



**Ministerio de Tecnologías de la
Información y las Comunicaciones**
República de Colombia
www.mintic.gov.co

vive digital
I+D+i

DOCUMENTO DE AGENDA ESTRATÉGICA DE INNOVACIÓN

© República de Colombia - Derechos Reservados

Bogotá D.C., Junio de 2012



DOCUMENTO DE AGENDA ESTRATÉGICA DE INNOVACIÓN

SISTEMA DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN
SUBSISTEMA DE INNOVACIÓN PARA EL USO Y APROPIACIÓN DE TIC
EN EL GOBIERNO

© República de Colombia - Derechos Reservados

Bogotá D.C., Junio de 2012

Ministerio de Tecnologías de la Información y las Comunicaciones

DOCUMENTO DE AGENDA ESTRATÉGICA DE INNOVACIÓN

Derechos de Autor:

Ministerio de Tecnologías de la Información y las Comunicaciones

Plan Vive Digital:

Hugo Sin Triana – Líder I+D+i

Con la colaboración de CINTEL.

TABLA DE CONTENIDO

1.	INTRODUCCIÓN	12
2.	METODOLOGÍA PARA DESARROLLAR LA AGENDA ESTRATÉGICA DE INNOVACIÓN	14
2.1	VIGILANCIA TECNOLÓGICA PARA CIERRE DE BRECHAS	14
2.2	PROSPECTIVA	17
2.2.1	Resultados de los ejercicios de prospectiva por cada NDI	19
2.3	AGENDA ESTRATÉGICA DE INNOVACIÓN	19
3.	USO Y APROPIACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – TIC EN EL GOBIERNO	21
3.1	OBJETIVO DEL E-GOVERNMENT	22
3.2	CARACTERÍSTICAS DEL E-GOVERNMENT	22
3.3	ELEMENTOS DE COMPOSICIÓN	23
3.4	INTERACCIONES EN EL SISTEMA E-GOVERNMENT	24
3.4.1.	e-Democracy	24
3.4.2.	e-Administration	24
3.5	INTERACCIÓN DE UN SISTEMA E-GOVERNMENT	25
3.5.1	Government to Citizens (G2C)	25
3.5.2	Government to Business (G2B)	25
3.5.3	Government to Employees (G2E)	25
3.5.4	Government to Government (G2G)	26
3.6	ELEMENTOS DE LA INTERACCIÓN EN EL SISTEMA E-GOVERNMENT	26
3.7	NIVELES DE MADUREZ EN SISTEMAS E-GOVERNMENT	27
4.	TENDENCIAS EN EL USO DE TIC EN EL GOBIERNO	29
4.1	ESTRATEGIAS EN LA IMPLEMENTACION UNA INICIATIVA DE GOBIERNO EN LINEA	29
4.2	ENFOQUE DE LA ESTRATEGIA	33



4.3	CASOS DE E-GOVERNMENT A NIVEL MUNDIAL	35
4.3.1	UN Public Administration Programme - UN E- Government Development Database	35
4.3.2	Análisis de los Factores de Selección	38
4.3.3	Capital Humano	40
4.4	PROGRAMA GOBIERNO EN LÍNEA	40
4.5	ESTADO ACTUAL	42
5.	NODO DE INNOVACIÓN – CIBERSEGURIDAD	44
5.1	ESTADO ACTUAL EN EL MUNDO	45
5.1.1	Conceptualización de Ciberseguridad	45
5.1.2	Objetivo de la Ciberseguridad	46
5.1.3	Globalización de la ciberdelincuencia	48
5.1.4	Implementación de la Ciberseguridad	49
5.1.5	Fundamentos de la ciberseguridad	51
5.1.6	Tecnologías	53
5.1.7	Modelo Ejemplo Republica De Corea del Sur	55
5.1.8	Roadmap de las iniciativas en ciberseguridad en los Estados Unidos	56
5.2	ESTADO ACTUAL EN COLOMBIA	59
5.2.1	Antecedentes en Colombia	65
5.2.2	Comparación con el Entorno Internacional	72
5.3	RESULTADOS DEL EJERCICIO DE PROSPECTIVA	77
5.3.1	Caracterización de los actores	77
5.3.2	Análisis del Nivel de Impacto de cada línea estratégica	79
5.3.3	Análisis de la Posición Competitiva del País	79
5.3.4	Priorización de Líneas de trabajo para el nodo	79
5.4	VISIÓN PROSPECTIVA DEL NODO	80
5.4.1	Vectores de desarrollo del nodo	80

5.5	AGENDA ESTRATÉGICA DE INNOVACIÓN - PRIORIDADES DE INNOVACIÓN EN CIBERSEGURIDAD	82
5.5.1	Estándares para protección de activos de información	82
5.5.2	Acceso seguro a sistemas	83
5.5.3	Base de datos de incidentes	83
5.5.4	Cuantificación de niveles de riesgos	83
5.5.5	Evaluación Continua de Riesgos	84
5.6	INICIATIVAS DE PROYECTOS POR PRIORIDAD	84
5.6.1	Estándares para protección de activos de información	84
5.6.2	Acceso Seguro	84
5.6.3	Base de datos de incidentes	84
5.6.4	Cuantificación de niveles de riesgos	85
5.6.5	Evaluación Continua de Riesgos	85
5.7	PERFILES DE PROYECTO	85
5.7.1	Proyecto 1	85
5.7.2	Proyecto 2	87
5.7.3	Proyecto 3	88
5.7.4	Proyecto 4	90
5.7.5	Proyecto 5	92
5.7.6	Proyecto 6	93
6.	NODO DE INNOVACIÓN EN ARQUITECTURA TI	96
6.1	IDENTIFICACIÓN DE BRECHAS	96
6.1.1	Estado Actual en el mundo	97
6.2	ESTADO ACTUAL EN COLOMBIA	111
6.3	CONCLUSIONES	112
6.4	RESULTADOS DEL EJERCICIO DE PROSPECTIVA	114
6.4.1	Caracterización de los actores	114



6.4.2	Análisis del Nivel de Impacto de cada línea estratégica	115
6.4.3	Análisis de la Posición Competitiva del País	116
6.4.4	Priorización de Líneas de trabajo para el nodo	116
6.5	VISIÓN PROSPECTIVA DEL NODO	117
6.5.1	Objetivo de la innovación	117
6.5.2	Vectores de Desarrollo del Nodo	117
6.6	AGENDA ESTRATÉGICA DE INNOVACIÓN - PRIORIDADES DE INNOVACIÓN EN ARQUITECTURA TI	120
6.6.1	Prioridad 1	120
6.6.2	Prioridad 2	120
6.6.3	Prioridad 3	120
6.7	INICIATIVAS DE PROYECTOS POR PRIORIDAD	120
6.7.1	Fases del trabajo de implementación	121
6.7.2	Medición y priorización de metas	121
6.7.3	Incremento del entendimiento y del desarrollo de interacciones	121
6.7.4	Implementación de un modelo de gobernanza	121
6.8	PERFILES DE LOS PROYECTOS	122
6.8.1	Proyecto 1	122
6.8.2	Proyecto 2	125
7.	NODO DE INNOVACIÓN – SERVICIOS AL CIUDADANO	130
7.1	IDENTIFICACIÓN DE BRECHAS	132
7.1.1	Estado actual en el Mundo	132
7.1.2	ESTADO ACTUAL EN COLOMBIA	140
7.2	RESULTADOS DEL EJERCICIO DE PROSPECTIVA	146
7.2.1	Caracterización de los actores	146
7.2.2	Análisis del Nivel de Impacto de cada línea estratégica	147

