Universidad de las Ciencias Informáticas

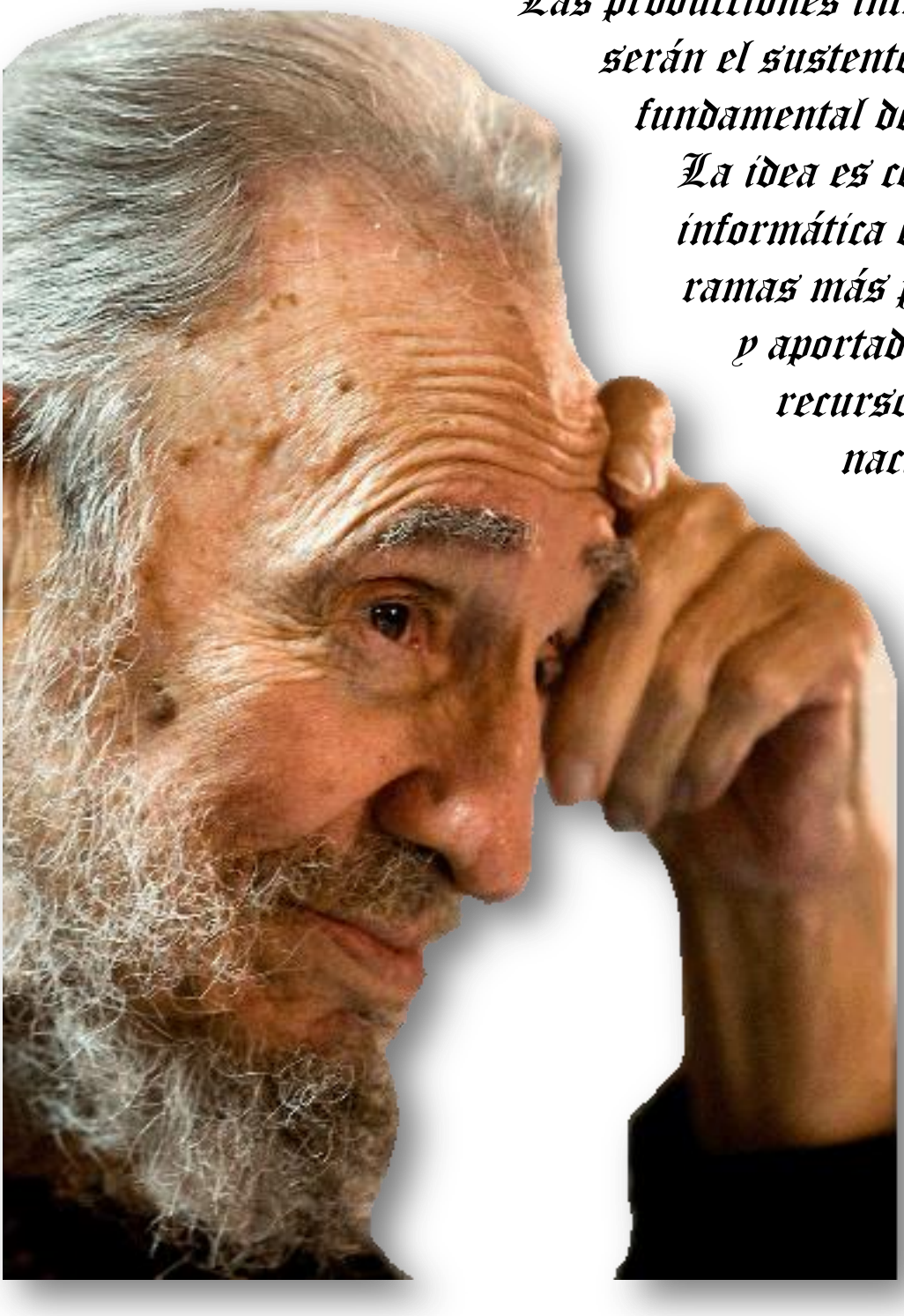
Facultad 1

Título: Propuesta de marco de trabajo conceptual para la identificación digital en el Gobierno Electrónico en Cuba.

Autor: Carlos Adrian Hernández Alonso.

Tutor: Ing. Irina Brito Reyes.

Ciudad de La Habana, junio 2012.



Las producciones intelectuales serán el sustento fundamental de Cuba. La idea es convertir la informática en una de las ramas más productivas y aportadoras de recursos para la nación…

Fidel Castro

Todos mis triunfos están dedicados a mis padres, pues simplemente he sido el reflejo de sus ejemplos, siempre han estado presente ante todas las circunstancias, me han sabido guiar y dar la confianza para cumplir todas mis metas. Espero que estén orgullosos del hombre que sin darse cuenta se formó entre sus manos.

A mi hermana por convertirse en toda una mujer cuando los tiempos arrecian y poder contar con ella en los momentos difíciles, aun cuando hay por medio miles de kilómetros y el anhelo de estar junto a su familia es el mayor consuelo.

Gracias a toda mi familia por darme el apoyo necesario para lograr convertir este sueño y muchos otros en realidad.

A todas las personas que a lo largo de mi carrera han dado su aporte para convertirme en profesional.

Sin duda estas son las líneas más difíciles de escribir para mí.
Quiero agradecerle:
A nuestro Comandante eterno Fidel Castro Ruz y a la Revolución por la oportunidad de estudiar en una universidad de excelencia.
A mi madre y a mi padre por ser los precursores de mis sueños.
A mi hermana por convertirse en el puntal de apoyo cuando más lo necesitó la familia.
A la niña por estar presente en todos los momentos y recordar todos los detalles que muchas ocasiones suelen parecer insignificantes pero siempre son muy importantes.
A Yosvani por estar presente en los buenos y malos tiempos.
A Mary Laura y a toda su familia que por más de ocho años fui miembro de ella y me apoyaron en todos los momentos como a un hijo.
A Israel por ser como un padre para mí y brindarme consejos y experiencias de tanto valor para la vida.
A Ernesto por ser más que un amigo, ser tutor incondicional.
A mis amigos de la universidad que han pasado a ser los de la vida, Frank, Juan, Ismel y Liuver, demostrando ser amigos ante cualquier circunstancia.
Al grupo 1501 por compartir experiencias inolvidables junto a ellos, por apoyarnos los unos a los otros aun cuando los caminos se muestran difíciles.
A María y Arely por tratarme como un hijo cuando estaba a miles de kilómetros de mi seno familiar.
A Yulisa por permitirme conocer a un ser tan especial y vivir momentos inolvidables a su lado.
A todas las personas que hicieron posible que mi anhelo de Ingeniero se convirtiera en realidad. Gracias!!!

Declaración de Autoría

Declaro ser autor de la presente investigación que lleva por título “Propuesta de marco de trabajo conceptual para la identificación digital en el Gobierno Electrónico en Cuba” y reconozco a la Universidad de las Ciencias Informáticas los derechos patrimoniales para hacer uso de la misma en su beneficio.

Para que así conste firmo la presente a los ___ días del mes de _____ del año 2012.

Carlos Adrian Hernández Alonso	Ing. Irina Brito Reyes
Firma del Autor	Firma del Tutor

El gobierno electrónico comprende la utilización de las tecnologías de la informática y las comunicaciones para facilitar la administración pública de los estados e incorporar a los ciudadanos en la toma de decisiones, informatiza servicios básicos como la educación, salud, transporte, deporte, entre otras ramas de la sociedad. Facilita las comunicaciones intergubernamentales y la cooperación entre los gobiernos.

La identidad digital es una parte fundamental para el funcionamiento del gobierno electrónico, garantizando la confiabilidad de los usurarios en la utilización de los servicios brindados, también asegura la autenticación de los usuarios que se benefician por los servicios, conservando la integridad de los datos en las transacciones que se realizan entre las aplicaciones que se sirven de los servicios ofrecidos por el gobierno o las que se acoplan de forma paralela a él para consolidarlo.

Para la construcción de estas aplicaciones se propondrá un marco de trabajo conceptual que facilite la gestión de la identidad en el gobierno electrónico, adecuándose a las características del gobierno electrónico en Cuba y permitiendo la integración con otras soluciones mediante los servicios. La identidad digital estará concebida para dos tipos de usuarios (personas y entidades), compuesta por datos personales o estructurales, patrones biométricos para el caso particular de las personas y certificado digital. La propuesta estará estructurada por la e-ID, que estará conformada por e-Identidad, e-Verificación, e-Certificado, e-Autenticación y e-Legislación los cuales serán los responsables de brindar los elementos de identidad en el gobierno electrónico a partir de servicios.

Palabras claves: gobierno electrónico, identidad digital, marco de trabajo, certificado digital, confiabilidad, integridad, autenticación, transacciones y servicios.

Índice

Índice de Figura

Introducción

Las Tecnologías de la Información y las Comunicaciones (TIC) se han venido desarrollando a partir de los años 80. Actualmente el uso de las TIC está siendo un paradigma para la sociedad, pues cada vez se hacen más vitales para la vida cotidiana de las personas, revolucionando el trabajo, el ocio, las comunicaciones y los servicios. Por otro lado, las TIC todavía tienen poco o ningún impacto en las vidas de innumerables personas en muchos países; esta disparidad en el impacto de las TIC principalmente en los países en vías de desarrollo es una muestra del progreso desigual del desarrollo económico en el mundo; los gobiernos también han influido en esta disparidad al no darle la importancia requerida a la nueva era de la información.

En este ámbito, las aplicaciones de las TIC son la promesa de mejorar la prestación de servicios públicos a los ciudadanos, no sólo mejora los procesos y la gestión de gobierno, sino también por la redefinición de los conceptos tradicionales de la ciudadanía y la democracia.

El Gobierno Electrónico también conocido como e-gob es uno de los elementos que en la actualidad ha tomado gran valor estratégico para las naciones del primer mundo y las naciones en vías de desarrollo, tales como la India, Malasia, China, Chile, Venezuela, México, entre otras; ya que a través del modelo de e-gob se genera valor tecnológico y transaccional a los gobiernos, proporcionando servicios gubernamentales mediante la integración de diferentes tecnologías, como internet, las telecomunicaciones, la videoconferencia y las multimedias [1], básicamente es la aplicación de las TIC a la administración pública, pero las tecnologías no son más que una mera herramienta para lograr una mayor eficiencia en el proceso de automatización de la administración pública, pero se necesita un sistema que sea flexible y que se adapte a las necesidades que la ciudadanía va teniendo.

El e-gob guia los esfuerzos del nuevo modelo de administración pública hacia un mismo fin, un fin democrático que responda a las necesidades de los ciudadanos.

Uno de los puntos delicados dentro del e-gob es la Identidad Digital o Electrónica por las características de los gobiernos, ya que manejan inumerables contenidos de información (personal, intergubernamental, etc.), por lo cual los sistemas de los gobiernos deben manejarse con seguridad.

La cantidad de usuarios de Internet en 2011 alcanzó los 2100 millones de personas, para un 30% de la población mundial, donde la mayoría de los internautas se concentran en Asia, Europa, América del Norte y en cuarto lugar de esta lista se

encuentra América Latina. Más del 50% de los usuarios son jóvenes que no superan los 25 años de edad. [2]

Debido al creciente uso de Internet el fenómeno de suplantación y robo de identidad es muy común en la actualidad, esto lo demuestra el elevado número de incidentes que se dan a diario en internet, lo cual disminuye la confianza y las transacciones en línea. La identidad digital está siendo expedida por varios países para garantizar la identificación y la autenticación en las transacciones del e-gob, además de proponerle seguridad al cliente, entidades y a los procesos de administración pública.

Cuba ha identificado desde muy temprano la conveniencia y necesidad de dominar e introducir en la práctica social las TIC; y lograr una cultura digital como una de las características imprescindibles del hombre nuevo, lo que facilitaría a nuestra sociedad acercarse más hacia el objetivo de un desarrollo sostenible.

El gobierno cubano a partir de los lineamientos definidos en el año 1996 creó una guía fundamental de trabajo para esta etapa de acercamiento a la sociedad de la información, la cual es conocida como el Programa Rector para la Informatización de la Sociedad Cubana. Este programa persigue promover el uso masivo de las TIC a escala nacional, teniendo en cuenta los objetivos generales estratégicos que el país se ha propuesto y buscando impulsar de manera coherente todos los sectores, con una identificación precisa de los actores de la Sociedad de la Información. [3]

Para dar cumplimiento a estos lineamientos se organizaron ocho programas generales, interrelacionados y coherentes, bajo los cuales se enmarcaron decenas de proyectos específicos. Ellos son:

- IS-ITH: Infraestructura, Tecnologías y Herramientas.
- IS-CIUD: Sistemas y Servicios Integrales para los ciudadanos.
- IS-GOB: Informatización del Gobierno, la Administración y la Economía.
- IS-MUN: Informatización Territorial.
- IS-CULT: Fomento de la Cultura digital.
- IS-JCLUB: Fortalecimiento del papel de los Joven Club.
- IS-ICSW: Fomento de la Industria Nacional de las Tecnologías de la Información y las Comunicaciones.
- IS-IDA: Investigación, desarrollo y asimilación tecnológica.

A raíz de la puesta en marcha de estos proyectos, nuestro país ha afrontado una serie de cambios y transformaciones en el accionar diario de la mayoría de la población, dígase estudiantes, trabajadores del sector público, profesionales, entre

otros, pues han sido beneficiados por más de uno de los programas llevados a cabo, de manera directa o indirecta.

En el 2007 se lleva a cabo la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado en la cual Cuba participa y firma la renovación de su compromiso con la Reforma del Estado, el fortalecimiento de sus instituciones públicas y la modernización de sus mecanismos de gestión, teniendo en cuenta que la calidad de los organismos públicos es fundamental para el desarrollo, la igualdad de oportunidades y el bienestar social.

A partir de esta conferencia surge la necesidad de replantear las estrategias hacia un nuevo modelo en la informatización de la sociedad o sea crear las bases o introducir el gobierno electrónico en el país.

El gobierno cubano ha influido en el desarrollo de la informatización, pero un importante paso para que se siga fortaleciendo este proceso sería mediante la integración de estos proyectos, buscando la estandarización de los procesos del gobierno, evitando que se hagan tediosos, lentos e insostenibles para el futuro y logrando que sean más ágiles, eficaces y gestionables.

Uno de estos pasos sería idear la identificación para este marco de trabajo o infraestructura digital (estructura conceptual y tecnológica definida con la cual se desarrolla un *software* de forma más ágil y organizada) que unificara varios proyectos, sin obviar el alto nivel de seguridad que debe presentar por tratarse de un sistema gubernamental. La identidad digital le aportará seguridad y confianza a la sociedad cubana que serán los usuarios primordiales de este nuevo modelo de gobierno electrónico.

De acuerdo a la situación planteada previamente, se identificó como **problema de la investigación** ¿Cómo facilitar, de manera segura, la gestión de la identidad electrónica durante la construcción de aplicaciones para el e-gob de Cuba?

Se estableció como **objeto de estudio**: marcos de trabajo para el e-gob, y se enmarca al **campo de acción**: marcos de trabajo para la identidad digital en el e-gob.

En este trabajo se parte de la **idea a defender**: a partir de la propuesta de un marco de trabajo conceptual capaz de soportar la gestión de la identidad digital, quedarán establecidas las pautas para el uso de la misma en el desarrollo del e-gob.

Se tiene como **objetivo general**: proponer un marco de trabajo conceptual que garantice la gestión de la identidad digital en el e-gob de Cuba.

Del objetivo trazado se derivan los siguientes **objetivos específicos**:

- Establecer los principales conceptos con los que se trabajará en la definición de la propuesta.
- Realizar un análisis de los principales marcos de trabajo en materia de identificación digital para el gobierno electrónico establecidos en otros países de referencia, teniendo en cuenta las experiencias tanto latinoamericanas como europeas.
- Identificar las principales características y elementos de cada una de las experiencias analizadas que puedan ser incorporados en la propuesta.
- Proponer un marco de trabajo conceptual que soporte la gestión de la identidad digital en el e-gob de Cuba.

Las **tareas científicas** propuestas a desarrollar para dar cumplimiento a los objetivos son las siguientes:

- Hacer un análisis crítico de la situación actual en Cuba
- Confeccionar el diseño teórico metodológico de la investigación estableciendo el problema científico y el objetivo general de la misma.
- Realizar un análisis de los conceptos y temas principales ajustándolo a los intereses del trabajo.
- Analizar cada uno de los marcos de trabajo más usados para soportar la identificación digital.
- Identificar las características o elementos que puedan ser incorporados en la propuesta.
- Confeccionar una propuesta de un marco de trabajo conceptual para gestionar la identificación digital en el e-gob de Cuba.
- Proponer elementos de arquitectura a tener en cuenta durante la implementación de la propuesta.

Consecuentemente para desempeñar las tareas propuestas se utilizaron varios **métodos investigativos** como el **método teórico** que se utiliza para la construcción de las teorías científicas, para la elaboración de las premisas metodológicas de la investigación y también en la construcción de las hipótesis científicas, dentro de los que se encuentran:

El **Analítico - Sintético** para definir las principales características que debe presentar el marco de trabajo conceptual de propuesta para la identificación digital en el gobierno electrónico de Cuba.

El **Inductivo - Deductivo** para comparar los marcos de trabajo de identificación digital de los gobiernos electrónicos que existen y llevar a soluciones del problema científico.

El **Histórico - Lógico** para determinar trayectoria, evolución y comportamiento del gobierno electrónico en el ámbito nacional e internacional.

La **Modelación** para representar gráficamente el marco de trabajo conceptual que se propone para la identificación digital del gobierno de Cuba, así como esquemas, gráficos para la comprensión a la solución de la problemática.

El método **sistémico** para la integración de las tecnologías.

Otro método investigativo que se utilizó fue el **método empírico** el cual le permite al investigador, la recopilación de datos reales acerca del comportamiento de los hechos, fenómenos, objetos y procesos de la naturaleza y de la sociedad, dentro de este tipo de método se utilizaron:

La **entrevista,** que se aplicó a varios entes, para determinar algunos requisitos funcionales que debe presentar el marco de trabajo conceptual.

La **observación**, que se utilizó para ver cómo ha sido el desarrollo de la informatización en Cuba a partir del uso de las TIC.

El presente documento se estructura en tres capítulos, recogiendo todo el trabajo investigativo realizado, así como también el análisis y el diseño de la solución en el mismo.

Capítulo I: Fundamentación Teórica, en este se recopila un estudio del estado del arte del tema a tratar y de las tendencias actuales. Además se abordarán los conceptos fundamentales de la investigación.

Capítulo II: Análisis de la Identidad Digital en el e-gob, se analizarán los distintos tipos de marcos de trabajo para identificación digital de algunos de los gobiernos electrónicos llevados a cabo en el mundo y se hará una comparación y análisis de las principales características de los elementos que pueden ser aplicados en la propuesta.

Capítulo III: Propuesta de Solución, en este se realizará la propuesta de diseño del marco de trabajo conceptual para la identificación digital en el gobierno de Cuba. Se describirá la propuesta de arquitectura para la infraestructura propuesta, los servicios y los clientes a los que van dirigido.

Fundamentación Teórica

1.1 Introducción

En este capítulo se analizan las principales definiciones y conceptos referentes a los temas que se tienen en cuenta para el desarrollo de la investigación. De acuerdo con esto, se ofrece un enfoque de los aspectos fundamentales relacionados con Gobierno Electrónico (e-gob), Identidad Digital o Electrónica, entre otros; como aspecto esencial en el aseguramiento del éxito en la propuesta de marco de trabajo conceptual que soporte la identidad digital en el gobierno electrónico de Cuba. Comenzando el análisis se abordará el concepto de gobierno.

