UNIDAD EJECU-TORA	Nº	NOMBRE DEL PROYECTO (MODALIDAD CONTRATA)	CRONOGRAMA DE DESEMBOLSOS PROYECTADOS			FINANCIA-MIENTO (S/.)
			MES 1	MES 2	MES 3	
EMAPICA	3	Rehabilitación integral para la recuperación d e l abastecimiento de agua potable en el sector del cercado de la ciudad de Ica afectado por el terremoto del 15 de agosto de 2007.	709,089.98	709,089.98	709,089.97	2,127,269.93
TOTALES			3,574,020.27	3,574,020.27	3,574,020.24	10,722,060.78

279660-1

Aprueban lineamientos y mecanismos para implementar la interconexión de equipos de procesamiento electrónico de información entre las entidades del Estado

RESOLUCIÓN MINISTERIAL
Nº 381-2008-PCM

Lima, 13 de noviembre de 2008

CONSIDERANDO:

Que, mediante la Primera Disposición Complementaria Final del Decreto Legislativo N° 1029 se estableció que en un plazo no mayor de 30 días hábiles, contados a partir de la vigencia de la referida norma, la Presidencia del Consejo de Ministros establecerá los lineamientos y mecanismos para implementar la interconexión de equipos de procesamiento electrónico de información entre las entidades del Estado, a que se refiere el numeral 76.2.2 del artículo 76° de la Ley N° 27444, con el fin de hacer efectivo el deber de colaboración entre las entidades del Estado.

De conformidad con el Decreto Supremo N° 063-2007-PCM que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, modificado por el Decreto Supremo N° 057-2008-PCM y con la Ley N° 29158 - Ley Orgánica del Poder Ejecutivo;

SE RESUELVE:

Artículo 1°.- Aprobación de los lineamientos y mecanismos para implementar la interconexión de equipos de procesamiento electrónico de información entre las entidades del Estado.

Apruébanse los lineamientos y mecanismos establecidos en el documento "Estándares y Especificaciones de Interoperabilidad del Estado Peruano", que forma parte integrante de la presente Resolución.

Artículo 2°.- Publicación.

La presente Resolución será publicada en el Diario Oficial El Peruano.

El documento "Estándares y Especificaciones de Interoperabilidad del Estado Peruano", aprobado por el artículo 1° de la presente norma, será publicado en el Portal del Estado Peruano (www.peru.gob.pe) y el Portal Institucional de la Presidencia del Consejo de Ministros, al día siguiente de publicada la presente norma en el Diario Oficial El Peruano.

Artículo 3°.- Vigencia.

La presente norma entrará en vigencia a partir del día siguiente de su publicación en los portales institucionales a que se refiere el artículo 2°.

Regístrese, comuníquese y publíquese.

YEHUDE SIMON MUNARO
Presidente del Consejo de Ministros

279660-3

Declaran a diversos Gobiernos Locales Distritales de Cusco como aptos para acceder a la transferencia de recursos presupuestales destinados a la ejecución de proyectos a cargo del FONCODES

RESOLUCIÓN DE SECRETARÍA DE DESCENTRALIZACIÓN
Nº 063-2008-PCM/SD

Miraflores, 18 de noviembre de 2008

VISTO:

El Informe Nº 050-2008-PCM/SD-WST.

CONSIDERANDO:

Que, mediante Decreto Supremo Nº 049-2008-PCM, que aprueba el "Plan Anual de Transferencia de Competencias Sectoriales a los Gobiernos Regionales y Locales del año 2008" se ha previsto culminar el proceso de verificación de seis (06) gobiernos locales distritales, con asignación presupuestal 2008 para proyectos de infraestructura social y productiva del FONCODES, aplicándose los mecanismos y procedimientos aprobados por la Secretaría de Descentralización en coordinación con el Ministerio de la Mujer y Desarrollo Social.

Que, mediante Resolución de Secretaría de Descentralización Nº 051-2008-PCM/SD, se aprobó la Directiva Nº 005-2008-PCM/SD, "Normas específicas para la transferencia de Programa de Infraestructura Social y Productiva a cargo del Fondo de Cooperación para el Desarrollo Social – FONCODES, del Ministerio de la Mujer y Desarrollo Social".

Que, mediante Informe Nº 050-2008-PCM/SD-WST, se recomienda declarar un grupo de Gobiernos Locales Distritales y Provinciales que se identifica en el artículo 1º de la presente resolución, aptos para acceder a la mencionada transferencia;

Que, asimismo el informe señalado recomienda ampliar los plazos establecidos en la Directiva Nº 005-2008-PCM/SD, en lo señalado por el inciso 3.2, ítem 3 Procedimientos y Plazos;

De conformidad a la Ley Nº 27783, Ley Nº 27972, Ley Nº 28273, y sus normas modificatorias y complementarias, el artículo 17 de la Ley Nº 27444; y, en uso de las atribuciones dispuestas por el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por Decreto Supremo Nº 063-2007-PCM.

SE RESUELVE:

Artículo 1º.- Cumplimiento de Mecanismos de Veri cación

Declarar a los Gobiernos Locales Distritales que se detallan en el Anexo que forma parte de la presente resolución, como aptos para acceder a la transferencia de los recursos presupuestales destinados a la ejecución de los Proyectos de Infraestructura Social y Productiva a cargo del Fondo de Cooperación para el Desarrollo Social - FONCODES del Ministerio de la Mujer y Desarrollo Social, incluidos en el Plan Anual de Transferencia de Competencias Sectoriales a los Gobiernos Regionales y Locales del año 2008, aprobado por Decreto Supremo Nº 049-2008-PCM.

Artículo 2º.- Ampliación de Plazo

Ampliar con eficacia anticipada a su término, el plazo previsto en el inciso 3.2 del ítem 3 Procedimientos y Plazos, de la Directiva Nº 005-2008-PCM/SD, de la siguiente manera:

- La vigencia de los Convenios de Cooperación, será hasta el 05 de diciembre de 2008.

Artículo 3º.- Publicación

Disponer la publicación de la presente Resolución Secretarial en el Diario Oficial El Peruano y en la página

PRESIDENCIA DEL CONSEJO DE MINISTROS

Estándares y Especificaciones de Interoperabilidad del Estado Peruano

LIMA - PERU

ÍNDICE

CAPITULO I

GENERALIDADES

1. PRESENTACIÓN

La Oficina Nacional de Gobierno Electrónico e Informática - ONGEI de la Presidencia del Consejo de Ministros - PCM, con la participación de la Intendencia Nacional de Sistemas de Información de la Superintendencia Nacional de Administración Tributaria - SUNAT, la Oficina de Informática del Ministerio Público, el Registro Nacional de Identificación y Estado Civil - RENIEC, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI, entre otros, ha elaborado el presente documento con el propósito de establecer los lineamientos, políticas, estándares y especificaciones para la interoperabilidad electrónica del Estado Peruano.

El propósito es contar con un instrumento técnico guía, que contiene políticas y especificaciones que deben desplegar las entidades del Estado a fin de hacer posible la interoperabilidad de sus servicios electrónicos, de acuerdo con lo establecido en el Decreto Legislativo N° 1029 que modifica la Ley del Procedimiento Administrativo General - Ley Nº 27444 y la Ley del Silencio Administrativo - Ley Nº 29060, específicamente relacionado con la Primera y Segunda Disposiciones Complementarias y Finales. Se ha considerado en este documento los siguientes aspectos:

1. Interconexión
2. Seguridad
3. Organización e intercambio de informaciones
4. Medios de acceso
5. Áreas de integración para Gobierno Electrónico

2. BASE NORMATIVA

- Ley Nº 29158 - Ley Orgánica del Poder Ejecutivo (LOPE): Que reconoce a la Presidencia del Consejo de Ministros, en adelante PCM, la calidad de Ministerio.

- Decreto Supremo Nº 063-2007-PCM: Que aprueba el Reglamento de Organización y Funciones de la PCM, en el cual se establece que la Oficina Nacional de Gobierno Electrónico e Informática de la PCM, tiene entre sus funciones implementar la Política Nacional de Gobierno Electrónico e Informática, así como, proponer los lineamientos de la política de contrataciones electrónicas del Sistema Electrónico de Adquisiciones y Contrataciones del Estado - SEACE;

- Decreto Supremo N° 066-2003-PCM: Que fusiona la Sub Jefatura de Informática (SJI) del INEI con la PCM, a través de su Secretaría de Gestión Pública.

- Decreto Supremo Nº 060-2001-PCM: Que crea el Portal de Estado Peruano.

- Decreto Supremo Nº 032-2006-PCM: Que crea el Portal de Servicios al Ciudadano y Empresas - PSCE.

- Resolución Ministerial Nº 179-2004-PCM: Que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2004 Tecnología de la Información. Procesos del Ciclo de Vida del Software. 1ª edición" en entidades del Sistema Nacional de Informática.

- Resolución Ministerial Nº 224-2004-PCM: Que aprueba uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información: Código de Buenas Prácticas para la gestión de la Seguridad de la Información. 1ª Edición. " en entidades del Sistema Nacional de Informática

- Decreto Supremo Nº 059-2004-PCM: Que establece disposiciones relativas a la administración del "Portal del Estado Peruano".

- Decreto Supremo N° 019-2007-PCM: Que establece el uso de la Ventanilla Única del Estado a través del Portal de Servicios al Ciudadano y Empresas y crea el Sistema Integrado de Servicios Públicos Virtuales – SISEV.

- Decreto Legislativo Nº 1029: Que modifica la Ley del Procedimiento Administrativo General - Ley N° 27444 y la Ley del Silencio Administrativo - Ley N° 29060.

- Decreto Legislativo N° 604 - Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática: Que establece como uno de los ámbitos de competencia del INEI al Sistema Nacional de Informática.

3. INTRODUCCIÓN

El desarrollo del Gobierno Electrónico en el Perú que propende impulsar el avance de la Sociedad de la Información y del Conocimiento se basa en la integración y optimización de sus procesos y servicios, que le permite facilitar el cumplimiento de sus obligaciones y el desarrollo de sus actividades al servicio del ciudadano, tanto de manera individual o en sus diversas formas de organización privada.

Es por tanto necesario llevar adelante un *enfoque de integración y calidad de los procesos, con el apoyo de las tecnologías de la información y de la comunicación, transformando la gestión del Estado, aumentando la competitividad global así como el desarrollo empresarial, procurando lograr una sociedad más equitativa, integrada y democrática*.

Este enfoque además se realiza dentro del marco del "Deber de Colaboración entre entidades del Estado" que contempla la siguiente base legal:

- Ley Nº 27444 del Procedimiento Administrativo General (en adelante LPAG).

- Decreto Legislativo Nº 1029, que modifica la LPAG - Ley Nº 27444 - y la Ley del Silencio Administrativo - Ley Nº 29060.

La LPAG regula en el Sub-Capítulo III, artículos 76º y siguiente, la "Colaboración entre entidades"; al respecto, en el numeral 76.1 del citado artículo 76° indica que: *"Las relaciones entre entidades se rigen por el criterio de colaboración, sin que ello importe renuncia a la competencia propia señalada por ley".*

Atendiendo a dicho "criterio de colaboración", en el numeral 76.2.2 del artículo 76° de la LPAG se manifiesta que las entidades deben: *"Proporcionar directamente los datos e información que posean, sea cual fuere su naturaleza jurídica o posición institucional, a través de cualquier medio, sin más limitación que la establecida por la Constitución o la ley, para lo cual se propenderá a la interconexión de equipos de procesamiento electrónico de información, u otros medios similares"*.

En ese sentido, el presente documento se centra en las políticas, en la identificación y el reconocimiento de los estándares como mecanismos para la interconexión de equipos de procesamiento electrónico de información, esto es, en el logro de la interoperabilidad.

INTEROPERABILIDAD: Según el *Institute of Electrical and Electronics Engineers* (IEEE[1]), la interoperabilidad es la capacidad de dos o más sistemas o componentes para intercambiar información y para utilizar la información que ha sido intercambiada.

Considerando la importancia del APEC en la determinación y la búsqueda de la interoperabilidad a nivel de dominios o economías miembros, y siendo el Perú parte de dicho foro, es que se admite el Proyecto de Interoperabilidad PKI del Foro PKI (PKI Forum[2]) en donde se define a la interoperabilidad en tres niveles: interoperabilidad a nivel de componentes, interoperabilidad a nivel de aplicaciones e interoperabilidad entre dominios:

- La interoperabilidad a nivel de componentes, se refiere a la interacción entre sistemas que directamente soportan y/o consumen servicios relativos a la PKI.

- La interoperabilidad a nivel de aplicación, está referida a la compatibilidad que debe de existir entre las aplicaciones que se ejecutan en las computadoras, que pueden ser suministradas por dos proveedores diferentes, que usan servicios de infraestructura PKI también diferentes para la realización de sus operaciones.

