información de Referencia del Proyecto</p> <p>Parte 5. Definición del Gestor de Recursos ICC</p> <p>Parte 6. Definición de la Interfaz del Surtidor de Servicio ICC</p> <p>Parte 7. Consideraciones del Proyecto de Dominio / Desarrollador de la Aplicación</p> <p>Parte 8. Recomendación para la Implementación de Dispositivos de Seguridad y Privacidad ICC.</p> | <b>A</b> | Todos.  | Para uso general en PCs. |
|                              | <p>Manual de Conductas Técnicas del TI – Volumen I.</p>  | <b>A</b> | Tarjetas con capacidad de gestión de certificados |                          |

Documento de Referencia de e-PING – Versión 3.0

| Componente                      | Especificación  | SIT | Aplicable a   | Observaciones   |
|---------------------------------|---|-----|---|---|
|                                 | Estándar FIPS-140-2.  | A   | digitales.<br>Todos.  | Segundo el tópico 1 del GT de la ICP-Brasil: seguir como mínimo las reglas establecidas para el nivel 1 de seguridad del FIPS-140-2. Seguir como mínimo las reglas establecidas para el nivel 2 de seguridad para verificación de violación hardware. |
| Tarjetas tipo <b>Java Card®</b> | API ( <i>Application Programming Interface</i> ) 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 <i>applets</i> puede ser construida. | Versión general para la tecnología Java Card es 2.2.1 (octubre de 2003), <a href="http://java.sun.com/products/javacard/">http://java.sun.com/products/javacard/</a>  |
|                                 | Especificación para el ambiente de ejecución ( <i>runtime environment</i> ) para la plataforma Java Card. | A   | Esta especificación describe el ambiente requerido para la ejecución de <i>applets</i> 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 12 – Especificaciones para Organización e Intercambio de Informaciones

| Componente  | Especificación  | SIT | Observaciones |
|---|---|-----|---------------|
|   | A = Adoptado<br>R = Recomendado<br>T = En Transición<br>E = En Estudio<br>F = Estudio Futuro  |     |               |
| Lenguaje para intercambio de datos                | XML ( <i>Extensible Markup Language</i> ) como definido Por el W3C<br><a href="http://www.w3.org/XML">http://www.w3.org/XML</a>   | R   |               |
| Transformación de datos                           | XSL ( <i>Extensible Stylesheet Language</i> ) como definido Por el W3C <a href="http://www.w3.org/TR/xsl">http://www.w3.org/TR/xsl</a><br>XSL <i>Transformation</i> (XSLT) como definido por el W3C<br><a href="http://www.w3.org/TR/xslt">http://www.w3.org/TR/xslt</a>  | R   |               |
| Definición de los datos para intercambio          | XML <i>Schema</i> como definido por el W3C:<br>- XML <i>Schema Part 0: Primer</i><br><a href="http://www.w3.org/TR/2004/RECxmldata-0-20041028/">http://www.w3.org/TR/2004/RECxmldata-0-20041028/</a><br>- XML <i>Schema Part 1: Structures</i><br><a href="http://www.w3.org/TR/xmldata-1/structures">http://www.w3.org/TR/xmldata-1/structures</a><br>- XML <i>Schema Part 2: Datatypes</i><br><a href="http://www.w3.org/TR/xmldata-2/datatypes">http://www.w3.org/TR/xmldata-2/datatypes</a><br>UML ( <i>Unified Modeling Language</i> ) como definido por el OMG<br><a href="http://www.omg.org/gettingstarted/specsandprods.html">http://www.omg.org/gettingstarted/specsandprods.html</a> | R   |               |
| Descripción de datos                              | RDF ( <i>Resource Description Framework</i> )<br>Como definido por la W3C.  | F   |               |
| Elementos de Metadatos para gestión de contenidos | e-PMG – Estándar de Metadatos para el Gobierno Electrónico.   | E   |               |
| Taxonomía para navegación                         | LAG - Lista de Asuntos do Governo, Versión 1.0.<br>Según definición en <a href="http://www.eping.e.gov.br">http://www.eping.e.gov.br</a>  | A   |               |
| Definición de datos                               | CPD - Catálogo de Padrones de Datos, Versión 1.0.<br>Según definición en <a href="http://www.eping.e.gov.br">http://www.eping.e.gov.br</a>  | A   |               |

### 9.3. Comentarios 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* según lo dispuesto en 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 donde existan razones fundamentales que justifiquen su utilización.



Figura 5 – Modelo XML Directo – Intercambio Directo.

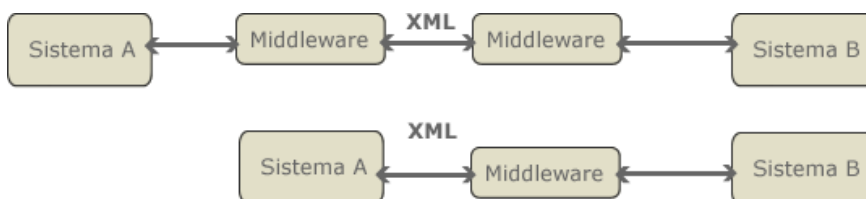


Figura 6 – Intercambios via *middleware*.

## 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 volcadas hacia el campo de Actuación de Gobierno, organizados bajo la forma de Catálogo, disponible en el sitio de e-PING y presentado con los contenidos actuales en tópico a continuación;
  - Componentes relacionados a temas transversales a las Áreas de Actuación de Gobierno, cuya estandarización sea relevante para la interoperabilidad de servicios de Gobierno Electrónico, como Procesos e Informaciones Geográficas.
- En lo que se refiere a XML *Schemas* con relación a aplicaciones orientadas hacia 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 instancias competentes en lo tocante a la prioridad que se deba conferir;
- 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 da a través de servicios inter operables:
  - Recomiéndase que la Arquitectura Orientada a Servicios (SOA) y las políticas técnicas relacionadas al Segmento Interconexión se observen en el proyecto e implementación de aplicaciones basadas en los XML *Schemas* referidos;
  - El segmento pasa a referenciar la iniciativa “Arquitectura Referencial de Inter operación de los Sistemas Informatizados de Gobierno (AR)”, que es un modelo de Arquitectura Orientada a Servicios, adaptado a la realidad de los Sistemas Informatizados de Gobierno y que, puede ser accedida en <http://i3gov.cos.ufrj.br/igov/>;
  - Existe fuerte interconexión entre el Catálogo de Padrones de Datos y el Catálogo de XML *Schemas* y, consideradas las especificidades de los contenidos, se trata de mantener los principios generales y los mecanismos de gestión compatibles.