7.2.3	Análisis de la Posición Competitiva del País	148
7.2.4	Priorización de Líneas de trabajo para el nodo	149
7.3	VISIÓN PROSPECTIVA DEL NODO DE SERVICIOS AL CIUDADANO	149
7.3.1	Vectores de Desarrollo del Nodo	150
7.4	AGENDA ESTRATÉGICA DE INNOVACIÓN (SERVICIO AL CIUDADANO)	152
7.4.1.	Línea: Mejores servicios	152
7.4.2	Línea: Participación, colaboración y democracia	152
7.4.3	Línea: Transparencia	153
7.4.4	Otras sublíneas	153
7.5	INICIATIVAS DE PROYECTOS POR PRIORIDAD	153
7.5.1	Línea: Mejores servicios	154
7.5.2	Línea: Participación, colaboración y democracia	154
7.5.3	Línea: Transparencia	155
7.6	PERFILES DE PROYECTO	155
7.6.1	Proyecto 1	155
7.6.2	Proyecto 2	156
7.6.3	Proyecto 3	157
7.6.4	Proyecto 4	159
7.6.5	Proyecto 5	162
8.	ANEXO 1	166
9.	BIBLIOGRAFÍA	171



LISTA DE TABLAS

Tabla 1: Análisis de entorno	31
Tabla 2: Análisis de gubernamental.	31
Tabla 3: Análisis de social y cultural.	32
Tabla 4: Comparación de Colombia contra tres países posicionados en el Ranking de sistemas E-Government.	38
Tabla 5: Capacidades de un sistema de gobierno en línea, objetivos y medios de seguridad	49
Tabla 6: Tendencias de ataques	53
Tabla 7: Conceptos asociados al elemento de medición de nivel empresarial de ciberseguridad.	57
Tabla 8: Usuarios reconocidos en la usabilidad de los elementos de seguridad por parte del Homeland Security para la proyección de las actividades en seguridad de la información en estados Unidos.	58
Tabla 9: Ejes estratégicos.	69
Tabla 10: Iniciativas de proyecto de gobierno en línea y su relación con arquitectura empresariales.	97
Tabla 11. Relación entre países que están aplicando Arquitectura Empresarial Nacional (NEA) desde gobierno y las principales temáticas abordadas	111
Tabla 12: Interacciones Electrónicas de e-Gobierno.	113
Tabla 13: Iniciativas de gobierno electrónico en servicios a la ciudadanía en los países líderes a nivel mundial	133
Tabla 14: Relación entre los países líderes en servicios electrónicos de gobierno y las principales temáticas de gobierno electrónico en sus iniciativas de orden nacional	139
Tabla 15: Relación entre líneas de trabajo con potencial de innovación en el contexto colombiano, y su relación con el trabajo de los países líderes en servicios de gobierno electrónico	140
Tabla 16: Resumen de la identificación de brechas en las temáticas estratégicas de gobierno electrónico en Colombia.	144

LISTA DE FIGURAS

Figura 1	Proceso Vigilancia Tecnológica.....	14
Figura 2.	Esquema para Estudio de Vigilancia Competitiva	15
Figura 3.	Esquema Metodológico Prospectiva	18
Figura 4.	Distribución Actores participantes ejercicio prospectivo	19
Figura 5.	Consolidación Agenda Estratégica de Innovación	20
Figura 6.	Niveles de Gestión en un Sistema E-Government.	23
Figura 7.	Elementos de constitución de un Sistema E-Government.....	23
Figura 8.	Interacción de un Sistema E-Government.....	25
Figura 9.	Interacción del Sistema E-Government.	27
Figura 10.	Composición en el Sistema frente a la información.	29
Figura 11.	Elementos de análisis en una estrategia de implementación E-Government.....	30
Figura 12.	Elementos de análisis en la estrategia de implementación.	31
Figura 13.	Interacción del e-Government con elementos externos y actuales paradigmas.....	32
Figura 14.	Nivel interno en la estrategia de implementación.....	33
Figura 15.	Nivel Externo en la estrategia de implementación.....	33
Figura 16.	Enfoque de estrategia en un sistema E-Government.	34
Figura 17.	Indexación a nivel mundial de sistemas E-Government.....	36
Figura 18.	Indexación a nivel Américas de sistemas E-Government.	37
Figura 19.	Ecosistema de Gobierno en línea	41
Figura 20.	Principios básicos de la estrategia GEL.....	42
Figura 21.	Ejes de acción de GEL	43
Figura 22.	Factores que componen las actividades en Ciberdelincuencia.....	46
Figura 23.	Características para la existencia y mantenimiento de servicios en un sistema de E-Government.....	47
Figura 24.	Elementos relacionados en la Seguridad Informática a nivel de gobierno	49



Figura 25: Criterios básicos de seguridad en todo sistema.	51
Figura 26: Mecanismos de seguridad.....	52
Figura 27: Áreas y principios del KISC.....	56
Figura 28 Aspectos de la seguridad en el GEL.....	59
Figura 29 Principios básicos en el GEL.	60
Figura 30 Ejes de acción GEL.	61
Figura 31: Modelo de coordinación.	62
Figura 32: Modelo Relacional ColCERT	63
Figura 33: Sistema Administrativo de Seguridad de la Información SASI.....	66
Figura 34: Ciclo PHVA asociado al SANSI.	67
Figura 35: Entidades involucradas en CIRTISI.	70
Figura 36. Nivel de Conocimiento de los Expertos con relación a las líneas estratégicas de Ciberseguridad.....	78
Figura 37: Nivel de Impacto de cada línea estratégica en el 2016	78
Figura 38 Posición Competitiva de Colombia en el 2016 en cada línea estratégica	79
Figura 39 Priorización de las líneas estratégicas del nodo	80
Figura 40 Nivel de Conocimiento de los Expertos con relación a las líneas estratégicas de Arquitectura IT	115
Figura 41 Nivel de Impacto de cada línea estratégica en el 2016	115
Figura 42 Posición Competitiva de Colombia en el 2016 en cada línea estratégica	116
Figura 43 Priorización de las líneas estratégicas del nodo	117
Figura 44. Conformación del nodo de servicios a la ciudadanía, vista a través de la interacción de los principales actores	130
Figura 45. Temáticas de gobierno electrónico recurrentes entre las iniciativas de los países líderes en servicios electrónicos a la ciudadanía	138
Figura 46. Estado de la implementación de la Estrategia de Gobierno en Línea en entidades de orden nacional y territorial.....	141

Figura 47 Nivel de Conocimiento de los Expertos con relación a las líneas estratégicas de Servicio Ciudadano	147
Figura 48 Nivel de Impacto de cada línea estratégica en el 2016	148
Figura 49 Posición Competitiva de Colombia en el 2016 en cada línea estratégica	148
Figura 50 Priorización de las líneas estratégicas del nodo	149



1. INTRODUCCIÓN

“La innovación es fundamental para permitir que las sociedades construyan los nuevos modelos de gobierno y de gobernabilidad que necesitamos para abordar los grandes retos del siglo XXI. Queda claro que los gobiernos que sean capaces de enfrentar estos retos no lo harán con métodos lentos y evolutivos, sino mediante niveles sin precedentes de innovación y liderazgo” (Gowher, 2009).