1.2 Gobierno

El término gobierno hace referencia al ejercicio del poder del Estado o a la conducción política general. Se entiende por gobierno al órgano al que la Constitución le ha atribuido el poder ejecutivo sobre una sociedad y que generalmente está formado por un Presidente o Primer Ministro y una cantidad determinada de Ministros, Secretarios y otros funcionarios. [4]

Aunque en muchas circunstancias se suele usar como sinónimos, los términos estado y gobierno no hacen referencia a lo mismo, gobierno es el que ejerce el poder, las tareas y tiene un tiempo de permanencia, mientras que el estado lo estructura y permanece inarterable ante los sucesivos gobiernos. Ahora se analizará el concepto desde el punto de vista del desarrollo y automatización del mismo.

1.2.1Gobierno Electrónico

¿Qué es el gobierno electrónico (e-gob)?

En la Conferencia Iberoamericana se entienden las expresiones de “Gobierno Electrónico” y de “Administración Electrónica” como sinónimas, ambas consideradas como el uso de las TIC en los órganos de la Administración para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos. Todo ello, sin perjuicio de las denominaciones establecidas en las legislaciones nacionales. [1]

El gobierno de Chile define el Gobierno Electrónico como el uso de las TIC para mejorar los servicios e información ofrecidos a los ciudadanos, aumentar la eficiencia y eficacia de la gestión pública e incrementar substantivamente la transparencia del sector público y la participación ciudadana. [5]

El gobierno de México define el Gobierno Electrónico como la innovación continua en la entrega de servicios, la participación de los ciudadanos y la forma de gobernar mediante la transformación de las relaciones externas e internas a través de la tecnología, la Internet y los nuevos medios de comunicación. [6]

Teniendo en cuenta algunos de estos conceptos anteriores se puede definir un concepto de e-gob que contemple las principales ideas con las que se trabajarán. Por tanto se considera al e-gob como la utilización de tecnología de la información para la libre circulación de la información superando los límites físicos del papel tradicional y mejorar el acceso y la prestación de servicios públicos en beneficio de los ciudadanos, socios comerciales y empleados. Se puede plantear que consiste en la automatización o informatización de los procesos actuales basados en el papel, de los procedimientos que conduzcan a los nuevos estilos de liderazgo, nuevas maneras de debatir y decidir las estrategias de nuevas formas de transacciones comerciales, nuevas formas de escuchar a los ciudadanos y las comunidades, y nuevas formas de organización y provisión de información.

Por último, el gobierno electrónico tiene como objetivo mejorar el acceso y la prestación de servicios públicos en beneficio de los ciudadanos. Más importante aún, tiene como objetivo ayudar a fortalecer la iniciativa de gobierno hacia una gobernanza eficaz y una mayor transparencia para administrar mejor los recursos sociales y económicos de un país para el desarrollo. [7]

Los objetivos del e-gob

El Grupo de Trabajo sobre Gobierno Electrónico en el Mundo en Desarrollo ha identificado cinco grandes categorías de objetivos comunes perseguidos por el e-gob. [8] Los objetivos no figuran en ningún orden particular de importancia, ya que cada país debe determinar sus prioridades en el e-gob.

1. **La creación de un mejor ambiente de negocios**.

   La tecnología es un catalizador demostrado para aumentar la productividad y el crecimiento económico, especialmente en las comunidades rurales y marginadas. [9] El uso de las TIC en el gobierno y el establecimiento de un e-gob ayudarían a la infraestructura orientada a crear un ambiente favorable a las

empresas mediante la simplificación y la mejora de la interacción entre el gobierno y los ciudadanos. Al eliminar las redundancias en los procedimientos y haciendo hincapié en la entrega inmediata y eficiente de los servicios, e-gob crea las condiciones para atraer inversionistas e inversiones.

Este objetivo depende en gran medida del país, sus puntos fuertes de la industria y su ventaja competitiva global. Una vez identificados, estos deben ser incorporados en la estrategia de gobierno electrónico del país, con las agencias, la burocracia y los servicios públicos alineados a la promoción de estos sectores. La contratación electrónica, por ejemplo, puede abrir nuevos mercados a las empresas locales mediante la apertura del proceso de contratación pública, por lo que es más competitivo y justo.

2. **Los clientes en línea y no en línea.**

Esto se refiere a la entrega efectiva de bienes y servicios públicos a los ciudadanos acompañados por el gobierno de respuesta rápida con un mínimo de intervención directa por un funcionario público.

3. **Fortalecimiento de la gobernabilidad y la ampliación de la participación del público.**

Promover la transparencia y la rendición de cuentas en el gobierno a través de la proliferación de las TIC en la gestión y las operaciones también abre oportunidades para que los ciudadanos participen más activamente en la formulación de políticas y toma de decisiones de gobierno.

Como una herramienta importante en la construcción de una tradición de transparencia y buen gobierno, e-gob puede avanzar en la lucha contra la corrupción. Sin embargo, el gobierno electrónico por sí solo no pondrá fin a la corrupción. Debe ir acompañado de otros mecanismos para ser plenamente eficaz.

Al mismo tiempo, el gobierno electrónico facilita la rápida entrega de información completa. La amplia difusión de la información ayuda a empoderar a los ciudadanos y facilitar la toma de decisiones. La transparencia de la información no sólo profundiza la democracia, sino también inculca un sentido de responsabilidad entre los líderes del gobierno y obliga a una gobernanza eficaz.

4. **La mejora de la productividad y la eficiencia de las agencias gubernamentales.**

La reingeniería de procesos y procedimientos para reducir los trámites burocráticos, facilitar la prestación de los servicios, aumentar la productividad de la burocracia, y aumentar el ahorro son beneficios inherentes a la administración electrónica. Más específicamente, el gobierno electrónico puede ayudar a:

- Aumentar la productividad del personal del gobierno, reducir los gastos generales de oficinas y gestión de papel, mejorar la capacidad de planificación de la gestión por parte del gobierno (con mejores herramientas y mejorar el acceso a la información), y aumentar los ingresos ya que las empresas y los ciudadanos en realidad se aplican a más licencias, por el hecho de que el proceso es mucho más fácil y menos corrupto.
- Inducir ahorros de costes a medio y largo plazo. En el corto plazo, sin embargo, el personal y los costos tienden a aumentar a medida que el gobierno debe ofrecer múltiples plataformas de entrega (tanto tradicionales como e-gob) durante la transición inicial.
- Racionalizar las operaciones del gobierno. La mayoría de los procesos de gobierno se han desarrollado durante muchos años, y por lo general implican muchos pasos, tareas y actividades. Agilizar los procesos de gobierno a través de las TIC se eliminan trámites redundantes y ayuda a reducir la burocracia.

5. **La mejora de la calidad de vida de las comunidades desfavorecidas.**

Las TIC hacen posible que el gobierno llegue a los grupos marginados y comunidades y mejorar su calidad de vida. Esto significa potenciar a través de su participación en el proceso político, así como la entrega de tan necesarios bienes y servicios públicos.

Sin perder el punto de vista principal de e-gob que es mejorar la interacción entre los tres principales actores en la sociedad, gobierno, ciudadanos y empresas también se estimula el progreso político, social y económico en el país.

¿Qué ventajas posee el e-gob? [8]

La clave para lograr el éxito en el gobierno electrónico es el establecimiento de servicios ininterrumpidos, donde se evite los procesos burocráticos, tediosos y lentos, donde se logre una mayor participación de una forma transparente, donde los principales beneficiados sean los ciudadanos y la principal estrategia sea siempre

mejorar continuamente sus necesidades, partiendo por brindarle mayor acceso a la información pública.

Por lo tanto, el gobierno electrónico debe traducirse en la entrega eficiente y rápida de bienes y servicios a los ciudadanos, las empresas, los empleados del gobierno y agencias. Para los ciudadanos y empresas, e-gob significa la simplificación de los procedimientos y la simplificación del proceso de aprobación. Para los empleados del gobierno y las agencias, significa la facilitación de la coordinación entre agencias y la colaboración para asegurar la adecuada y oportuna toma de decisiones.

Tipos de transacciones del e-gob [8]

Las transacciones de los servicios de administración electrónica se concentran en cuatro principales clientes:

- Ciudadanos
- Comunidad empresarial
- Empleados del gobierno
- Agencias gubernamentales

El e-gob trata de hacer la interacción con los ciudadanos, las empresas, los empleados del gobierno, agencias gubernamentales y otros gobiernos, más cómoda, agradable, transparente, barata y eficaz.

En un sistema de e-gob, los individuos son capaces de iniciar una solicitud de servicio de un gobierno en particular y luego recibir el servicio del gobierno a través de internet o algún otro mecanismo computarizado. En algunos casos, la administración pública se entrega a través de una oficina del gobierno. En otros casos, una transacción de gobierno se completa sin contacto directo con un empleado del gobierno.

Tipos específicos de servicios prestados a través de e-gob

Los cuatro tipos de servicios de gobierno electrónico [8] son:

- **Gobierno a ciudadano (G2C)**

  Incluye la difusión de información a los servicios públicos como la renovación de la licencia, pedidos de certificados de nacimiento, muerte o matrimonio y la presentación de impuestos sobre la renta, así como de atención al ciudadano de los servicios básicos como educación, salud, información de los hospitales, bibliotecas y similares.

- **Gobierno a Negocio (G2B)**

Incluyen diversos servicios intercambiados entre el gobierno y la comunidad empresarial, incluida la difusión de las políticas, notas, normas y reglamentos. Los servicios a las empresas que se ofrecen incluyen la obtención de información de negocios actual, la descarga de formularios de solicitud, renovación de licencias, el registro de empresas, obtención de permisos, y el pago de impuestos. Los servicios ofrecidos a través de transacciones G2B también ayudan en el desarrollo empresarial, específicamente el desarrollo de las pequeñas y medianas empresas. Simplificación de los procedimientos de aplicación que faciliten el proceso de aprobación de las solicitudes que fomenten el desarrollo de negocios.

En un nivel superior, los servicios G2B incluyen la contratación electrónica, un gobierno en línea y el proveedor a cambio de la compra de bienes y servicios por parte del gobierno. Por lo general, existen sitios web que permiten a los usuarios calificados y registrados para buscar compradores o vendedores de bienes y servicios. Dependiendo del enfoque, los compradores o vendedores pueden especificar los precios o llamar a licitación. Favorece al proceso de licitación transparente y permite a las pequeñas empresas presentar ofertas para grandes proyectos de contratación pública. El sistema también ayuda al gobierno a generar un mayor ahorro, como los costos de los intermediarios y la sobrecarga de los agentes de compra se reduce.

- **Gobierno a Empleado (G2E)**

Servicios de G2E abarcan servicios G2C, así como servicios especializados que cubren sólo a los empleados del gobierno, tales como la provisión de la formación de recursos humanos y el desarrollo, que mejoren la burocracia del día a día las funciones y relaciones con los ciudadanos.

- **Gobierno a gobierno (G2G)**

Servicios G2G se llevará a cabo en dos niveles: a nivel local o nacional como a nivel internacional. Servicios G2G son las transacciones entre el gobierno central, nacional y local, y entre los organismos a nivel departamental. Al mismo tiempo, los servicios de G2G son las transacciones entre gobiernos, y puede ser utilizado como un instrumento de las relaciones internacionales y la diplomacia.

La propuesta se enfocará solamente en dos servicios del e-gob, el proceso de construcción del e-gob es continuo y abarcador, el gobierno cubano en una primera fase debe centrar sus esfuerzos en los servicios G2C y G2G, pues los clientes a los

que van dirigidos estos servicios son los principales actores de la sociedad cubana. Los ciudadanos deben ser el principal punto de enfoque en cualquier e-gob. El proceso de desarrollo en sus inicios arrojará significativos gastos económicos, es por ello que este proceso deberá realizarse en fases continuas en dependencia de las estrategias identificadas por el gobierno de Cuba para cada fase.

Infraestructura de gobierno electrónico [8]

La implementación del gobierno electrónico requiere un fuerte liderazgo y visión. También se requiere una estrategia integral que no sólo es punto de referencia sobre las mejores prácticas globales, pero también es sensible a las condiciones políticas y económicas.

Para que el gobierno electrónico sea una realidad, los gobiernos, en consulta con los interesados, recomiendan desarrollar un marco estratégico nacional, que articula la visión del gobierno, los objetivos y metas, el enfoque y las normas técnicas para los sistemas de gobierno electrónico. Dicho marco debe abordar la privacidad de la información, seguridad, mantenimiento, y estándares.

Sin embargo, hay que decir desde el principio que un marco nacional no es un requisito previo a cualquier proyecto de gobierno electrónico. Hay demasiados gobiernos que invierten años y recursos valiosos en el proceso de desarrollo de una estrategia nacional, cuando podrían estar avanzando en proyectos críticos. Lo que los gobiernos deben darse cuenta de que un marco estratégico nacional es un proceso continuo y no un documento estático.

Construcción de una adecuada infraestructura [8]

Una infraestructura es necesaria para garantizar que los ciudadanos disfruten de los beneficios del gobierno electrónico. Los siguientes aspectos deben ser considerados en la construcción de una columna vertebral del gobierno electrónico:

- **Las repercusiones financieras**.

  Es necesario un estudio de viabilidad financiera, este análisis de costo y beneficio pueden ayudar a los gobiernos decidir, o bien para abrir partes de la columna vertebral del gobierno y cobran una tarifa de acceso para operadores de telecomunicaciones o de los operadores para mantener las operaciones, o para montar en conjunto en una red privada existente, debido a limitaciones de coste.

- **Los problemas de infraestructura**.

Estos incluyen la infraestructura existente en el país, el nivel actual de penetración de Internet, la densidad telefónica, la velocidad actual de cambio tecnológico, los subsidios para la convergencia, y la inversión en banda ancha.

- **Los beneficios y riesgos**.

Garantiza que las comunicaciones del gobierno estén abiertas y seguras las 24 horas del día, 7 días a la semana y 365 días al año. Sin embargo, esto puede significar un financiamiento regular de las actualizaciones y el mantenimiento de la red, para lo que sería necesario un equipo para apoyar la red a tiempo completo.

Algunos gobiernos pueden decidir que la construcción de su propia estructura es demasiado costosa y consume mucho tiempo. La construcción de una columna vertebral puede llevar años y miles de millones de dólares para completar, y si los gobiernos quieren participar de inmediato en el gobierno electrónico, puede que no haya suficiente tiempo ni dinero para hacerlo.

Igualdad de acceso a la información y servicios del gobierno [8]

La implementación del gobierno electrónico facilita la participación ciudadana en el gobierno mediante el aumento de los canales de acceso al gobierno. Que amplía las oportunidades para la participación ciudadana, abriendo nuevos canales de comunicación entre electores y sus representantes y reunir a los grupos marginales (es decir, mujeres, discapacitados, pueblos indígenas) en la corriente principal de canales de participación.

Pero así como iniciativas de gobierno electrónico tienen la posibilidad de democratizar la prestación de servicios básicos y nivel de los efectos del desarrollo, estas mismas iniciativas también pueden hacer a los ciudadanos más lejos del gobierno e incluso profundizar la privación de los derechos existentes. Los responsables políticos, para tratar de lograr objetivos de desarrollo a través de e-gob, deben considerar los proyectos que ofrecen los mayores beneficios para el mayor número de personas.

Mejorar el acceso a la información pública y los servicios. El gobierno lleva la carga y la responsabilidad de asegurar que los ciudadanos, comunidades, empresas y la sociedad civil cuentan con información completa para que puedan tomar decisiones de vida adecuada y oportuna.

A través de las TIC en sentido amplio, se ha incluido la televisión, la radio y los teléfonos al público para que pueda acceder más fácilmente a la información y los

servicios. Al ofrecer al público los detalles de las actividades del gobierno y darles lugares para participar activamente en estas actividades, el gobierno electrónico obliga a los funcionarios a ser más transparentes y responsables de sus actos y decisiones, así como para mejorar no sólo la prestación de servicios, pero también la calidad de estos servicios.

Mejorar la participación política. Las TIC han posibilitado a muchos ciudadanos de muchos países que se hallan vinculado a los procesos políticos, para hacer oír su voz, para participar en el proceso de elaboración de políticas, y en última instancia, influir en la toma de decisiones. Las TIC han abierto numerosos canales de participación que normalmente no están abiertos o disponibles al público en general. Muchos casos en todo el mundo de hoy han demostrado el potencial de las TIC para cambiar la sociedad a través de la participación de una amplia variedad de personas de diversos orígenes sociales y culturales, clases sociales y creencias religiosas.

Seguridad y protección de la privacidad [8]

La seguridad en general se refiere a la protección de los activos del sistema de información y control de acceso a la información. Políticas y estrategias de seguridad dependen del contexto y de información específica.

Privacidad se refiere al derecho de información atribuida a una persona a ser tratado con un nivel adecuado de protección. Información de las leyes de protección de la privacidad a menudo puesto en marcha para regular esto.

Proteger la privacidad de los ciudadanos y asegurarles que su información personal no se verá comprometida es fundamental en el gobierno electrónico, porque es la clave para la confianza del usuario. Sin esta seguridad nadie utilizará los servicios del gobierno electrónico.

1.3 Identidad Digital o Electrónica

Primero como definición de identidad, el Diccionario de la Real Academia Española (RAE) establece que se trata del “conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás.” [10]

La identidad es aquel conjunto de rasgos propios de un individuo o colectividad que los caracterizan frente a los demás. La verificación de estos rasgos es lo que nos permite determinar que un individuo es quien dice ser. Algunos de estos rasgos son propios del individuo, otros son adquiridos con el tiempo. Al conjunto de rasgos que

caracterizan a un individuo o colectivo en un medio de transmisión digital se le conoce como Identidad Digital. [11]

En la identidad digital se encuentra el conjunto de elementos donde se conjuga la informática, la seguridad, la privacidad y el derecho.

Constituye el conjunto de elementos técnicos a la que se le vincula únicamente una persona o entidad física o jurídica, esta toma un conjunto de rasgos adquiridos por un tiempo para lograr identificarse y ser diferenciado por el resto de usuarios en sus acciones electrónicas. Estas personas o entidades a las que se les vincularon sus características con una identidad digital podrán realizar transacciones con un nivel de confianza y seguridad.

La verificación de estas características es lo que brinda la posibilidad de establecer que un individuo que opera en Internet es quien dice ser. La oportunidad de conocer la verdadera identidad de un individuo en la red es uno de los principales retos que existen para lograr que el comercio y la administración electrónica se conviertan en procesos habituales para los ciudadanos.

1.3.1 Principales medios para disponer de una identidad digital

Siempre que se habla de identidad digital se tiende a pensar que esta se corresponde con el empleo de elementos técnicos que buscan la plena identificación del usuario en un sistema concreto. Entre los principales medios para lograr la identidad digital se pueden resaltar los siguientes:

Usuario y contraseña

Desde el punto de vista legal, se debe considerar también como una firma electrónica, ya que según lo dispuesto en el artículo 3.1 de la Ley 59/2003, del 19 de diciembre, de Firma Electrónica, se denomina como tal al “conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante”.

Ahora bien, a pesar de que se puede considerar como una modalidad de identidad digital, esta no es el ideal de identificación en la red, ya que no consigue garantizar la conexión plena entre una acción realizada y la persona física que la ha llevado a cabo.

PIN (Número de Identificación Personal)

Es una contraseña o clave numérica, compuesta por cuatro números que sólo debe ser conocida por el titular de una tarjeta de crédito o de débito y cuya custodia es responsabilidad del mismo. [12]

Es un valor numérico (contraseña) usado para identificarse y poder acceder a sistemas, como un celular o un cajero automático, etc. Totalmente personalizable, e incluso se puede suprimir. [13]

Certificados digitales

Uno de los problemas al usar servicios en línea es la falta de seguridad del medio tanto para proteger las transferencias de datos como para asegurar la identidad del usuario. Por tal razón surgen los certificados digitales.