- Los temas y opciones relativos a la interoperabilidad entre dominios están en relación al logro de interoperabilidad entre dos dominios PKI que necesitan comunicarse entre sí.

En relación a la interoperabilidad a nivel de dominios, un elemento adicional a considerar es la interoperabilidad a nivel de datos, dentro del marco del Foro de APEC.

[1] Institute of Electrical and Electronics Engineers. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries

[2] *PKI Interoperability Framework Whitepaper*, March 2001. Documento disponible en: http://www.oasis-pki.org/pdfs/PKIInteroperabilityFramework.pdf.

La presente guía también considera los lineamientos de la Organización Mundial de Aduanas - OMA, que es una organización intergubernamental, reconocida internacionalmente como un centro global de prácticas aduaneras y juega un rol de liderazgo en la discusión, desarrollo, promoción e implementación de un sistema moderno y seguro de procedimientos aduaneros.

También recoge lineamientos en materia de interoperabilidad de otras organizaciones, de las que nuestro país forma parte, como Naciones Unidas, ISO, OGC, entre otras.

Por lo tanto, la interoperabilidad no está referida sólo a los aspectos técnicos, sino implica también consideraciones funcionales, operacionales, normativas y de política, que permiten desarrollar actuaciones coordinadas y cohesionadas, en este caso entre los organismos del Estado y de la Sociedad Civil.

3.1. Plataforma de interoperabilidad del Gobierno Electrónico del Estado Peruano

La plataforma de interoperabilidad del Gobierno Electrónico se refiere al sistema de políticas, lineamientos y especificaciones que definen los estándares empleados en el Estado Peruano que permite de manera efectiva la interoperabilidad de los servicios electrónicos de las distintas entidades de la Administración Pública.

4. ALCANCES, ADMINISTRACION Y OBLIGATORIEDAD

4.1. Alcances

Estas políticas y lineamientos deben permitir la interoperabilidad de los sistemas de información y la gestión compartida de la información del Estado Peruano.

La estructura básica de los estándares y especificaciones de interoperabilidad del Gobierno Electrónico alcanzan las necesidades conectivas en el ámbito interno del Estado, como en relación con la interacción con la sociedad, tanto a nivel local, nacional y global (especialmente en el marco del APEC), así como entre personas y organizaciones.

Se promueve que la información del Estado pueda ser localizada e intercambiada en forma rápida y sencilla entre las entidades que conforman el Sistema Nacional de Informática, así como también con el sector privado y la sociedad, en condiciones de privacidad y seguridad.

La arquitectura definida en este documento contempla el intercambio de información entre los sistemas de información del Estado Peruano y abarca las interacciones con los siguientes ámbitos:

- Poderes del Estado Peruano (Ejecutivo, Legislativo y Judicial).
- Organismos públicos y privados, nacionales y extranjeros.
- Ciudadanos y otras personas individuales.

- Empresas y entidades no gubernamentales.
- Otros Estados y organismos internacionales, en especial los referidos a las economías miembros del APEC específicamente a la interoperabilidad de documentos electrónicos no repudiables, esto es, basados en tecnología de certificación digital (PKI).

4.2. Administración

La plataforma de interoperabilidad del Gobierno Electrónico es administrada por el Grupo de Trabajo de Interoperabilidad del Estado - GTIE.

El GTIE es un grupo de trabajo multisectorial, dependiente de la Presidencia del Consejo de Ministros, que tiene por finalidad establecer las políticas, estándares y mecanismos de interoperabilidad entre entidades públicas, de acuerdo a lo establecido en el Decreto Legislativo N° 1029.

4.3 Funciones del GTIE

1. Proponer a PCM los lineamientos de política, los estándares y las especificaciones de interoperabilidad del Estado Peruano.

2. Recoger, clasificar y catalogar las propuestas de nuevos componentes o mejoras de la plataforma de interoperabilidad del Gobierno Electrónico.

3. Proponer a PCM los procedimientos a fin de asegurar una adecuada administración de los estándares y especificaciones de interoperabilidad.

4. Elaborar el Plan de Interoperabilidad del Estado Peruano – PIEP que considere la implementación estratégica y progresiva de los Estándares y Especificaciones de Interoperabilidad de Gobierno Electrónico en el Perú.

5. Proponer a PCM directivas y lineamientos que sean necesarios para una adecuada aplicación de las especificaciones de interoperabilidad.

6. Emitir opinión técnica en caso de controversia o dudas respecto a los estándares de interoperabilidad.

7. Ejercer la labor de seguimiento y monitoreo del Plan de Interoperabilidad del Estado Peruano.

8. Elaborar un informe anual de los avances del Plan de Interoperabilidad del Estado Peruano.

4.4 Obligatoriedad

Para las Entidades que pertenecen al Poder Ejectuvito, Poder Legislativo y Poder Judicial, y los organismos autónomos, la adopción de los estándares y políticas contenidos en este documento es de carácter obligatorio, en forma

progresiva, de acuerdo a los lineamientos establecidos en el Plan de Interoperabilidad del Estado Peruano - PIEP.

Las especificaciones contempladas en este documento pueden ser adoptadas por los gobiernos regionales y gobiernos locales, para el logro de la interoperabilidad con el Estado y entre ellos mismos.

La ONGEI será la responsable de supervisar el cumplimiento de las políticas y lineamientos de interoperabilidad y de las facilidades brindadas por los organismos del Estado para implementar servicios interoperables basados en los estándares reconocidos propuestos por el GTIE.

5. POLÍTICAS GENERALES

A fin de establecer un marco general y condiciones de desarrollo tecnológico que permitan llevar adelante un esquema de conectividad e interoperabilidad viable, se establecen las siguientes políticas generales:

Enfoque de Sistemas. El desarrollo de Sistemas de Información y las soluciones informáticas del Estado deberán ser enmarcadas en un modelo de negocio integrado y contemplando el entorno en el que interopera la organización.

Estándares Abiertos. Se define la adopción fundamentalmente de estándares abiertos en las especificaciones técnicas de las soluciones informáticas del Estado. En el caso de la interacción con el sector privado, se respetará la plataforma establecida en cada caso y se establecerá un plan de operación temporal.

Estándares Internacionales. Los estándares y patrones establecidos por el Estado, deberán mantener la mayor correspondencia posible con los Estándares Internacionales de reconocimiento mundial, regional y nacional, según esté disponible, en dicho orden de prioridad.

Software Libre. El Estado preferirá emplear esta tecnología cuando existan soluciones y componentes en software libre, preferirá asimismo la libre disponibilidad del código fuente -entre otras- por razones de seguridad, las que deberán contar con el soporte técnico sólido correspondiente y con la capacidad comprobada de soportar eficientemente los servicios electrónicos, de acuerdo con la Resolución Jefatural N° 199-2003-INEI.

Independencia tecnológica y soporte técnico. Todas las especificaciones y soluciones informáticas, deben estar ampliamente apoyadas por soporte técnico alternativo en el mercado, evitando la dependencia tecnológica y reduciendo los riesgos de su adopción.

Intercambio Electrónico de Datos en el marco de la colaboración entre entidades del Estado. Las relaciones entre entidades se rigen por el criterio de colaboración, sin que ello importe renuncia a la competencia propia señalada por ley. El criterio de colaboración no debe atentar contra la calidad del servicio prestado, esto es, no se debe disminuir ni degradar la prestación del servicio y tampoco debe de causar perjuicio a los colaboradores en el sentido de infringir gastos en infraestructura de

Tecnología Informática y de Telecomunicaciones TICs a efectos de realizar dicha colaboración.

Intercambio Electrónico de Datos en el marco de Naciones Unidas (UN/EDI). El Estado Peruano adopta en forma homologada, para lo que esté establecido, las normas internacionales que en materia de normalización están definidas por Naciones Unidas en particular en materia de definición de datos, para su intercambio electrónico.

ISO. En todo lo que esté establecido, se considerará en forma prioritaria los estándares de la *International Organization for Standardization* (ISO), especialmente los que se han constituido en Norma Técnica Peruana por INDECOPI.

XML. Se adopta como estándar primario el Extensible Markup Language para la definición, transmisión, validación e interpretación de datos entre aplicaciones en el intercambio electrónico de datos.

Seguridad y privacidad de la información. Todos los organismos responsables de los servicios electrónicos del Estado implementarán progresivamente medios seguros, garantizando la privacidad de la información y respetando lo dispuesto en la legislación peruana en materia de validez, seguridad y protección de datos.

Desarrollo de Metadatos del Estado. Basado en estándares internacionales, se adopta un Modelo Arquitectural General de Datos del Estado, cuyo Metadatos es actualizado por las entidades del Estado, bajo la administración y responsabilidad de la ONGEI.

OGC. Open Geospatial Consortium; las entidades del Estado que generen, desarrollen e implementen aplicaciones que incorporen datos espaciales deberán implementar progresivamente aquellos estándares que faciliten el intercambio de la información geográfica

6. GESTIÓN DE LA PLATAFORMA DE INTEROPERABILIDAD DEL GOBIERNO ELECTRÓNICO

La plataforma de interoperabilidad del Gobierno Electrónico es una definición sistémica y dinámica que requiere contar con atributos de coordinación y cohesión integrada. Es por ello que se requiere establecer los mecanismos que permitan tomar las acciones oportunas y prospectivas, que devengan de los cambios en los procesos y en las tecnologías, aplicando para ello inteligencia colaborativa y estableciendo los mecanismos de definición de políticas, identificación y reconocimiento de estándares que permitan hacer el balance entre los cambios y la estabilidad de dicha plataforma.

6.1. Estrategia de Gestión

La plataforma de interoperabilidad del Gobierno Electrónico establece un esquema de versiones, debiendo estos ser revisados en forma continúa por el GTIE, fundamentalmente para la publicación de adendas de mejora a fin de generar la publicación de una nueva versión en -al menos- un evento especializado anual.

6.2. Conformación del Grupo de Trabajo

6.2.1. Integrantes del Grupo de Trabajo

El Grupo de Trabajo de Interoperabilidad del Estado - GTIE está conformado por los siguientes miembros:

- El Jefe de la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI de la PCM, quien la presidirá;
- Un representante del Ministerio de Transportes y Comunicaciones
- Un representante de la Superintendencia Nacional de Administración Tributaria - SUNAT
- Un representante del Registro Nacional de Identificación y Estado Civil – RENIEC
- Un representante del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI-

6.2.2. Del Secretario del GTIE

- El Secretario será el representante de la Superintendencia Nacional de Administración Tributaria.

- Entre las funciones a cargo del Secretario están las siguientes:

  1. Convocar, por encargo del Presidente del GTIE, a las sesiones ordinarias y extraordinarias;

  2. Preparar la agenda y los documentos que correspondan para cada sesión;

  3. Redactar las actas de las sesiones y servir de depositario de ellas;

  4. Brindar apoyo administrativo y logístico al GTIE;

  5. Presentar en cada reunión del GTIE, informes sobre el avance de las labores encomendadas por éste, para lo cual solicitará a los Presidentes de los Sub Grupos de Trabajo la información respectiva.

  6. Presentar al GTIE, para su consideración, planes, programas, proyectos de dispositivos normativos, otros trabajos realizados al interior de ésta, elaborados por los Sub Grupos de Trabajo, relacionados con el tema de Interoperabilidad en el Estado;

  7. Solicitar información y documentación a otras entidades públicas, entidades privadas o especialistas;

  8. Coordinar y realizar el seguimiento de las labores de los grupos de trabajo y llevar el registro de reuniones de dichos

grupos, para lo cual los Coordinadores de los Sub Grupos de Trabajo informarán mensualmente de sus actividades al Secretario.

9. El Secretario podrá solicitar a las entidades públicas o privadas y especialistas, el asesoramiento, información y apoyo necesarios para el cumplimiento de la labor encomendada.

10. Las demás que le encomiende el Presidente del GTIE.

6.2.3. De los Sub Grupos de Trabajo

El GTIE podrá contar con Sub Grupos de Trabajo que colaborarán con su gestión. Los Sub Grupos se referirán a áreas específicas que son:

SUB GRUPOS DE TRABAJO	COORDINADORES
Sub Grupo N°. 1: Interconexión	MTC
Sub Grupo N°. 2: Seguridad	ONGEI – PCM
Sub Grupo N°. 3: Organización e Intercambio de Información	SUNAT
Sub Grupo N°. 4: Medios de Acceso	RENIEC

6.2.4. Funciones de los Sub Grupos de Trabajo

1. Proponer los planes de seguimiento y evaluación del Plan de Interoperabilidad del Estado Peruano (PIEP).

2. Opinar y proponer estándares y especificaciones de interoperabilidad para el Estado Peruano, en la materia que le compete.