Para la Organización para la Cooperación y el Desarrollo Económicos (OECD) (2009) la innovación radica en “la aplicación de una nueva o significativa mejora en un producto (bien y/o servicio) o proceso, un nuevo método de comercialización, o un nuevo método de organización en las prácticas de negocio, lugar de trabajo o en las relaciones externas”. En las actividades de innovación, según la tercera edición del Manual de Oslo, se incluyen todos los pasos científicos, tecnológicos, organizacionales, financieros y comerciales que conlleven a la implementación de la innovación.

Así es como la innovación se ha definido como un factor clave en el crecimiento y desarrollo de las economías, pasando rápidamente, de ser una moda pasajera, a un imperativo de supervivencia para la competitividad de las empresas, países y finalmente, los Estados y sus instituciones.

En el sector público la innovación comienza a posicionarse en las agendas de distintos gobiernos, se instala en los foros y debates académicos como un ámbito de creciente interés y de rápida ampliación de sus horizontes, y en los últimos diez años, se ha transformado en un eje esencial del proceso de adaptación de las organizaciones (públicas y privadas) a los continuos cambios a los que se ven enfrentadas, en su lucha por la conservación y adecuación a un entorno dinámico y en permanente movimiento.

En este sentido, se ha referido recientemente Christopher Pollitt, reconocido estudioso de los procesos de reforma del Estado en el mundo, al intentar resolver las dudas sobre las perspectivas y desafíos que involucra su estudio como ámbito de investigación dentro de las ciencias en la Administración Pública: “La innovación en el sector público no es nada nuevo y hay que descartar la suposición común de que es algo que sucede principal o casi exclusivamente en el sector privado, y que, por lo tanto, necesariamente se tiene que ir allí para encontrar la manera de llevarla a cabo” (Pollitt, 2008).

En este contexto, el Ministerio de Tecnologías de la Información y las Comunicaciones, mediante la implementación del Plan Vive Digital, que plantea un ecosistema digital abarcando cuatro dimensiones: infraestructura, servicios, aplicaciones y usuarios; propone la creación de un Sistema de I+D+i que apoye de manera transversal la consolidación de dicho ecosistema. Adicionalmente, el Ministerio ha desarrollado iniciativas enfocadas a promover el desarrollo de capacidades científicas, tecnológicas y de investigación en el sector TIC, las cuales se deberán integrar mediante la consolidación de este Sistema de I+D+i, en el marco del Plan Nacional de Desarrollo y el Plan Vive Digital.

Dentro del Sistema de I+D+i del Ministerio TIC se prevé la creación del Subsistema de Innovación para el uso y apropiación de TIC en el gobierno, el cual, a través de la conformación de Nodos de Innovación (NDI), propenderá por acelerar y asegurar la innovación y la transferencia tecnológica dentro de las entidades públicas. Para obtener una visión transversal de innovación, Estos nodos contarán con la

participación de las entidades públicas, la academia y la industria y serán coordinados por una única Secretaría Técnica.

Dentro de la primera fase para consolidar el subsistema de innovación para el uso apropiado de TIC en el Gobierno, que corresponde a la constitución de los nodos de innovación, se tiene previsto la elaboración de una agenda estratégica de innovación para cada uno de los nodos, está según Nagji y Quinn (2010) se constituye en una herramienta muy útil a la hora de crear la claridad organizativa necesaria para la puesta en práctica de la innovación de manera eficiente y con éxito.

El presente documento comprende las Agendas Estratégicas de Innovación de los tres Nodos identificados en la fase piloto del Sistema de I+D+i. Previo a la formulación de las agendas, se realizó un completo estudio de Vigilancia Tecnológica enfocado en la identificación de brechas, la aplicación de prospectiva para definir la visión futura, los vectores de desarrollo de cada Nodo y la identificación de proyectos de innovación que permitan aportar en el cumplimiento de las metas y objetivos trazados en el marco del subsistema de innovación para el uso y apropiación de TIC en el gobierno.

2. METODOLOGÍA PARA DESARROLLAR LA AGENDA ESTRATÉGICA DE INNOVACIÓN

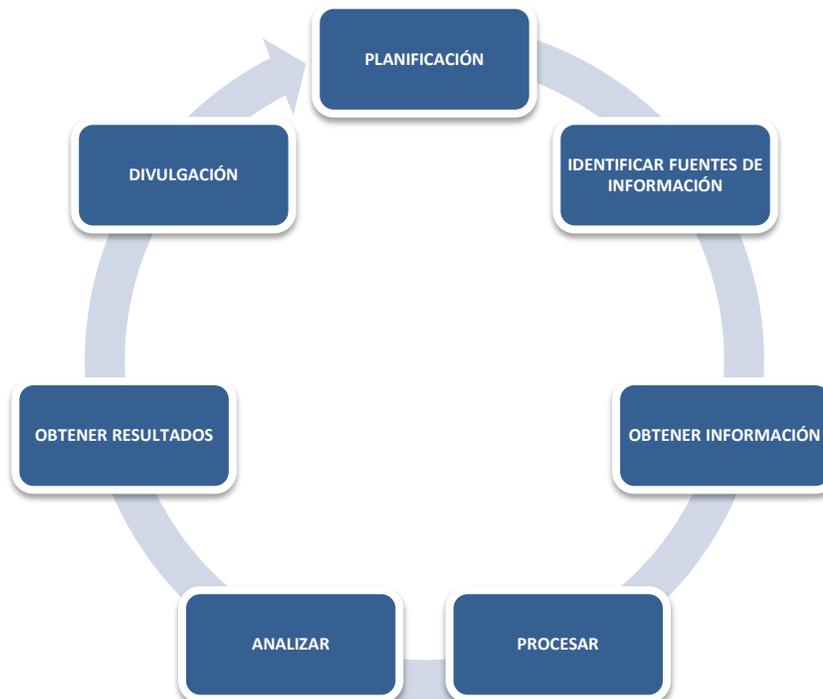
Los siguientes numerales describen la metodología propuesta para desarrollar la Agenda Estratégica de Innovación de cualquier Nodo de Innovación que se encuentre en el marco del subsistema de Innovación y que se llevó a cabo para la elaboración de las AEI propuestas por este documento.