El Certificado Digital permite verificar la identidad de un ciudadano, garantizando que únicamente él puede acceder a su información personal, evitando suplantaciones. También es el elemento usado para firmar electrónicamente solicitudes o documentos. La firma electrónica basada en un certificado digital, como los utilizados en la administración electrónica, tiene la misma validez jurídica que la firma manuscrita. Asimismo, la identificación basada en un certificado digital es equivalente a la presentación del DNI electrónico en la atención presencial. [14]

En otras palabras un certificado digital es un documento digital concedido por una Autoridad Certificadora (AC) que garantiza la asociación de personas o entidades físicas o jurídicas con uno o varios elementos técnicos que vinculan la parte digital o electrónica con la física.

Básicamente, el certificado digital es el mecanismo que permite obtener una firma digital válida para firmar documentos digitales y asegurar la integridad de estos. La firma digital ofrecerá la misma garantía que la firma manuscrita dependiendo para ello del nivel de seguridad que contenga.

El certificado sin más no puede ser utilizado como medio de identificación, pero es una pieza imprescindible en los protocolos usados para autenticar a las partes de una comunicación digital, al garantizar la relación entre una clave pública y una identidad. Un certificado digital está compuesto por dos claves:

Clave Privada: poseída únicamente por su dueño. También se le llama Porción Privada y junto con la Clave Pública (Porción Pública) conforma un par de claves únicas.

Clave Pública: es publicada por la AC, después de ser aprobada por esta. Para aprobar un certificado digital, la AC firma con su clave privada, la clave pública del certificado digital no necesita conocer la clave privada del certificado digital.

Para comprender el proceso de emisión de un certificado consulte la Figura 1.

Figura 1. Certificado digital

Como mecanismo para asegurar ambos conceptos (integridad e identidad), el certificado digital utiliza algoritmos de criptografía. El certificado debe contener al menos lo siguiente:

- La identidad del propietario del certificado (identidad a certificar).
- La clave pública asociada a esa identidad.
- La identidad de la entidad que expide y firma el certificado.
- El algoritmo criptográfico usado para firmar el certificado.

Los dos primeros apartados son el contenido fundamental del certificado (identidad y clave pública asociada), en tanto que los otros dos son datos imprescindibles para poder validar el certificado.

Los certificados pueden almacenarse en la computadora, pueden estar guardados en una tarjeta con chip y como cualquier otro elemento electrónico puede guardarlo en un USB (Universal Serial Bus), en un CD (Disco Compacto) o en cualquier otro soporte óptico o magnético.

Firma digital

Puede ser definida como una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación de un algoritmo (fórmula matemática) de cifrado asimétricos o de clave pública y que equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje. Desde un punto de vista

material, la firma digital es una simple cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente. [15]

La firma digital está basada en tres características primordiales, las cuales son:

Identidad: esta implica que el mensaje o el documento está firmado digitalmente por la persona autora.

Integridad: este implica la certeza de que el mensaje recibido por el receptor es exactamente igual al emitido por el emisor o sea que el mensaje no haya sufrido alteraciones en el tránsito de la transmisión del emisor al receptor.

No repudio: no se puede rechazar o negar el envío del mensaje pues ha sido enviado por el emisor.

Por otra parte a estos tres elementos se le une otro, este va implícito, es la confidencialidad. La confidencialidad implica que el mensaje no haya podido ser leído por terceras personas distintas del emisor y del receptor durante el proceso de transmisión del mismo.

El proceso de encriptado puede ser muy lento en el caso de documentos voluminosos, por ello la firma cuenta también con lo que se conoce como "función hash". Al firmar electrónicamente, el emisor obtiene un resumen del mensaje mediante la función hash. El resumen es una operación que se realiza sobre un conjunto de datos, de forma que el resultado obtenido es otro conjunto que está asociado a los datos iniciales. El receptor, al recibir el mensaje, obtiene de nuevo su resumen mediante la función hash. Es imposible que existan dos hash iguales, de manera que esta función viene a reforzar la seguridad del sistema

Dirección Electrónica Única (DEU)

Una dirección, también dirección electrónica, o dirección de Internet, o dirección de Red, o dirección Web, es una serie de letras, números y símbolos con los que se identificaría a sí mismo y por los cuáles Internet lo identifica a usted, en realidad a su computadora. Una dirección puede ser también un lugar donde se almacena información. [16]

El requisito previo para dar de alta una dirección única por persona física o jurídica pasa por tener una cuenta de correo electrónico y la firma electrónica correspondiente. Las bondades de estas notificaciones telemáticas son evidentes, ahorran tiempo y les da una mayor agilidad a todas las gestiones con las distintas administraciones. [17]

Mediante la DEU cualquier persona física o jurídica que lo solicite dispondrá de una dirección electrónica, que será única para la recepción de las notificaciones

administrativas que se pueden firmar y aceptar o firmar y rechazar que por vía telemática pueda practicar la Administración General del Estado y sus organismos públicos. En definitiva, no deja de ser una nueva forma de que los ciudadanos se identifiquen digitalmente con la Administración Pública.

PKI (Infraestructura de Claves Públicas)

Un tema que ha alcanzado gran valor tecnológico en cuanto la identificación de un usuario en internet de una forma segura. El acrónimo PKI deriva de Infraestructura de Clave Pública y es la forma común de referirse a un sistema complejo necesario para la gestión de certificados digitales y aplicaciones de la Firma Digital. [18]

Está basada en el uso de un par de claves, una de distribución pública y otra en poder únicamente del propietario. La clave del propietario debe ser guardada de forma segura y se denomina clave privada; mientras que la clave pública se da a conocer a todos aquellos que quieran comunicarse de forma segura con el propietario.

Mediante la clave privada el propietario firmará los documentos o los mensajes de forma digital. La firma electrónica permite comprobar que un mensaje enviado o recibido no ha sido modificado desde su creación. El emisor calcula un resumen del mensaje a firmar está operación es llamada función hash. El destinatario comprueba usando la clave pública del firmante el contenido del hash y lo compara con otro hash que calcula, verificando que el mensaje no ha sido alterado.

Un sistema definido con PKI debe proporcionar las siguientes características de seguridad:

Autenticidad: la firma digital tendrá la misma validez que la firma manuscrita.

Confidencialidad: que la información transmitida se intercambie entre las partes adecuadas, de tal manera que en un tercero no pueda interferir entre estas partes.

Integridad: determina si un tercero ha manipulado el documento después de firmado digitalmente o si conserva la integridad con la cual fue firmado.

No repudio: no se puede rechazar un documento que ha sido firmado digitalmente.

Cuando se habla de sistemas de firma basados en certificados PKI, se hace referencia a los sistemas informáticos de firma digital avanzada en los que se emplea una doble clave, la pública y la privada.

Sin duda alguna el hecho de que se empleen dos tipos de clave, una que únicamente puede y debe conocer el propietario (privada) y otra públicamente conocida por todos los usuarios (pública), hace que una vez aplicado el proceso

técnico que se expone más adelante, se pueda garantizar la identidad e integridad de las transacciones realizadas a través de la red.

DNI electrónico

El Carné de Identidad, oficialmente y según la legislación Cédula de Identidad (CI) o Documento Nacional de Identidad (DNI), es un documento emitido por una autoridad administrativa competente para permitir la identificación personal de los ciudadanos.

El Documento Nacional de Identidad electrónico (DNI electrónico) emitido por la Dirección General de la Policía (Ministerio del Interior), es el documento que acredita con un certificado electrónico a un titular. La Figura 2 muestra un DNI electrónico.

Figura 2. DNI electrónico

Un certificado electrónico es un documento digital que expedido por una Autoridad de Certificación identifica a una persona (física o jurídica) con sus respectivas claves. [19]

Con el DNI electrónico contiene un certificado que tiene dos propósitos:

1. **Autenticar**:

   Tiene como finalidad garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática. Asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular podrá a través de su certificado acreditar su identidad frente a cualquiera ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.

   Este certificado no vincula al ciudadano en ninguna forma. Debería por tanto ser utilizado única y exclusivamente para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio). En base a la autenticación con este certificado, los

proveedores de servicios de certificación no deberían dar acceso a información de carácter personal ni solicitar firmas de trámites ni documentos.

Puede ser utilizado también como medio de identificación para la realización de un registro fuerte que permita la expedición de certificados reconocidos por parte de entidades privadas, sin estar obligadas a realizar una fuerte inversión en el despliegue y mantenimiento de una infraestructura de registro.

2. **Firma:**

Con este propósito se permite al ciudadano firmar trámites o documentos, sustituyendo a la firma manuscrita por la electrónica, otorgándole una validez jurídica equivalente a la que les proporciona la firma manuscrita. Por tanto, garantiza la identidad del suscriptor y del poseedor de la clave privada de identificación y firma.

La principal novedad del documento es que incorpora un pequeño circuito integrado (chip), que contiene los mismos datos que aparecen impresos en la tarjeta (datos personales, fotografía, firma digitalizada, huella dactilar digitalizada) junto con los certificados de Autenticación y de Firma Electrónica.

¿A qué se enfrenta la identidad digital?

La identidad digital es un concepto dinámico, en continua evolución gracias a las facilidades que los equipos y periféricos informáticos ofrecen a los usuarios para realizar las transacciones. A estas oportunidades se enfrentan las demandas de los usuarios ante la recolección, almacenamiento y difusión no deseada de sus datos personales.

El robo, la usurpación y el uso engañoso de la identidad son problemas comunes en el mundo virtual, de difícil solución. Así como pueden robar la identidad de una persona a través de una aplicación espía, pueden robar también la identidad digital mediante la manipulación o intromisión en sus datos digitales.

En el mundo virtual estos problemas se acrecientan, ya que el anonimato desvincula la identidad y eliminan la responsabilidad. Entonces, ¿cómo operar con seguridad en un medio donde existen identidades fiables y fraudulentas a la vez, que desaparecen con la misma rapidez con la que nacen sin dejar rastros?

La falta de correlación entre un usuario y una identidad, y la dificultad de obtener evidencias para identificar al responsable y proceder al reclamo, facilita la impunidad de estos delitos. La posibilidad de eludir controles administrativos es amplia, siendo un

tema de preocupación para los organismos responsables del cumplimiento de la legislación por la que se rigen.

¿Qué garantiza la identidad digital?

El rápido desarrollo de las TIC en nuestra sociedad hace necesario que estas respondan a nuevos retos, cada vez más solicitados por los usuarios. Uno de estos retos es el de dotar y garantizar a todos los ciudadanos de mecanismos adecuados que aseguren su identidad, privacidad, libertad y derechos, en el actual marco democrático.

Para utilizar muchos de los servicios públicos en Internet, es preciso un sistema de identificación que depende en gran medida de las características del servicio al que se accede, algunos requieren la aportación de un dato que sólo conoce el usuario y el suministrador del servicio, otros requieren la inscripción previa en un registro del propio servicio, donde se facilitan unas claves o contraseñas para acceder y utilizarlo.

Actualmente, una de las formas más comunes de acceso a los servicios electrónicos de las Administraciones Públicas es mediante el DNI electrónico, que otorga una identidad personal y digital a los ciudadanos.

También se puede acceder a los servicios públicos mediante certificados electrónicos, que acreditan y garantizan la identidad en la red de una persona o empresa, para el acceso seguro a los servicios públicos.

De cualquiera de estas formas los usuarios podrán realizar múltiples gestiones en línea de forma segura con las Administraciones Públicas, con las empresas públicas y privadas y con otros ciudadanos, a cualquier hora y sin tener que desplazarse de un lugar a otro, ni hacer colas.

Elementos básicos en la identidad digital

Existen un grupo de elementos claves que no se pueden obviar cuando se habla de Identidad Digital, que garantizarán la vinculación de algo o alguien que existe en realidad.

Confidencialidad: es la capacidad de intercambiar información de forma segura, además de garantizar que la información es accesible sólo para aquellos autorizados a tener acceso a ella. También se entiende como la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros.

Integridad: es la garantía de que la información no ha sido modificada ni alterada, se busca mantener los datos libres de modificaciones no autorizadas, de cierto modo,

la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad, la firma digital es uno de los pilares fundamentales de la seguridad de la información.

Autenticación: es una validación de identificación, es la técnica mediante la cual un proceso comprueba que el emisor de la información es quien se supone que es y no se trata de un impostor.

No repudio: garantía que tiene el receptor de que el emisor ha realizado una transacción, se proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente.

Comunicación Segura

Para garantizar estos elementos básicos para la identidad digital es necesario realizar una comunicación segura entre cliente y servidor, permitiendo que se interactúe con la persona adecuada en la comunicación de una transacción. Una forma de realizar una comunicación segura es mediante la utilización de protocolos, dentro de los más usados se encuentra SSL (Capa de Conexión Segura).

SSL es un protocolo de transferencia segura de datos mediante encriptación, proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Los protocolos permiten a las aplicaciones cliente-servidor comunicarse de una forma para prevenir ser escuchado por un tercero, la falsificación de la identidad del remitente y mantener la integridad del mensaje. [20]

Primero se debe hacer una solicitud, esto implica un cliente haciendo una solicitud de un URL a un servidor que soporte SSL, SSL acepta solicitudes por un puerto diferente al utilizado normalmente para ese servicio. Una vez se ha hecho la solicitud, el cliente y el servidor empiezan a hacer el *Handshake* (Protocolo de Enlace).

Durante el *handshake* se cumplen varios propósitos. Se hace autenticación del servidor y opcionalmente del cliente, se determina que algoritmos de criptografía serán utilizados y se genera una clave secreta para ser utilizada durante el intercambio de mensajes subsiguientes durante la comunicación.

Luego que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un resumen utilizando un algoritmo de *hash* de una vía acordado durante el

handshake, se encriptan el mensaje y el resumen y se envía, cada mensaje que se intercambia es verificado mediante el resumen.

Cuando el cliente deja una sesión SSL, generalmente la aplicación presenta un mensaje advirtiendo que la comunicación no es segura y confirma que el cliente efectivamente desea abandonar la sesión.

1.4 Marco de trabajo o *Framework*

En el desarrollo de *software* es una estructura de soporte definida en la cual un proyecto puede ser organizado y desarrollado. Típicamente, puede incluir soporte de programas, bibliotecas y un lenguaje interpretado entre otros para ayudar a desarrollar y unir los diferentes componentes de un proyecto. [21]

En la construcción de aplicaciones un marco de trabajo es una estructura conceptual y tecnológica de soporte definida, normalmente con artefactos o módulos concretos, en base a la cual una aplicación puede ser desplegada. Típicamente, puede incluir soporte de programas, bibliotecas y un lenguaje interpretado entre otros programas para ayudar a desarrollar y unir los diferentes componentes de un proyecto.

Representa una arquitectura de *software* que modela las relaciones generales de las entidades del dominio. Provee una estructura y una metodología de trabajo la cual extiende o utiliza las aplicaciones del dominio.

El marco de trabajo que se propondrá será enfocado en los puntos significativos de la arquitectura de aplicaciones para la gestión de la identidad en el e-gob de Cuba, también se incorporarán algunos elementos técnicos.

Ventajas y desventajas

Las principales ventajas de la utilización son:

- El desarrollo rápido de aplicaciones. Los componentes incluidos en un *framework* constituyen una capa que libera al programador de la escritura de código de bajo nivel.
- La reutilización de componentes, estos resultan una paradigma de la reutilización.
- El uso y la programación de componentes que siguen una política de diseño uniforme, lo que hace su curva de aprendizaje más fácil de aprender y usar.

Las desventajas son:

- La dependencia del código fuente de una aplicación. Si se desea cambiar de la infraestructura, la mayor parte del código debe reescribirse.

- La demanda de grandes cantidades de recursos computacionales debido a que la característica de reutilización de los marcos de trabajos tiende a generalizar la funcionalidad de los componentes. El resultado es que se incluyen características que están de más, provocando una sobrecarga de recursos que se hace más grande en cuanto más amplio es el campo de reutilización.

El término *framework* tiene una acepción más amplia, en donde además de incluir una biblioteca de componentes reutilizables, es toda una tecnología o modelo de programación que contiene máquinas virtuales, compiladores, bibliotecas de administración de recursos en tiempo de ejecución y especificaciones de lenguajes.

1.5 Problema científico

Con su énfasis en el uso de tecnología de la información en la prestación de servicios en el e-gob es una de las alternativas de los gobiernos para guiar los esfuerzos y que exista una democracia plena, aportando transparencia a los procesos de la administración pública y generando oportunidades a los gobiernos. En concreto, el gobierno electrónico ofrece la oportunidad de: examinar sus actuales operaciones y procedimientos, identificar los procesos y prácticas que se pueden simplificar, poner en práctica los procedimientos operativos más ágiles, e implementar nuevas tecnologías que mejoren estas prácticas. En el proceso de racionalización de las operaciones de negocio, una aplicación del gobierno electrónico ofrece una solución de concentrar sus recursos en los esfuerzos de la prestación de servicios que se proporcionan más eficientemente a través del contacto directo frente a otros medios.

Las TIC rediseñan los procesos de gobierno y transforman la manera de gobernar. No es suficiente para prestar servicios con eficiencia y eficacia mediante la compresión de los pasos necesarios para cumplir con ciertos requisitos de procedimiento. Lo más importante es el de simplificar los procesos de gobierno en conjunto, cambiar el concepto de gobernanza, y por lo tanto transformar la relación entre el gobierno y los ciudadanos.

Por otra parte, un mayor acceso de la información y la transparencia en los procesos de gobierno conduce a una mayor rendición de cuentas y transparencia, como los procesos en línea o informatizados, eliminar la discreción de los funcionarios de gobierno y proporcionar a los grupos de vigilancia y altos funcionarios del gobierno

con un mecanismo para controlar posibles abusos de corrupción por funcionarios de menor nivel de gobierno.

En el paso de los últimos años Cuba ha tenido un avance significativo científico técnico, uno de los factores que han propiciado este desarrollo es la Universidad de Ciencias Informáticas (UCI), una brillante idea de nuestro comandante Fidel Castro, denominado al principio "Proyecto Futuro", con dos objetivos: informatizar el país y desarrollar la industria del *software*, para contribuir al desarrollo económico del mismo. Más del 60% de los estudiantes están incorporados a proyectos productivos e investigativos de *software* en interés y por encargo de la sociedad cubana y de otros países, en campos como los de la educación, salud, deporte, gobierno en línea, *software* libre, sitios web, multimedia y otros.

Además de la UCI existen otras instituciones que aportan mucho al desarrollo científico técnico del país, todas estas instituciones han aportado infinidades de servicios o proyectos que favorecen al proyecto de la revolución de elevar el índice cultural e informatización del pueblo.

Debido a la innumerable cantidad de servicios que han surgido en la última década surgió la idea de establecer un gobierno electrónico en el país que guie los esfuerzos de las distintas instituciones que aportan tanto al desarrollo tecnológico pero que se encuentran muy desvinculados, además de vincular más al pueblo a los procesos del gobierno. El gobierno electrónico seguiría el mismo objetivo de desarrollo socio-económico, aunque si reordenaría los esfuerzos, sería necesario proporcionar una reducción de la brecha digital lo que logrará un avance en el tiempo.

Uno de los principales eslabones de esta cadena del nuevo modelo de administración es sin duda la Identidad Digital, es uno de los factores más significativo por el peso en la seguridad para sus usuarios, por el gran volumen de información que se manejará y por tratarse de un modelo de administración gubernamental.