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

#### 10.2.1. Consideraciones Iniciales

La arquitectura e-PING - Estándares de Inter Operabilidad de Gobierno Electrónico defiende la adopción del XML y el desarrollo de XML *Schemas* como fundamentos para la integración y la interoperabilidad electrónica del gobierno. En este sentido, la constitución de repositorio que permita a gestores y proyectistas de aplicaciones de Gobierno Electrónico consultar XML *Schemas* consolidados, bien como proponer la catalogación de esquemas bajo su responsabilidad, es una indiscutible contribución para la consolidación de buenas prácticas de interoperabilidad en el ámbito gubernamental.

#### 10.2.2. Objetivo

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

#### 10.2.3. Ámbito

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

La publicación de XML *Schemas* no garantiza, automáticamente, acceso a los contenidos correspondientes o servicios asociados, para lo que se pueden definir reglas específicas por el gestor respectivo.

### 10.2.4. Propiedad y Responsabilidad

La Coordinación de e-PING es responsable por este Catálogo, en especial por la gestión de los procesos de cambio y por estimular a que los estándares se utilicen en desenvolvimientos futuros.

En este sentido, se recomienda que el desarrollo o mantenimiento de sistemas que dan soporte a la oferta de servicios de Gobierno Electrónico correlacionados a áreas principales/áreas dependientes de actuación de gobierno contempladas en el Catálogo consideren los XML *Schemas* publicados.

El desarrollo y mantenimiento 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 se pueden dar por intermedio de los siguientes caminos:

- a) Proposición seguida de aceptación de propuesta de contenido para el Catálogo de Padrones de Datos (CPD);
- b) Sumisión seguida de aceptación de propuesta de contenido a la Arquitectura Referencial de Interoperación 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 forma electrónica disponible a partir del sitio de e-PING.

En las situaciones descritas en los tópicos (b) y (c) los contenidos se encaminarán para el 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 XML *Schemas* será sometida a análisis de los integrantes del Grupo

Áreas de Integración para Gobierno Electrónico por medio de forma electrónica específica, disponible en el sitio de e-PING ([www.e-ping.e.gov.br](http://www.e-ping.e.gov.br)). Se mantendrán en el Catálogo solamente las proposiciones aceptadas, siendo que las que aún se encuentren en estudio, las rechazadas y las versiones anteriores de XML *Schemas* aceptadas, serán mantenidas en ambiente “de trabajo” que oportunamente será concebido e implementado.

Los criterios de evaluación empleados incluirán:

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

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

Solicitudes de cambio para XML *Schemas* ya publicadas serán evaluadas preliminarmente por los integrantes del Grupo Áreas de Integración para Gobierno Electrónico. La decisión de aceptación es de competencia de la Coordinación Central de e-PING, que podrá adoptar las mudanzas propuestas según su alcance e impacto o someterlas a consulta pública, a través del sitio <http://www.governoeletronico.gov.br>.

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

Los contenidos consolidados en la carga inicial y las actualizaciones pueden ser consultadas en la página de e-PING ([www.e-ping.e.gov.br](http://www.e-ping.e.gov.br)).

### 10.2.6. Plantilla de XML Schemas

Cada XML *Schema*, o agrupamiento de XML *Schemas* correlacionados, debe ser documentado de acuerdo con la siguiente plantilla:

**ORGANISMO PROPONENTE:** Nombre del Organismo 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 ASIGNACIÓN:** Unidad de asignación del responsable por la propuesta de catastro. Señalar la secuencia de unidades hasta el Organismo 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 el profesional responsable por la proposición del XML *Schema*;

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

**INDICADOR DE GESTIÓN:** Indicación de la situación del proponente en relación a la gestión del área principal/área dependiente a que se refiere el XML *Schema*. Debe ser relleno mediante señal en una de las opciones (Sí o No);

**ORGANISMO GESTOR:** Aquél organismo con atribuciones para la gestión del área principal/área dependiente a cual se refiere el XML *Schema*. Debe ser relleno solamente cuando la señal de gestión sea “No” y el organismo gestor 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 en detalle sobre el (conjunto de) XML *Schema*;

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

**ÁREA DEPENDIENTE:** Denominación usual dentro del área de actuación de gobierno a que el conjunto de XML *Schema* se refiere, debe ser informada solamente cuando el área no sea suficiente para cualificar 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 la que serán relacionados XML *Schemas* organizados según clasificación de 1<sup>er</sup> nivel dada por la Lista de Áreas de Actuación de Gobierno, que tiene como referencia el Plan Plurianual (PPA), y se presentada a continuación:

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. Vivienda;
8. Ciencia y Tecnología;
9. Comercio y Servicios;
10. Relaciones Exteriores;
11. Defensa Nacional;
12. Encargos Especiales;

- 13. Cultura;
- 14. Gestión Ambiental;
- 15. Previdencia 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. Industria;
- 28. Saneamiento;
- 29. Urbanismo.