2.1 VIGILANCIA TECNOLÓGICA PARA CIERRE DE BRECHAS

El punto de partida en la metodología de elaboración de la Agenda Estratégica de Innovación es la definición de vigilancia tecnológica – VT, la cual trata de la obtención de información de las fuentes disponibles, tanto formales como informales. Esta información puede ser procesada, tratada y analizada de tal manera que los resultados del análisis puedan ser difundidos según las necesidades existentes en un momento dado, para apoyar así la toma de decisiones y la ejecución de acciones concretas.

En la Figura 1 se muestra el ciclo de la VT:

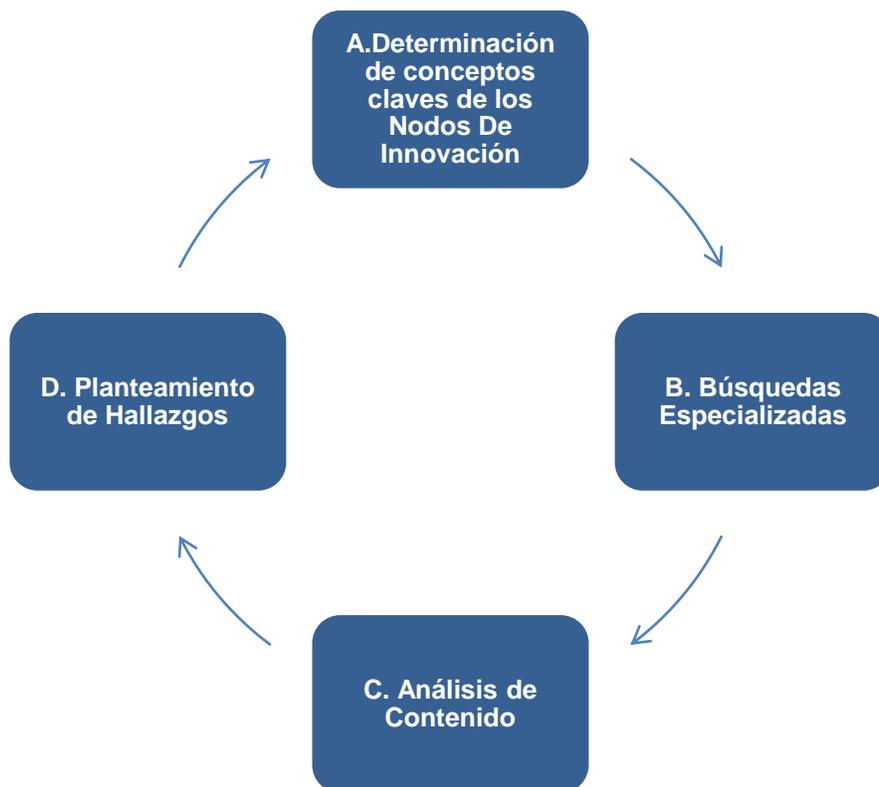
Figura 1 Proceso Vigilancia Tecnológica



Fuente: Curso Vigilancia Tecnológica IALE. Adaptado por CINTEL (2011)

Adicionalmente, para suplir las necesidades estratégicas particulares en la elaboración de las Agendas Estratégicas de Innovación se diseñó un proceso de Inteligencia Competitiva basado en el ciclo básico de la vigilancia tecnológica presentado anteriormente, el cual se puede observar en la Figura 2.

Figura 2. Esquema para Estudio de Vigilancia Competitiva



Fuente: CINTEL (2011).

A. Determinación de los conceptos clave de los Nodos de Innovación:

En esta primera actividad, se realiza una revisión documental enfocada a información de orden no estructurado, con el objetivo de profundizar conceptualmente en la temática de cada uno de los nodos de innovación planteados, así se garantiza un contexto profundo y con enfoque en Colombia, el cual oficie como el punto de partida para la definición de la Agenda Estratégica de Innovación.

En esta actividad es valioso contar con la participación activa de delegados de Gobierno, quienes pueden colaborar en la alineación de la estrategia del estudio con las necesidades identificadas en el Gobierno, específicamente en lo relacionado con su apropiación y uso de TIC.

La determinación de los conceptos claves de los nodos de Innovación se realiza analizando los resultados del estudio mencionado. De esta actividad se derivan los descriptores de búsqueda y de análisis.



B. Búsquedas especializadas:

En esta actividad se determinan las fuentes de información basadas en aquellas que contengan información pertinente de la temática de los Nodos, con el fin de definir estrategias de búsqueda y recolección de documentos. Para ello se realizan las siguientes actividades:

- Identificación de los descriptores asociados a los Nodos de Innovación, para ser utilizados en las fuentes de información seleccionadas.
- Validación de los descriptores identificados por expertos temáticos, de forma que se garantice que la información buscada conducirá a los documentos con conocimiento relacionado a la temática.
- Una vez validados los descriptores, se elaboran las ecuaciones de búsqueda, que permitan una correcta recolección de información de las distintas fuentes de información seleccionadas.

Cabe aclarar que la Vigilancia Tecnológica propuesta para la creación de las Agendas Estratégicas de Innovación estará enfocada a la identificación de brechas. Esto incluye partir de identificar referentes a nivel mundial en la temática de análisis, específicamente en lo que tiene que ver con casos exitosos en incorporación de TIC en Gobierno, para luego, hacer un levantamiento de información secundaria para identificar el estado de la temática a nivel nacional y de allí identificar las principales brechas que serán en punto de partida de trabajo y profundización de la Agenda.

En esta etapa es imprescindible contar en el apoyo de un experto temático en el área específica del Nodo.

C. Análisis de Contenido:

Para esta actividad, se realiza el procesamiento de la información obtenida en las actividades anteriores, este procesamiento es liderado por los expertos temáticos, quienes participan en el análisis de la información, orientando la formulación de resultados de tal forma que responda a los objetivos de los estudios de Vigilancia Tecnológica.

Los análisis de Vigilancia Tecnológica deben, entre otras cosas: identificar oportunidades industriales o avances tecnológicos; conocer las líneas en las que se está investigando en una determinada área tecnológica, identificar quiénes son los expertos y las instituciones líderes; detectar las tecnologías emergentes y nuevos ejes de desarrollo; y estar al tanto de lo que está haciendo cada una de las empresas competidoras desde el punto de vista tecnológico.

A partir de la información recolectada y validada por los expertos metodológicos, los expertos temáticos van a dar sentido a la información:

- Analizando la información recolectada y poniendo los elementos en perspectiva.
- Poniendo la información en el contexto empresarial o sectorial.
- Analizando a través de sus conocimientos y experiencia el valor y alcance de la información recolectada.
- Interpretando la información.

D. Planteamiento de Hallazgos:

La actividad final de proceso de Vigilancia tecnológica consiste del planteamiento de los hallazgos y conclusiones, la cual estará enfocada al análisis de los siguientes aspectos:

Estado Actual en el Mundo

- Estado Actual en Colombia
- Identificación de brechas y líneas de interés del Nodo de Innovación (NDI)

2.2 PROSPECTIVA

La prospectiva resulta útil para la construcción de visiones de futuro, así Castro, Jonhson, D Ápice, & Filho Castro, (2002) mencionan que el análisis prospectivo es una técnica de planeación que viene siendo utilizada de manera intensiva en muchos sectores económicos, para mejorar la base de información disponible sobre la cual se sustenta la toma de decisiones estratégicas. Para Castellanos (2007) la prospectiva parte del futuro y enfoca las acciones presentes hacia él, teniendo en cuenta las posibilidades o limitaciones que brinda la evolución anterior para alcanzar el futuro deseado, por otra parte, Miklos y Tello (1997) indican que además de diseñar el futuro deseable y hacerlo posible, la prospectiva aporta una serie de elementos al proceso de toma de decisiones y, lo que es más importante, facilita la concertación del mejor futuro posible y la definición de las acciones para alcanzarlo.