En la UCI la facultad 3 está vinculada al análisis y desarrollo de aplicaciones de gobierno electrónico puesto que su perfil principal es precisamente el “Gobierno Electrónico”. El CISED (Centro de Identificación y Seguridad Digital) es el que trata todos los temas de identidad y seguridad digital en el desarrollo de aplicaciones enmarcadas en el entorno de la universidad, nacional e internacional.

1.6 Conclusiones

Se realizó un estudio de los principales conceptos relacionados con la situación problemática definida en esta investigación, entre los que se encuentra el e-gob, identidad digital, definiéndose las principales características y ventajas de su aplicación. Se identificó al DNI electrónico como el medio más seguro para soportar la identidad digital aunque resulta muy costosa su implementación, aproximadamente entre 12 y 15 dólares por persona. Es por ello que se contarán con otros medios que soporten los certificados digitales y otros aspectos identificativos para conformar la identidad digital.

Análisis de la Identidad Digital en el e-gob

2.1 Introducción

Se realiza una investigación sobre las principales tecnologías usadas para construir marcos de trabajo para la identificación digital de los gobiernos electrónicos propuestos por compañías internacionales en esta materia, realizando una valoración y análisis de las características usadas por las compañías que puedan ser aplicadas en la propuesta.

2.2 Análisis de marcos de trabajos

A continuación se describirán los marcos de trabajo usados por distintos países para gestionar la identidad digital en su e-gob. También se abordará la experiencia de 9 países de Iberoamérica en el desarrollo del e-gob municipal.

2.2.1 Japón

En agosto del 2003, los gobiernos locales a través de Japón comenzaron a alimentar la información básica sobre sus ciudadanos en una base de datos central, como parte de una red de registro de residente, a pesar de las quejas sobre el sistema de defensores de la privacidad y la negativa a participar por parte de algunos municipios.

Bajo el nuevo sistema, para todos los que viven en Japón se emitirá un número de identificación de 11 dígitos que puede ser utilizado en muchos tratos con el gobierno local. Sustituye a un sistema en el que la gente tenía que producir certificados de residencia para demostrar donde vivían cada vez que tratan con el gobierno local y que requiere la gente a ir a través de procedimientos que requieren mucho tiempo cada vez que se movían.

Información como el nombre de la persona, fecha de nacimiento, el sexo y la dirección se incluirá en el expediente de cada persona y todos los datos se almacenan en un servidor del gobierno central de gestión. El sistema tiene como objetivo hacer la vida más fácil tanto para los ciudadanos y las municipalidades locales y se conoce con el nombre de Jumin Kihon Daicho de red o Juki Net a corto plazo. Los ayuntamientos de todo Japón tendrán acceso a la base de datos, por lo que tratar con el gobierno será tan simple como encender con su número de identificación.

Sin embargo, esta facilidad de acceso hizo sonar las alarmas a través de Japón. Temiendo que la privacidad de sus ciudadanos puede estar en riesgo, algunos municipios se niegan a conectarse al sistema.

La reacción de los defensores de la privacidad se esperaban este efecto, pero la negativa de algunas ciudades para unirse a Juki-Net ha venido como una vergüenza para el gobierno, pues se considera el sistema como una parte clave de su programa de E-Japón (programa que tiene como objetivo hacer de Japón el más avanzado del mundo TIC). Uno de sus objetivos principales es la entrega en línea de muchos servicios gubernamentales, un servicio para el que una base de datos centralizada de las personas que viven en Japón sería esencial. [8]

2.2.2 España

Para dar respuesta al reto de la identificación electrónica personal, el Ministerio del Interior, mediante el organismo aliado de la Dirección General de la Policía (DGP), proporcionará a todos los ciudadanos del Estado Español un nuevo mecanismo de identificación basado en el actual Documento Nacional de Identidad (DNI). Este nuevo mecanismo permitirá al ciudadano establecer sus relaciones de confianza con terceros. [22]

Los principales objetivos que la DGP pretende poner en marcha con el nuevo DNI electrónico son los siguientes:

1. Proporcionar un mecanismo de identificación al ciudadano, de manera que tanto física como electrónicamente, se pueda acreditar la identidad del titular del DNI electrónico.
2. Posibilitar que se lleve a cabo la firma digital de documentos mediante protocolos de identificación, autenticación y firma electrónica.
3. Fomentar, en todo el Estado Español, la confianza en la Sociedad de la Información y en los nuevos medios electrónicos, proporcionando un mecanismo adecuado que garantice la identidad, privacidad y derechos fundamentales de los ciudadanos.
4. Cooperar con los diferentes proyectos europeos relacionados con la identificación digital.
5. Mantener su funcionalidad y características como documento de viaje (futuro Pasaporte), teniendo en cuenta al Reconocedor Óptico de Caracteres de la Organización Internacional de Aviación Civil2.

Para ello, la DGP tiene previsto implantar una infraestructura de clave pública (PKI) que dotará el nuevo DNI electrónico de los mecanismos necesarios para cumplir con los objetivos anteriores.

La tarjeta del DNI electrónico consiste en un soporte de policarbonato, con una durabilidad estimada de 10 años. Dicha tarjeta es similar a cualquier otra tarjeta de crédito o tarjeta con chip que se puede encontrar actualmente.

La información contenida en el chip estará firmada electrónicamente por la autoridad de certificación del DNI electrónico, con el fin de garantizar su autenticidad e integridad. Los certificados de ciudadano que se almacenan en el DNI electrónico no disponen del habitual número de desbloqueo (PUK).

Firma electrónica y Certificados digitales

Según lo dispuesto en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica (LFE) existen tres tipos diferentes de firma electrónica:

1. **Firma electrónica**: es el conjunto de datos, en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
2. **Firma electrónica avanzada**: es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
3. **Firma electrónica reconocida**: es la firma electrónica avanzada basada en un certificado reconocido y generada mediante dispositivos seguros de creación de firma.

Para poder implementar cualquiera de ellas, hace falta tener instalados los certificados correspondientes. Por otra parte, los ejes en los que se fundamenta la puesta en marcha del DNI electrónico son los siguientes: confidencialidad (capacidad de intercambiar información de forma segura y secreta), integridad (garantía de que la información no ha sido modificada ni alterada), autenticación (prueba de la identidad del emisor) y no repudio (garantía que tiene el receptor de que el emisor ha realizado una transacción).

El marco tecnológico elegido en España para el DNI electrónico se basa en el uso de tarjetas inteligentes, estarán fabricadas en torno al chip SLE66CX320P de la empresa Alemana “Infineon Technologies”. Este chip que tiene un coste aproximado

de 12 euros por tarjeta fabricada, cuenta con el certificado de evaluación de alta seguridad para el nivel E4 del ITSEC (Criterios de Evaluación de Seguridad de Tecnología de la Información*)* y está clasificado como de altas características. Según el fabricante este chip ha sido sustituido por otro más moderno, con la denominación SLE66CX322P que tiene unas prestaciones similares. Aquí la primera alerta, en una aplicación de este tipo, no cabe una implementación que en función de la economía, sea razonablemente segura, o que se sacrifiquen determinados requisitos de seguridad, para lograr otras capacidades tecnológicas. El DNI electrónico debe ser completamente seguro y en el caso de dejar de serlo, debería dejar de usarse hasta que vuelva a serlo.

Este chip pertenece a la familia “66 Plus de Infineon”. Se trata de un procesador de 16 bits fabricado con tecnología de 0,25 micrones. Está especializado en tareas criptográficas, por lo que puede procesar los algoritmos RSA (Rivest, Shamir y Adelman) con claves de hasta 2048 bits, en menos de 290 microsegundos, o trabajar con DES (Encriptación Estándar de Datos), triple DES y con criptografía de curvas elípticas. En su interior integra una gran cantidad de dispositivos, como un generador de números aleatorios por *hardware*, lógica de seguridad anti monitorización de datos y claves, una unidad de manejo de memoria (MMU), un generador de frecuencias, cifrado y descifrado DES y triple DES por *hardware*, dos temporizadores de 16 bits, un circuito de comprobación de redundancia cíclica (CRC) y la lógica de interrupciones del dispositivo. Para almacenamiento de datos y programas, cuenta con 32 kb (kilobytes) de memoria EEPROM (Memoria de Sólo Lectura Programable y Borrable Eléctricamente), 64 Kb de memoria ROM (Memoria de Solo Lectura) y 3 kb de RAM (Memoria de Acceso Aleatorio). Entre sus medidas de seguridad destacan un número de identificación único para cada chip, un dispositivo de encriptación y desencriptación de memoria para la RAM, ROM y EEPROM, un generador de números aleatorios por *hardware* verificable internamente, una disposición de elementos optimizada para dificultar el acceso a los componentes, contramedidas para el análisis de fallos diferencial, la alimentación diferencial o de análisis simple de potencia y un blindaje activo con detección de ataques.

Si en lugar del SLE66CX320P se usa un chip como el SLE66CLX320P, que tiene características similares al anterior, se dispondría de la capacidad RFID (Radio Frecuencia de Identificación). Esta tecnología, que es la misma a la utilizada en los dispositivos antirrobo de los comercios, en las llaves con inmovilizador electrónico de

los coches o en los chips para la identificación de animales de compañía, permite interactuar con la tarjeta sin necesidad de un contacto físico con ella. Dependiendo del modelo, se encuentra ante un dispositivo con interfaz dual, es decir, al que se puede acceder mediante contactos el estándar 7816 de las ISO y IEC (Organización Internacional de Normalización y Comisión Electrotécnica Internacional) o mediante una interfaz multimodo sin contactos ISO y IEC 14443.

La distancia máxima con la que se puede interactuar con estos dispositivos, varía con la frecuencia de transmisión y otros factores como el ruido electrónico, la presencia de masas metálicas o la potencia y sensibilidad del emisor e interrogador, etc., pero puede variar entre 60 centímetros y 2 metros.

2.2.3 Austria

Al igual que España, dispone desde el año 2004 de una Ley de Gobierno Electrónico que ha apostado claramente por los certificados de firma electrónica para la autenticación de los ciudadanos frente a la Administración Pública.

Derivado de esta apuesta, nace la Tarjeta de Ciudadano como eje central sobre el que giran todas las comunicaciones del ciudadano con la Administración Pública. Ahora bien, a diferencia del concepto de DNI electrónico impulsado en estados como España, Reino Unido, Bélgica o Alemania, la Tarjeta de Ciudadano no está vinculada a un tipo concreto de tecnología y ni siquiera debe ser un documento físico expedido por la propia Administración Pública, sino que basta con una tarjeta inteligente con capacidad para almacenar datos del titular, certificados electrónicos y firma digital. Incluso se puede decir que no es requisito indispensable el uso de tarjetas criptográficas, sino que basta con un dispositivo USB seguro fabricado para firmar electrónicamente.

Austria ha hecho especial hincapié, no en el documento físico, sino en el contenido del mismo, especialmente en los certificados de firma electrónica, logrando así disminuir en gran medida los costes y consiguiendo una difusión del uso de los certificados.

Por todo ello, en Austria no se puede hablar de la existencia de DNI electrónico propiamente dicho, sino del uso de certificados de firma electrónica para que los ciudadanos actúen frente a la Administración Pública de forma segura.

Esta comunidad autónoma uniprovincial que se ubica al norte de España, con una superficie total de 10.603,57 km2, con una población de 1.070.215 (2,38% de España), consta de un alto índice de dispersión geográfica con 100 habitantes por km^2.

En 2004, el Principado de Asturias disponía de más de 800 servidores, con casi 500 aplicativos desarrollados en más de 20 entornos de desarrollo distintos. La Figura 3 referencia la Diversidad tecnológica de Austria.

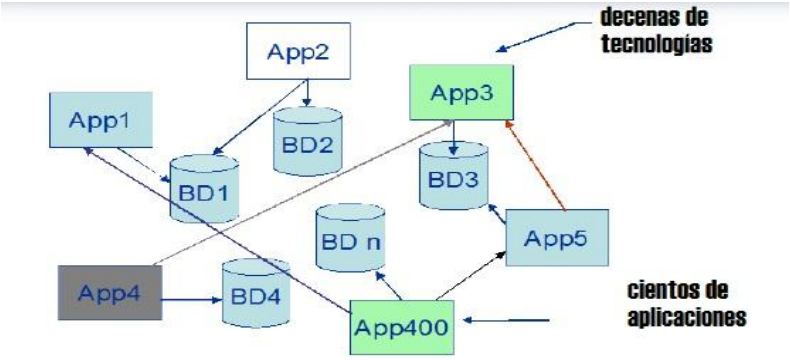


Figura 3. Diversidad tecnológica de Austria

Ante la presencia de esta problemática se planteó la idea de unir estas aplicaciones y trata de centrar las ideas con un mismo fin, pues existían muchas aplicaciones que implementaban componentes muy parecidos a los que otra aplicaciones.

Para solucionar el problema anterior el gobierno australiano decidió llevar a cabo la creación del *framework* "openFWPA", desarrollado para sistemas de gobierno electrónico basado en la tecnología J2EE, iniciativa impulsada desde la Dirección General de Informática del Gobierno del Principado de Asturias.

La solución consiste en más de 100000 líneas de código de desarrollo. Las decenas de sistemas en producción que funcionan sobre él reflejan su solidez y estabilidad, pieza clave en el éxito del modelo de e-gob de Asturias, que le ha permitido ser un punto de referencia a nivel nacional. [23] La Figura 4 se modela el *framework* openFWPA

El openFWPA está basado sobre las tecnologías libres:

Libertad de elección: no depende ni está condicionado por un solo proveedor

Seguridad y privacidad de sistemas y de datos: permite la auditoría completa del sistema informático.

Perdurabilidad de la información: garantiza el acceso a los documentos en el presente o futuro usando cualquier plataforma.

Fomento de la industria local: la inversión en el desarrollo tecnológico repercute sobre la industria y el empleo local.

Reutilización del código: no hace falta realizar una y otra vez lo mismo por diferentes organizaciones.

Desarrollo cooperativo: mejora de la calidad y disminución del coste del desarrollo y mantenimiento.

Fomento de los estándares: cumplimiento de la Ley de Administración Electrónica

No discriminación: el *software* libre da mejor soporte a la diversidad tecnológica de la ciudadanía.

Coherencia con otras administraciones: cada vez más organizaciones usan, implantan o desarrollan *software* libre.

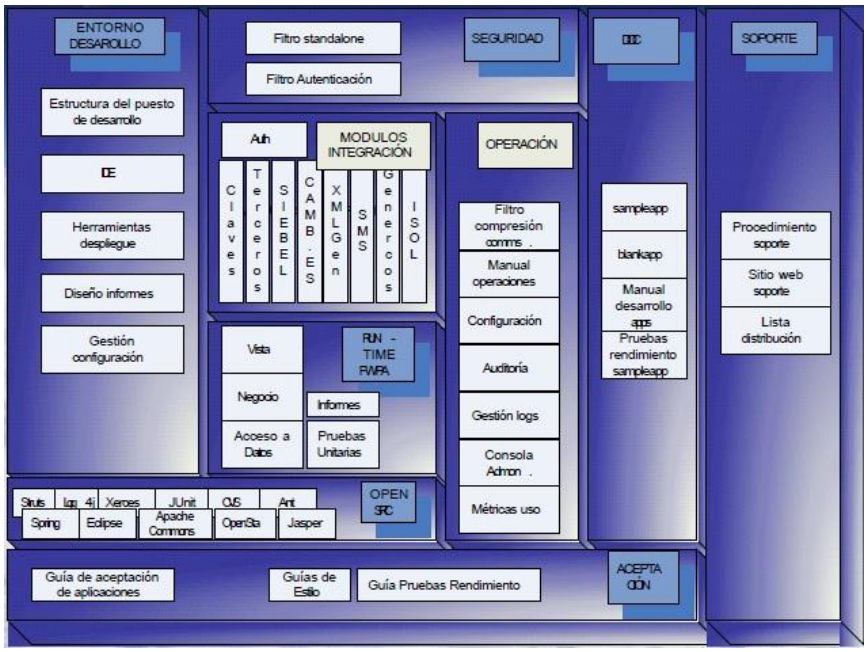


Figura 4. Visión global del *framework* openFWPA

2.2.4 México

Tener una identidad en la red es el poder contar con un conjunto de atributos que son contenidos en varias cuentas individuales con diferentes proveedores de servicios; dichos atributos incluyen información como el nombre, números de teléfono, claves de identidad ciudadana, direcciones, información de pagos, registros de crédito, etc. El conocer estos atributos, permite generar mayores ambientes de interoperabilidad y la habilidad de tener mayor conocimiento de los ciudadanos para poder interactuar con estos de mejor manera y poder brindarles mayores oportunidades.

Los círculos de confianza son los principales habilitadores de la identidad federada. Es un grupo de proveedores de servicio que comparten identidades con los debidos acuerdos de negocio, para establecer cómo hacer negocios e interactuar con identidades. Una vez que un ciudadano (o en su caso otra dependencia) ha sido autenticado por un proveedor de identidad de un círculo de confianza, puede acceder a los servicios definidos por los demás proveedores de servicio en dicho círculo de confianza.

Establecer dichos acuerdos entre las dependencias o entidades participantes es el primer paso para poder generar una identidad en la red y así lograr interoperabilidad entre servicios.

Un proveedor de identidad, es la entidad en el esquema de autenticación que crea, mantiene y administra la información entre los círculos de confianza. Para la arquitectura tecnológica de servicios electrónicos gubernamentales el proveedor de identidad podría delegarse al Portal Ciudadano del Gobierno Federal.

Un proveedor de servicio es la entidad que publica los servicios en un círculo de confianza, los cuales podrían ser: las dependencias del Gobierno Federal, empresas que participen en los procesos de negocio de los servicios electrónicos (bancos, afianzadoras, etc.).

El desarrollo de una arquitectura tecnológica de servicios electrónicos para el Gobierno Federal, implica establecer fundamentos que soporten la implementación y la ejecución de servicios en un ambiente de interoperabilidad mediante la reutilización de componentes y mejores prácticas de una Arquitectura Orientada a Servicios. La Figura 5 representa el esquema utilizado por el gobierno de México.

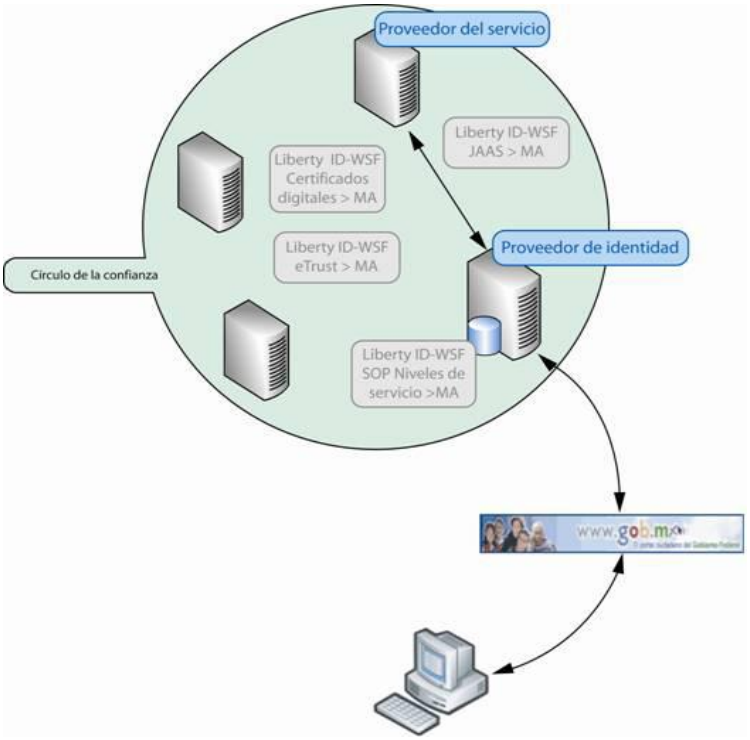


Figura 5. Esquema de federación de identidad

Los servicios web surgen de la necesidad de establecer un sistema de intercambio de datos normalizado entre aplicaciones, es decir de la necesidad de integrar datos y procesos entre aplicaciones que están programadas con lenguajes diferentes, y que se ejecutan en equipos con sistemas operativos basados en distintas tecnologías.