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

### 10.3. Áreas de Integración para Gobierno Electrónico: Especificaciones Técnicas

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

**Tabla 13 – Especificaciones para Áreas de Integración para Gobierno Electrónico – Temas Transversales a Áreas de Actuación de Gobierno**

| Temas  | Especificación   | SIT | Observaciones  |
|--|--|-----|--|
|  | A – Adoptado<br>R – Recomendado<br>T – En Transición<br>E – En Estudio<br>F – Estudio Futuro   |     |  |
| PROCESOS – Lenguaje para Ejecución de procesos             | BPEL4WS V1.1, según definido por el OASIS<br><a href="http://www.oasisopen.org/committees/download.php/2046/BPEL%20V1-1%20May%205%202003%20Final.pdf">http://www.oasisopen.org/committees/download.php/2046/BPEL%20V1-1%20May%205%202003%20Final.pdf</a> | R   | El grupo acompañará la evolución del BPEL4WS versión 2.0. Estudios referentes a la Orquestación de procesos y coreografía serán futuramente conducidos por el grupo. |
| PROCESOS – Notación de Moldeo de Procesos                  | BPMN 1.0, según definido por el OMG<br><a href="http://www.bpmn.org/Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf">http://www.bpmn.org/Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf</a>                       | R   |  |
| INFORMACIONES REFERENCIADAS GEOGRÁFICAMENTE                | WMS versión 1.0 o posterior<br><a href="http://www.opengeospatial.org/standards">http://www.opengeospatial.org/standards</a>   | A   |  |
|  | WFS versión 1.0 o posterior<br><a href="http://www.opengeospatial.org/standards">http://www.opengeospatial.org/standards</a>   | A   |  |
| Interoperabilidad entre sistemas de información geográfica | WCS versión 1.0 o posterior<br><a href="http://www.opengeospatial.org/standards">http://www.opengeospatial.org/standards</a>   | A   |  |
|  | CAT  | E   |  |

| Temas | Especificación | SIT | Observaciones |
|-------|----------------|-----|---------------|
|       | WFS-T          | E   |               |

**Tabla 14 – Especificaciones para Áreas de Integración para Gobierno Electrónico – Catálogo de XML Schemas referentes a Áreas de Actuación de Gobierno**

| Área Principal/Área Dependiente                        | Especificación   | Observaciones  |
|--|--|--|
| ADMINISTRACIÓN – Compras Gubernamentales               | <a href="https://www.comprasnet.gov.br/xml/aviso.xsd">https://www.comprasnet.gov.br/xml/aviso.xsd</a><br><a href="https://www.comprasnet.gov.br/xml/consultamatserv.xsd">https://www.comprasnet.gov.br/xml/consultamatserv.xsd</a><br><a href="https://www.comprasnet.gov.br/xml/dispinex.xsd">https://www.comprasnet.gov.br/xml/dispinex.xsd</a><br><a href="https://www.comprasnet.gov.br/xml/contratoent.xsd">https://www.comprasnet.gov.br/xml/contratoent.xsd</a><br><a href="https://www.comprasnet.gov.br/xml/empenho.xsd">https://www.comprasnet.gov.br/xml/empenho.xsd</a><br><a href="https://www.comprasnet.gov.br/xml/resultado.xsd">https://www.comprasnet.gov.br/xml/resultado.xsd</a> | XML Schemas por el sistema ComprasNet referentes a Clausura de Resultado de Licitación, Empeño, Dispensa / Inexigibilidad de Licitación, Consulta de Material vía CATMAT, Contrato de entidades no SISG y Aviso de Licitación.   |
| ADMINISTRACIÓN – Estructuras de Gobierno               | <a href="http://guialivre.governoeletronico.gov.br/igov/">http://guialivre.governoeletronico.gov.br/igov/</a>  | Conjunto de XML Schemas relacionados a los sistemas de gestión administrativa de la Administración Pública Federal.  |
| ADMINISTRACIÓN – Gestión de Redes Locales/CACIC        | <a href="http://guialivre.governoeletronico.gov.br/cacic/sisp2/invent/Invent.html">http://guialivre.governoeletronico.gov.br/cacic/sisp2/invent/Invent.html</a>  | Estos Schemas hacen parte de la solución CACIC, que fue Desarrollada por Dataprev, y son utilizados para transmisión de datos de inventario de hardware y de sus componentes conectados en ambiente de red.<br>La implementación de estos Schemas se dio en Conjunto con el Ministerio del Medio Ambiente (MMA).                           |
| ADMINISTRACIÓN TRIBUTARIA – Factura Fiscal Electrónica | <a href="http://200.198.224.29/portal/info/Schemas.htm">http://200.198.224.29/portal/info/Schemas.htm</a>  | Schema XML utilizado para emisión de la factura fiscal electrónica, en sustitución a la de papel y con valor jurídico para todos los fines. Este proyecto es coordinado por el Encuentro Nacional de los Administradores y Coordinadores Tributarios Estaduales (ENCAT) y desarrollado en conjunto con la Secretaría de la Receta Federal. |
| DERECHOS DE LA CIUDADANÍA – Notarios                   | <a href="http://www.mj.gov.br/Schemas/Cartorio/ConsultaCartorio.xsd">http://www.mj.gov.br/Schemas/Cartorio/ConsultaCartorio.xsd</a>  | Es responsabilidad del Ministerio de la Justicia mantener el Catastro Nacional de Juntas Notariales.<br>Este esquema, a partir de un filtro generado por la unidad de la federación y/o por el municipio y/o barrio y/   |