La aplicación de la visión prospectiva en la construcción de agendas se basa en sus características, conocidas como las cinco C (Martín 1996, citado por Castellanos, Torres & Domínguez (2009)):

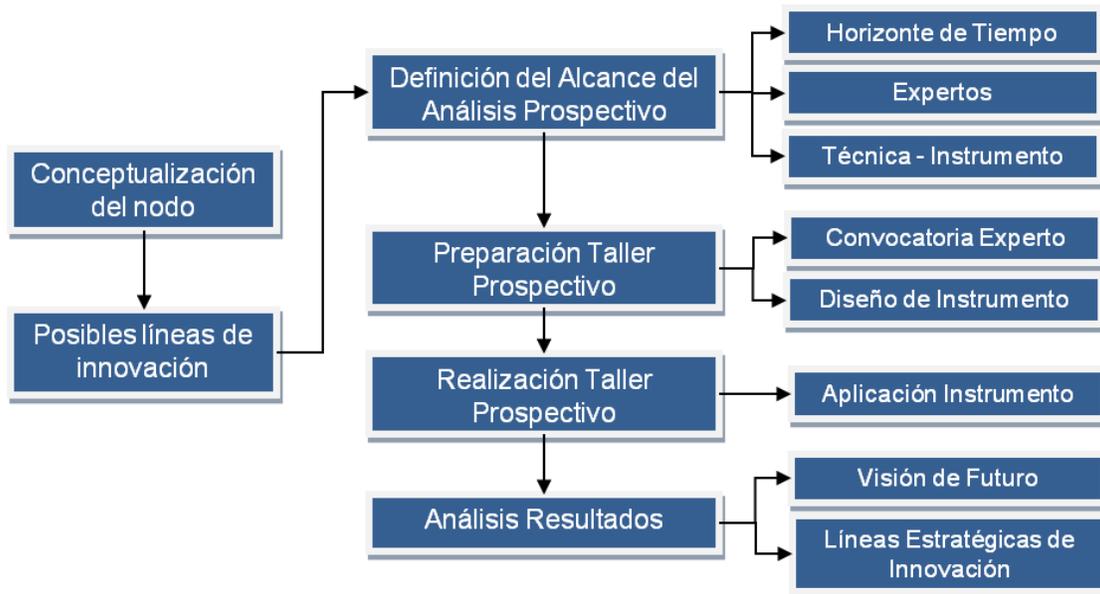
- **Comunicación:** el proceso pone en contacto empresarios, científicos, políticos, expertos en prospectiva, periodistas y personal implicado en el futuro de la ciencia, la tecnología y la innovación, y facilita la comunicación entre ellos.
- **Concentración en el largo plazo:** se demanda a los participantes que se concentren seria y sistemáticamente en el largo plazo, impidiendo que dominen los problemas a corto plazo.
- **Coordinación:** permite a los participantes coordinar sus actividades políticas y estrategias de I+D+i y ajustarlas, tras conocer las predicciones de sus competidores.
- **Consenso:** ayuda a los participantes a establecer acuerdos para la determinación de prioridades compartidas orientadas a diseñar el futuro que se quiere crear.
- **Compromiso:** la implicación de todos los actores en este proceso genera un sentimiento de responsabilidad compartida que refuerza el compromiso para que las predicciones se conviertan en objetivos nacionales a realizar en los tiempos estimados, e incluso antes.

Tres elementos son básicos al momento de realizar un proceso prospectivo: i) establecimiento del horizonte de tiempo a trabajar, ii) identificación del grupo de expertos que participarán en el ejercicio y, iii) la selección de los instrumentos metodológicos a utilizar. El horizonte de tiempo corresponde al año que se manejará como referencia para plantear la visión de futuro, este horizonte depende de las particularidades del sistema que se esté analizando. Los expertos son aquellas personas que tienen un amplio y profundo conocimiento en la temática o fenómeno respectivo y que serán consultadas durante el proceso prospectivo.

En relación a los instrumentos metodológicos se dispone de un portafolio amplio (Popper 2008, citado por Medina y Sánchez 2008) que se pueden clasificar en: i) Instrumentos cualitativos, que son aquellos que brindan significados a eventos y percepciones, y cuyas interpretaciones están basadas normalmente en la subjetividad y la creatividad, encontrándose aquí por ejemplo la lluvia de ideas y los paneles de expertos; ii) Instrumentos cuantitativos, los cuales miden variables y aplican análisis estadístico tales como bibliometría, análisis de series de tiempo y análisis de patentes y; iii) Instrumentos semi cuantitativos, los cuales aplican principios matemáticos para cuantificar o medir los juicios racionales y puntos de vista de expertos, tales como Delphi y escenarios.

La selección de los instrumentos metodológicos depende principalmente de la especificidad del sistema analizado y de los recursos disponibles. En la Figura 3 se presenta el esquema metodológico utilizado para la prospectiva.

Figura 3. Esquema Metodológico Prospectiva



Fuente: CINTEL (2011)

De esta forma, la prospectiva es el enfoque metodológico que permite identificar para cada uno de los Nodos su visión futura, cuyo horizonte prospectivo es de cinco años, es decir 2016. Dicha visión incluyó las líneas estratégicas en las cuales se centró cada nodo convirtiéndose en el foco orientador hacia el cual deben tender cada uno de los proyectos de innovación que constituyen la Agenda Estratégica de Innovación.

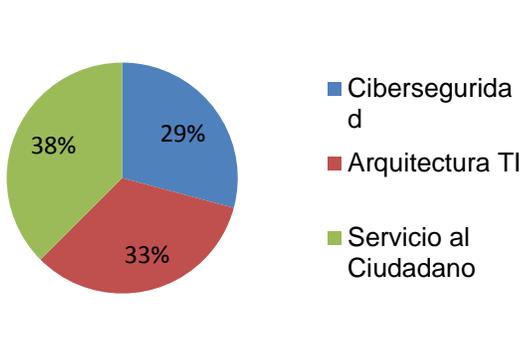
Para efectos de este proyecto se desarrollaron los Nodos de Innovación en ciberseguridad, arquitectura TI y servicios al ciudadano.