Los servicios web por sí mismos son muy simples, ya que proporcionan un lenguaje estándar para el intercambio de datos XML (Lenguaje de Marcas Extensibles) que es independiente de la plataforma empleada, y además viaja a través del protocolo HTTP (Protocolo de Transferencia de Hipertextos), por lo que puede emplearse a través de internet siendo una característica más para lograr dicha integración. [24]

2.2.5 Bélgica

El gobierno electrónico se ha convertido en un fenómeno global. Ha habido algo de grandes innovaciones en el gobierno electrónico sobre la última década. Muchos gobiernos compiten por el liderazgo en ofrecer servicios en línea. La mayoría han desarrollado estrategias detalladas para darse cuenta de sus programas de gobierno electrónico. Aunque las metas detrás de estos programas discrepan a través de los países, hay todavía muchos populachos entre ellas. Tales populachos resultan de la aplicación de mejores prácticas.

Los gobiernos tienen la tendencia para aprender el uno del otro. Se podrá identificar ciertas tendencias en las estrategias del gobierno electrónico de aplicación, pero los problemas son en su mayor parte asociados con la implementación.

Se estudiaron las estrategias de 21 países además de la Unión Europea para proponer un *framework* estratégico genérico para el gobierno electrónico. El propósito de este estudio es introducir una mejor infraestructura para ponerla en práctica que sea lo suficientemente genérica para ser adoptada por cualquier estrategia de un gobierno, donde se sostienen los beneficios que esta pueda aportar a las aplicaciones.

El *framework* propuesto incorpora elementos y principios muy importantes, tiene características deseables que le pueden añadir valores en dependencia de la estrategia del gobierno electrónico. A diferencia de otros estudios, en este se definen bloques constructivos de e-gob basado en implementaciones de otros que se encuentran desplegados por los países revisados. Posee un diseño modular, es flexible, capaz de ser usados por varios gobiernos y extensible. Para este se tomaron en consideración las tendencias más exitosas, además que supere prácticas de trabajos pertinentes de otros estudios. Este es muy útil para incorporar las estrategias, simplemente le añade las estrategias definidas por el gobierno.

El *framework* propuesto le ofrece una visión global del programa de gobierno electrónico e incorpora componentes muy importantes, así como los distintos tipos de usuarios con sus respectivas relaciones y además de los canales de comunicación. Para generar una mayor eficiencia y calidad ha sido modularizado para lograr una mejor flexibilidad, extensibilidades y menor costo de la aplicación.

A diferencia de otros esta es una propuesta muy sólida pues está basada en los gobiernos electrónicos de 21 países además de la Unión Europea. Obteniendo como resultado un *framework* con estrategias generales que puede ser adoptado por distintos tipos de gobiernos, esperando que ayude a los practicantes y los investigadores para la mejor implementación y comprensión de gobierno electrónico. [25] La Figura 6 modela el marco de trabajo propuesto por Bélgica.

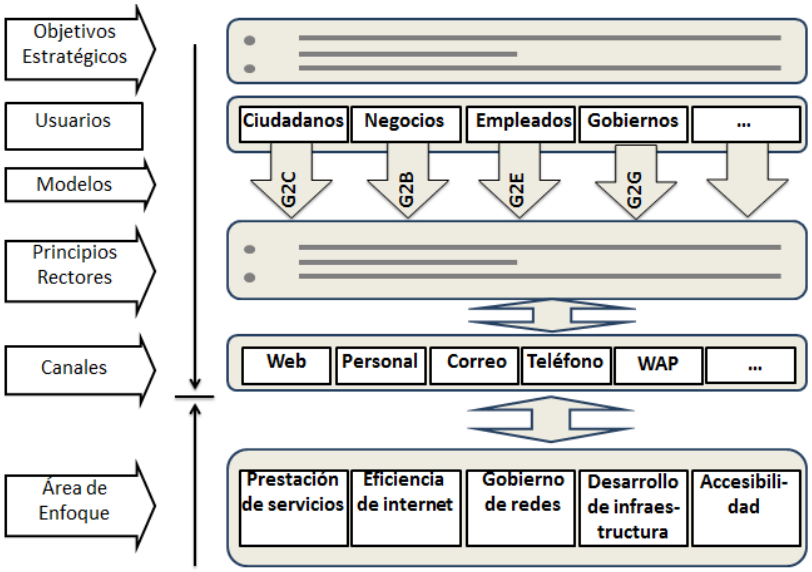


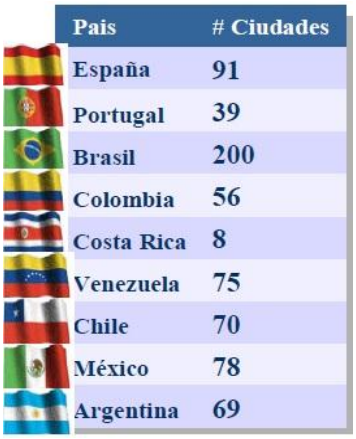
Figura 6. *Framework* estratégico de Bélgica

2.2.6 Iberoamérica

En los últimos años, las municipalidades de Iberoamérica han hecho grandes esfuerzos para potenciar la implantación y el uso de las tecnologías de información. Los portales municipales se han convertido en un importante medio de comunicación entre las autoridades y los ciudadanos, dentro del ámbito que se denomina gobierno electrónico.

Para evaluar el resultado de este desarrollo y definir estrategias y mejores prácticas que podrían ser transferidas entre municipios, se decidió estudiar los servicios de gobierno electrónico que se ofrecen en el entorno municipal de Iberoamérica.

Este trabajo es resultado de una amplia investigación que considera nueve países (México, Brasil, Costa Rica, Colombia, Venezuela, Argentina, Chile, España y Portugal) y 686 ciudades, y que se ha realizado en el marco de la Cátedra Alianza SUMAQ en e-Government. La Figura 7 muestra la cantidad de países con las ciudades que emplean este tipo de gobierno electrónico.



Pais	# Ciudades
España	91
Portugal	39
Brasil	200
Colombia	56
Costa Rica	8
Venezuela	75
Chile	70
México	78
Argentina	69

Figura 7. Número de ciudades evaluadas por país

Las principales razones para hacer un estudio del gobierno electrónico municipal son:

- Es más cercano al ciudadano.
- La mayoría de los servicios son de carácter local y municipal.
- Existe la posibilidad de adaptar los servicios a las características locales y regionales.
- El nivel local tiene una dimensión apropiada para generar procesos innovadores y hacer con que se crean mejores prácticas.
- El Portal es la imagen de la ciudad

Modernizar el gobierno local es mejorar la calidad de los servicios locales y la eficiencia de la democracia local.

Una vez definida la muestra se aplicó el modelo de gobierno electrónico formulado. Este modelo contempla cinco fases, las que representan distintos grados de madurez y sofisticación tecnológica de manera creciente. Cada fase posee ciertos servicios, que dan cuenta de las prestaciones que ofrece el portal municipal. La Figura 8 muestra las fases y los servicios que desarrollan en cada una de ellas

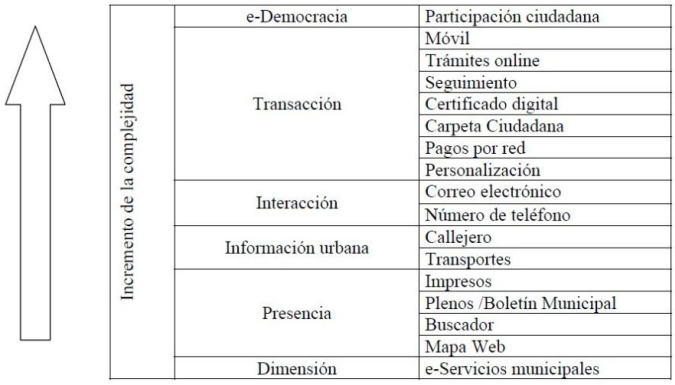


Figura 8. Modelo de gobierno electrónico municipal

Cada una de estas fases se define de la siguiente forma:

Presencia: en esta fase los servicios tienen la capacidad de proveer información sobre su acción al ciudadano, es decir, existe información en línea y la incorporación de esquemas de búsqueda básicas; permite, por ejemplo, la descarga de archivos y formularios.

Información urbana: proveer información sobre las calles y transportes urbanos. Esta información exige en muchos casos herramientas tecnológicas avanzadas como el GIS (Sistema de Información Geográfica), y la posibilidad de búsquedas rápidas.

Interacción: considera comunicaciones simples entre el servicio y el ciudadano, el contacto se realiza por teléfono o correo electrónico.

Transacción: incluye una interacción electrónica bidireccional entre el ciudadano y el servicio, en forma alternativa a la atención presencial en las dependencias del órgano, incluye autentificación, procesamiento de formularios, etc.

e-democracia: incluye servicios de participación ciudadana como foros de conversación sobre cuestiones municipales o páginas adaptadas a discapacitados.

Se puede establecer que las municipalidades están aprovechando, fundamentalmente, sus portales como un buen medio de comunicación unidireccional, sólo desde la municipalidad hacia el ciudadano.

El grado de desarrollo o complejidad de los portales municipales se puede considerar en general bastante bajo, muy pocas ciudades alcanzan un nivel de excelencia en este sentido.

Para que el gobierno electrónico sea una realidad en Iberoamérica es importante que se avance rápidamente en la implantación de sistemas como el DNI electrónico o el certificado digital. Sin estos medios será imposible hacer realidad los servicios

electrónicos y ofrecer al ciudadano servicios con calidad y que realmente le traigan beneficios.

Finalmente, se está usando el tema de gobierno electrónico y democracia digital como medios de potenciar la comunicación entre los gobiernos y los ciudadanos, además potenciar la confianza de los ciudadanos en las instituciones públicas, sin embargo y de forma contradictoria a este discurso, muy pocas ciudades ofrecen medios para que los ciudadanos puedan participar e interactuar con sus municipios. [26]

Se adquirieron varias características o elementos que pudieran ser incluidos en la propuestas de marco de trabajo conceptual.

El DNI electrónico es uno de los medios más seguro para soportar la identidad digital, consta con un chip que contiene los datos del usuario y certificado digital que asegura sus transacciones. Le permite al usuario identificarse a simple vsita, además la tarjeta presenta marcas de seguridad que evitan su falsificación.

Uno de los puntos interesantes que se observaron es que varios países optan por las tecnologias libres por varias razones. El desarrollo de la propuesta se deberá realizar sobre tecnologías libres, para lograr que no existan barreras tecnológicas que impidan su desarrollo.

Los certificados digitales son un punto clave para la identidad digital, mediante ellos se pueden asegurar las transacciones, existen varias formas alternativas de implementarlos, unas más caras que otras, por ejemplo, el DNI electrónico, USB dedicado a esta acción de certificar.

La Arquitectura Orientada a Servicios utilizada para exponer los servicios del gobierno electrónico de varios países, aportándole agilidad y rapidez en la contrución de un determinado servicio necesitado por los usuarios, también se suele adaptar con gran rapidez a los cambios.

Tambien se obtuvieron varios canales de comunicación que se deberán aboradar en la propuesta, por los cuales se debe trasmitir la información de manera segura y confiable para ambas partes del intercambio de la misma.

Se identificaron los servicios y clientes en los que se debe enfocar el e-gob electrónico de Cuba.

2.3 Patrones de Arquitectura

Un aspecto importante cuando se va a construir un *software* es sin duda su arquitectura, mediante ella se guían los esfuerzos hacia un fin.

La Arquitectura de *Software* se refiere a un grupo de abstracciones y patrones que brindan un esquema de referencia útil para guiar el desarrollo de *software* dentro de un sistema informático. [27]

Se puede definir como un campo específico de estudio para los investigadores e ingenieros del *software*, su ámbito se centra en el nivel del proceso de diseño en el que se deciden las propiedades estructurales del sistema.

La importancia de representar de forma explícita la arquitectura de los sistemas de *software* es evidente. En primer lugar, estas representaciones elevan el nivel de abstracción, facilitando la comprensión de los sistemas de *software* complejos. En segundo lugar, hacen que aumenten las posibilidades de reutilizar tanto la arquitectura como los componentes que aparecen en ella. Por último, es posible analizar la arquitectura del sistema determinando cuáles son sus propiedades aún antes de construirlo.

Los patrones arquitectónicos son estructuras conceptuales en términos de organización de *software*, donde se definen componentes y la forma de comunicación entre ellos, además de un conjunto de restricciones que pueden ser combinadas y presenta un conjunto de reglas para la construcción de la aplicación.

2.3.1 Arquitectura Orientada a Servicio (SOA)

Actualmente, no existe una definición única de lo que es SOA, o dicho de otra manera, existen múltiples definiciones, que dependen del organismo de estandarización, empresa o consultora del sector de las Tecnologías de la Información (TI) que la emita.

A continuación se citan algunas de las definiciones de SOA creadas por las principales organizaciones especializadas en la estandarización:

- Según la Organización para la Mejora de las Normas de Información Estructurada (conocida como OASIS[1]), SOA es un paradigma para organizar y utilizar capacidades distribuidas, funciones que pueden estar bajo el control de

[1] OASIS: *Organization for the Advancement of Structured Information Standards*; es un consorcio internacional sin fines de lucro que orienta el desarrollo, la convergencia y la adopción de estándares de comercio electrónico y servicios web.

diferentes dominios, proporcionando un medio uniforme para ofrecer, descubrir y utilizar dichas capacidades para producir los efectos deseados para cubrir una necesidad [28].

- Para el Grupo Abierto (*Open Group*[2]), una arquitectura SOA no es más que un estilo arquitectural que soporta orientación a servicios [29]. Por estilo arquitectural se entienden los aspectos que definen o expresan un tipo específico de arquitectura, y por orientación a servicios el modo de pensar y enfocar el desarrollo basándose en la definición del concepto de servicio.
- Para el Grupo de Gestión de Objetos (conocido como OMG[3]), una arquitectura SOA es un estilo arquitectural para una comunidad de consumidores y proveedores de servicios para alcanzar valor mutuo [30], de forma que:
    - Se permite a los participantes de la comunidad, el trabajo conjunto con mínima dependencia tecnológica.
    - Especifica los contratos a los que las organizaciones, personas y tecnologías deben adherirse para participar en la comunidad.
    - Garantiza que el valor y los procesos de negocio son aportados por la comunidad.
    - Permite el uso de una variedad de tecnologías para facilitar las interacciones dentro de la comunidad.

Para definir SOA se puede sencillamente optar por tomar en cuenta su propia representación, puede considerarse como un paradigma o un estilo arquitectónico, pero más allá se puede ver como una forma de pensar, solo se debe tener en cuenta que la clave fundamental son los servicios.

Las Arquitecturas Orientadas a Servicios están formadas por servicios de aplicación débilmente acoplados y altamente interoperables. Para comunicarse entre sí, estos servicios se basan en una definición formal independiente de la plataforma y del lenguaje de programación. La definición de la interface encapsula las particularidades de una implementación, lo que la hace independiente del fabricante, del lenguaje de

[2] ***Open Group:*** es un consorcio de la industria del software que provee estándares abiertos neutrales para la infraestructura de la informática. Es muy famoso por sus sistemas de certificación de la marca UNIX.

[3] **OMG**: *Object Management Group*; es un consorcio dedicado al cuidado y el establecimiento de diversos estándares de tecnologías orientadas a objetos tales como UML, XMI y CORBA. El grupo está formado por compañías y organizaciones de software como son: Hewlett-Packard (HP), IBM, Sun Microsystems y Apple Computer.

programación o de la tecnología de desarrollo. Con esta arquitectura se pretende que los componentes de *software* desarrollados sean muy reusables, ya que la interfaz se define siguiendo un estándar; así un servicio desarrollado en CSharp podría ser usado por una aplicación Java o viceversa, no importa en qué lenguaje se construyó un servicio para ser utilizado.

SOA es un estilo de arquitectura en el cual se exponen los procesos de negocio del sistema a construir como servicios independientes de alta cohesión y bajo acoplamiento que encapsulan dichos procesos y pueden ser invocados a través de interfaces bien definidas.

La SOA es un concepto de arquitectura de *software* que define la utilización de servicios como construcciones básicas para el desarrollo de aplicaciones. Es una arquitectura de una aplicación donde las funcionalidades se definen como servicios independientes, con interfaces accesibles, bien definidas, que pueden ser llamadas en secuencias dadas para formar procesos de negocios.

SOA está resultando un paradigma para la integración de sistemas empresariales, que no sólo integra diferentes tipos de *software* sino que además es independiente de la plataforma, el sistema operativo y el dispositivo.

Razones para usar SOA

Existen varias razones para adoptar un enfoque SOA, y más concretamente un enfoque SOA basado en servicios web:

Reutilización: el factor fundamental en el cambio a SOA es la reutilización de los servicios de negocio. Las funciones de negocio, dentro de una empresa y los socios del negocio, pueden ser expuestos como servicios web y ser reutilizadas para cubrir nuevas necesidades de negocio.

Interoperabilidad: el objetivo de una arquitectura débilmente acoplada es que los clientes y servicios se comuniquen independientemente de la plataforma en que residan. Los protocolos de comunicación con servicios web son independientes de la plataforma, lenguaje de codificación y sistema operativo por lo que facilitan la comunicación.

Escalabilidad: como los servicios de SOA están débilmente acoplados, las aplicaciones que usan esos servicios escalan fácilmente. Esto es debido a que existe muy poca dependencia entre las aplicaciones clientes y los servicios que usan.

Flexibilidad: es otra de las características que proporciona el acoplamiento débil entre los servicios. Cualquier cambio en la implementación de uno de ellos no afectaría al resto siempre que se mantenga la interface.

Eficiencia de coste: se basa en la exposición de servicios ya existentes para ser reutilizados. Al usar servicios web, para exponer estos servicios, se reutilizan la infraestructura web existente virtualmente todas las organizaciones por lo que se limita considerablemente el costo.

2.3.1.1 Servicios Web

Los servicios son actividades identificables dentro de un negocio, son el resultado de esfuerzos humanos o mecánicos que producen un desempeño o un esfuerzo que implican generalmente la participación del cliente y que no es posible poseer físicamente o almacenarlos, pero que pueden ser ofrecidos a los clientes para satisfacer sus necesidades.

Un servicio web es cualquier servicio que está disponible a través de Internet, utiliza un estándar XML (Lenguaje de Marcas Extensible) sistema de mensajería, y no está ligado a ningún sistema operativo o un lenguaje de programación.

Un servicio web debe ser autodescriptible. Si publica un nuevo servicio web también debe publicar una interface para el servicio. Como mínimo el servicio debe incluir la documentación legible para que otros desarrolladores puedan integrar fácilmente el servicio a sus aplicaciones.

Un servicio web debe ser visible. Si crea un servicio web, debe haber un mecanismo relativamente sencillo para que usted pueda publicar este hecho, debe ser un mecanismo sencillo mediante el cual los interesados pueden encontrar el servicio y localizar su interface pública. El mecanismo exacto podría ser a través de un completo sistema descentralizado o un sistema de registro más lógico centralizado.