| Área Principal/Área Dependiente                    | Especificación  | Observaciones   |
|--|---|---|
|  |   | o la atribución de la junta notarial, consulta el catastro de juntas notariales de Brasil devolviendo una lista de las juntas notariales que atienden al filtro. El esquema permite, aún, entregar el detalle de cada junta notarial listada  |
| DERECHOS DE LA CIUDADANÍA – Defensa del Consumidor | <a href="http://www.mj.gov.br/Schemas/DireitoConsumidor/SINDEC.xsd">http://www.mj.gov.br/Schemas/DireitoConsumidor/SINDEC.xsd</a> | Este esquema permite la consulta a la estadística consolidada sobre la atención en los Procons que tienen convenio con el Sistema Nacional de Informaciones de Defensa del Consumidor (SINDEC) por unidad de la federación o nombre del que facilita el CNPJ, regresando las estadísticas de atención adherentes a los criterios investigados.  |
| DIRECHOS DE LA CIUDADANÍA – Defensa del Consumidor | <a href="http://www.mj.gov.br/Schemas/Recall/ConsultaRecall.xsd">http://www.mj.gov.br/Schemas/Recall/ConsultaRecall.xsd</a>       | Es responsabilidad del Ministerio de la Justicia formular, estimular, supervisar y coordinar la política de protección del orden económico, en los temas de concurrencia y defensa del consumidor. El trámite por el que el que ofrece un producto informa al público sobre los defectos detectados en los productos o servicios que había puesto en el mercado é llamado de <i>recall</i> . Os objetivos esenciales de ese tipo de procedimiento son el de proteger y preservar la vida, la salud, la integridad y la seguridad del consumidor, bien como de evitar o aminorar toda especie de perjuicios, sean de orden material, sean de orden moral.<br>Este esquema permite consultar la base de banco de datos de <i>recall</i> del Departamento de Protección y Defensa del Consumidor para verificar si un determinado producto está siendo objeto de <i>recall</i> . Para eso, el esquema al ser accionado regresa a la lista de suministradores/modelos |

| Área Principal/Área Dependiente             | Especificación  | Observaciones   |
|---|---|---|
|   |   | que han hecho <i>recall</i> , posibilitando verificar detalles del <i>recall</i> a partir de la opción por el producto o el número de serie, chasis, partida entre otros.   |
| DERECHOS DE LA CIUDADANÍA                   | <a href="http://www.mj.gov.br/Schemas/ClassificacaoIndicativa/ConsultaClassindFilmes.xsd">http://www.mj.gov.br/Schemas/ClassificacaoIndicativa/ConsultaClassindFilmes.xsd</a>   | Es de responsabilidad del Ministerio de la Justicia ejercer la clasificación, para efecto indicativo, de entretenimiento público y de programas de radio y televisión. A partir del nombre de la película o programa, este esquema consulta el banco de datos de Clasificación Indicativa y devuelve una lista de coincidentes para los cuales se pueden exhibir detalles de la clasificación indicativa y la justificación.  |
| GESTIÓN AMBIENTAL – Licencia Ambiental/PNLA | <a href="http://integradorpnla.mma.gov.br/integrador/schemas/licenciamiento_ambiental_completo.xsd">http://integradorpnla.mma.gov.br/integrador/schemas/licenciamiento_ambiental_completo.xsd</a><br><a href="http://integradorpnla.mma.gov.br/integrador/schemas/licenciamiento_ambiental_simples.xsd">http://integradorpnla.mma.gov.br/integrador/schemas/licenciamiento_ambiental_simples.xsd</a><br><a href="http://integradorpnla.mma.gov.br/integrador/schemas/licenciamiento_ambiental_totalizadores.xsd">http://integradorpnla.mma.gov.br/integrador/schemas/licenciamiento_ambiental_totalizadores.xsd</a> | <p>Los <i>Schemas</i> se emplean en el ámbito de la licencia ambiental y son adoptados por la plataforma del Portal Nacional de Licencias Ambientales (PNLA) del MMA que consolida las informaciones sobre licencias ambientales de varios estados por medio de <i>Web Services</i>. A continuación hay una descripción del propósito de cada esquema:</p> <ul style="list-style-type: none"> <li>•licenciamiento_ambiental_completo.xsd – ofrece el esquema de las informaciones pertinentes a una licencia ambiental, llevando en cuenta los datos frecuentes en los distintos organismos licenciadores investigados;</li> <li>•licenciamiento_ambiental_simples.xsd – ofrece el esquema para la composición de un reporte que contiene un conjunto de licencias con los datos mínimos de su</li> </ul> |

## Documento de Referencia de e-PING – Versión 3.0

| Área Principal/Área Dependiente                                   | Especificación   | Observaciones  |
|---|--|--|
|   |  | <p>identificación. Es útil para la navegación preliminar sobre las licencias para un posterior puesta en detalle que se hace por medio del primer esquema;</p> <ul style="list-style-type: none"> <li>•licenciamiento_ambiental_t otalizadores.xsd – consolida el cuantitativo de licencias basado en un tema arbitrario.</li> </ul> |
| PODER JUDICIAL<br>–<br>Servicios<br>Notariales<br>Extrajudiciales | <a href="http://www.anoregsp.org.br/arquivos">www.anoregsp.org.br/arquivos</a> | Los XML Schemas se refieren a la estandarización de las consultas a los servicios de notarios extrajudiciales  |

### 11. Glosario de siglas y Términos Técnicos<sup>34</sup>

En este tópico se presentan los significados de los principales términos técnicos utilizados en 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, resúmenes, reseñas, reseñas, reseñas y otros.

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

**APF – Administración Pública Federal:** Reúne Instituciones de la administración pública directa (servicios integrados en la estructura administrativa, Presidencia de la República y de los Ministerios) e indirecta (Autarquías, Empresas Públicas, Sociedad de Economía Mezclada y Fundaciones Públicas) del Poder Ejecutivo. [https://www.planalto.gov.br/ccivil\\_03/decreto-lei/del0200.htm](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, sirviéndose de padrones de representación de notación, ejecución y coordinación en XML, cuyo rigor semántico posibilita su interoperabilidad entre sistemas de plataformas distintas, siendo, de este modo, un fundamento para la implementación de soluciones basadas en arquitectura orientada hacia los servicios. Cuando la coordinación de la ejecución de los servicios se realiza con subordinación a un proceso maestro, en general, dentro de la organización, se denomina a esa coordinación como organización de la orquesta. Cuando, la coordinación se da sin la subordinación a un proceso maestro, por lo general, entre organizaciones, 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 la computadora del usuario, acompañar los enlaces 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 una señal, transformándolo en un texto ilegible, por intermedio de la utilización de algoritmos matemáticos complejos.

**CAT – Catalog Service Implementation Specification:** Especificación OpenGIS que define interfaces para publicar, acceder, navegar y consultar metadatos sobre informaciones georeferenciadas. El término más empleado actualmente para *Catalog Service* es CSW.