2.2.1 Resultados de los ejercicios de prospectiva por cada NDI

Para efectos de la primera etapa de la primera fase de Constitución del Subsistema de Innovación, se desarrolló un ejercicio prospectivo para los Nodos de innovación en ciberseguridad, arquitectura TI para gobierno y servicios al ciudadano. Para ello se construyó un instrumento con el cual se buscó, a través de una sola sesión, capturar la percepción de los expertos acerca del futuro de cada Nodo, así como de las líneas estratégicas en las cuales deberían enfocarse, para a partir de ello consolidar un portafolio de proyectos de innovación. El instrumento se estructuró en cinco grandes componentes: i) identificación de los participantes, ii) presentación del instrumento, iii) visión de futuro del Nodo al 2016, iv) identificación de las líneas estratégicas de innovación para el Nodo y v) identificación de posibles proyectos de innovación. La plantilla del instrumento se presenta en el Anexo 1.

La implementación del ejercicio prospectivo se llevó a cabo el 1 de Diciembre del 2011 en las instalaciones de CINTEL, para ello fue importante definir y convocar el grupo de expertos que participarían de forma activa en el ejercicio, considerando que se deseaba intervención por parte de entidades del Estado, las empresas y la academia. Como se presenta en la Figura 4, un total de 24 actores diligenciaron los instrumentos, el 38% de ellos identificados con el nodo de Servicio al ciudadano, 33% con el de Arquitectura TI y 29% con el de Ciberseguridad.

Figura 4. Distribución Actores participantes ejercicio prospectivo



Fuente: CINTEL (2011)

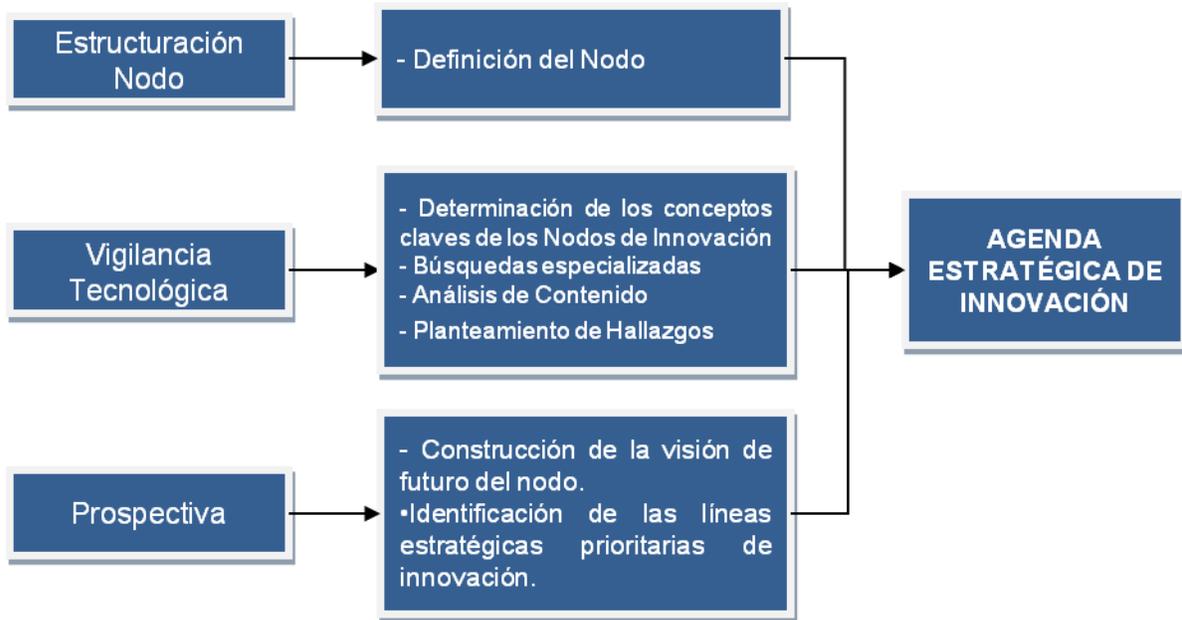
Los resultados principales y específicos para cada uno de los nodos se presentan en los numerales 5.3, 6.4 y 7.2.

2.3 AGENDA ESTRATÉGICA DE INNOVACIÓN

Cada uno de los Nodos de Innovación del Subsistema dispone de una Agenda Estratégica de Innovación la cual, según Nagji y Quinn (2010) se constituye en una herramienta muy útil a la hora de crear la claridad organizativa necesaria para la puesta en práctica de la innovación de manera eficiente y con éxito. Según Euskadi+Innova (s.f) una agenda de innovación es un plan directriz sostenido en el tiempo, donde aparecen planificadas y priorizadas en sus distintos horizontes, las actuaciones y proyectos que satisfagan suficientemente los retos más importantes que, en materia de competitividad e innovación, se le plantean a un sistema.

Las agendas estratégicas de innovación para los nodos son el resultado de un proceso que incluye la implementación y articulación de herramientas de gestión tecnológica, específicamente: vigilancia y prospectiva. Cada una de ellas arroja insumos valiosos para la consolidación de la agenda, tal como se presenta en la Figura 5.

Figura 5. Consolidación Agenda Estratégica de Innovación



Fuente: CINTEL (2011)

3. USO Y APROPIACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – TIC EN EL GOBIERNO

Un gobierno es una organización enorme y compleja, sus operaciones y objetivos estratégicos pueden ser ampliamente mejorados mediante la correcta aplicación de las TIC, pues estas se convierten en el soporte para mejorar la productividad, la efectividad en la gestión, y la calidad de los servicios ofertados a los ciudadanos (Gichoya, 2005). En el gobierno, el tradicional paradigma burocrático está caracterizado por buscar eficiencia en la productividad interna, racionalidad funcional, departamentalización, control jerárquico y gestión basada en reglamentación, está empezando a ser remplazado por competitividad y por requerimientos basados en el conocimiento, tales como: la flexibilidad, la organización en red, la integración vertical y horizontal, el emprendimiento innovador, el aprendizaje organizacional, la agilidad en la entrega de servicios y las estrategias dirigidas al cliente, aspectos que enfatizan la construcción de redes para coordinación y la colaboración externa, todo soportado por TIC (Ndou, 2004).

Es por esto que los gobiernos estructuran sistemas informáticos como medio para modernizar la gestión pública a través de las TIC, en busca de mejores prácticas, mayor control, transparencia y agilidad, siendo estas plataformas una oportunidad para acceder y participar activamente en los servicios públicos, de forma más flexible y sin acudir a las dependencias del Estado por parte de los usuarios. (Mestre, 2011)

Asimismo, el valor de las TIC está en la habilidad que éstas poseen para asistir al gobierno en encontrar soluciones a sus problemas, por lo que el gasto en TIC sólo puede ser justificado si existen beneficios devengados de la aplicación de estas tecnologías. Los beneficios buscados por todo gobierno son (Gichoya, 2005):

- Reducción de costos
- Calidad en la entrega de servicios
- Incrementar la capacidad del gobierno
- Mejorar la toma de decisiones
- Transparencia
- Mejora en la eficiencia
- Mejoras en el acceso de información
- Otros beneficios tecnológicos.