3. Atender los requerimientos de estudio para el mejoramiento o incorporación de nuevas especificaciones.

4. Opinar sobre la baja o derogatoria de los estándares y especificaciones de interoperabilidad.

5. Opinar sobre la propuesta de directivas, lineamientos, requisitos, condiciones, ambiente, metodologías y procedimientos, para una adecuada aplicación de los estándares y especificaciones.

6. Emitir opinión técnica y hacer propuestas, a pedido de la ONGEI, en caso de controversia o dudas respecto a los estándares y especificaciones de interoperabilidad.

7. Otros que se encomiende a cada Sub Grupo en la resolución que lo conforme.

CAPITULO II
ESTÁNDARES Y ESPECIFICACIONES DE INTEROPERABILIDAD DEL ESTADO PERUANO

7. INTERCONEXIÓN

7.1. Políticas técnicas

1. Los organismos deberán interconectarse utilizando Ipv4 y planeando su futura migración para Ipv6. Las nuevas contrataciones y actualizaciones de redes deben contemplar soporte a la coexistencia de los protocolos Ipv4 e Ipv6 y a productos que contemplen ambos protocolos.

2. Los sistemas de mensajería electrónica de documentos electrónicos de carácter no repudiable (firmados digitalmente) deben estar basados en los domicilios electrónicos, especificados en la Guía de Acreditación de software (SW) y en la Guía de Servicios de Valor Añadido (SVA) aprobados por la Autoridad Administrativa Competente, INDECOPI.

3. Los sistemas de correo electrónico deben utilizar SMTP/MIME para el transporte de mensajes. Para acceso a los mensajes, se deben utilizar protocolos POP3 y/o IMAP, y se promueve el uso de interfaces Web para el acceso al correo electrónico, teniendo siempre en cuenta aspectos de seguridad.

4. Los organismos deben usar un esquema de Directorio compatible, no propietario e interoperable.

5. Los organismos deben obedecer la política de nombramiento de dominios establecida por el Sistema Peruano de Nombres de Dominio (ccTLD pe).

6. El DNS - Domain Name System - se debe utilizar para la resolución de nombres de dominios en Internet, convirtiéndolos en direcciones IP e, inversamente, convirtiendo direcciones IP en nombres de dominio.

7. Los protocolos FTP y/o HTTP deben ser utilizados para transferencia de archivos, observando sus funcionalidades para recuperación de interrupciones y seguridad, cuando sea necesario. El protocolo HTTP debe ser priorizado para transferencia de archivos oriundos de páginas de sitios de Internet.

8. Siempre que sea posible, se debe emplear tecnología basada en la Web en aplicaciones que utilizaron Emulación de Terminal, anteriormente.

9. La tecnología de Web Services es recomendada como estándar de interoperabilidad entre los organismos.

10. 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.

11. El protocolo SOAP es recomendado para la comunicación entre los clientes y los Web Services y la especificación del servicio deberá utilizar el lenguaje WSDL.

12. Los Web Servicies para datos Espaciales emplearán los estándares XML y SOAP

7.2. Especificaciones técnicas

Componente	Especificación	SIT	Observaciones
	A : Adoptado R : Recomendado T : En transición E : En estudio F : Estudio futuro		
Protocolo de transferencia de hipertexto	Utilizar HTTP/1.1 (RF 2616) y/o HTTPS (RFC 2660)	A	
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, RFC2822, RFC 2045, RFC 2046, RFC 2646, RFC 2047, RFC 2231, RFC 2183, RFC 2048, RFC 3023 y RFC 2049	R	
Envío de calendarios	Para enviar calendarios de eventos y/o citas, se debe utilizar el estándar iCalendar: RFC 2445.		
Aplicaciones móviles	El protocolo WAP 2.0 deberá utilizarse para la comunicación de aplicaciones inalámbricas, de acuerdo a lo definido por la Open Mobile Alliance (OMA). Para mostrar el contenido se utilizará el lenguaje XHTML-MP y WCSS. http://www.wapforum.org/what/WAPWhite_Paper1.pdf	R	
Envío de modelos UML	Para compartir modelos de UML, se debe de utilizar el estándar XMI de la OMG. ISO 19503:2005 *Information technology - XML Metadata Interchange (XMI)*.	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 y RFC 3851	R	
Acceso al apartado postal	A excepción de que las exigencias de seguridad lo determinen de otra manera, programas de correo deberán, como mínimo, estar de acuerdo con POP3 para acceso remoto al apartado postal. RFCs correlacionadas: RFC 1939, RFC 1957 y RFC 2449. 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 (siempre teniendo en cuenta las políticas de seguridad). RFCs correlacionadas: RFC 3501, RFC 2342, RFC 2971, RFC 3502, RFC 3503, RFC 3510 Y RFC 2910.	R	
Acceso seguro al apartado postal	El acceso al apartado postal, por medio de redes no seguras, deberá utilizar HTTPS, de acuerdo con los padrones de seguridad en el transporte. Cuando sea necesario utilizar IMAP o POP, usarlo a través de TLS, según RFC 2595.	R	
Directorio	Utilizar el esquema de Directorio central, basado en LDAP v3.	R	
Servicios de nombramiento de dominio	El DNS debe ser utilizado para resolución de nombres de dominios Internet, conforme la RFC 1035. Siguiendo las políticas y formativas de Sistema Peruano de	A	

Componente	Especificación	SIT	Observaciones
	Nombres de Dominio. Los dominios del estado deben seguir la directiva No. 010-2002-INEI/DTPN que regula la utilización de nombres de dominio en las entidades de la Administración Pública emitida por INEI, y las demás que le sean aplicables en el presente reglamento.		
Direcciones de apartado postal electrónico	Se debe revisar si existe una norma a nivel Gobierno, pero al parecer está definido por cada institución.	E	
Protocolos de transferencia de archivos	FTP (RFC 959 y 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 uno o más participantes.	R	
Mensajería en tiempo real	El modelo y requisitos para *Instant Messaging and Presence Protocol* (IMPP) son definidos por la RFC 2778 y RFC 2779	T	
	El modelo y requisitos para *Extensible Messaging and Presence Protocol* (XMPP) son definidos por la RFC 3920 y RFC 3921	R	
Servicio de mensajes cortos	El Servicio de Mensajes Cortos (SMS por sus siglas en inglés) deberá utilizar el protocolo SMPP, de acuerdo a lo definido por el *SMS Forum*.	R	
Intercomunicación LAN/WAN	IPv4 (RFC 791)	A	
	Ipv6 (RFC 2460)	E	
Transporte	TCP (RFC 793) UDP (RFC 768) cuando sea necesario, siempre sometido a las limitaciones de seguridad	R	
Tráfico avanzado	Cuando sea 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	Se debe utilizar la norma IEEE 802.11 b/g, en conformidad con las determinaciones del *Wi-Fi Alliance*.	R	
Red metropolitana inalámbrica	Se debe utilizar la norma IEEE 802.16, en conformidad con las determinaciones del *WiMax Forum*.		
Información Geográfica distribuida	Se debe utilizar la especificación de OpenGIS Web Feature Service (WFS) para requerir datos espaciales en forma de entidades vectoriales a partir de consultas a bases de datos geográficas distribuidas, mediante GML	R	
Mapas georeferenciados distribuidos	Se debe utilizar la especificación de OpenGIS WebMap Service para requerir datos espaciales en forma de imágenes georeferenciadas a partir de consultas a bases de datos geográficas distribuidas		

7.3. Web Services

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

a. Publicable: Al crear un Web Service, su publicación debe ser hecha mediante registro en un catálogo de servicios para que potenciales usuarios puedan encontrarlo y utilizarlo de ser el caso. El catálogo puede utilizar UDDI.

b. Auto describible: Los Web Services ofrecen una descripción completa de sus servicios y de cómo los usuarios podrán crear aplicaciones para interactuar con ellos. Esa descripción es realizada a través de WSDL.

La necesidad de integración entre los diversos sistemas de información del Gobierno, implementados en diferentes tecnologías conlleva la adopción de un estándar de interoperabilidad que garantice escalabilidad, facilidad de uso, además de brindar la capacidad de actualización de forma simultánea.

En ese contexto, se entiende que el uso de Web Services, es adecuado para esas necesidades.

El soporte de Web Services para integración directa con otras aplicaciones de software utiliza mensajes escritos en XML como estándar de interoperabilidad. Esos mensajes son involucrados en protocolos de aplicación estándar de Internet (SOAP).

Componente	Especificación	SIT	Observaciones
	A : Adoptado R : Recomendado T : En transición E : En estudio F : Estudio futuro		
Protocolo de intercambio de informaciones	Utilizar SOAP v1.2 como definido por el W3C. http://www.w3.org/TR/soap12-part1 http://www.w3.org/TR/soap12-part2	R	
Infraestructura de registro	Utilizar la especificación UDDI v3.0.2 (*Universal Description, Discovery and Integration* por sus siglas en inglés)definida por OASIS http://uddi.org/pubs/uddi_v3.htm	R	
Lenguaje de definición del servicio	WSDL 1.1 (*Web Services Description Language*) como definido por la W3C. http://www.w3.org/TR/wsdl	R	
	WSDL 2.0 (*Web Services Description Language*) como definido por la W3C. http://www.w3.org/TR/wsdl20	E	
Perfil básico de interoperabilidad	Basic Profile 1.1 SE, como definido por la WS-I http://www.ws-i.org/Profiles/BasicProfile-1.1.html	E	
Portles Remotos	WSRP 1.0 (Web Services for Remote Portles) como definido por OASIS. http://www.oasis-open.org/committees/wsrp	E	

Componente	Especificación	SIT	Observaciones
Mashup	Aplicación Web híbrida, que utiliza contenido de distintas webs para generar un contenido más rico y completo.	E	Actualmente la W3C está en proceso de crear un estándar para su manejo.

7.4. Mensajería electrónica

7.4.1. Certificación Digital

Para el caso de los documentos electrónicos de carácter no repudiable, específicamente los generados mediante Servicios de Certificación Digital (PKI), la mensajería electrónica se realizará a través de Sistemas de Intermediación Digital (SID), como se especifica en el Reglamento de la Ley de Firmas y Certificados Digitales, Ley N° 27269[3], en la SECCIÓN III, De los Prestadores de Servicios de Valor Añadido.

La operación de los SID están regulados por la Autoridad Administrativa Competente a través de las respectivas Guías de Acreditación (Guía de Acreditación de Servicios de Valor Añadido SVA) y las Guías de Acreditación de Software.

7.4.2. Correo electrónico

Transporte de mensaje electrónico

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

Acceso al apartado postal

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

Red Privada Virtual

VPN por sus siglas en inglés (Virtual Private Network), es un túnel virtual privado construido sobre la infraestructura de una red pública o privada. En vez de servirse de circuitos digitales dedicados o redes de paquetes para conectar redes remotas, utiliza usualmente, de la infraestructura de la Internet.

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

Los túneles virtuales trasmiten datos cifrados sobre redes públicas o privadas, formando un canal virtual seguro a través de esas redes. Por tanto, se utilizan protocolos de túneles virtuales.

[3] Aprobado por Decreto Supremo N° 052-2008-PCM, el 18 de julio de 2008 y publicado en el diario oficial El Peruano el 19 del mismo mes.

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

7.5. Redes punto a punto

También conocidas por las siglas 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 de nodos, mientras mantienen conectividad y resultados aceptables, sin depender de la intermediación o soporte de una autoridad (servidor) central.

8. SEGURIDAD

8.1. Políticas técnicas

1. Los datos, informaciones y sistemas de información del Gobierno deben ser protegidos contra amenazas y vulnerabilidades para así reducir riesgos y garantizar la integridad, confidencialidad y disponibilidad.

2. Los sistemas operativos para aplicaciones de servidores que almacenan información y bases de datos relativas a los ciudadanos y aquéllas concernientes a aspectos de la seguridad nacional, preferentemente deben de permitir disponer libremente del código fuente de dichos sistemas operativos.

3. Los datos e informaciones deben ser mantenidos con el mismo nivel de protección, independiente del medio en que sean procesados, almacenados o en tránsito.

4. Las informaciones que transitan en redes inseguras, incluyendo aquellas inalámbricas, deben adoptar los controles de seguridad necesarios.

5. 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.

6. 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. La seguridad es un proceso que debe estar presente en todas las etapas del ciclo de desarrollo del sistema y todos los componentes relacionados a la comunicación.

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

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

10. 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.

11. 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 Guías de Acreditación respectivas aprobadas por la Autoridad Administrativa Competente INDECOPI.

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

13. 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.