La arquitectura de servicios web, ofrece una alternativa interesante para desacoplamiento de presentación de los contenidos.

Un consumidor de un servicio web no está vinculado directamente al servicio web, la interfaz del servicio web puede cambiar con el tiempo sin comprometer la capacidad del cliente para interactuar con el servicio. Un sistema fuertemente acoplado implica que el cliente y el servidor de la lógica son estrechamente vinculados entre sí, lo que implica que si uno cambia la interfaz, el otro también debe cambiarla. La adopción de

una arquitectura de acoplamiento flexible tiende a hacer los sistemas de *software* más manejables y sencillos, permitiendo la integración entre diferentes sistemas.

2.4 Conclusiones

Se realizó un estudio de homólogos analizando la aplicación de los e-gob en el mundo, el tipo de identidad y la infraestructura que se usa para la construcción de aplicaciones para el mismo, analizando las características que pueden ser aplicadas a Cuba. Los sistemas de gobiernos electrónicos deben construirse mediante aplicaciones web, enfocándose en los servicios web, permitiéndole ser usadas por varias plataformas.

Se identificaron elementos interesantes para la propuesta que se pudieran usar en ella tales como: canales de comunicación y clientes en los que el e-gob debe enfocarse; el DNI electrónico como uno de los medios para soportar los elementos de la identidad digital más convincente pero a su vez muy costoso para desplegarse en Cuba; los certificados digitales proporcionan seguridad a las transacciones realizadas entre usuarios y sistemas; las arquitecturas orientadas a servicios le brindan mayor agilidad y eficiencia a los procesos de desarrollo de aplicaciones de gobierno electrónico, convirtiéndolos más sostenibles y graduables a cambios futuros.

Propuesta de Solución

3.1 Introducción

En este capítulo a partir del análisis realizado sobre las tendencias de marcos de trabajos para los e-gob se realizará la propuesta de marco de trabajo conceptual para la identificación digital en el gobierno de Cuba, esta se basará sobre los principios de las tecnologías libres para lograr independencias tecnológicas. Se especificarán los tipos de servicios y los clientes en los que debe enfocarse el e-gob de Cuba. Se describirán aspectos a tener en cuenta en el diseño del marco de trabajo como SOA y cómo se garantizará la identidad digital en el e-gob de Cuba.

3.2 Tecnologías libres

El *software* libre es la denominación del *software* que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, cambiado y redistribuido libremente. Según la *Free Software Foundation*[4], el *software* libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el *software* [31].

De manera general se puede resumir que el *software* libre es aquel que puede ser distribuido, modificado, copiado y usado; por lo tanto, debe venir acompañado del código fuente para hacer efectivas las libertades que lo caracterizan. Es conveniente no confundir el *software* libre con el *software* gratuito, este no cuesta nada, hecho que no lo convierte en *software* libre, porque no es una cuestión de precio, sino de libertad.

Los motivos más importantes para que un país en desarrollo utilice el *software* libre [23] son los siguientes:

Reutilización: no hace falta realizar una y otra vez lo mismo por diferentes organizaciones.

Desarrollo cooperativo: mejora de la calidad, disminuye los costos del desarrollo y mantenimiento.

No discriminación: el *software* libre da mejor soporte a la diversidad tecnológica de la ciudadanía.

[4] ***Free Software Foundation*** (Fundación para el *software* libre): es una organización creada en octubre de 1985 por Richard Stallman y otros entusiastas del *software* libre con el propósito de difundir este movimiento.

Seguridad y privacidad: permite la auditoría completa del sistema informático, corrigen sus errores con mayor rapidez que el *software* propietario.

Acceso a la información: el *software* representa conocimiento en las reglas, procedimientos, métodos, y estructura de datos. Este conocimiento puede ser utilizado en educación, por los sectores productivos, impulsando la sociedad del conocimiento. Garantiza el acceso a los documentos en el presente o en el futuro usando cualquier plataforma.

Independencia tecnológica: mediante el uso de *software* libre, el estado deja de tener sus sistemas controlados por una entidad externa (con frecuencia empresas extranjeras). De esta forma rompe la dependencia tecnológica que lo tiene actualmente atado y obtiene las libertades que el *software* libre otorga.

Confiabilidad y estabilidad: el *software* libre, al ser público, está sometido a la inspección de una multitud de personas, que pueden buscar problemas, solucionarlos, y compartir la solución con los demás. Debido a esto los programas libres gozan de un excelente nivel de confiabilidad y estabilidad, requerido para las aplicaciones de gobierno.

El *software* libre ofrece grandes beneficios a una nación en desarrollo. Cuba es un país en vísperas de desarrollo que ha buscado siempre obtener una independencia tecnológica y lograr un desarrollo socioeconómico elevado, el cual siempre ha estado frustrado por las barreras económicas a las que se ha visto sometido, por eso como país en desarrollo la mejor opción será optar por las tecnologías libres para lograr sus metas.

3.3 Tipos de servicios

En la propuesta el e-gob de Cuba se centrará en dos tipos de servicios:

- Gobierno a ciudadano (G2C)

En este servicio será fundamental para el gobierno cubano, se vinculará a los ciudadanos más de cerca con la propagación de la información de los servicios públicos, así como de atención al ciudadano de los servicios básicos como educación, salud, información de los hospitales, bibliotecas, etc.

- Gobierno a gobierno (G2G)

Servicios G2G llevará a cabo en dos niveles: a nivel local o nacional como a nivel internacional. Servicios G2G son las transacciones entre el gobierno central, nacional y local, y entre los organismos a nivel departamental. Al mismo tiempo, los servicios de

G2G son las transacciones entre gobiernos, y puede ser utilizado como un instrumento de las relaciones internacionales y la diplomacia.

3.4 Clientes

Las transacciones de los servicios del e-gob de Cuba deben enfocarse en los siguientes clientes:

- Ciudadanos: serán todas las personas que estén vinculados al gobierno cubano y que tenga una residencia permanente, temporal o transitoria en el país.
- Agencias gubernamentales: serán todo tipo de entidades nacionales e internacionales, así como agencias gubernamentales que realicen transacciones con el gobierno cubano.

3.5 Propuesta de Arquitectura

La propuesta constará de este estilo arquitectónico (SOA), pensando en lo rápido que avanza el desarrollo tecnológico a nivel internacional y la necesidad de un gobierno electrónico en nuestro país, esta arquitectura será fundamental pues brindará una mayor rapidez y una reducción importante del costo de la aplicación. Con SOA se logrará agilidad en el negocio y hacerlo más competitivo, de forma que no se demore en brindar el servicio que necesite un usuario con el fin de satisfacer sus necesidades en un corto tiempo y lograr un aumento de la satisfacción y la lealtad del cliente ofreciendo una perspectiva única y coherente de la información integral, precisa y oportuna.

Aportará a la arquitectura un fortalecimiento en la adaptabilidad y la agilidad de respuesta a las necesidades cambiantes del negocio con una capa de abstracción de datos que reduce la fragilidad de la infraestructura.

Reduce los costos del desarrollo y puesta en práctica con una tecnología flexible basada en estándares que fomenta la reutilización de la lógica y las habilidades de integración de datos en las líneas de negocio. Disminución de la complejidad mediante la integración fluida y la limitación de sus puntos. Minimiza los riesgos de tiempo de inactividad o pérdidas de datos ofreciendo rendimiento, escalabilidad, seguridad y alta disponibilidad sin precedentes.

Además pues para que los gobiernos electrónicos tengan influencia en una nueva sociedad deberá brindar servicios ininterrumpidos y que satisfagan las necesidades de

los ciudadanos, mediante SOA se podrá brindar servicios con este tipo de exigencias por parte de e-gob de Cuba, además le dará la posibilidad de adaptarse a nuevos cambios tecnológicos que pudieran surgir y se podrán integrar con otros sistemas independientes.

Los usuarios que interactúan con la aplicación estarán generalizados en dos grupos compuestos por:

Personas: serán las personas físicas o jurídicas las cuales posean características biométricas.

Sistemas: serán aplicaciones pertenecientes a entidades, empresas y agencias gubernamentales nacionales o extranjeras, todas deben ser físicas o legales, o sea no serán entidades reales que estén respaldas legalmente.

En el intercambio con la propuesta no se deben admitir usuarios virtuales, a los cuales no se le puedan relacionar características físicas o al menos no tengan respaldo legal. Este requerimiento será una medida de seguridad para que puedan existir responsables de las acciones que se realizan virtualmente.

El Bus de servicios proporciona una capa de abstracción para comunicar mediante servicios las capas inferiores a él con los usuarios a que van dirigido los servicios. Contendrá una serie de servicios que serán brindados por la aplicación, un servicio puede estar concebido por un proceso (flujo de pasos en un orden lógico).

El Control de Acceso asegurar que los servicios que se brindan lo consuman los usuarios que estén autorizados a usarlos, cuando se solicite el acceso a un servicio primero deberá consultar si el usuario que está realizando la solicitud puede consumir este servicio. El acceso a un servicio se establecerá mediante políticas, estas se le establecerán a cada usuario o grupo de usuarios, también se pueden definir políticas para cada servicio o grupo de servicios. A cada grupo se le pueden relacionar una o varias políticas o simple mente ninguna, por ejemplo, un usuario que no tenga ninguna política asignada podrá consumir todos los servicios que estén disponibles, en otro caso, cuando un usuario realiza una llamada a un servicio en específico se le realizará un control de acceso, se verificarán las políticas para comprobar que el usuario no tenga ninguna restricción sobre el servicio que necesita, si esta validación resulta positiva el usuario se beneficiará con la utilización del servicio, en otro caso se le negará el acceso a este. La Figura 9 muestra como ocurre el flujo descrito anteriormente.

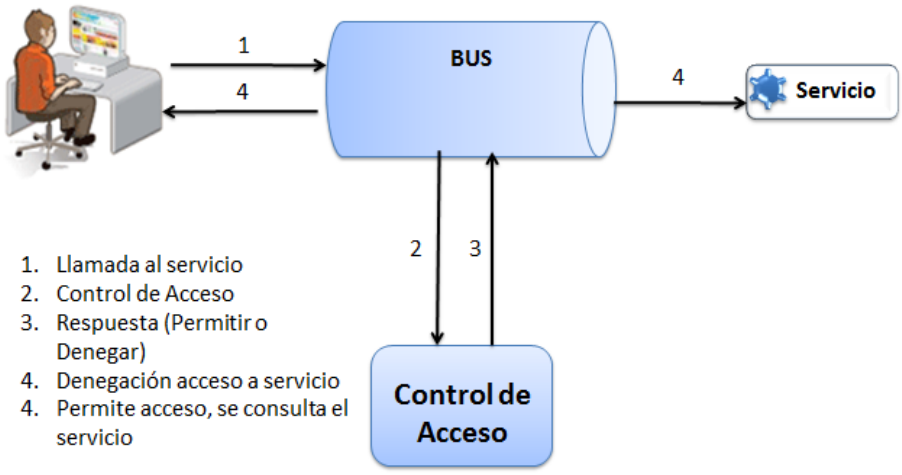


Figura 9. Control de Acceso a un servicio

Una política se genera a partir de parámetros, a continuación se muestran algunos de los parámetros que deberá poseer una política:

- Nombre de la política.
- Servicio o lista de servicios.
- Periodo de validación que tendrá la política.
- Usuario o grupo de usuarios a los que va dirigida esta política.
- Operación que realizará, puede estar dado por una Aceptación o Denegación.

Un ejemplo de una política pudiera estar definido como se muestra en la Figura 10

	Política
Nombre de Política	Política A
Restringir a	Servicio de Identidad Servicio Autenticación
Periodo de Validación	09/06/2012 a 10/06/2012
Asignar a	chalonso
Tipo de Operación	Aceptación

Figura 10. Estructura de Política

La Capa de Servicios de Procesos será la responsable de desarrollar el flujo de pasos en un orden lógico para cada servicio que requiera un proceso, de esta manera se simplificarán los problemas haciéndolos más sencillos y comprensibles para el grupo de trabajo de desarrollo e incluso para los usuarios. Además como

características de los procesos se podrán detener y continuar en un momento determinado.

La Capa de Negocio es aquí donde se establecen todas las reglas que deben cumplirse. Esta capa se comunica con las capas superiores a ellas (BUS, Capa de Servicios de Procesos y Control de Acceso), para recibir solicitudes de servicios que son tratadas según las reglas del negocio definidas y presentar los resultados a partir de servicios, comunicándose con la Capa de Acceso a Datos para solicitar al proveedor los datos almacenados para su gestión.

La Capa de Acceso a los Datos sirve como puente entre la Capa de Negocio y el proveedor de datos, su propósito primario es separar al proveedor de datos del resto de la aplicación, de manera que si se emigra hacia otro proveedor de datos no afecte este cambio al resto de la aplicación y los cambios solo sean en esta capa.

La Figura 11 representa gráficamente la arquitectura propuesta.

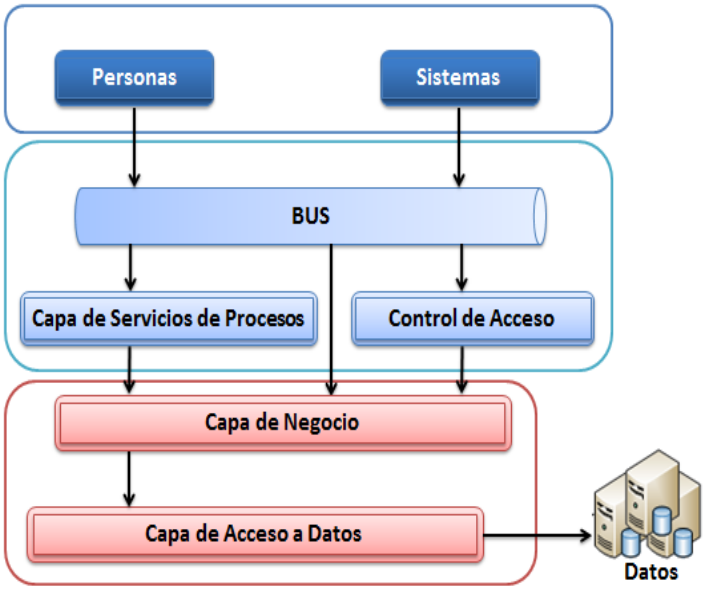


Figura 11. Propuesta de Arquitectura

Seguridad del canal de transmisión y los mensajes

La manera más fácil de asegurar las comunicaciones es estableciendo un canal seguro a través del cual la información viaje sin complicaciones. Mediante los protocolos HTTP (Protocolo de Transferencia de Hipertexto) y SSL, conformando lo que normalmente se conoce como HTTPS (Protocolo Seguro de Transferencia de Hipertexto).

SSL es un protocolo de transferencia segura de datos mediante encriptación con el cual se permitirá realizar una comunicación segura entre los usuarios (en este caso

específico serán Personas o Entidades) y sistemas, proporcionando autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Los protocolos permiten a las aplicaciones cliente servidor comunicarse de una forma para prevenir que los mensajes no sean intervenidos por usuarios no deseados.

La comunicación lo que se hace es encriptar el canal usando para ello claves simétricas, se utiliza la misma clave tanto para encriptar como para desencriptar y que es negociada entre los puntos extremos donde se establece la conexión. Toda la información que viaje por dentro de este canal está protegida por dicha encriptación aunque no exenta de sufrir alteraciones o acceso no autorizado.

Para encriptar el canal, el navegador del cliente envía una clave maestra, cifrándola primero con la clave pública del servidor, contenida en el certificado, para a partir de ella entonces generar en conjunto con el servidor una clave de sesión para el intercambio de toda la información. Y así es como se genera una conexión SSL, a groso modo para asegurar las comunicaciones. La Figura 12 muestra el proceso descrito anteriormente.

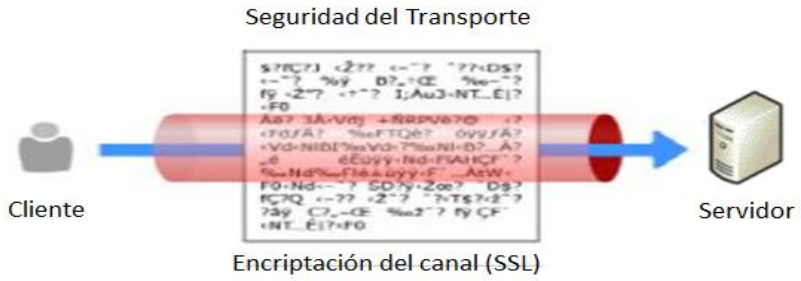


Figura 12. Encriptación del Canal de comunicación

Pero además se debe asegurar el mensaje, pues se aseguró el canal por donde viaja la información pero esta viaja en texto plano, la cual pudiera ser leída fácilmente por un usuario no deseado. Para asegurar que el mensaje viaje de una forma segura se encriptará con un algoritmo de cifrado y se impide que pueda ser leída o modificada.

Existen varios tipos de sistemas de cifrado cada uno con diferentes fortalezas y debilidades. Típicamente, se dividen en dos clases; aquellos que son fuertes, pero lentos en su ejecución y aquellos que son rápidos pero menos seguros. A menudo, se usa una combinación de ambos, donde se establece la conexión con un algoritmo seguro.

Los algoritmos simétricos comparten un secreto común (contraseña o clave). Los datos son cifrados y descifrados usando la misma clave. Estos son muy rápidos, pero no deberían usar a menos que se haya intercambiado la clave antes de establecer la comunicación.

Sería prudente usar los algoritmos asimétricos, ya que usan dos claves, una para cifrar los datos y otra para descifrarlos. Estas claves interdependientes se generan a la vez, a una se le denomina la clave pública y es distribuida libremente, la clave privada debe mantenerse segura. Cifrando los datos con la clave pública de un usuario (la cual está públicamente disponible), se pueden enviar los datos sobre una red insegura sabiendo que sólo la clave privada asociada será capaz de descifrar los datos. De esta manera se asegura que el mensaje es confidencial. Independientemente del algoritmo que se utilice se puede encriptar una parte del mensaje que sea importante o delicada o todo el mensaje, pero se debe tener en cuenta a la hora de encriptar el volumen de la información, pues este es proporcional al tiempo de encriptación, lo que haría el algoritmo mucho más lento en dependencia del volumen. La Figura 13 representa la encriptación de un mensaje.

Para reforzar la seguridad del mensaje y que este llegue a su destino final sin sufrir cambios se puede aplicar hash. Estas funciones toman algunos datos como una contraseña o una parte delicada del mensaje, se genera un hash único o suma de chequeo de la parte seleccionada. Dado que es una función de un solo camino, se usa normalmente para proporcionar detección de engaños y verificar que la información no fue alterada.

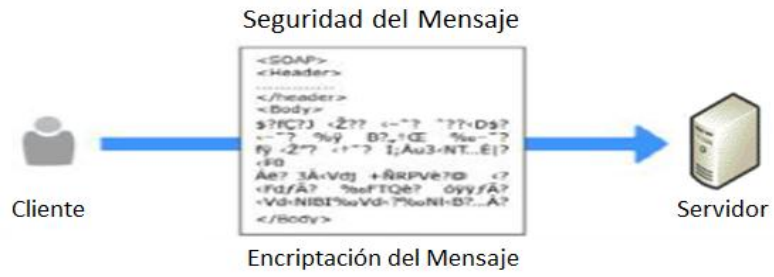


Figura 13. Encriptación del mensaje

Existirán varios canales de comunicación por los cuales los usuarios se comunicarán con la aplicación, de manera que por los canales puedan consumir servicios de manera segura y que no se ponga en riesgo la identidad de los usuarios. En el caso de los sistemas podrán comunicarse por los siguientes canales: Correo, Móvil e Internet, en el caso específico de las personas podrán comunicarse por estos

canales y además de forma Personal, este canal consiste en la comunicación persona a persona para interactuar con la aplicación.