Las consecuencias de buscar estos beneficios al implementar TIC influyen en la estructura interna del gobierno y en sus relaciones externas con los ciudadanos. Aparece entonces la perspectiva de redes de gobierno con una dimensión interna y otra externa. Internamente se podría llamar “gobierno integrado” que conecta varios niveles y agencias de gobierno para proveer más servicios integrados; y, externamente, “gobierno en red”, centrado en aliados público-privados, donde se ha notado una creciente tendencia a tercerizar servicios de gobierno, ambas dimensiones habrían sido imposibles sin la incorporación de TIC (Dijk, 2010).

En este escenario de cambio de paradigmas, de la burocracia clásica hacia la integración en red a través de TIC, el concepto de gobernanza cobra mayor relevancia, enmarcando la forma y la regulación en la que los gobiernos transforman paulatinamente sus funciones y servicios. Esta e-gobernanza tiene tres



componentes: e-government, ó gobierno electrónico; e-commerce ó comercio electrónico; y e-democracy ó democracia electrónica (Song & Hee, 2006), no obstante, e-commerce y e-democracy son dimensiones que, aunque tienen control y participación de los gobiernos, dependen mayoritariamente de las comunidades e individuos, en tanto que la informática gubernamental podría definirse entonces como la aplicación de información, sistemas de información y tecnologías de información en el gobierno (Gichoya, 2005), definición que está directamente relacionada por un lado con la aplicación de e-government, que se enfoca principalmente en la prestación más eficiente de servicios de gobierno (Bannister & Remenyi, 2005) y por el otro, con el concepto de arquitectura TI que se enfoca principalmente con la integración de procesos, servicios y actividades dispares (Escobar Moreno & Et.Al, 2007).

A continuación se describe el contexto de e-government a nivel mundial, el cual, desde un punto de vista tecnológico, está asociado a la capacidad que ofrecen las TIC para desarrollar y ofrecer información y servicios públicos a través de medios telemáticos, habitualmente Internet (Mestre, 2011). En cuanto a la descripción de arquitectura TI, esta se describe en el respectivo Nodo de innovación en Arquitectura TI para gobierno (ver capítulo 6).

Desde un punto de vista tecnológico, el gobierno electrónico está asociado a la capacidad que ofrecen las TIC para desarrollar y ofrecer información y servicios públicos a través de medios telemáticos, habitualmente Internet (Mestre, 2011).

Para ello, el gobierno estructura sistemas informáticos como medio para modernizar la gestión pública a través de las TIC, en busca de mejores prácticas, mayor control, transparencia y agilidad, siendo estas plataformas una oportunidad para acceder y participar activamente en los servicios públicos, de forma más flexible y sin acudir a las dependencias del Estado por parte de los usuarios. (Mestre, 2011)

3.1 OBJETIVO DEL E-GOVERNMENT

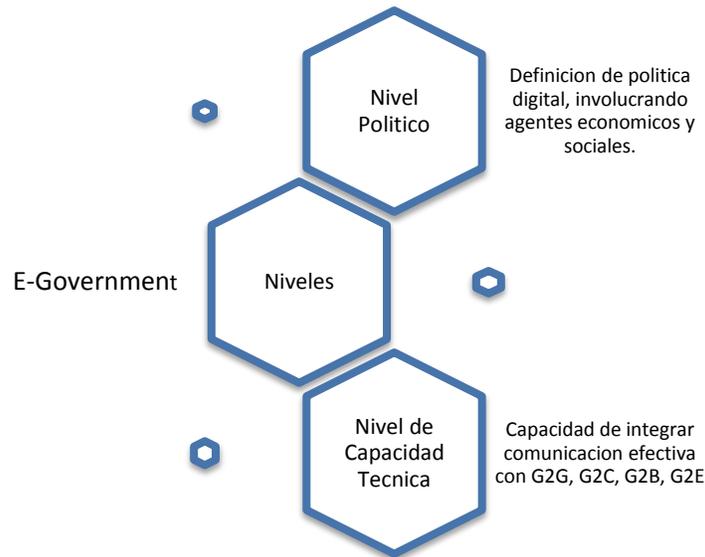
Un sistema E-Government tiene por objetivo: *“Crear condiciones institucionales que favorezcan el desarrollo y la promoción, a través de una estrategia de alcance nacional y/o internacional”¹*

3.2 CARACTERÍSTICAS DEL E-GOVERNMENT

La conformación de un sistema E-Government se encuentra fundamentado en dos niveles que deben ser gestionables para el cumplimiento de su objetivo, estos se pueden ver en la Figura 6.

¹ MESTRE Hemando, Gobierno Efectividad Y Transparencia: E-Government, 2011.

Figura 6. Niveles de Gestión en un Sistema E-Government.

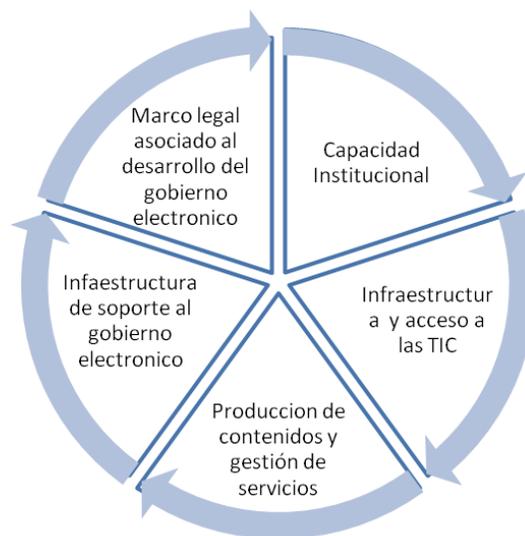


Fuente: Hernando Mestre Gobierno efectividad y Transparencia 2011.

3.3 ELEMENTOS DE COMPOSICIÓN

Dentro del funcionamiento de un Sistema E-Government, se evidencian cinco elementos constitutivos, que transforman las estructuras tradicionales de la administración pública en modelos informáticos de acceso, generalmente por Internet.

Figura 7. Elementos de constitución de un Sistema E-Government



Fuente: Hernando Mestre Gobierno Efectividad y Transparencia 2011.



Cada uno de los elementos está definido de la siguiente manera (Mestre, 2011):

1. **Capacidad institucional para el desarrollo del Sistema:** Es el componente que reúne los elementos de la organización institucional y la capacidad de reestructurar los procesos administrativos, que vayan en concordancia con las políticas, desarrollo y gestión del Sistema E-Government.
2. **Incentivos a la demanda en el acceso y uso de las TIC:** Se encuentra referido al diseño de los mecanismos de estímulo para un incremento en la participación por parte de los clientes a los cuales se enfoca el sistema.
3. **Producción de contenidos y gestión de servicios:** Hace referencia a las necesidades de producción de contenidos y la gestión asociada; generalmente contenidos en el portal web.
4. **Infraestructura de soporte al gobierno electrónico:** Contiene aquellas consideraciones referidas al diseño bajo el uso de hardware y software. Para la comunicación con los diferentes actores, con características de robustez, fiabilidad y seguridad.
5. **Marco legal asociado al desarrollo del gobierno electrónico:** Involucra la definición de normas y reglamentos técnico-legales para dar validez a los servicios y apoyar la promoción entre los usuarios, con énfasis en la seguridad técnica y jurídica de los servicios.