14. Los organismos de la administración pública, teniendo como objetivo la mejora de la seguridad, deben tener como referencia la norma NTP ISO/IEC 17799:2007 EDI código de buenas prácticas para la gestión de la seguridad de la información**.**

8.2. Especificaciones técnicas

8.2.1. Seguridad de IP

Componente	Especificación	SIT	Observaciones
	A = Adoptado R =Recomendado T = En transición E = En estudio F = Estudio futuro		
Transferencia de datos en redes inseguras por los protocolos HTTP, LDAP, IMAP, POP3, Telnet siempre que sea posible. – Seguridad de redes IPv4 en la capa de transporte	TLS – *Transport Layer Security*, RFC4346 (http://www.ietf.org/rfc/rfc4346.txt). HTTP sobre TLS, RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt) Pudiendo implementar los siguientes algoritmos criptográficos: - Algoritmos para cambio de llaves de sesión, durante el *handshake*: RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA; - Algoritmos para definición de llave de cifra: RC4,	R	

Componente	Especificación	SIT	Observaciones
	IDEA, 3DES, AES; - Algoritmos que implementan la función de *hash* para definición del MAC: SHA-256 o SHA-512. - Tipo de Certificado Digital - X.509 v3 SASL - *Simple Authentication and Security Layer*, RFC 4422 (http://www.ietf.org/rfc/rfc4422.txt).		
Seguridad de redes Ipv4	*IPSec Authentication Header* RFC 2402 y RFC 2404 para autenticación de cabecera del IP. http://www.ietf.org/rfc/rfc2402.txt http://www.ietf.org/rfc/rfc2404.txt IKE v.2 – *Internet Key Exchange*, RFC 4306 (http://www.ietf.org/rfc/rfc4306.txt), debe ser utilizado siempre que necesario para negociación de la asociación de seguridad entre dos entidades para cambio de material de cierre. ESP – *Encapsulating Security Payload,* RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt) Requisito para VPN – Virtual Private Network.	R	
Seguridad de redes IPv4 para protocolos de aplicación	El S/MIME v3.1 ,RFC3851 (http://www.ietf.org/rfc/rfc3851.txt) deberá ser utilizado cuando sea apropiado para seguridad de mensajes generales de Gobierno.	R	
Seguridad de redes IPv6 en la capa de red	El IPv6 definido en la RFC2460 (http://www.ietf.org/rfc/rfc2460.txt) presenta Implementaciones de seguridad nativas en el protocolo. Las especificaciones del IPv6 definieron dos mecanismos de seguridad: la autenticación de encabezamiento AH (*Authentication Header*) RFC4302 (http://www.ietf.org/rfc/rfc4302.txt) o autenticación IP, y la seguridad del ambiente IP, ESP (*Encrypted Security Payload*) RFC4305 (http://www.ietf.org/rfc/rfc4305.txt).	R	

8.2.2. Seguridad de correo electrónico

Componente	Especificación	SIT	Observaciones
	A = Adoptado R =Recomendado T = En transición E = En Estudio F = Estudio futuro		
Acceso a casilleros electrónicos	El acceso al casillero electrónico 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 casillero electrónico 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 (http://www.ietf.org/rfc/rfc2595.txt), que trata de la utilización del TLS con IMAP, POP3 y ACAP.	R	
Contenido de	El S/MIME V3 deberá ser utilizado cuando sea	R	

e-mail	adecuado para seguridad de mensajes generales de Gobierno. Eso incluye RFC 3369 (http://www.ietf.org/rfc/rfc3369.txt), RFC 3370 (http://www.ietf.org/rfc/rfc3370.txt), RFC 2631 (http://www.ietf.org/rfc/rfc2631.txt), RFC 3850 (http://www.ietf.org/rfc/rfc3850.txt) y RFC 3851 (http://www.ietf.org/rfc/rfc3851.txt).		
Firma	Utilizar estándar de firma digital para la firma de e-mail, cuando sea necesario.	R	

8.2.3. Criptografía y PKI

Componente	Especificación	SIT	Observaciones
	A = Adoptado R =Recomendado T = En transición E = En Estudio F = Estudio futuro		
Algoritmo de cifrado	DES, 3DES o AES, SKIPJACK	R	
Algoritmo para firma	DSA		
Algoritmos de Hashing	SHA-1, SHA 224, SHA-256, SHA 384, SHA-512, RFC 1231	R	
Algoritmos asimétricos	RSA, Eliptic Curve DSA	R	
Algoritmo de intercambio de claves públicas	KEA	R	
Formatos estándar para certificados de claves públicas	X.509 v3, ETSI TS 102 280	R	
Formatos de nombres para certificados de claves públicas	X.500, X.501, X.509, X.521	R	
Requisitos de seguridad para módulos criptográficos.	FIPS 140-2 – requisitos mínimos para las soluciones de almacenamiento de llaves privadas y certificados digitales que utilizan dispositivos tanto de *software* como de *hardware* tipo *token* o *smart card*, Adherencia al estándar: Utilizar los niveles del 1 al 4 de acuerdo a la sensibilidad de la información manejada.	R	
Gestión de sistemas EC de confianza	CWA 14167(1-4)	R	
Conformidad con las Directivas CEN para apropiación y operación de EC	CWA 14172 (1-8)	R	
Dispositivos de creación de firma segura	CWA 14355	R	
Uso de las Firmas Electrónicas: Aspectos legales y técnicos	CWA 14365 (1-2)	R	
Interfaz de aplicación para tarjetas inteligentes utilizadas como dispositivos de creación de firma segura	CWA 14890 (1-2)	R	
Infraestructuras y firmas electrónicas (ESI) – Algoritmos y Parámetros para firmas electrónicas seguras	ETSI SR 002 176	R	

Componente	Especificación	SIT	Observaciones
Perfil de estampa de tiempo	ETSI TS 101 861	R	
Infraestructuras y firmas electrónicas (ESI) – Requisitos de Política para Autoridades de Time-Stamping	ETSI TS 102 023	R	
Infraestructuras y firmas electrónicas (ESI) – Armonización Internacional de Requisitos de Política para EC	ETSI TS 102 040	R	
Requisitos de Política para EC que emiten Certificados de Clave Pública	ETSI TS 102 042	R	
Juegos de caracteres arbitrarios	IETF RFC 373	R	
Certificados Digitales, gestión de claves y Lista de Certificados Revocados (CRL)	IETF RFC 1422	R	
Protocolo OCSP X.509 para PKI	IETF RFC 2560	R	
Certificado y perfil CRL X.509 para PKI	IETF RFC 2459, IETF RFC 3280	R	
Perfil de certificados calificados X.509 para PKI	IETF RFC 3039	R	
Formato de conversión de la norma ISO 10646	IETF RFC 3629	R	
Sistema básico de Política de Certificados y Prácticas de Certificación X.509 para PKI	IETF RFC 3647	R	
Criptografía RSA	PKCS#1	R	
Acuerdo de clave Diffie-Hellman	PKCS#3	R	
Criptografía basada en contraseña	PKCS#5	R	
Sintaxis de mensaje criptográfico	PKCS#7	R	
Sintaxis de información de clave privada	PKCS#8	R	
Clases de objetos seleccionados y tipos de atributos	PKCS#9	R	
Sintaxis de solicitud de certificación	PKCS#10	R	

Componente	Especificación	SIT	Observaciones
Interfaz de token criptográfico	PKCS#11	R	
Intercambio de información personal	PKCS#12	R	
Formato estándar de la información del token criptográfico	PKCS#15	R	
Lineamientos para Declaración de Prácticas de Certificación (CPS) y Políticas de Certificados (CP)	RFC 3647 (RFC2527)	R	
Diagrama LDAPv2 X.509 para PKI	RFC 2587	R	
HTTP sobre TLS	RFC 2818	R	
Requisitos para validación de ruta delegada y para el protocolo de descubrimiento de Ruta Delegada	RFC 3379	R	
Generadores de números aleatorios (RNG)	FIPS 140-2 Anexo C	R	
Generadores determinísticos de bit aleatorios (DRBG)	NIST SP 800-90	R	
Algoritmo MAC basado en cifrado de bloques (CMAC)	NIST SP 800-38B	R	
Contador con modo de encadenamiento de bloques cifrados (*Counter Chipre-block chaining mode* - CCM)	NIST SP 800-38C	R	
Suma de chequeo para corroborar la integridad de los datos (*Keyed – Hashing for Message Authentication*)	FIPS 198	R	
Requisitos de seguridad para módulos criptográficos: hardware y firmware	FIPS 140-2	R	
Microcontrolador y Unidad de Procesamiento Numérico (NPU) suplementario capaces de calcular operaciones criptográficas acordes con PKCS#11 y PKCS #15, de conformidad con los requisitos del ISO/IEC 7816-1 al 7816-5	ISO 7816 1-5	R	
Certificación para tarjeta inteligente	Certificación EMC	R	
Protocolo de sello de tiempo (TSP) X.509 para PKI	RFC 3161	R	

Componente	Especificación	SIT	Observaciones
Requerimientos de políticas para autoridades de sello de tiempo (TSA)	RFC 3628	R	
Protocolo TSL	RFC 2246	R	
Protocolos de administración de certificados X.509 para PKI	RFC 2510	R	
Sintaxis para mensajes criptográficos	RFC 2630	R	
Optimización de los servicios de seguridad para S/MIME	RFC 2634	R	
Proveedor de servicios criptográficos en el sistema operativo del chip en tarjeta inteligente	Software CSP	R	
Formato de firma electrónica para formas electrónicas a largo plazo	RFC 3126	R	

8.2.4. Seguridad para desarrollo de sistemas

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En transición E = En Estudio F = Estudio futuro		
Firmas XML	Sintaxis y Procesamiento de firma XML (XMLsig) conforme definido por el W3C http://www.w3.org/TR/xmldsig-core/	R	
Cifra XML	Sintaxis y Procesamiento de Cifra XML (XMLenc) Conforme definido por el W3C http://www.w3.org/TR/xmlenc-core/	R	
Firma y cifra XML	Transformación de decodificación para firma XML conforme definido por el W3C http://www.w3.org/TR/xmlenc-decrypt	R	
Principales gestiones XML cuando un ambiente PKI es utilizado	XML – *Key Management Specification* (XKMS 2.0) (Especificaciones de Gestión de Llave XML) conforme definido por el W3C http://www.w3.org/TR/xkms2/	R	
Autenticación y autorización de acceso XML	SAML – conforme definido por el OASIS cuando un ambiente ICP es utilizado http://www.oasisopen.org/committees/security/index.sHTML	R	
Intermediación o Federación de Identidades	WS-Security 1.1 - conjunto de estándares para garantizar integridad y confidencialidad en mensajes SOAP. (http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-soapmessage-security-1.0.pdf). WS-Trust 1.3 – extensiones para el estándar WSSecurity, definiendo el uso de credenciales de seguridad y gestión de confianza distribuida. (http://docs.oasis-open.org/ws-sx/ws-trust/200512).	E	El componente anterior (SAML) podrá juntarse a este componente después de estudios.

8.2.5. Seguridad para servicios de red

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En transición E = En estudio F = Estudio futuro (http://www.ietf.org/rfc/rfc2251.txt).		
Directorio	LDAPv3 RFC 3377 LDAP v3 extensión para TLS RFC3377 (http://www.ietf.org/rfc/rfc3377.txt).	R	
DNS	Resolución no. 7 de 29/07/2002 – Comité Ejecutivo del Gobierno Electrónico Prácticas de Seguridad para Administradores de Redes Internet NIC BR Security Office http://www.nbso.nic.br/docs/seg-adm-redes/seg-admchklist.pdf Versión 1.2 16 de mayo de 2003 Securing an internet name server, CERT – ago/2002.	R	
Transferencia de archivos de forma segura	HTTPS RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt). Securing FTP with TLS, RFC 4217 http://www.faqs.org/rfcs/rfc4217.html y RFC 2246 http://www.faqs.org/rfcs/rfc2246.html	R E	
Mensaje instantáneo	RFC 2778 (http://www.ietf.org/rfc/rfc2778.txt), RFC 3261 (http://www.ietf.org/rfc/rfc3261.txt), RFC 3262 (http://www.ietf.org/rfc/rfc3262.txt), RFC 3263 (http://www.ietf.org/rfc/rfc3263.txt), RFC 3264 (http://www.ietf.org/rfc/rfc3264.txt) y RFC 3265 (http://www.ietf.org/rfc/rfc3265.txt).	E	
Sincronismo de tiempo	RFC 1305 IETF-*Network Time Protocol* – NTP *version* 3.0 (http://www.ietf.org/rfc/rfc1305.txt). RFC 2030 IETF- *Simple Network Time Protocol* - SNTP *version* 4.0 (http://www.ietf.org/rfc/rfc2030.txt).	R	
Sello de tiempo	RFC 3628 TSAs - *Policy Requirements for Time*-Stamping Authorities (http://www.ietf.org/rfc/rfc3628.txt), *Time-Stamp Protocol*, RFC 3161 ETSI TS101861 (*Time-Stamping Profile*) (http://www.ietf.org/rfc/rfc3161.txt)	R	

8.2.6. Seguridad para redes inalámbricas

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En transición E = En estudio F = Estudio futuro		
MAN[4] inalámbrico 802.16-2004[5] 802.16.2-2004[6] 802.16e[7] e 802.16f[8]	Utilizar PKM-EAP (*Privacy Key Management - Extensible Autentication Protocol*) com: • EAP – TLS ou TTLS; • AES (Advanced Encryption Standard). http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf.	E	
LAN inalámbrico 802.11	Utilizar la especificación WPA2 (Wi-Fi *Protect Access*).	R	

8.2.7. Seguridad para colecta, tratamiento y archivo de evidencias

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

[4] El 802.16 es definido por el IEEE como una interfaz tecnológica para redes de acceso inalámbrico metropolitanas o WMAN (Wireless Metropolitan Access Network).
[5] http://standards.ieee.org/getieee802/download/802.16-2004.pdf.
[6] http://standards.ieee.org/getieee802/download/802.16.2-2004.pdf.
[7] http://standards.ieee.org/getieee802/download/802.16e-2005.pdf.
[8] http://standards.ieee.org/getieee802/download/802.16f-2005.pdf.