Entonces existirán dos tipos de comunicaciones: **Persona a Sistema** y **Sistema a Sistema**, donde se realizarán comunicaciones seguras y confiables mediante SSL.

Descripción de los Canales de Comunicación

Para que un usuario pueda utilizar este canal primeramente debe poseer un nivel de seguridad medio, que consiste en tener registrados datos personales o datos de estructura y constar con un certificado digital.

El proceso comenzaría con un usuario que entra en el portal del e-gob para crear su identidad digital con el nivel de seguridad requerido (medio).

Un usuario primeramente debe poseer los datos personales o de estructura, para ello consumirá un servicio que le posibilitará gestionar estos datos (nombre, apellidos, sexo, dirección electrónica, usuario, contraseña, entre otros).

Después de realizado el proceso anteriormente explicado se procede con la gestión de un certificado digital. El usuario debe hacer una solicitud de certificado a la AC (Autoridad Certificadora), la cual debe aceptar su solicitud y enviarle por correo electrónico una contraseña para poder confeccionar el certificado. Luego el usuario consumirá el servicio para crear un certificado digital, para hacer uso del servicio debe tener en su poder la contraseña que se le envió a su correo electrónico. Una vez concluido este flujo, el usuario descargará un ejecutable que instalará en su equipo computacional (Computadora de Escritorio o Portátil, Móvil, entre otros).

Canal de Correo

Una vez instalado el certificado en su equipo podrá firmar documentos y mensajes de correo electrónico de forma digital, pero cada vez que firme deberá introducir la contraseña que solamente debe ser conocida por su propietario, se consumirá un servicio que autenticará al usuario para poder firmar, si la autenticación no tiene éxito entonces la firma no tendrá validez. Al firmar electrónicamente, el emisor obtiene un resumen del mensaje mediante la función hash, esta operación se realiza sobre un conjunto de datos, de forma que el resultado obtenido es otro conjunto que está asociado a los datos iniciales. Antes de enviar el correo a su destino se debe encriptar la información para que no viaje en texto plano, aunque ya se tiene asegurado el canal de transporte mediante la utilización de SSL será prudente utilizar la encriptación del mensaje. Una vez que el receptor tenga en su dominio correo tendrá en su poder un

correo encriptado y el resumen hash que se envía con él, se realizará el proceso de desencriptación del correo y se le aplicará la función hash la cual se comparará con la que envió el emisor, se podrá saber si fue modificado después de firmado el mensaje y si el emisor es confiable.

Los documentos y mensajes firmados digitalmente serán enviados por correo mediante el protocolo SMTP (Protocolo Simple de Transferencia de Correo) y serán recibidos a través del protocolo POP3 (Protocolo de Oficina de Correos).

Se deberá utilizar POP3 y no IMAP (Protocolo de Acceso a Mensajes de Internet) porque el acceso a Internet en el país es muy limitado, POP3 se conecta cada cierto tiempo al servidor y descarga para el equipo computacional los correos, posibilitándole al usuario revisar sus correos sin estar conectado. El protocolo IMAP es un protocolo alternativo al de POP3 pero se mantiene conectado constantemente, reduciendo el ancho de banda al resto de los usuarios. La Figura 14 detalla gráficamente como ocurre el proceso explicado anteriormente.

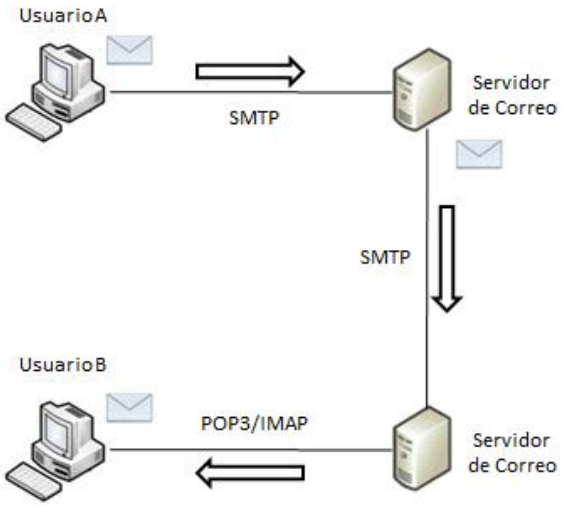


Figura 14. Descripción de envió de correo

Canal de Internet

SSL es un protocolo para transmitir documentos privados de manera segura a través de Internet. Los navegadores web como Safari 1.0, Firefox 1.0, Chrome 0.3, Internet Explorer 5.01 y Opera 6.1 son compatibles con SSL a partir de estas versiones, gran cantidad de sitios web utilizan este protocolo para transferir información confidencial del usuario. Las URL (Localización de Recurso Uniforme) que requieren conexión SSL comenzarán con HTTPS, se utilizará el puerto 443 para las transferencias de datos seguros y limitar el acceso de usuarios no certificados.

Un usuario que utilice un servicio para autenticarse debe conectarse mediante HTTPS, existirán varias formas de autenticar en dependencia de las credenciales presentadas:

- **Usuario y Contraseña**: consiste en la entrada de un usuario y contraseña válida para el sistema o una contraseña o frase definida por el sistema de una entidad o empresa.
- **Tarjeta de Identidad y PIN**: parte de la lectura de un código de barra leído por un dispositivo de entrada y una contraseña numérica de cuatro dígitos.
- **Certificado Digital**: consiste en una contraseña o frase conocida por el propietario del certificado.
- **Parámetros Biométricos**: parte de la lectura de alguno de los parámetros biométricos (patrones de escritura, voz, oculares y huellas digitales) de una persona.

Canal del Móvil

Mediante un móvil también se les permitirá a los usuarios instalar el certificado en su móvil y establecerle la firma digital a los documentos y mensajes, estos podrán ser transportados mediante el correo electrónico, USB, CD y disco duro.

A través de este canal se podrá usar el servicio para autenticar, de la misma forma que en el canal de Internet debe establecerse una comunicación segura mediante HTTPS, para esto existirán varias formas de autenticación:

- **Usuario y Contraseña**: consiste en la entrada de un usuario y contraseña válida para el sistema o una contraseña o frase definida por el sistema de una entidad o empresa.
- **PIN**: es una contraseña numérica de cuatro dígitos que se le asociará al número del móvil.
- **Certificado Digital**: consiste en una contraseña o frase conocida por el propietario del certificado.

Canal Personal

La comunicación a partir de este canal se define para lograr que los servicios lleguen a la mayoría de la población, ya que en el país no existe un desarrollo tecnológico elevado. En este canal un usuario podrá interactuar con una persona que tenga experiencia en la utilización de estos servicios, pudiera ser un funcionario del estado dedicado a esta labor, permitiendo al usuario que no consta de la tecnología

que pueda beneficiarse de estos servicios que serán brindados por el gobierno electrónico.

El usuario podrá consumir distintos servicios como: gestionar una identidad digital, autenticarse mediante alguna de las formas planteadas, gestionar su certificado, entre otros.

La Figura 15 representa como se realizará la comunicación con los distintos usuarios mediante los distintos canales.

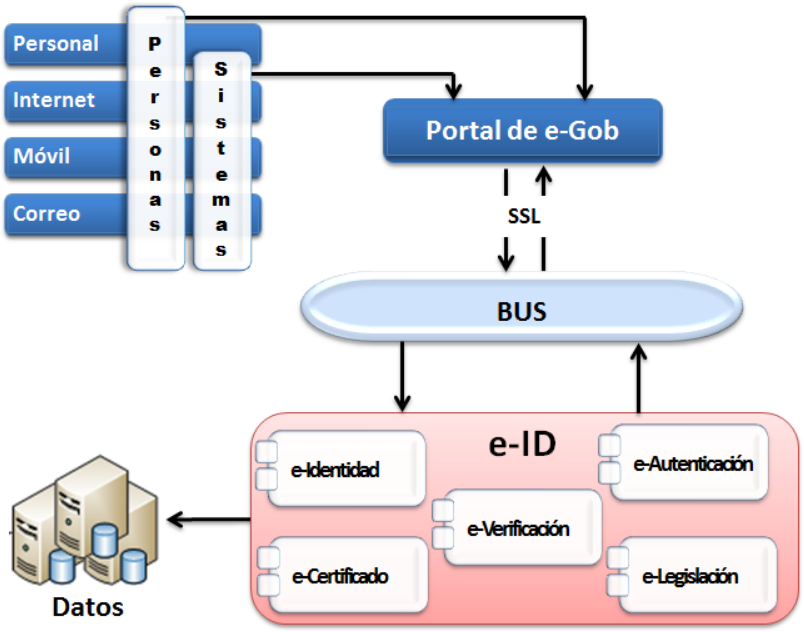


Figura 15. Comunicación con los usuarios

3.6 Descripción de los elementos e-ID

En e-ID se gestionará la identidad digital de manera segura para las transacciones del e-gob de Cuba, para garantizar esta identidad digital se describen a continuación cinco elementos fundamentales para su construcción.

3.6.1 E-Identidad

En E-Identidad se busca proveer a los usuarios una Identidad Digital única para la realización de trámites en línea en los sitios electrónicos del Estado, eliminando la necesidad de contar con múltiples registros para cada servicio.

Se dispondrá de mecanismos para la autenticación en línea, cuyo enrolamiento y verificación será realizado mediante servicios que se brindarán y en donde los datos de identificación se transmitirán de manera segura y confiable a través de SSL.

La Identidad Digital para una persona o para entidad física o jurídica estará compuesta por los siguientes parámetros:

Datos Personales (Personas) o Datos de Estructura (Entidades) se recopilarán los datos referentes a:

- Persona (nombres, apellidos, dirección, carnet de identidad, sexo, dirección electrónica, usuario y contraseña)
- Entidad (nombre, dirección física y electrónica, órgano al que pertenece, usuario y contraseña)

Datos Biométricos se recopilarán los datos referentes a:

- Persona (huellas digitales, parámetros de voz, patrones oculares y de escritura).

Para generar un Identidad Digital además de estos datos que se recopilan para poder identificar a una persona o una entidad, se necesitará un Certificado Digital para proporcionar una identidad con un nivel de seguridad medio y que proporcione confianza a los clientes para realizar las transacciones sin el temor de que vaya a ser suplantada su entidad o que esta transacción no va a llegar a la otra parte con la que están interactuando. A continuación en la Figura 16 se grafica el proceso de “Crear una Identidad Digital” que fue descrito anteriormente.

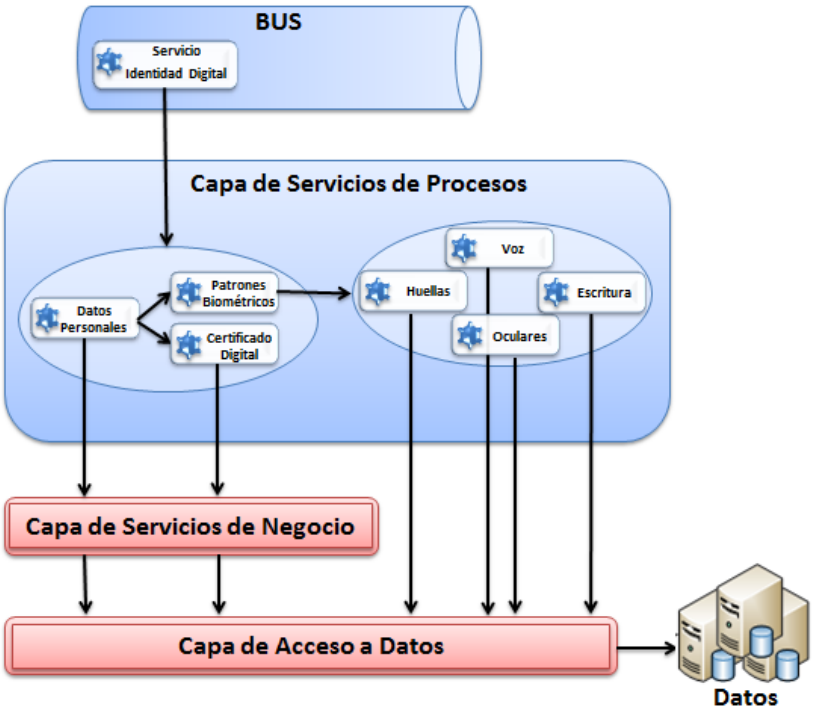


Figura 16. Proceso "Crear Identidad Digital"

Se proporcionarán diferentes niveles de seguridad en dependencia de que interactúe con la aplicación, se definirá niveles de seguridad para los usuarios y otro para los sistemas o aplicaciones externas que se comunicarán o utilizarán los servicios de Identidad que se brindarán.

Niveles de seguridad para Usuarios

Nivel Básico

- Usuario y contraseña: el usuario poseerá en su poder un usuario y contraseña, el usuario debe ser único y la contraseña tiene que tener un combinación fuertemente acoplada de letras, números, caracteres especiales y con una longitud de la cadena que debe ser de no menos de ocho caracteres, de manera que sea segura y difícil de concebir por un tercero.
- Tarjeta de identificación y PIN: esta tarjeta de identificación tendrá calcados una serie de datos personales que podrán identificar al usuario a simple vista (nombre, apellidos, sexo, edad, número de carnet de identidad y foto), también consta de un código de barras que será único para cada tarjeta. Para interactuar con la aplicación se necesitará de un equipo que pueda interpretar códigos de barras además de un PIN que solo conocerá el portador de la tarjeta de identificación.

Nivel Medio

- Certificado digital: constará de un certificado digital que tendrá una identidad vinculada, lo que hará la transacción más confiable, además se le permitirá firmar de forma digital documentos y mensajes obteniéndose una mayor autenticidad y no repudio en las acciones realizadas en las transacciones.

Nivel Alto

- Patrones de Voz, Patrones de Escritura, Patrones de Huellas digitales, Patrones Oculares: estos patrones se obtienen mediante la lectura de equipos especializados en estas características, estas son guardadas en una base de datos, al validar la identidad digital del usuario a partir de estos patrones lo que hace es comparar la lectura por lo que está registrado.

Niveles de seguridad para Entidades

Nivel Básico

- Usuario y Frase o contraseña: el usuario debe poseer un usuario relacionado con una cadena de caracteres que tienen una combinación de letras, números, caracteres especiales y la cadena debe ser mayor que ocho caracteres, es algo concebido por ambos sistema de tal manera que solo lo sepan las dos partes de las transacciones que están interactuando entre sí.

Nivel Medio

- Certificado digital: constará de un certificado digital que tendrá una identidad vinculada, lo que hará la transacción más confiable, además se le permitirá firmar de forma digital documentos y mensajes obteniéndose una mayor autenticidad y no repudio en las acciones realizadas en las transacciones.

Para interactuar con la aplicación se va requerir como mínimo de seguridad un nivel medio, pues con este nivel se podrá contener de una identidad digital que sea segura para realizar las transacciones entre las dos partes, además que le dará la posibilidad de firmar digitalmente documentos y le brindará agilidad, seguridad e integridad a los procesos que requieran una identidad digital.

El nivel medio de seguridad tendrá incluido en él, nivel básico, o sea para que un usuario tenga una Identidad Digital con un nivel de seguridad medio debe poseer datos personales o datos de estructura en caso de una entidad y un certificado digital. En el caso de un nivel alto debe poseer los elementos requeridos para el nivel medio y básico, además de los datos o patrones biométricos para el caso de los usuarios que sean personas físicas. La Figura 17 ejemplifica como estarán conformados los niveles de seguridad.

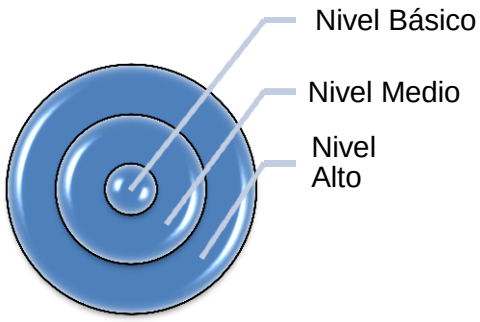


Figura 17. Nivel de Seguridad

3.6.2 E-Autenticación

La autenticación es el proceso de detectar y comprobar la identidad digital de una persona o entidad en la red mediante la presentación de los certificados que se le soliciten al usuario y la validación de los mismos, si estos certificados son correctos pues se le definirá un nivel de acceso a la información que dependerá en gran medida de la confianza que tenga mediante los certificados que presente y también en dependencia del tipo de usuario o sea que un usuario puede ser un administrador o usuario clásico. Es un modo de asegurar que los usuarios son quienes dicen ser y que el usuario que intenta realizar o utilizar determinadas funciones en un sistema es el usuario que tiene la autorización para hacerlo.

Autenticación o mejor dicho la acreditación en términos de seguridad de redes de datos, consta de los siguientes pasos para lograr el éxito de este proceso:

Autenticación: es la acción de verificar la identidad digital del remitente de una petición para registrarse en una aplicación. El remitente puede ser una persona que usa un equipo computacional, un equipo por sí mismo o un programa que está siendo ejecutado en un equipo.

Autorización: se autoriza al usuario identificado a acceder a determinados recursos o se define el nivel de seguridad que se le otorgará. Un nivel de seguridad contendrá los recursos que un usuario podrá acceder ya sea en la red o en una aplicación, se define a partir de restricciones de sensibilidad de información, de manera que cuando más sensibles o comprometidos sean los datos a tratar mayor será el nivel de seguridad que se requerirá. Siempre que se definan niveles de seguridad para una aplicación deben presentarse más de un nivel, pues no cumple objetivo tener un solo nivel donde todos los usuarios autenticados presenten el mismo nivel.

Auditoría: es mediante una estrategia que se lleva a cabo para registrar todos y cada uno de los accesos a los recursos que realiza el usuario autorizado o no.

Los métodos de autenticación están en función de lo que utilizan para la verificación y estos se dividen en tres categorías:

Sistemas basados en algo conocido:

- Usuario y contraseña
- PIN (número de identificación personal)

Sistemas basados en algo poseído:

- Tarjeta de identidad

- Tarjeta inteligente (smartcard)
- Dispositivo usb con *software*

Sistemas basados en una característica física o un acto involuntario del usuario:

- Patrones de voz
- Patrones de escritura
- Huellas digitales
- Patrones oculares

En muchos casos en la actualidad se requieren de la combinación de varios métodos de autenticación, un ejemplo es en los bancos que necesitan de una tarjeta inteligente y PIN.

El flujo del proceso de autenticación consta de los siguientes pasos:

1. El usuario solicita acceso a un sistema.
2. El sistema solicita al usuario que se autentique.
3. El usuario aporta las credenciales que le identifican.
4. Se verifican las credenciales y validan la autenticación de la identificación.
5. El sistema validará según sus reglas y las comparará con las credenciales registradas en la base de datos.
6. Se emite un resultado de la consulta realizada a los datos
7. Se da una respuesta al usuario:
    a. Aceptación: se le da acceso a los servicios a los que pueda acceder según sus credenciales.
    b. Denegación: se le solicitan las credenciales necesarias para este sistema, como máximo puede realizar 3 intentos para lograr la aceptación, de no lograrlo se le denegará la solicitud de acceso al sistema por un tiempo determinado.

La Figura 18 representa el proceso de Autenticación explicado anteriormente.