**CSW – Catalog Service Implementation Specification.** Especificación OpenGIS que define interfaces para publicar, acceder, navegar y consultar metadatos sobre informaciones georeferenciadas.

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

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

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

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

<sup>34</sup> Microsoft Press. Dicionário de Informática. Tradutor e Consultor Editorial Fernando Barcellos Ximenes - KPMG Peat Marwick. Editora Campus LTDA, 1993. ISBN 85-7001-748-0.

Thing, Lowell (ed.) Dicionário de Tecnologia. Tradução de Bazán Tecnologia e Linguística e Texto Digital. São Paulo: Futura, 2003. ISBN 85-7413-138-5.

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

**Handshake:** en una comunicación por teléfono, intercambio de informaciones entre dos demoduladores 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. Se utiliza para indexar y recuperar tópicos en un banco de datos, porque es más rápido encontrar el tópico utilizando la menor llave transformada que el valor original. También se utiliza en algoritmos de criptografía.

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

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

**HTTPS – Secure Hiper Text Transfer Protocol** (Protocolo de Transferencia de Hipertexto Seguro): Protocolo Web desarrollado por Netscape y acoplado al navegador. Criptografía y criptoanálisis pedidos y retornos de páginas retornadas por el servidor web. El HTTPS es solamente la utilización del SSL (Secure Sockets Layer) del Netscape, como una camada inferior bajo la organización normal de los problemas de las aplicaciones http.

**ICP – Brasil:** Conjunto de técnicas, prácticas y procedimientos, que se deben implementar 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 padrones y normas que, a menudo, se tornan nacionales e internacionales.

**IETF – Internet Engineering Task Force** (Forza tarea de Ingeniería de Internet): Entidad que define protocolos operaciones estándar de internet, como el TCP/IP.

**IMAP – Internet Mensaje Access Protocol** (Protocolo de Acceso a Mensajes en Internet): Protocolo estándar para el acceso de e-mail partiendo 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 por medio del cual los datos son enviados de una computadora en Internet. Cada computadora en Internet, posee, al menos, una dirección IP que lo identifica únicamente respecto a todas las demás computadoras en Internet.

**IPSec – Internet Protocol Security** (Seguridad de Protocolo de Internet): Estándar de desarrollo relativo a la seguridad en el nivel de la red o del procesamiento de paquetes de la comunicación en red. Una gran ventaja del IPSec es que las disposiciones de seguridad pueden utilizarse sin exigir cambio en las computadoras de usuarios individuales. El IPSec posibilita dos opciones de servicios de seguridad: *Authentication Header* (AH), que, en esencia, posibilita la autenticación del remitente de datos, y *Encapsulating Security Payload* (ESP), que soporta tanto la autenticación del remitente como 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 computadoras. Formalmente, IPv6 es un conjunto de especificaciones de la IETF. El IPv6 fue proyectado como un conjunto evolutivo de perfeccionamientos realizados en el IPv4. El perfeccionamiento más significativo del IPv6 respecto al IPv4 es que las direcciones de IP se aumentan de 32 bits para 128 bits.

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

**LDAP – Lightweight Directory Access Protocol** (Protocolo de Acceso a Directorio Liviano):

## Documento de Referencia de e-PING – Versión 3.0

Protocolo de Software para permitir la localización de organizaciones, de personas y de otros recursos como archivos y dispositivos en una red, sea en una Internet pública o en una intranet corporativa.

**Forma de Acceso:** Conjunto de componentes físicos (dispositivos de acceso) y de no físicos (software básico, aplicativos, etc.) que posibilita al usuario el acceso a un servicio de gobierno electrónico.

**Mensajería en Tiempo Real o Mensaje Instantáneo:** es un tipo de comunicación que permite que un usuario intercambie mensajes en tiempo real con otro usuario, también conectado a la red.

**Metadatos:** son informaciones adicionales y necesarias para que los datos se tornen útiles. Es información esencial para que se haga utilización de los datos. En resumen, metadatos son el conjunto de características sobre los datos, que no están incluidas normalmente, en los datos, propiamente dichos. <http://www.isa.utl.pt/dm/cig/cig20002001/TEMAMetadados/trabalho.htm>.

**Middleware:** es un término general que sirve para mediar dos programas separados y, normalmente, ya existentes. Aplicaciones distintas se pueden comunicar por intermedio del servicio de *messaging* facilitado por programas *middleware*.

**Newsgroup** (Grupo de Noticias): discusión sobre un determinado asunto que consiste en mensajes enviados a un sitio central en 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** (Consortio Internacional *Open Geospatial*): posee la misión de desarrollar especificaciones para interfaces espaciales que serán puestas a disposición, de manera libre para utilización general.

**OWS – OGC Web Services:** Se refiere a todas las especificaciones *OpenGIS* que emplean geoprocetamiento por intermedio de la Web.

**Estándar Abierto:** Cualquier estándar tecnológico establecido por Organismos Internacionales o por consorcios de empresas del mercado que desarrollan especificaciones que se encuentran públicamente disponibles. El PC (computadora personal) fue lanzado y se desarrolla con estándar abierto. Las especificaciones de Internet y su desarrollo también. Gran parte de los lenguajes de programación también.

**Estándar de Metadatos:** El conjunto de metadatos es un estándar, definido por una comunidad de usuarios, que acapara un Vocabulario de elementos descriptivos y un Esquema o reglas de codificación de estos elementos en el medio legible, en computadora. <http://www.uff.br/gdo/htm/tsld013.htm>.

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

**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 que el e-mail es recibido y almacenado por el servidor de Internet.

**Portal:** Sitio en Internet que congrega servicios, noticias y gran volumen de contenido de información y/o de entretenimiento.

**Red Gobierno:** es el portal de entrada para todas las páginas del gobierno federal en Internet. [http://www.federativo.bndes.gov.br/destaques/egov/egov\\_redegoverno.htm](http://www.federativo.bndes.gov.br/destaques/egov/egov_redegoverno.htm).