8.2.8. Gestión de la seguridad de la información

Componente	Especificación	SIT	Observaciones
Tecnologías de la información – Técnicas de seguridad - Requerimientos	ISO 27001	R	
Tecnologías de la información – Técnicas de seguridad - Código de prácticas para la gestión de la seguridad de la información	ISO 27002	R	
Tecnologías de la información – Criterios de evaluación de Técnicas de seguridad para TI	ISO 15408	R	
Tecnología de la información – Guías para la gestión de la Seguridad TI – Directrices respecto al tipo de controles que deben ser implementados y deben ser especificados por una EC	ISO/IEC TR13335	R	

8.2.9. Infraestructura

Componente	Especificación	SIT	Observaciones
Infraestructura de Telecomunicaciones para Centros de Datos	TIA 942	R	

8.2.10. Usabilidad

Componente	Especificación	SIT	Observaciones
Metodología de usabilidad	ISO/TR 16982:2002: Ergonomics of human-system interaction-- Usability methods supporting human-centred design	R	
Guía de interfaces WWW para usuarios	ISO 9241-151:2008: Ergonomics of human-system interaction--Part 151: Guidance on World Wide Web user interfaces	R	
Guía de accesibilidad en software	ISO 9241-171:2008: Ergonomics of human-system interaction--Part 171: Guidance on software accessibility	R	
CIF para reportes de pruebas de usabilidad	ISO/IEC 25062:2006: Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Common Industry Format (CIF) for usability test reports	R	
Principios y requerimientos para dispositivos físicos de entrada	ISO 9241-400:2007: Ergonomics of human--system interaction -- Part 400: Principles and requirements for physical input devices	R	
Criterios de diseño para dispositivos físicos de entrada	ISO 9241-410:2008: Ergonomics of human-system interaction -- Part 410: Design criteria for physical input devices	R	
Interfaz de descripción de contenido multimedia	ISO/IEC 15938-9:2005: Information technology -- Multimedia content description interface -- Part 9: Profiles and levels	R	

9. ORGANIZACIÓN E INTERCAMBIO DE INFORMACIÓN

9.1. Políticas técnicas

1. Uso de XML para el intercambio de datos.

2. Uso de XML *Schema* y de UML(cuando sea el caso) para definición de los datos para intercambio.

3. Uso de XSL para transformación de datos.

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

5. Uso del estándar ISO 19115 para elaboración de metadatos usando como mínimo el perfil básico de metadatos para la gestión de información espacial recomendado por la IDEp

6. Uso del estándar ISO 19139 catálogo de metadatos para los metadatos en XML. La representación de los metadatos en la web a través de un sistema de transformación dinámica del XML en base a estilos, generalizando lo más posible la representación de los tags del árbol XML del metadato, para que el usuario pueda discriminar fácilmente la información que le hace falta en cada momento.

7. Uso de la Norma ISO 19128: “Geographic Information – Web Map Server Interface”, para los servicios Web Map Services Permite la superposición visual de información geográfica compleja y distribuida en diferentes tipos de servidores. Tiene establecidas tres tipos de peticiones:

    a. GetCapabilities: investiga las capacidades del servidor de mapas interrogado mediante un mensaje XML. El servidor le devuelve la información mediante otro mensaje XML.

    b. GetMap: conociendo las capacidades del servidor, requiere un mapa mediante un mensaje XML y el servidor interrogado devuelve un mapa en formato ráster (PNG, JPEG, GIF). Estos mapas pueden superponerse al definir colores transparentes.

    c. GetFeatureInfo: sobre el mapa devuelto se puede interrogar al servidor remoto sobre información asociada a algún elemento (que se puede seleccionar, por ejemplo, mediante un clic sobre un pixel del elemento). Tanto la pregunta como la respuesta se vuelven a realizar mediante mensajes XML.

8. Uso del estándar ISO1917 define representación de Información Geografica.

9. Uso de la Norma ISO 19119:2002 “Geographic Information- Services”

9.2. Especificaciones técnicas

GRUPO 1

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En transición E = En estudio F = Estudio futuro		
Lenguaje de Intercambio de datos	XML (Extensible Markup Language) como definido Por el W3C http://www.w3.org/XML	R	
Transformación de Datos	XSL (Extensible Stylesheet Language) como definido por el W3C http://www.w3.org/TR/xsl XSL Transformation (XSLT) como definido por el W3C http://www.w3.org/TR/xslt	R	
Definición de los datos para intercambio	XML Schema como definido por el W3C: - XML Schema Part 0: Primer http://www.w3.org/TR/2004/RECxmlschema-0-20041028/ - XML Schema Part 1: Structures http://www.w3.org/TR/xmlschema-1/structures - XML Schema Part 2: Datatypes http://www.w3.org/TR/xmlschema-2/datatypes	R	

	UML (Unified Modeling Language) como definido por el OMG http://www.omg.org/gettingstarted/specsandprods.htm/		
Descripción de Datos	RDF (Resource Description Framework) como definido por la W3C.	F	
Elementos de Metadatos para gestión de contenidos	ebXML(Electronic Business XML).	R	
	HL7(Health Level Seven).		
	Definir un catálogo de metadatos del estado.	E	
Perfil básico de metadatos geograficos IDEP	Perfil Basico de Metadatos IDEP v1.4 SE, por el Grupo de Trabajo Nº 2 IDEPI http://www.ccidep.gob.pe	E	
Datos Espaciales	http://www.opengeospatial.org/standards		
Definición de datos	Creación de un catálogo de Padrones de Datos.	E	

GRUPO 2

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En transición E = En estudio F = Estudio futuro		
Agricultura	AgXML http://www.agxml.org/	**R**	
Negocios	CXML http://www.cxml.org/	R	
	XAML	R	
	IATA http://www.iata.org/index.htm	R	
	TOGAF http://www.togaf.org/	R	
	OTA http://www.ota.com/index.html	R	
	XCBL http://www.xcbl.org/		
	UBL http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ubl		
	XBRL http://www.xbrl.org/Home/		
	BSML		
	Acord http://www.acord.org/home/home.aspx#		
	CATXML		
	XCAT		
Comercio	GCI http://xml.coverpages.org/gci.html	R	
	Rossetanet http://www.rosettanet.org/cms/sites/RosettaNet/		
	Bolero http://www.bolero.net/		
	EHD		
	VICS		
	HR-XML http://www.hr-xml.org/hr-xml/wms/hr-xml-1-org/index.php?language=2		

Componente	Especificación	SIT	Observaciones
Petróleo	PIDX http://www.pidx.org/	R	
Industria química	CIDX http://www.cidx.org/	R	
Salud	HL7 http://www.hl7.org/	R	
Industria marítima	SMDG http://www.smdg.org/	R	
Finanzas	SWIFT http://www.swift.com/	R	
Geografia	GML http://www.opengeospatial.org/standards/gml	R	
	Opentrans	R	
Construcción	E-construct	R	
Comercio electrónico	UNeDocs - Naciones Unidas http://www.unece.org/etrades/unedocs/	R	

GRUPO 3:

APLICACIONES

SUNAT:

1. Generación de RUC:
   i. Web Services:
      1. http://wsgr.sunat.gob.pe:8089/ol-ti-etinscripcionsunarp/GeneraRucService
   ii. Descripción: Genera RUC en SUNAT, previa verificación de datos recibidos de SUNARP
   iii. Requisitos:

RENIEC:

2. Validación de DNIs:
   i. Web Services:
      1. http://wservices.reniec.gob.pe/wsauth/WSAuthentication
      2. http://wservices.reniec.gob.pe/wsauth/WSDataVerification
   ii. Descripción: Dado el número de DNI, devuelve apellidos y nombres.
   iii. Requisitos:

SUNARP:

3. Recepción de datos de CNL:
   i. Web Services:
      1. http://enlinea.sunarp.gob.pe/webapp/extranet/services/SunarpServiceProvider?wsdl
   ii. Descripción: Recibe datos de notarías que prestan servicios de constitución de empresas en línea.
   iii. Requisitos:

PCM:

4. Generación de Código Único de Operación - CUO:
   i. Web Services:

1. http://190.81.122.150/PortalServicios/WS_PSC
2. WSDL: http://190.81.122.150/PortalServicios/WS_PSC_NOTARIOS.wsdl

ii. Descripción: Genera códigos de operación para trámites que dependen de 2 o más instituciones.
iii. Requisitos:

9.3. XML y Middleware

No todos los sistemas necesitan tener capacidad de comunicarse directamente en XML, en algunos casos es apropiada la utilización de un middleware.

9.4. ebXML

ebXML (Electronic Business eXtensible Markup Language) es un framework que establece las condiciones para hacer comercio electrónico entre las empresas. Proporciona una serie de especificaciones, que deberán ser respetadas por el software y los servicios desarrollados sobre ellas. Se basa en la experiencia acumulada con el EDI (Electronic Data Interchange), pero también saca provecho de nuevas tecnologías que usa, como la flexibilidad de XML y la ubicuidad de Internet.

ebXML es fruto del trabajo conjunto por parte de OASIS (Organization for the Advancement of Structured Information Standards), encargada de la parte tecnológica, y UN/CEFACT (United Nation's Centre for Trade Facilitation and Electronic Business), que aporta los conocimientos sobre el comercio. Las especificaciones se realizaron en 18 meses y colaboró gente de todo el mundo, siendo la primera versión liberada de mayo del 2001.

9.5. HL7

HL7 (Health Level Seven) es un conjunto de estándares para el intercambio electrónico de información médica. Level Seven hace referencia al nivel siete (aplicación) del modelo OSI. Los estándares HL7 son desarrollados por la organización ANSI del mismo nombre.