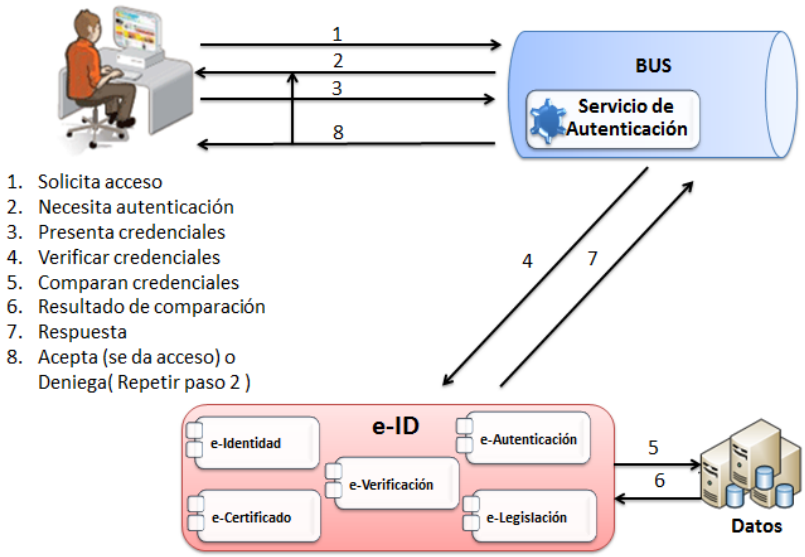


Figura 18. Flujo de Autenticación

3.6.3 E-Certificados

En E-Certificado se propone proporcionarle a los usuarios certificados digitales, con ellos asegurar sus transacciones en línea y vincular una identidad digital a cada usuario para aumentar el nivel de confianza en los intercambios de informaciones digitales. También les permitirá, a los usuarios, valerse de una de las ventajas más significativas que presentan los certificados digitales, la firma digital de documentos y mensajes, lo que asegura que se está interactuando con la contraparte que contiene el certificado digital que permitirá comunicarse con la otra parte.

Para que un usuario pueda disfrutar de estas ventajas o sea de poseer un certificado digital, este debe tener una identidad para vincular este usuario con una persona o entidad física o jurídica, para esto se requieren los datos referentes a los Datos Personales o Datos de Estructura.

Las dos claves serán generadas mediantes algoritmos de cifrados asimétricos, estos algoritmos solo se conocerán por el equipo de trabajo del proyecto que despliegue la propuesta. La clave privada que solo será conocida por su propietario la cual se utilizará para firmar digitalmente. La clave pública para poder leer los documentos y mensajes que fueron firmados por otro usuario con su perteneciente llave privada.

Un certificado digital debe tener muy bien registrada la identidad de la AC que expidió el certificado, este debe estar firmado por la AC. Las AC deben estar bien concebidas, pues serán la máxima autoridad para darle validez a un certificado. Los

certificados estarán respaldados por un conjunto de normas y leyes (Legislación), que le darán valor tecnológico y velarán que se traten de una forma apropiada.

3.6.4 E-Verificación

E-Verificación se encargará de realizar todas las verificaciones y validaciones de identidad digital, certificados digitales y autenticaciones, donde según el negocio que se haya planteado para cada uno de ellos se comprobará su autenticidad.

Cuando se compruebe la identidad de un usuario se dividirá en dos partes para lograr una mejor comprensión. Una primera parte sería los Datos Personales de una persona o en el caso de una entidad los Datos de Estructura de esta, aquí se desglosarán cada uno de los parámetros que se poseen y se procederá a verificar cada uno por separado. La segunda parte será los Datos Biométricos, esto solo para el caso de los usurarios que sean personas, este comprobará los datos biométricos que tenga, o sea, una persona puede tener varios datos biométricos, estos pueden ser patrones de escritura, de huellas digitales, de voz y oculares, pero para el caso de una persona puede ser que no tenga ningún dato biométrico o que solamente tenga uno de ellos o varios, entre más elementos biométricos presente más alta será su seguridad.

También permitirá validar los certificados digitales, en este se comparará un certificado que se presenta con un certificado registrado, se dividirán en dos partes para hacer más simple el trabajo. Una primera parte será comprobar que se está interactuando con la persona que dice ser. La segunda parte sería la verificación de las llaves, verificar que sean legítimas pues mediante ella se realizará el firmado a documentos de manera digital, lo que implicará que deberá tener un nivel de seguridad elevado para que tenga una aceptación para la contraparte de una transacción.

Comprobará también los documentos que requieran de un equipo para su lectura, como por ejemplo las tarjetas de identidad o un futuro DNI electrónico, controlará las marcas de seguridad que presenten estos documentos para que no sean falsificados.

3.6.5 E-Legislación

Se denomina legislación al cuerpo de leyes que regularán determinada materia o ciencia o al conjunto de leyes a través del cual se ordena la vida en un país, es decir, lo que popularmente se llama ordenamiento jurídico y que establece aquellas conductas y acciones aceptables o rechazables de un individuo, institución, empresa, entre otras. [32]

Es un conjunto de normas que dirán como actuar, responder ante determinadas situaciones y le darán valor tecnológico a las infraestructuras digitales, pues el hecho de que sean argumentos que en muchos casos son teóricos, no significan que se le otorgue una determinada importancia. La legislación digital surgió con el objetivo de darle una estructura y una educación digital a las personas que interactúan con las tecnologías digitales, ya que no todas las personas suelen respetar el derecho de los otros ni tampoco desplegar sus obligaciones, por eso y atendiendo a esta cuestión es que una legislación es la mejor manera que existe para que una comunidad subsista, se desarrolle y crezca.

Hay dos concepciones básicas acerca del origen de la legislación u ordenamiento jurídico. Por un lado la corriente normativa señala que el ordenamiento está expresado en un conjunto de normas que se entienden y se rigen con una serie de juicios de valor, creencias y convicciones. Y por otro lado, la corriente institucional supone que ese orden estará establecido por la sociedad, por aquellos mecanismos que aplican y producen las normas y por todas aquellas instituciones y criterios de aplicación.

En el caso de la propuesta que se brinda será un punto importante la legislación, pues tiene que existir un mecanismo que respalde los certificados digitales e identidad digital, donde estos puedan alcanzar un gran valor tecnológico y que de esta forma tengan una mayor aceptación por los ciudadanos y entidades que estarán relacionados con la aplicación.

3.7 Conclusiones

En el presente capítulo se explicaron los tipos de servicios del e-gob de Cuba y los clientes a los que van dirigidos. Se definió el patrón de arquitectura que se usará (SOA) explicándose como se hará uso del mismo, se estructuró la arquitectura que usará el marco de trabajo conceptual que se propone y los niveles de seguridad para crear una identidad digital, donde el nivel alto contendrá a los niveles básico y medio, evitando la suplantación de identidad. Para gestionar la identidad digital en el e-gob de Cuba se describió la e-ID, que será el que asegura las transacciones del e-gob, se desglosó el funcionamiento en partes, E-Identidad, E-Autenticación, E-Certificado, E-Verificación y E-Legislación, explicando cómo funcionarán cada uno de ellos para proporcionarle confiabilidad, autenticidad, integridad, disponibilidad y seguridad a los usuarios en sus transacciones.

Conclusiones

Al término de la investigación se pueden arribar a las siguientes conclusiones:

- Se abordaron los temas principales que se trataron en la investigación como el gobierno electrónico y la identidad digital, se expusieron las características esenciales de los medios fundamentales para soportar una identidad digital. La identidad digital del e-gob debe estar conformada por medios que soporten los certificados digitales.
- Se realizó un extenso estudio acerca de los marcos de trabajo para la construcción de aplicación del e-gob basadas en la identidad digital de administraciones públicas, a nivel internacional y en Cuba, aportando conocimiento para hacer una propuesta de un marco de trabajo conceptual que se usará en la construcción de aplicaciones que gestionarán la identidad digital del e-gob de Cuba y que permitirá interactuar con otros sistemas, se fundamentaron las tecnologías a usar basándose en las aplicaciones web.
- Se obtuvieron elementos sustanciales para adaptar a la propuesta a partir del estudio de los sistemas analizados. La arquitectura para el marco de trabajo conceptual que se propuso está sustentada en servicios web, mediante los cuales se gestionará la identidad digital utilizando los certificados digitales para asegurar la autenticación y la seguridad de los intercambios de información entre los usuarios y sistemas.
- El marco de trabajo conceptual está basado en las tendencias de la identidad digital enfocado en el gobierno electrónico de Cuba, a partir del análisis del funcionamiento de los existentes a nivel global, ajustando a la propuesta las características y experiencias obtenidas en dicho estudio. Para la gestión de la identidad digital se describió como se conformó la e-ID en el e-gob de Cuba, la gestión se realizará a partir de servicios web que podrán ser utilizados por sistemas que interactúen con la aplicación o por los usuarios finales a los que van dirigidos los servicios. Se asegurarán los intercambios entre los usuarios y el sistema mediante protocolos de comunicación seguros, requiriendo para ello un nivel de seguridad apoyado en certificados digitales.

Recomendaciones

- Se recomienda la implementación de aplicaciones del e-gov en Cuba a partir de la propuesta obtenida después de culminada la investigación, teniendo en cuenta las especificidades del funcionamiento del gobierno electrónico como objetivos, metas y estrategias basadas en la identidad digital en Cuba.

Referencias Bibliográficas

1. IX Conferencia Iberoamericana de Administración Pública y Reforma del Estado. Pucón, Chile : s.n., 2007.

2. **Cubadebate**. Acceso a Internet alcanza a un 30% de la población mundial. [En línea] 2009. [Citado el: 1 de febrero de 2012.] http://www.cubadebate.cu/.

3. **Ecured**. Gestor de Documentos Administrativos eXcriba. [En línea] [Citado el: 10 de Diciembre de 2010.] http://www.ecured.cu/index.php/Gestor_de_Documentos_Administrativos_eXcriba.

4. Definición de. Gobierno. [En línea] [Citado el: 3 de noviembre de 2011.] http://definicion.de/gobierno/.

5. PRYME. Gobierno electrónico. [En línea] [Citado el: 26 de marzo de 2012.] http://www.modernizacion.cl.

6. OPIG. Gobierno electrónico. [En línea] [Citado el: 6 de abril de 2012.] http://www.innova.presidencia.gob.mx.

7. ADB Board Paper on Governance: Sound Development Managemen. 1995.

8. **Pascual, Patricia J.** e-Goverment. 2003.

9. **Konrad, Rachel.** News.com. Luchando contra la brecha digital de Bush. [En línea] [Citado el: 20 de noviembre de 2011.] http://news.com.com/2100-1023-834645.html.

10. Real Academia Española. Identidad. [En línea] [Citado el: 5 de Diciembre de 2011.] http://www.rae.es/rae.html.

11. Evolucy. Identidad Digital. [En línea] [Citado el: 12 de mayo de 2012.] http://www.evolucy.com/esp/digital_identity.html.

12. Educación Finaciera en la Red. PIN (Número de Identificación Personal). [En línea] [Citado el: 5 de mayo de 2012.] http://www.edufinet.com/index.php?option=com_glossary&func=display&letter=P&Itemid=27&catid=13&page=1.

13. Pergamino Virtual. PIN. [En línea] http://www.pergaminovirtual.com.ar/definicion/PIN.html.

14. Málaga. Certificados Digitales. [En línea] [Citado el: 6 de mayo de 2012.] http://www.malaga.eu/recursos/ayto/m_gestiones/firma/debesaber/3_1.html.

15. **Ecured**. Firma Digital. [En línea] [Citado el: 9 de mayo de 2012.] http://www.ecured.cu/index.php/Firma_Digital.

16. Masadelante.com. Dirección. [En línea] [Citado el: 12 de abril de 2012.] http://www.masadelante.com/faqs/direccion.

17. Pymes y Autonomos. La dirección electrónica única. [En línea] [Citado el: 12 de abril de 2012.] http://www.pymesyautonomos.com/administracion-finanzas/la-direccion-electronica-unica.

18. Macro Seguridad. Firma Digital y PKI. [En línea] [Citado el: 14 de mayo de 2012.] http://www.macroseguridad.com/index.php/soluciones/firma-digital-y-pki.

19. Portal Oficial sobre DNI electrónico. DNI electrónico. [En línea] [Citado el: 20 de noviembre de 2011.] http://www.dnielectronico.es/.

20. Hooping.net. SSL. [En línea] http://www.hooping.net/glossary/ssl-110.aspx.

21. CodeBox. *Framework*. [En línea] [Citado el: 19 de mayo de 2012.] http://www.codebox.es/glosario.

22. **J. Crespo Sánchez, J. Espinosa García, L. Hernández Encinas, H. Rifµa Pous, M. Torres Hernández.** Hacia una nueva identificación electrónica del ciudadano: DNI-e. Madrid, España : s.n.

23. openFWPA. *Framework* Libre de Gobierno Electrónico del Principado de Asturias. [En línea] [Citado el: 4 de abril de 2012.] http://www.asturias.es/openFWPA.

24. Marco de referencia de servicios electrónicos gubernamentales. México : s.n., 2008.

25. **Abdelbaset Rabaiah, Eddy Vandijck.** A Strategic *Framework* of e-Government: Generic and Best Practice. 2009.

26. **Sumaq, Alianza de.** Análisis del Gobierno Electrónico Municipal en Iberoamérica. 2006.

27. Mastermagazine. *Definición de Arquitectura* Software*.* [En línea] [Citado el: 11 de mayo de 2012.] http://www.mastermagazine.info/termino/3916.php.

28. **Harrison, Victor.** OMG. *SOA,Technical Risks, and Emerging Standards.* [En línea] 27 de febrero de 2007. [Citado el: 26 de mayo de 2012.] http://www.omg.org/news/meetings/workshops/SWA_2007_Presentations/02-2_Harrison.pdf..

29. **OASIS.** *Reference Model for Service Oriented Architecture.* [En línea] 7 de febrero de 2006. [Citado el: 24 de mayo de 2012.] http://www.oasis-open.org/committees/download.php/16587/wd-soa-rm-cd1ED.pdf..

30. **Harding.** *The Open Group. Service Oriented Architecture (SOA).* [En línea] 8 de junio de 2006. [Citado el: 25 de mayo de 2012.] http://opengroup.org/projects/soa/doc.tpl?gdid=10632..

31. **Ecured.** *Software* Libre. [En línea] [Citado el: 10 de junio de 2012.] http://www.ecured.cu/index.php/Software_libre.

32. Definición ABC. Legislación. [En línea] [Citado el: 15 de mayo de 2012.] http://www.definicionabc.com/derecho/legislacion.php.

Bibliografías

1. Agencia de Gobierno Electrónico y Sociedad de la Información. Agencia de Gobierno Electrónico y Sociedad de la Información. [En línea] 10 de Febrero de 2010. [Citado el: 25 de Noviembre de 2011.] http://www.agesic.gub.uy/.

2. Breaking Barriers to e-Government. Breaking Barriers to e-Government. [En línea] [Citado el: 7 de Diciembre de 2011.] http://www.egovbarriers.org/?view=home.

3. DigitalGovernance.org. Digital governance. [En línea] 2003. [Citado el: 19 de diciembre de 2011.] http://www.cddc.vt.edu/digitalgov/gov-publications.html.

4. Revista Cubana de Informática Cubana. Revista Cubana de Informática Cubana. [En línea] CECAM, 2002. [Citado el: 15 de Diciembre de 2011.] http://www.rcim.sld.cu/.

5. The World Bank. Public Sector & Governance. [En línea] 2002. [Citado el: 19 de diciembre de 2011.] http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTPUBLICSECTORANDGOVERNANCE/0,,contentMDK:20206128~pagePK:210058~piPK:210062~theSitePK:286305,00.html.

6. **Aedo, D.R.** Los métodos de evaluación de expertos para valorar resultados de las investigaciones. Folleto sobre métodos de evaluación de expertos. MES. Cuba : s.n., 2006.

7. **Astigarraga, Eneko.** EL MÉTODO DELPHI. Universidad de Deusto. San Sebastián : s.n., 2008. E-20.080.

8. Gobierno Electrónico en América Latina. [aut. libro] Olga Cavalli. Argentina : s.n., 2009.

9. Silicontrust. Chip de DNI electrónico. [En línea] [Citado el: 2 de abril de 2012.] http://www.silicontrust.com/redirect.asp?path=/background/backgr_overview.htm.

10. **Windley, Phillip J.** Identidad Digital. 2005.

11. **Prado, José Aldo Díaz.** Transferencia. [En línea] 2011. [Citado el: 3 de diciembre de 2011.] http://www.mty.itesm.mx/die/ddre/transferencia/57/57-III.05.html#Arriba.

12. **Gómez, José Jorge Márquez.** Arquitectura MVC, Visión General. [En línea] [Citado el: 24 de abril de 2012.] http://www.google.com.cu/#hl=es&q=definicion+de++MVC&oq=definicion+de++MVC&aq=f&aqi=&aql=&gs_l=serp.12...0.0.1.11504.0.0.0.0.0.0.0.0..2.0...0.0.K9DCKk-lyIE&bav=on.2,or.r_gc.r_pw.,cf.osb&fp=c496a43ba2d27592&biw=1280&bih=801 <http://www.google.com.cu/.

13. **Amsden, Jim.** IBM. Modelado de SOA: Parte 1. Identificación del servicio. [En línea] 2011. [Citado el: 25 de abril de 2012.] http://www.ibm.com/developerworks/ssa/rational/library/07/1002_amsden/index.html.

14. Observatorio Regional de la Sociedad de la Información. [En línea] 2010. [Citado el: 10 de noviembre de 2011.] http://www.orsi.jcyl.es/web/jcyl/ORSI/es/Plantilla100Detalle/1262861006271/_/1277228396599/Redaccion.

15. Oficina Precidencial de la Información y Comunicación. Oficina Precidencial de la Información y Comunicación. [En línea] 2004. [Citado el: 5 de Diciembre de 2011.] http://www.optic.gob.do/.

16. **Herrera, Jose Villanueva.** Scribd. Trabajo Convención (SOA). [En línea] 2008. [Citado el: 25 de abril de 2012.] http://es.scribd.com/doc/8141189/Soa.

17. **The Open Web Application Security Project (OWASP).** *Una Guía para Construir Aplicaciones y Servicios Web Seguros.* 2005.

Glosario de Términos

Automatización: es la acción de transferir las tareas de producción realizadas habitualmente por operadores humanos a un conjunto de elementos tecnológicos para agilizar el proceso.

Cifrado: es el tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos.

Código fuente: es un conjunto de líneas de texto que son las instrucciones que debe seguir un programa informático o *software*.

E-gob: gobierno electrónico.

Encriptación: es el proceso para volver ilegible información considerada importante.

Informatización: acción y efecto de informatizar; pasar a usar computadores allí donde antes no se hacía.

Infraestructura digital: estructura conceptual y tecnológica definida con la cual se desarrolla un *software* de forma más ágil y organizada.

Interface: parte visual de una aplicación con la que interactúa el usuario.

J2EE: es una plataforma de programación para desarrollar y ejecutar *software* de aplicaciones en el lenguaje de programación Java.

Micrones: es la unidad de medida equivalente a una millonésima parte de un metro, su símbolo científico es µm.

Paradigma: modelo o patrón fundamental desde el cual se piensa o se realizan hechos y teorías predominantes.

Plataforma: sobre la cual un *software* puede ejecutarse y desarrollarse.

Proliferación: multiplicación abundante de alguna cosa.

Protocolos: es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red por medio de intercambio de mensajes.

Reingeniería: se enfoca en la revisión de los procesos y rediseñarlos nuevamente con el fin de alcanzar mejoras en costo, calidad y rapidez.

Transacción: es una operación que se realiza entre dos o más partes y que supone el intercambio de bienes o servicios.