**Resolución número 7, del Gobierno Electrónico:** establece reglas y directrices para los sitios en Internet de la Administración Pública Federal (gov.br y mil.br). Dividida en siete capítulos, la resolución trata de la estructura de la información, del control y monitoreo, de la gestión de los elementos interactivos, del modelo organizacional, de la identidad visual y de la seguridad de los sitios gubernamentales en la red mundial de computadoras. <http://www.governoeletronico.e.gov.br>.

**RFC - Request For Comments** (Solicitud de Comentarios): documento formal de la IETF, resultante de modelos y revisiones de partes interesadas. La versión final del RFC se transformó en un estándar en que ni comentarios ni cambios se permiten. Las mudanzas pueden darse, no obstante, por intermedio de RFCs subsecuentes, que sustituyen o elaboran en todas las partes de

## Documento de Referencia de e-PING – Versión 3.0

los RFCs precedentes. RFC también es la abreviación de Remote Function Call (llamada funcional remota).

**RSA – Rivest-Shamir-Adleman:** cifración 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 oferta de servicios del gobierno para ciudadanos, suministradores y servidores. En aspectos 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 monitoreo de la ejecución presupuestaria.
4. Enseñanza a distancia, alfabetización digital y mantenimiento de bibliotecas virtuales.
5. Difusión cultural con énfasis en las identidades locales, fomento y preservación de culturas locales.
6. e-procurement, o sea, adquisición de bienes y servicios por intermedio de Internet, como licitaciones públicas electrónicas, subastas electrónicas, espacios de compras públicas virtuales y otros tipos de mercados digitales para los bienes adquiridos por el gobierno.
7. Estímulo a los e-negocios, por medio de la creación de ambientes para trámites seguros, especialmente para pequeñas y medianas empresas.

<http://www.governoeletronico.gov.br/r1>.

**Sistemas de Informação do Governo Federal:** sistemas que dan soporte a actividades de:

- Gestión de gobierno: Planeamiento, Presupuesto, Ejecución Presupuestaria, Administración Financiera, Administración de Recursos Humanos, Organización 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 distintos organismos 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](http://www.redegoverno.gov.br/projetos/reg_gestao.asp).

**SFS – Simple Features Specification for SQL:** especificación *OpenGIS* que define la padronización del esquema SQL que comporta almacenamiento, recuperación, consulta y actualización sobre informaciones referenciadas geográficamente.

**Smart Cards:** tarjeta de plástico, con el tamaño aproximado de una tarjeta de crédito, con un microchip inserido que puede ser cargado con datos y puede utilizarse para realizar llamadas por teléfono, pagos electrónicos al contado y otras aplicaciones. Es actualizado periódicamente para recibir otros servicios.

**S/MIME – Secure Multi-Purpose Internet Mail Extensions** (Extensiones de Correo de Internet Multipropósito Seguras): método seguro para envío de e-mail que utiliza el sistema de cifras RSA (Rivest-Shamir-Adleman). S/MIME describe como informaciones encriptadas y un certificado digital se puede incluir como parte del cuerpo del mensaje.

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

**SOA – Service Oriented Architecture** (Arquitectura Orientada hacia Servicios): Arquitectura propuesta para interoperabilidad de sistemas por intermedio de conjunto de interfaces de servicios débilmente acoplados (*loosely coupled*), donde los servicios no necesitan de detalles técnicos de la plataforma de los demás servicios para que el cambio de informaciones se realice.

**SOAP – Simple Object Access Protocol** (Protocolo Simple para Acceso a Objetos): describe un modelo para el empaquetamiento de preguntas y respuestas XML. El envío de mensajes SOAP se utiliza para permitir el intercambio de una variedad de informaciones XML. La norma de SOAP

asume la tarea de transmitir pedidos y respuestas sobre servicios entre usuarios y proveedores de servicios.

**Software Libre:** programa de ordenador disponible a través de su código fuente y con la posibilidad de uso, de copia y de distribución para cualquiera, sea en su forma original o con mudanzas, sea gratuitamente o con coste. El software libre es necesariamente no propietario, pero es importante no confundir software libre con software gratis.

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

**SSL – Secure Sockets Layer (Capa de Conexión Segura):** es un protocolo muy utilizado para gerencia de la seguridad de una transmisión de mensaje en 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 la descubierta de información a través de la navegación.

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

**Telnet:** la manera de acceder al ordenador de otra persona, asumiendo que la permisión haya sido dada. En términos técnicos, Telnet es un comando de usuario y un protocolo subliminal TCP/IP para tener acceso a ordenadores remotos.

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

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

**UDDI – Universal Description Discovery and Integration (Descripción, Descubierta e Integración Universales):** es el repositorio en el cual los desarrolladores registran los *Web Services* disponibles que posibilitan a los clientes la descubierta y la utilización de los servicios alojados en Extranets e Intranets.

**UDP – User Datagram Protocol (Protocolo de Datagrama de Usuarios):** protocolo de comunicación que ofrece una cantidad limitada de servicio cuando los mensajes se intercambian entre ordenadores en una red que utiliza el IP. El UDP es una alternativa para el TCP y, con el IP, es referido como UDP/IP. De la misma forma que con el TCP, el UDP utiliza el IP para llevar una unidad de datos de un ordenador para otro. A diferencia del TCP, el UDP no suministra el servicio de dividir un mensaje en paquetes y remontarla en la otra extremidad. El UDP no suministra la secuencia dos paquetes en que llegan los datos. Eso significa que el programa de aplicativo que usa el UDP debe garantizar que el mensaje completo ha llegado y que está en orden. Los aplicativos de red que quieren ahorrar el tiempo de procesamiento porque tienen unidades de datos muy pequeñas para cambiar, pueden preferir el UDP en vez del TCP.