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En transición E = En estudio F = Estudio futuro		
Agricultura	AgXML http://www.agxml.org/	**R**	
Negocios	CXML http://www.cxml.org/	R	
	XAML	R	
	IATA http://www.iata.org/index.htm	R	
	TOGAF http://www.togaf.org/	R	

Componente	Especificación	SIT	Observaciones
	OTA http://www.ota.com/index.html	R	
	XCBL http://www.xcbl.org/		
	UBL http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ubl		
	XBRL http://www.xbrl.org/Home/		
	BSML		
	Acord http://www.acord.org/home/home.aspx#		
	CATXML		
	XCAT		
Comercio	GCI http://xml.coverpages.org/gci.html	R	
	Rossetanet http://www.rosettanet.org/cms/sites/RosettaNet/		
	Bolero http://www.bolero.net/		
	EHD		
	VICS		
	HR-XML http://www.hr-xml.org/hr-xml/wms/hr-xml-1-org/index.php?language=2		
Petróleo	PIDX http://www.pidx.org/	R	
Industria química	CIDX http://www.cidx.org/	R	
Salud	HL7 http://www.hl7.org/	R	
Industria marítima	SMDG http://www.smdg.org/	R	
Finanzas	SWIFT http://www.swift.com/	R	
Geografia	GML http://www.opengeospatial.org/standards/gml	R	
	Opentrans	R	
Construcción	E-construct	R	
Comercio electrónico	UNeDocs - Naciones Unidas http://www.unece.org/etrades/unedocs/	R	

9.6. Especificaciones del Grupo Metadatos IDEP

Perfil Básico de Metadatos IDEP

Componente	Especificación	SIT	Observaciones
	A = Adoptado R = Recomendado T = En transición E = En estudio F = Estudio futuro		
Identificación	Titulo	A	
	Fecha	A	
	Tipo de Fecha	R	
	Forma de Presentación	A	
	Resumen	A	
	Propósito	R	
	Estado	R	

Componente	Especificación	SIT	Observaciones
	Punto de Contacto	R	
	Palabras Claves	A	
	Tipo der epresentación Espacial	R	
	Escala	A	
	Tema o Categoría	R	
	Extensión	A	
Restricciones	Limitaciones de Uso	R	
	Limitaciones de Acceso	R	
Mantenimiento	Frecuencia de Mantenimiento y Actualización	R	
	Fecha de actualización	A	
Distribución	Recurso en línea Web	R	
	Recurso en línea WMS	R	
	Nombre	T	
	Versión	T	
Sistema de referencia	Código	A	
	Nombre	R	
Calidad	Nivel Jerárquico	R	
	Declaración	R	
Representación Espacial	Nivel de Topología	E	
	Tipo de Objeto geométrico	E	
Metadato	Identificador	A	
	Norma y version	A	
	Idioma	R	
	Juego de Caracteres	R	
	Fecha de creación	R	
	Autor del Metadato	A	

10. MEDIOS DE ACCESO

10.1. Políticas Técnicas

Las políticas técnicas para permitir el acceso a los servicios electrónicos del Gobierno dirigidas a la sociedad en general, incluyendo a ciudadanos, empresas privadas, esferas y Poderes de Gobierno, servidores públicos y otras instituciones, son:

10.1.1. Los servicios que presta el Gobierno mediante sistemas informáticos deben ser concebidos dentro del respeto a la normatividad vigente, facilitando el acceso a los mismos, particularmente a aquellos ciudadanos con necesidades especiales y a aquellos cuyo riesgo de exclusión social o digital sea elevado. Los servicios de Gobierno Electrónico deberían incluso extenderse a aquellos sectores de población que no puede tener acceso directo a los mismos por medio de los dispositivos previstos.

10.1.2. En relación a los sistemas informáticos orientados a la prestación de servicios de Gobierno Electrónico:

- Deberán proyectarse para brindar a los usuarios, servicios de Gobierno Electrónico por intermedio de diversos medios de acceso;
- Se utilizará la Internet como medio de comunicación y las estaciones de trabajo o computadoras personales como medios de acceso, facilitándose la disponibilidad de la información con el uso de tecnologías y protocolos de comunicación *web* basados en navegadores (*browsers*);
- Al valerse de otros dispositivos de acceso, como por ejemplo teléfonos móviles, televisión digital y tarjetas inteligentes (*smart cards*), podrá usarse otras interfaces además de los navegadores *web*;
- Deben contemplar la sustitución gradual del uso del "login/contraseña" por la autenticación de usuarios con la utilización de certificados digitales, conforme a la normatividad establecida para la IOFE (Infraestructura Oficial de Firma Electrónica);
- Los nuevos servicios deberán crearse ya incorporando soporte a la autenticación de usuarios por medio de certificados digitales de la IOFE;
- En esta versión del documento de definición de lineamientos y mecanismos de interoperabilidad que se requiere en el D.L. 1029, se trata de los siguientes medios de acceso:
    - Estaciones de trabajo;
    - Tarjetas inteligentes, *tokens* y otras tarjetas;
- Otros mecanismos de acceso, como teléfonos móviles, *hand-helds* y televisión digital serán objeto de estudio futuro para la determinación de los estándares a ser aceptados por el Gobierno.

10.1.3. Los sistemas de informática del Gobierno, implementados para dar soporte a un determinado dispositivo de acceso, deben seguir, obligatoriamente, las especificaciones señaladas en este documento para el dispositivo correspondiente.

10.1.4. 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.

10.1.5. El desarrollo de los servicios de Gobierno Electrónico debe orientarse de manera tal que permitan el dar atención a aquellos usuarios sin acceso a las tecnologías más recientes disponibles en el mercado. Por otra parte, también se debe considerar la necesidad de atender a aquellos usuarios con necesidades especiales, lo que involucrará la utilización de recursos más sofisticados y de uso específico. En particular, respecto de las facilidades de acceso a Internet para personas con discapacidad y a la adecuación de las cabinas públicas que brindan este servicio, se seguirá lo señalado en la Ley 28530 y su Reglamento.

10.1.6. Al utilizarse la Internet como medio de comunicación, los sistemas informáticos del Gobierno deben contemplar el que se pueda acceder a una cantidad máxima de información mediante aquellos navegadores que cumplan con el estándar mínimo requerido según las Especificaciones Técnicas para Estaciones de Trabajo que se observan a continuación. Se recomienda que cualquier servicio de Gobierno Electrónico especifique en su página web inicial, las Versiones mínimas de navegadores que soportan las funcionalidades requeridas por el servicio asociado. En relación al estándar mínimo referido arriba, pueden considerarse las excepciones que involucren cuestiones de seguridad en el trato de la información.

10.1.7. Cuando la Internet sea utilizada como medio de comunicación, si no hay alternativa técnicamente posible, podrá utilizarse middleware o plug-ins adicionales para optimizar la funcionalidad del navegador en las estaciones de trabajo. En este caso, ese software adicional deberá ofrecerse sin el pago de tasa por licencia, debiendo cumplir las especificaciones técnicas correspondientes señaladas en el presente documento. Además, el mismo debería mantenerse en un repositorio seguro del organismo gubernamental responsable de la aplicación y estar firmado digitalmente con un certificado para firma de código, de manera tal que se garantice la disponibilidad y la autenticidad de la aplicación y la integridad del código.

10.1.8. Los servicios de Gobierno Electrónico deben concebirse de manera que garanticen a los usuarios la autenticidad de su contenido con la utilización de certificados digitales para servidores web, conforme a los estándares señalados para la IOFE. En ese sentido, todos los sitios web deberán, de modo obligatorio, utilizar “https” en vez de “http”.

10.1.9. La necesidad de la sociedad aunada a la voluntad del Gobierno de desarrollar e implementar servicios electrónicos posibilitará la definición de las especificaciones técnicas necesarias para los medios de acceso disponibles. Podrá usarse técnicas de administración de contenidos y tecnologías que posibiliten la adaptación de los dispositivos para soportar los servicios de Gobierno Electrónico, de manera tal que se facilite el acceso por medio del estándar mínimo de navegador web establecido. Se

facilitará así el uso de quioscos públicos multiservicios y de Centros de Acceso Ciudadano.

10.1.10. Los sistemas informáticos del Gobierno deben considerar cuando sea necesario, además de técnica y económicamente viable, el desarrollo de adaptadores que posibiliten el acceso a la información de los servicios electrónicos en la web dentro de una diversidad de ambientes, presentando tiempos de respuesta aceptables y costos reducidos.

Estos adaptadores pueden utilizarse para poner en cola, convertir y reformatear dinámicamente el contenido *web*, de modo que se adapte 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, posibilitando el que se señalen preferencias del usuario y parámetros de red y de dispositivos de acceso.

Esos adaptadores también podrán utilizarse como una forma alternativa de posibilitar el acceso a minorías lingüísticas o con discapacidades como la deficiencia visual (utilización de traductores de textos, fuentes y gráficos de tamaño grande, audio, etc.).

10.1.11. Se considerará preferencialmente aquellos tipos de archivo que tienen como estándar de empaquetamiento el “xml”, de forma que se facilite la interoperabilidad entre los servicios de Gobierno Electrónico.

10.1.12. 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 origen, versión, fecha de publicación y formato. Por fecha de publicación se entiende aquella en la que el documento fue publicado en el diario oficial El Peruano, para los casos en que esta medida se exija, o la fecha de la publicación en el sitio web, para los otros casos. Otra información sobre el documento, tal como, autor, redactor, emisor u otra de relevancia para su identificación precisa, deberá constar en el campo de propiedades del propio documento.

10.2. Especificaciones Técnicas para Estaciones de Trabajo

Para la elaboración de documentos o trabajos a ser creados en colaboración por más de una persona y/u organismo, pueden utilizarse los formatos previstos en la Tabla 10.

Para la construcción de la versión final de documentos, a ser enviada a otros organismos o incluso archivada digitalmente, se recomienda la utilización del formato PDF/A.

Aquellos documentos que necesiten de garantía de integridad y/o autoría deben ser firmados digitalmente por su autor utilizando certificados digitales de la IOFE, siendo recomendable que se encuentren en formato PDF/A.

La mención a los productos que generan los formatos de archivos referidos en la Tabla 10 tiene como objetivo único la identificación de una **referencia mínima** a partir de la cual los servicios de Gobierno Electrónico habrán de intercambiar información, de manera tal que queden aptos para 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 R = Recomendado T = En Transición E = En Estudio F = Estudio Futuro		
Conjunto de caracteres y alfabetos	UNICODE estándar versión 4.0, latin-1, UTF8, ISBN 0-321-18578-1.	**R**	
Formato de intercambio de hipertexto	HTML versión 4.01 (.html o .htm), generado conforme especificaciones del W3C[15]	**A**	
	XHTML versiones 1.0 o 1.1 (.xhtml), generado conforme especificaciones del W3C[16]	**A**	
	XML versiones 1.0 o 1.1 (.xml), generado conforme especificaciones del W3C[17]	**A**	
	SHTML (.shtml).	**R**	
	MHTML (.mhtl o .mht)[18].	**R**	
Archivos del tipo documento	XML versiones 1.0 o 1.1 (.xml), o con formato (opcional) XSL (.xsl), generado conforme especificaciones del W3C[19].	**R**	
	Open Document (.odt), generado conforme especificaciones del estándar ISO/IEC 26300[20].	**R**	
	OpenOffice.org XML (.sxw), generado en el formato del OpenOffice version 1.0.	**R**	
	Rich Text Format (.rtf).	**R**	
	PDF (.pdf) generado en formato versión 1.3.	**R**	

15 HTML 4.01 Specification – W3C Recommendation 24 December 1999. Disponible en: http://www.w3.org/TR/html4/.
16 *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/.
17 *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/.
18 (*Mime Enscapsulation of Aggregate HTML Documents*).
Disponible en : http://tools.ietf.org/html/rfc2557

19 *Extensible Stylesheet Language (XSL) Version 1.0 – W3C Recommendation 15 October 2001*. Disponible en: http://www.w3.org/TR/xsl/.
20 *Open Document Format for Office Applications (OpenDocument)* v1.0 – estándar ISO/IEC 26300. Disponible en: http://www.iso.org/.

Componente	Especificación	SIT	Observaciones
	PDF versión abierta PDF/A[21].	**R**	
	Texto puro (.txt).	**A**	
	HTML versión 4.01 (.html ou .htm), generado conforme especificaciones del W3C.	**R**	
	Office Open XML , formato de documento electrónico ISO/IEC DIS 29500	**R**	
	Microsoft Word document (.doc), generado en el formato del MS Office versión 2000.	**R**	
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.	**R**	
	Planilla MS Excel (.xls), generado en el formato del MS Office versión 2000.	**R**	
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.	**R**	
	HTML (.html o .htm), generado conforme especificaciones del W3C.	**R**	
	Presentación MS Power Point (.ppt), generado en el formato del MS Office versión 2000.	**R**	
Archivos del tipo “banco de datos” para estaciones de trabajo	XML versiones 1.0 o 1.1 (.xml)	**R**	En las opciones texto plano (txt) y csv, 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 versión 2000.	**R**	
	PDF versión abierta PDF/A[21].	**R**	
Intercambio de informaciones gráficas e	PNG (.png), generado conforme especificaciones del W3C[22]– ISO/IEC 15948:2003 (E).	**R**	
	TIFF (.tif)[23]	**A**	

imágenes estáticas	SVG (.svg), generado conforme especificaciones del W3C[24].	**R**	
	JPEG File Interchange Format (.jpeg, .jpg o .jfif)[25]	**A**	

21 *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/.
22 *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/
23 Tagged Image File Format (Adobe Systems).
24 *Scalable Vector Graphics (SVG) 1.1 Specification. W3C Recommendation 14 January 2003. Disponible en:* http://www.w3.org/TR/2003/REC-SVG11-20030114/.
25 *JPEG File Interchange Format (version 1.02) 1 September 1992. Disponible en:* http://www.jpeg.org/public/jfif.pdf y http://www.w3.org/Graphics/JPEG/itu-t81.pdf

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.	**R**	
	XCF (.xcf), generado en el formato del GIMP versión 1.0 o superior.	**R**	
	BMP (.bmp).	**A**	
	GIF (.gif), generado conforme las especificaciones GIF87a y GIF89a[26]	**A**	
	Imagen Corel Photo-Paint (.cpt), generado en el formato de la suite Corel Draw hasta versión 7.	**R**	
	|Imagen Photoshop (.psd), generado en el formato del Adobe Photoshop versión 4.	**R**	
	WSQ (.wsq), generado conforme a ANSI/NIST-ITL 1-2000, formato de datos para el intercambio de imágenes de huellas dactilares, rostro, cicatrices y tatuajes	**R**	
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.	**R**	
	Gráfico Corel Draw (.cdr), generado en el formato hasta versión 7.	**R**	
	MSX (.msx), generado en el formato de la suite Corel Draw hasta versión 7.	**R**	
	Gráfico MS Visio (.vss o .vsd), generados en el formato hasta versión 2000.	**R**	

	Windows Metafile (.wmf).	**R**	
Especificación de estándares de animación	SVG (.svg), generado conforme especificaciones del W3C.	**R**	
	GIF (.gif), gerado conforme a especificación GIF89a.	**A**	
	Shockwave Flash (.swf), generado en formato de Macromedia Flash versión 4, de Macromedia Shockwave version 1.	**R**	
Archivos del tipo audio y del tipo video	.mpg	**A**	
	Audio y video MPEG-4, Part 14 (.mp4)[27]	**A**	
	MIDI (.mid)[28]	**A**	
	Audio Ogg Vorbis I (.ogg)[29]	**R**	
	Audio-Video Interleaved (.avi), con codificación Xvid.	**A**	
	Audio-Video Interleaved (.avi), con codificación divX.	**A**	
	Audio MPEG-1, Audio Layer 3 (.mp3)[30]	**A**	

26 Graphics Interchange Format (CompuServe/America Online, Inc.). http://www.w3.org/Graphics/GIF/spec-gif89a.txt

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

28 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.shtm.

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

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

Componente	Especificación	SIT	Observaciones
	Real Media (.rm o .rmm), generado en el formato de los aplicativos Real Audio Media Player, versión 8.	**A**	
	Real Audio (.ra o .ram), generado en el formato de los aplicativos Real Audio Media Player, versión 8.	**A**	
	WAVE (.wav)	**A**	
	Shockwave Flash (.swf), generado en el formato del Macromedia Flash, hasta versión 4 o por el Macromedia Shockwave, versión 1.	**R**	
	Windows Media Video (.wmv), generado en el formato del Windows Media Player, versión 6.4.	**A**	
	Windows Media Audio (.wma), generado en el formato del Windows Media Player, versión 6.4.	**A**	
	QuickTime (.mov), generado en el formato del Apple Quicktime, versión 6.	**A**	
	QuickTime (.qt), generado en el formato del Apple Quicktime, versión 6.	**R**	

Compresión de archivos de uso general	ZIP (.zip).	**A**	
	RAR (.rar).	**R**	
	GNU ZIP (.gz).	**R**	
	Paquete TAR (.tar).	**R**	
	Paquete TAR compactado (.tgz o .tar.gz).	**R**	
	BZIP2 (.bz2).	**R**	
	Paquete TAR compactado con BZIP2 (.tar.bz2).	**R**	
	MS Cabinet (.cab).	**R**	
Informaciones georreferenciadas – estándares de archivos para intercambio entre estaciones de trabajo	GML versión 1.0 o superior[31].	**F**	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[32].	**F**	Señalado para estructuras vectoriales limitadas a líneas, puntos y polígonos, cuyos atributos textuales no sobrepasen 256 caracteres. Puede almacenar también las dimensiones M y Z.

31 *Geography Markup Language*. Especificaciones disponibles en: http://www.opengeospatial.org/standards.
32 *ESRI Shapefile Technical Description*. Disponible en: http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf.

Componente	Especificación	SIT	Observaciones
	GeoTIFF[33].	**F**	Señalado para estructuras matriciales limitadas a matrices de pixel.
	SFS.	**F**	
Programación Extendida (Plugins)	Tema para consideración futura.	**F**	

33 *GeoTIFF Format Especification*. Disponible en: http://remotesensing.org/geotiff/geotiff.html.

10.3. Especificaciones Técnicas para tokens, Tarjetas Inteligentes y Tarjetas en General

Las especificaciones sobre tarjetas inteligentes y *tokens* se basan fundamentalmente en la familia de estándares ISO/IEC (7816 partes 1 a 6).

Los dispositivos criptográficos a utilizarse para la firma digital dentro de la IOFE, según los alcances de lo que señala la Ley de Firmas y Certificados Digitales y su Reglamento, se guiarán además de por estas normas, por lo referido en las Guías de Acreditación emitidas por la Autoridad Administrativa Competente (INDECOPI). Así, serán pasibles de acreditación según lo señalado en las guías pertinentes, las entidades de certificación, las de registro o verificación, el software de firma digital, además de las entidades prestadoras de servicios de valor añadido como el sellado de tiempo, entre otros. Según allí se señala, los medios que generan y almacenan el material criptográfico (certificados digitales y claves), además de los sistemas, software y equipos necesarios para la realización de la certificación digital (como los HSM), deberán obedecer a estándares 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.

Es importante observar que el acceso a los datos almacenados en una determinada tarjeta inteligente o *token* no deberá limitarse bajo ningún tipo de licenciamiento de software que prohíba su lectura a excepción del que pertenece a aquella tarjeta inteligente o *token*.

Se considera también el estándar 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). Se incluyó además normas ISO correspondientes a tarjetas magnéticas y ópticas.

Para cada estándar se señalan las versiones vigentes (año de publicación a la fecha).

Para versiones futuras de este documento se deberán considerar los estándares de otras tarjetas utilizadas o por utilizarse por los organismos de Gobierno. De verificarse un uso intensivo, será evaluada su inclusión. De igual manera, serán evaluados los estándares orientados a la comunidad europea.

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

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

Definición de datos	Tarjetas de identificación -- Tarjetas de Circuito(s) Integrado(s) ISO/IEC 7816-6:2004 Parte 6: Elementos de datos para el intercambio intersectorial.	**A**	Todos	Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange.
	Tarjetas de identificación -- Identificación de los emisores ISO/IEC 7812-1:2006 Parte 1: Sistema de Numeración.	**R**	Todos	Identification cards -- Identification of issuers -- Part 1: Numbering system
	Tarjetas de transacciones financieras Mensajes entre la tarjeta de circuito integrado y el dispositivo de aceptación de la tarjeta ISO 9992-2:1998 Parte 2: Funciones, mensajes (comandos y respuestas), elementos y estructuras de datos.	**F**	Tarjetas financieras	Financial transaction cards -- Messages between the integrated circuit card and the card accepting device -- Part 2: Functions, messages (commands and responses), data elements and structures.
	Sistemas de tarjeta de identificación. Monedero electrónico intersectorial – BS EN 1546-3:1999 Parte 3: Elementos e intercambio de datos. BS EN 1546-4:1999 Parte 4: Objetos de datos.	**F**	Todos	Identification card systems. Inter-sector electronic purse. Data elements and interchanges. Identification card systems. Inter-sector electronic purse. Data objects La actual edición de este estándar británico es base del trabajo del CEN/TC224/WG10.
	Tecnología de la información – Formatos de intercambio de biometría ISO/IEC 19794-2:2005 Parte 2: Datos de minucias de huella dactilar. ISO/IEC 19794-2:2005 Parte 2: Formato de imagen del rostro para el intercambio de datos	**R** **R**	Biometría en tarjetas inteligentes	Information technology – Biometric data interchange formats – Part 2: Finger minutiae data. Information technology – Biometric data interchange formats – Part 5: Face Image Format for Data Interchange

Aplicaciones, incluyendo multiaplicaciones	Tarjetas de identificación – Tarjetas de circuito integrado ISO/IEC 7816-4:2005 Parte 4: Comandos intersectoriales para intercambio. ISO/IEC 7816-5:2004 Parte 5: Sistema de numeración y tramitación de registro para identificadores de aplicación. ISO/IEC 7816-7:1999 Parte 7: Comandos intersectoriales para Structured Card Query Language (SCQL); ISO/IEC 7816-11:2004 Parte 11: Estructura para el uso dinámico de aplicaciones múltiples en tarjetas de circuitos integrados. ISO/IEC 7816-15:2004 Parte 15: Aplicación de información criptográfica. (con sus correcciones y adendas)	 **A** **A** **R** **R** **F**	Tarjetas de Circuito(s) Integrado(s) con contactos.	 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange Identification cards -- Integrated circuit cards -- Part 5: Registration of application providers Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL) Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application Se señalan los años de publicación de las versiones vigentes. Existen disponibles adendas y correcciones en el web site de ISO (http://www.iso.org). Partes 4 y 5 requeridas en Anexo 11 de la Guía de Acreditación de Entidades de Certificación EC de la IOFE. La Parte 15 da continuidad al estándar RSA PKCS#15 mencionado en el Anexo 11 de la Guía de Acreditación de Entidades de Certificación EC de la IOFE. en lo que se refiere a estructuras de archivos para aplicaciones criptográficas en tarjetas inteligentes.

Tarjetas de identificación ISO/IEC 7813:2006 Tarjetas de transacciones financieras.	**R**	Tarjetas financieras.	Information technology -- Identification cards -- Financial transaction cards
Tarjetas de identificación-- Identificación de los emisores ISO/IEC 7812-2:2007 Parte 2: Procedimientos de aplicación y registro.	**R**	Todos	Identification cards -- Identification of issuers -- Part 2: Application and registration procedures
Sistemas de tarjeta de identificación BS EN 1332-1:1999 Interfaz hombre/máquina – Parte 1: Principios de proyecto para interfaz de usuario BS EN 1332-4:1999 Interfaz hombre/máquina – Parte 4: Codificación de exigencias de usuario para personas con necesidades especiales.	**R**	Todos	Identification card systems. Man-machine interface. Design principles for the user interface Identification card systems. Man-machine interface. Coding of user requirements for people with special needs Estándar británico.

Componente	Especificación	SIT	Aplicable a	Observaciones
Eléctrico	Tarjetas de identificación Tarjetas de circuito(s) Integrado(s) con contactos ISO/IEC 7816-10:1999 Parte 10: Señales electrónicas y respuesta a reinicio de tarjetas síncronas. ISO/IEC 7816-12:2005 Parte 12: Interfaz USB.	**R**	Tarjetas de circuito(s) integrado(s) con contactos.	Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards Esta parte se encuentra en revisión por ISO. Identification cards - Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures

	Tarjetas de identificación – Tarjetas de circuito(s) Integrado(s) sin contacto (CICC) – Tarjetas de Proximidad ISO/IEC 14443-2:2001 Parte 2: Interfaz de potencia y señal de frecuencia de radio.	**R**	Tarjetas de circuito integrado de proximidad sin contacto.	Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 2: Radio frequency power and signal interface Esta parte define la interfaz de frecuencia de radio, y contiene dos técnicas de modulación (Tipos A y B) para la comunicación de datos entre tarjeta y terminal. Se señala la versión vigente, aunque se encuentra en revisión por ISO.
	Tarjetas de identificación -- Tarjetas de circuito(s) integrado(s) sin contacto (CICC) -- Tarjetas de Acoplamiento Cercano ISO/IEC 10536-3:1996 Parte 3: Procesamiento de señales electrónicas y reinicialización.	**F**	Tarjetas de circuito(s) integrado(s) de acoplamiento cercano sin contacto.	Identification cards -- Contactless integrated circuit(s) cards -- Part 3: Electronic signals and reset procedures Se señala la versión vigente, aunque se encuentra en revisión por ISO.
	Tarjetas de identificación -- Tarjetas de circuito(s) integrado(s) sin contacto (CICC) -- Tarjetas de Vecindad ISO/IEC 15693-2:2006 Parte 2: Interfaz aérea e inicialización.	**R**	Tarjetas de circuito(s) integrado(s) de vecindad sin contacto.	Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 2: Air interface and initialization

Componente	Especificación	SIT	Aplicable a	Observaciones
Protocolos de Comunicación	Tarjetas de identificación – Tarjetas de circuito integrado con contactos ISO/IEC 7816-3:2006 Parte 3: Protocolos de señales y transmisiones electrónicas.	**R**	Tarjetas de circuito(s) integrado(s) con contactos.	Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols Señalado en Anexo 11 de la Guía de Acreditación de Entidades de Certificación EC de la IOFE.