**UML – Unified Modeling Language (Lenguaje de Moldeo Unificado):** El UML es mucho más que la estandarización de una notación, es decir, ella es un lenguaje estándar para la elaboración de la estructura de proyectos de *software*, incluyendo aspectos conceptuales tales como procesos de negocios y funciones del sistema, además de tópicos específicos como las clases escritas en determinado lenguaje de programación, esquemas de banco de datos y componentes de *softwares que se pueden* reutilizar. El UML se puede emplear para la visualización, la especificación, la construcción y la documentación de artefactos de sistemas de *software*, puede, también, utilizarse en el moldeo de negocios y otros tipos de sistemas y no solamente de *software*.

**URI - Uniform Resource Identifier (Identificador Único de Recurso):** estándar de codificación de nombres y direcciones en Internet. Una URI está compuesta por un nombre (ex.: file, http, ftp, news, mailto, gopher), seguido por dos puntos, y por fin, un camino, estandarizado por un rol de esquemas que sigue la RFC 1630. El URI congrega los conceptos URNs y URLs.

**Usenet:** colección de comentarios y mensajes sometidos por usuarios sobre varios temas, que son enviados a los servidores en una red mundial. Cada colección de comentarios enviados se conoce como un newsgroup.

**VPN – Virtual Private Networks** (Red Privada Virtual): Red particular, que se sirve 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 da por intermedio de túneles virtuales, por los que 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 trata fomentar padrones 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 ordenadores que abarca extensas áreas geográficas como un estado, un país o un continente.

**WCS – Web Coverage Service Implementation Specification:** especificación *OpenGIS* que define interfaces para acceder y desarrollar operaciones (*GetCapabilities*, *DescribeCoverage* e *GetCoverage*) sobre informaciones referenciadas geográficamente en el formato Coverage.

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

**WFS – Web Feature Service Implementation Specification:** especificación *OpenGIS* que define interfaces para acceder y desarrollar operaciones (*GetCapabilities*, *DescribeFeatureType*, *GetFeature*, *Transaction* y *LockFeature*) sobre informaciones referenciadas geográficamente, por medio del protocolo HTTP. Basado en esas operaciones, dos clases de servicios pueden definirse:

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

**WMS – Web Map Service Implementation Specification:** especificación *OpenGIS* que define interfaces para acceder y desarrollar operaciones (*GetCapabilities*, *GetMap*, *GetFeatureInfo*) sobre múltiples camadas (*layers*) de informaciones referenciadas geográficamente, 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. Él describe las funcionalidades de los servicios ofrecidos por el proveedor de servicios, bien como su ubicación y forma de acceso.

**XML – eXtensible Markup Language** (Lenguaje Markup Extensible): manera flexible para crear formatos de informaciones comunes y compartir ambos formatos y los datos en la *World Wide Web*, en las intranets y en cualquier sitio. El XML es extensible porque, a diferencia 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., es decir, la sintaxis del documento. Los Esquemas de un conjunto de documentos XML, de tipo semejante, 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 enviado por medio de la *Web*, usando el XML, y es presentado al usuario. El XSL es un lenguaje para formatear un documento XML.

**XSLT – eXtensible Stylesheet Language Transformations:** forma estándar de descripción sobre 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

## Documento de Referencia de e-PING – Versión 3.0



debe ser reorganizado en otra estructura de datos (que se puede presentar siguiendo una planilla del XSL).

## 12. Integrantes

### Coordinación de e-PING

Asociación Brasileña de Empresas Estaduales de Procesamiento de Datos (ABEP)

Dayse Vianna  
Paulo Cezar Coelho

Banco do Brasil (BB)

Ulisses de Sousa Penna

Caixa Econômica Federal (CAIXA)

Ângela B. Baylo

Empresa de Tecnología e Informaciones de la Previdencia Social (DATAPREV)

Humberto Degrazia Campedelli  
José Antônio Borba Soares  
Rodrigo Novais Coutinho

Ministerio de la Justicia (MJ)

Jorilson da Silva Rodrigues

Ministerio de la Salud (MS)

Eliane Pereira dos Santos  
Ermani Bento Bandarra  
Márcia Helena Gonçalves Rollemberg

Ministerio de las Relaciones Exteriores (MRE)

Celso Ricardo Hottum Meira

Ministerio del Planeamiento, Presupuesto y Gestión – Secretaría de Logística y Tecnología de la Información (MP/SLTI)

Leandro Corte (Coordinador Geral)  
Ednylton Maria Franzosi  
Eduardo Favero  
José Ney de Oliveira Lima  
Leonardo Boselli da Motta  
Leonardo Lanna Guillén  
Nazaré Lopes Bretas  
Rogério Santanna dos Santos  
Sylmara Campos Pinho Garcia

Presidencia de la República (PR)

Marcelo André de Barros Oliveira

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

Mauricio Augusto Coelho  
Renato da Silveira Martini  
Viviane Regina Lemos Bertol

Serviço Federal de Procesamiento de Datos (SERPRO)

Antônio Sérgio Borba Cangiano  
Elói Juniti Yamaoka  
Geancarlo Noronha Vinhal  
Paulo Cezar Czarnewski  
Wagner Junqueira Araújo

### Grupo de Trabajo Interconexión

## Documento de Referencia de e-PING – Versión 3.0

Leonardo Lanna Guillén (MP/SLTI) - Coordinador  
Adriano Soriano (CAIXA)  
Areno Pires Filho (MC)  
Carlos Bellone Neto (RFB)  
Daniel Moreira Guilhon (CGU)  
Filipe Guimarães (MRE)  
Frederico Duarte Guerra de Macedo (ME)  
José Rodrigues Gonçalves Júnior (ITI)  
Júlio César Japiassu Lyra (MJ)  
Leonardo Boselli da Motta (MP/SLTI)  
Luciene Pinheiro Capra (ANS)  
Odilon de Freitas Militão Neto (CAIXA)  
Paulo Guilherme Lanzillotti Jannuzzi (DATAPREV)  
Ruben César Macedo (CELEPAR-PR)  
Sérgio de Oliveira Barcellos (MCT)  
Sílvia Aparecida da Cunha (MP/CGTI)  
Ulisses de Sousa Penna (BB)