	Tarjetas de identificación – Tarjetas de circuito(s) Integrado(s) sin contacto (CICC) – Tarjetas de Proximidad ISO/IEC 14443-3:2001 Parte 3: Inicialización y anticolisión. ISO/IEC 14443-4:2008 Parte 4: Protocolos de transmisión.	**R**	Tarjetas de circuito(s) integrado(s) de proximidad sin contacto.	Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and anticollision Los procedimientos de anticolisión son métodos utilizados para identificar y seleccionar una tarjeta cuando varias tarjetas estén activas dentro del campo RF del terminal. La Parte 3 tiene diversas adendas e ingresará a revisión por ISO. Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 4: Transmission protocol La Parte 4 contiene informaciones de alto nivel (nivel de mensaje) de protocolo de transmisión de datos, equivalentes al protocolo T=1 del ISO/IEC 7816, y es un puente sobre dicho estándar. El ISO/IEC 14443-4 incluye un procedimiento de inicialización de protocolo para tarjetas Tipo A.
	Tarjetas de identificación -- Tarjetas de circuito(s) integrado(s) sin contacto (CICC) -- Tarjetas de Vecindad ISO/IEC 15693-3:2001 Parte 3: Protocolo de anticolisión y transmisión.	**R**	Tarjetas de circuito integrado de proximidad sin contacto.	Identification cards - Contactless integrated circuit(s) cards - Vicinity cards -- Part 3: Anticollision and transmission protocol Se señala la versión vigente, aunque será revisada por ISO.

Mensajes originados por tarjetas de transacciones financieras ISO 8583-1:2003 Parte 1: Mensajes, elementos de datos y valores de código. ISO 8583-2:1998 Parte 2: Procedimientos de solicitud y registro para códigos de identificación de instituciones. ISO 8583-3:2003 Parte 3: Procedimientos de mantenimiento para mensajes, elementos de datos y valores de código.	**F**	Tarjetas financieras.	Financial transaction card originated messages -- Interchange message specifications -- Part 1: Messages, data elements and code values Financial transaction card originated messages -- Interchange message specifications -- Part 2: Application and registration procedures for Institution Identification Codes (IIC) Financial transaction card originated messages -- Interchange message specifications -- Part 3: Maintenance procedures for messages, data elements and code values Las versiones señaladas de las Partes 2 y 3 se encuentran en revisión periódica por ISO.
Tarjetas de transacciones financieras -- Mensajes entre la tarjeta de circuito integrado y el dispositivo de aceptación de la tarjeta. ISO 9992-1:1990 Parte 1: Conceptos y estructuras ISO 9992-2:1998 Parte 2: Funciones, mensajes (comandos y respuestas), elementos y estructuras de datos.	**F**	Tarjetas financieras.	Financial transaction cards -- Messages between the integrated circuit card and the card accepting device -- Part 2: Functions, messages (commands and responses), data elements and structures. Financial transaction cards -- Messages between the integrated circuit card and the card accepting device -- Part 1: Concepts and structures

Componente	Especificación	SIT	Aplicable a	Observaciones
Estándares de Características Físicas. Cubren las dimensiones de la tarjeta además de la ubicación de los elementos para el almacenamiento de datos.	Características físicas -- Tarjetas de identificación ISO/IEC 7810:2003	**R**	Todas las tarjetas de contacto y combinación.	Identification cards -- Physical characteristics Todas las tarjetas deben seguir el formato ID-1, según se define en ISO/IEC 7810, para asegurar que puedan ser leídas en lectoras estándar. Este estándar será revisado por ISO.
	Tarjeta Magnética ISO/IEC 7811-2:2001 Parte 2: Banda magnética – Baja coercitividad.	**R**	Tarjetas con banda magnética.	Identification cards -- Recording technique -- Part 2: Magnetic stripe -- Low coercivity Define las propiedades, ubicación y codificación (coding) de la banda magnética de la tarjeta.

	Tarjeta de memoria óptica ISO/IEC 11693:2005 ISO/IEC 11694-1:2005 ISO/IEC 11694-2:2005 ISO/IEC 11694-3:2008	**F**	Tarjetas ópticas	Identification cards -- Optical memory cards -- General characteristics Estándar a ser revisado por ISO. Identification cards -- Optical memory cards -- Linear recording method -- Part 1: Physical characteristics Identification cards -- Optical memory cards -- Linear recording method -- Part 2: Dimensions and location of the accessible optical area Identification cards -- Optical memory cards -- Linear recording method -- Part 3: Optical properties and characteristics Serie de estándares que describe los parámetros para las tarjetas de memoria óptica y su uso para el almacenamiento e intercambio de datos. Ambos reconocen la existencia de diferentes métodos de grabación y lectura en tarjetas con memoria óptica Estas tarjetas soportan el almacenamiento de varios megabytes. Las Partes 4, 5 y 6 del ISO/IEC 11694 cubren aspectos de datos y biometría en tarjetas de memoria óptica.

	Tarjetas de identificación ISO/IEC 7816-1:1998 Parte 1: Características físicas Tarjetas de identificación ISO/IEC 7816-2:2007 Tarjetas de circuito(s) integrado(s) con contactos Parte 2: Dimensiones y ubicación de los contactos.	**A**	Tarjetas de circuito(s) integrado(s) con contactos.	Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics Esta parte suplementa la norma ISO/IEC 7810, estableciendo las características físicas particulares de las tarjetas de CI con contactos. Señalados en Anexo 11 de la Guía de Acreditación de Entidades de Certificación EC de la IOFE.
	Tarjetas de identificación Tarjetas de circuito(s) integrado(s) sin contactos – Tarjetas de proximidad ISO/IEC 14443-1:2008 Parte 1: Características físicas.	**R**	Tarjetas de circuito integrado de proximidad sin contacto.	Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics Esta parte suplementa las características físicas definidas en el ISO/IEC 7810.
	Tarjetas de identificación – Tarjetas de circuito(s) integrado(s) sin contactos – Tarjetas de proximidad ISO/IEC 15693-1:2000 Parte 1: Características físicas.	**R**	Tarjetas de circuito(s) integrado(s) de vecindad sin contacto.	Identification cards -- Contactless integrated circuit(s) cards -- Vicinity cards -- Part 1: Physical characteristics Esta parte suplementa las características físicas definidas en el ISO/IEC 7810.

Componente	Especificación	SIT	Aplicable a	Observaciones
	Tarjetas de identificación – Tarjetas de circuito(s) integrado(s) sin contacto ISO/IEC 10536-1:2000 Parte 1: Características físicas ISO/IEC 10536-2:1995 Parte 2: Dimensiones y ubicación de las áreas de acoplamiento.	**F**	Tarjetas de circuito(s) integrado(s) de acoplamiento cercano sin contacto.	Identification cards -- Contactless integrated circuit(s) cards -- Close-coupled cards -- Part 1: Physical characteristics Identification cards -- Contactless integrated circuit(s) cards -- Part 2: Dimensions and location of coupling areas Esta parte suplementa las características físicas definidas en el ISO/IEC 7810.

	Sistemas de Tarjetas de identificación -- Interfaz hombre/máquina -- Identificadores táctiles. BS EN 1332-2 Parte 2: Dimensiones y ubicación -un identificador táctil para tarjetas ID-1.	**F**	Para identificar el sentido en el que se introducirá la tarjeta en el lector, un identificador táctil ayudará a quienes sufren de deficiencias visuales.	Identification card systems. Man-machine interface. Dimensions and location of a tactile identifier for ID-1 cards Según el estándar británico, Identificadores táctiles del tipo 'notch' ('relieve') deberían solicitarse a los fabricantes o a quienes personalicen las tarjetas.
Seguridad	Tarjetas de identificación -- Tarjetas de circuito(s) integrado(s): ISO/IEC 7816-8:2004 Parte 8: Comandos de seguridad intersectoriales ISO/ IEC 7816-9:2004 Parte 9: Comandos adicionales intersectoriales y atributos de Seguridad. ISO/IEC 7816-11:2004 Parte 11: Verificación personal Por medio de métodos biométricos. Tarjetas de identificación ISO/IEC 7816-15:2004 Parte 15: Información de dispositivo Criptográfico en tarjetas CI.	**A**	Tarjetas de circuito(s) integrado(s) con contactos.	Identification cards -- Integrated circuit cards -- Part 8: Commands for security operations Identification cards -- Integrated circuit cards -- Part 9: Commands for card management Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application
	Estándar FIPS-140-2	**A**	Todos.	Para usos criptográficos dentro de la IOFE, siguiendo, en cuanto a la aplicación de los diversos niveles de exigencia de este estándar lo señalado en la Guía de Acreditación de Entidades de Certificación EC, en su punto 6.IV, Niveles de seguridad de PKI y en su Anexo 11.

	Common Criteria Para el IC bajo perfiles de protección como: BSI-PP-0002:2001 PP/9806:1998 Como dispositivo seguro de creación de firmas digitales, bajo los perfiles de protección señalados en: CWA 14169:2004	**R**		Niveles EAL4+ o superiores Smartcard IC Protection Profile. Bundesamtes für Sicherheit in der Informationstechnik Smartcard Integrated Circuit Protection Profile Registered at the French Certification Body under the number PP/9806 CEN Workshop Agreement Secure signature-creation devices “EAL 4+” Se hace mención al nivel EAL4+ en el Anexo 11 de la Guía de Acreditación de Entidades de Certificación EC de la IOFE.
Infraestructura del terminal	Tecnología de la información – Diseños de teclados para texto y sistemas de oficina ISO/IEC 9995-1:2006 Parte 1: Principios generales que gobiernan el diseño de los teclados.	**R**	Todos.	Information technology -- Keyboard layouts for text and office systems -- Part 1: General principles governing keyboard layouts

	Especificación de Interoperabilidad para ICCs y Sistemas de Ordenador Personal Estándares del Consorcio Grupo de Trabajo PC/SC Parte 1. Introducción y Visión General de la Arquitectura Parte 2. Requisitos de Interfaz para Tarjetas Compatibles con CI y Dispositivos de Interfaz Parte 3. Requisitos para Dispositivos de Interfaz Conectados a PC Parte 4. Consideraciones del proyecto IFD e Información de Referencia del Proyect Parte 5. Definición del Gestor de Recursos ICC Parte 6. Definición de la Interfaz del Surtidor de Servicio ICC Parte 7. Consideraciones del Proyecto de Dominio / Desarrollador de la Aplicación Parte 8. Recomendación para la Implementación de Dispositivos de Seguridad y Privacidad ICC.	**A**	Todos.	Para uso general en PCs.
	Certificación EMC (de compatibilidad electromagnética)	**A**	Para lectores de tarjetas inteligentes	Según el Anexo 11 de la Guía de Acreditación de Entidades de Certificación EC de la IOFE.

Componente	Especificación	SIT	Aplicable a	Observaciones
Tarjetas tipo Java Card®	API (Application Programming Interface) para la plataforma de tarjetas Java Card.	**A**	Esta API define un conjunto de clases a partir de las cuales la tecnología Java Card basada en applets puede ser construida.	Versión general para la tecnología Java Card es 2.2.2 (marzo de 2006), http://java.sun.com/products/javacard/
	Especificación para el ambiente de ejecución (runtime environment) para la plataforma Java Card.	**A**	Esta especificación describe el ambiente requerido para la ejecución de applets basado en tarjetas Java Card.	
	Especificación para la máquina virtual para la plataforma Java Card.	**A**	Esta Especificación define la configuración requerida para la máquina virtual de la tarjeta.	
	Especificaciones de Tarjeta GlobalPlatform:2006	**R**	Especificación de tarjeta que permite una implementación neutral en cuanto a hardware, proveedores y aplicaciones, posibilitando una arquitectura de seguridad y gestión común.	GlobalPlatform Card Specification, Version 2.2 March 2006.

Infraestructura de soporte a tarjetas ICC GlobalPlatform®	Requerimientos Funcionales para el Sistema de gestión de Tarjetas Inteligentes GlobalPlatform Requerimientos Funcionales para el Sistema de Gestión de Claves GlobalPlatform Guía a la Personalización Común GlobalPlatform Especificaciones de Requerimientos de Seguridad para Tarjetas GlobalPlatform Especificación de Mensajería GlobalPlatform Guía de Configuración de Tarjetas GlobalPlatform Especificaciones del Lenguaje Interpretado para los Sistemas (ECMAScript) GlobalPlatform Especificaciones de Perfiles para los Sistemas GlobalPlatform	**F**	Permite una implementación estandarizada para la infraestructura de soporte de las tarjetas ICC.	GlobalPlatform Smart Card Management System Functional Requirements, Version 4.0, 21 December 2004. GlobalPlatform Key Management System Functional Requirements, Version 1.0, November 2003. GlobalPlatform Guide to Common Personalization, Version 1.0, March 2003. GlobalPlatform Card Security Requirements Specification, Version 1.0, May 2003. GlobalPlatform Messaging Specification, Version 1.0, October 2003. GlobalPlatform Card Customization Guide, Version 1.0, 13 August 2002. GlobalPlatform Systems Scripting Language Specification, An ECMAScript Representation, Version 1.1.0, 24 September 2003. GlobalPlatform Systems Profiles Specification, An XML Representation, Version 1.1.0, 24 September 2003.