### **Subgrupo: Web Services**

Ednylton Maria Franzosi (MP/SLTI) – Coordinador  
Bruno Pacheco (SERPRO)  
Carlos Falcão Maranhão (MS/ANS)  
Cláudio Muniz Machado (MS)  
Elaine Fabiano Tocantins (MJ)  
Louise Neves (SERPRO)  
Mauricio Dayrell (MMA)  
Paulo Azevedo (BB)

### **Colaboradores**

Claudia do Socorro Ferreira Mesquita (MP/SLTI)  
Patrycia Barros de Lima Klaydianos (MP/SLTI)

### **Grupo de Trabajo Seguridad**

Jorilson da Silva Rodrigues (MJ) – Coordinador  
Alessandra Silva Moura (ANS)  
Dante de Matos Gomes (PRODEB)  
Edgar Luciano Morais Martins (MP/SLTI)  
Érica Dantas (STJ)  
Filipe Carneiro Guimarães (MRE)  
Gleyner Martins Novais (SERPRO)  
Humberto Degrazia Campedelli (DATAPREV)  
Igor Guimarães (MC)  
José D'Aleluia Nascimento (MinC)  
José Maria Leocádio (SERPRO)  
Júlio César de Magalhães (FNDE)  
Luiz Augusto Barbosa Mozzer (CGU)  
Maise Netto Ludemer (MC)  
Marcelo Henrique Rios dos Reis (MT)  
Marco Antônio Reis Henriques (RFB)  
Marcos José Cândido Euzébio (BACEN)  
Ricardo Luiz Chiacchio (MCidades)  
Roberto dos Santos Rodrigues (MCT)  
Rodrigo Costa dos Santos (ELETROBRÁS)  
Sérgio Carreira dos Santos (IPHAN)

### **Grupo de Trabajo Formas de Acceso**

Mauricio Augusto Coelho (ITI) – Coordinador  
Renato da Silveira Martini (ITI) – Coordinador  
Carlos Bellone Neto (RFB)

## Documento de Referencia de e-PING – Versión 3.0

Cleisson Rodrigues (MTur)  
Eduardo Viola (MCT)  
Eliane Aristóteles Moreira (DATAPREV)  
Eliane Pereira dos Santos (MS)  
Ellio Alves de O. Soares (CEF)  
Geancarlo Noronha Vinha (SERPRO)  
Hilton P. Mendes Sobrinho (MS)  
Jean Carlo Rodrigues (ITI)  
Paloma Nascimento (MT)  
Paulo Édison de Souza (MEC)  
Rosane dos Santos Lourenço (MT)  
Rubem César Macedo (CELEPAR-PR)  
Thimoteo Borges (CGU)  
Viviane Regina Lemos Bertol (ITI)

### Grupo de Trabajo Organización e Intercambio de Informaciones

Eloi Juniti Yamaoka (SERPRO) – Coordinador  
Aline Ramalho Bezerra (MJ)  
Ana Lúcia de Medeiros (CORREIOS)  
Ângela B. Baylo (CAIXA)  
Aurélia Dolores Gonçalves Bruner (ELETROBRAS)  
Beatriz Barreto Brasileiro Lanza (CELEPAR)  
Brenda Couto de Brito Rocco (AN-CC)  
Cláudia Carvalho Masset Lacombe Rocha (AN-CC)  
Dalva Clementina Luca (MJ)  
Dayse Vianna (PRODERJ)  
Dilma de Fátima Avellar Cabral da Costa (AN-CC)  
Eliane Pereira dos Santos (MS)  
Elizabeth da Silva Maçulo (AN-CC)  
Fernanda Hoffmann Lobato (MP/SLTI)  
Geny Conte Pessoa (SERPRO)  
Hilda Pimentel (ANCINE)  
João Alberto Lima (Senado Federal)  
Lígia Leindorf Bartz Kraemer (UFPR)  
Luciana Ferreira Pinto da Silva (INEP)  
Luciano Seite Nishikawa (CAIXA)  
Marcia Helena Gonçalves Rollemberg (MS)  
Márcia Izabel Fugizawa Souza (EMBRAPA)  
Márcia Luzia Albertini (MS)  
Márcio Imamura (IBGE)  
Marcos Augusto Francisco Borges (CPqD)  
Margareth da Silva (AN-CC)  
Maria de Fátima Porcaro (IPT)  
Maria do Socorro Rodrigo de Medeiros (INEP)  
Maria Valéria Lins Tenório (ATI-PE)  
Neuza Arantes Silva (MAPA)  
Paulo César Pereira Soares (FUNARTE)  
Paulo Cezar Czarnewski (SERPRO)  
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)  
Virgílio Dantas Lins Filho (ME)  
Vivianne Muniz Veras Barrozo (SERPRO)  
Wilson Yociteru Yamaji (AGU)

## Documento de Referencia de e-PING – Versión 3.0

### Grupo de Trabajo Áreas de Integración para Gobierno Electrónico

Nazaré Lopes Bretas (MP/SLTI) – COORDINADORA  
Adelino Fernando Correia (DATASUS/MS)  
Adriano de Medeiros (INCRA)  
Ana Lúcia Viçoso da Cruz Almeida (DATAPREV)  
Antônio Albuquerque (PR)  
Carlos Bellone Neto (RFB)  
Ceres Albuquerque (ANS)  
Cláudio Manoel Cordeiro (SERPRO)  
Frederico Duarte Guerra de Macedo (ESPORTES)  
Maurício M. Martinez (MEC)  
Mônica Lucatelli (DATAPREV)  
Paulo Henrique Santana (MMA)  
Pedro Paulo Cirineo (BB)  
Ricardo de Lima (INCRA)  
Rogério Werneck (DIRTI/PR)  
Sylmara Campos Pinho Garcia (MP/SLTI)  
Wagner Gardusi Guarizo (PR)

#### Colaboradores

Igor de Freitas (MDS)  
Felix de Sousa (MDS)

#### Subgrupo: Estándares para Intercambio de Informaciones Espaciales

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

#### Colaboradores

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

#### Ilustraciones

Hezrai de Souza Cruz (MP/SLTI)