3.4 INTERACCIONES EN EL SISTEMA E-GOVERNMENT

3.4.1. e-Democracy

En el ámbito académico, es aquel término que hace referencia *a todos aquellos mecanismos electrónicos que permiten la participación ciudadana en la vida política mediante el uso de las TIC, ya sea de forma directa en la toma de decisiones políticas, o por medio de una elite o representación política, según el modelo de democracia considerado*². El vínculo tecnológico a este tipo de iniciativas debe asegurar elementos de formación, información, debate y votación.

3.4.2. e-Administration

En el ámbito académico este término hace referencia a aquellos *“mecanismos electrónicos que permiten la prestación de servicios públicos del gobierno tanto a la ciudadanía como a las empresas*³”. Incluyendo además los mecanismos que permiten la interactividad y la gestión al interior de los distintos departamentos que componen la administración pública.

² *Ibíd.* Pág. 1.

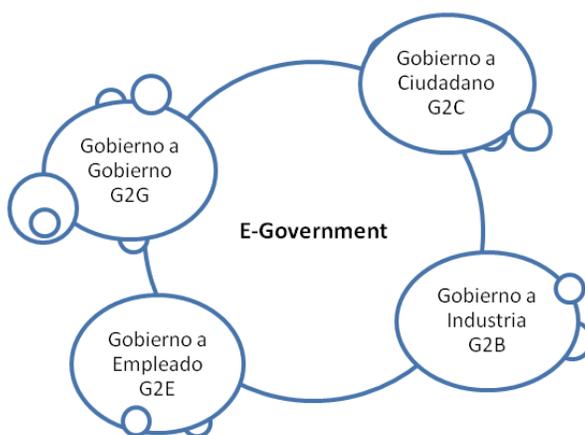
³ *Ibíd.* Pág. 1.

3.5 INTERACCIÓN DE UN SISTEMA E-GOVERNMENT

La eficacia y eficiencia de un Sistema de gobierno electrónico varía en cuanto a la capacidad de responder a los diferentes agentes presentes en una sociedad. Estos agentes cumplen funciones específicas dentro de la conformación de una nación; enmarcadas en áreas económicas, sociales, culturales y políticas.

La atención de un gobierno electrónico a su participación es fundamental por cuanto genera una democratización del servicio, la información asociada y los servicios prestados. Se han reconocido en cada interacción del sistema los agentes presentes en la Figura 8.

Figura 8. Interacción de un Sistema E-Government



Fuente: (ORACLE, 2002)

La característica en el acceso a información, dada según el tipo de agente que accede, permite clasificar el sistema, ejemplo de ello se encuentra en la relación Administración Pública (G2G y G2E) y su comunicación con el exterior (G2C y G2B), llegando a ser esta de alcance nacional, regional o local (metropolitano).

3.5.1 Government to Citizens (G2C)

El e-gobierno ofrece importantes posibilidades para mejorar la experiencia e interactividad del público con su ente gubernamental.

3.5.2 Government to Business (G2B)

Dado el rol variable de las empresas siempre regulado a través de la legislación (suministradoras de información, elementos de asociación, clientes y en ocasiones competidores del gobierno), se presenta un alto flujo de información estrictamente ligada a la participación del estado en la relación con las empresas.

3.5.3 Government to Employees (G2E)



Los gobiernos pueden usar una intranet para interactuar de forma sencilla con sus empleados en temas relativos a la información de recursos humanos, jubilación, noticias de interés y otro tipo de temas relacionados con los trabajadores de la administración⁴. Es así como este vínculo gobierno – empleados se convierte en un medio efectivo para proporcionar el *e-learning* y promocionar la gestión del conocimiento.

3.5.4 Government to Government (G2G)

Los gobiernos también pueden comunicarse eficientemente con otros gobiernos a través de servicios *on-line*. Algunos de estos esfuerzos pueden requerir más acceso a bases de datos y aplicaciones, mientras que otras iniciativas de e-gobierno pueden ser tan simples como la pura transferencia de datos, transacciones o acceso a información. Los servicios G2G pueden requerir más enlaces directos a través de las intranets de los estados y tendrán lugar en todos los niveles del gobierno. (Mestre, 2011)

3.6 ELEMENTOS DE LA INTERACCIÓN EN EL SISTEMA E-GOVERNMENT

La interacción de la Información en un Sistema E-Government, se fundamenta en dos actividades principalmente, vistas desde el actor gobierno: el acceso a información y el recaudo de información. La finalidad de estas acciones puede estar fundamentada en la realización de trámites, búsqueda de información de operaciones, datos nacionales, entre otros.

Sin importar el motivo de la esta interacción, ésta debe estar fundamentada en la seguridad de la información a la que se accede y que se otorga, y en el acceso democratizado de dicha información.

⁴ *Ibid.* Pág. 1.

Figura 9. Interacción del Sistema E-Government.



Fuente: Cintel (2011)

3.7 NIVELES DE MADUREZ EN SISTEMAS E-GOVERNMENT

Los sistemas de e-gobierno se pueden catalogar en diversos niveles de madurez, según un análisis realizado por ORACLE⁵. Estos niveles son:

1. Presencia Primaria:

Hace referencia a la creación de un sitio de Internet, a través de los cuales se interactúa de forma no interactiva, ya que no se puede realizar una gestión de la información, al sólo tener presencia web con la exposición de información básica. (D.R. Instituto Tecnológico y de Estudios Superiores de Monterrey, 2007)

2. Presencia Mejorada:

En este nivel de iniciativas de gobierno en línea, se evidencia la capacidad de ofrecer mayor información al público en forma más avanzada, a través de un portal con capacidad de realizar una gestión de conocimiento ligada a la comunicación con el usuario. Ello se ve representado con la posibilidad de búsqueda e impresión de documentos. (D.R. Instituto Tecnológico y de Estudios Superiores de Monterrey, 2007)

3. Presencia Interactiva:

⁵ ORACLE, E-Government: Conectando ciudadanos, empleados y proveedores, 2002.



Este nivel se caracteriza por la posibilidad de solicitar e intercambiar información con el gobierno, con la posibilidad de permitir una distinción de los datos sensibles de las diferentes áreas de la institución con la finalidad de tener la información reunida en un solo lugar "business warehouse" para que sea útil en el momento de tomar decisiones y tener sistemas de apoyo a decisiones e informes gerenciales. (D.R. Instituto Tecnológico y de Estudios Superiores de Monterrey, 2007)

4. Presencia Transaccional:

El nivel transaccional se caracteriza por la oportunidad de realizar transacciones monetarias, con la adición de servicios más integrados. Las posibilidades son amplias en la integración de operaciones monetarias, éstas incluyen pagos tributarios, operaciones de banca en web. (D.R. Instituto Tecnológico y de Estudios Superiores de Monterrey, 2007)

5. Integración Total:

Este nivel reúne los servicios de varios ministerios, secretarías, gobiernos o municipios, donde los procesos de negocio están coordinados y rediseñados, en base a la infraestructura tecnológica. (D.R. Instituto Tecnológico y de Estudios Superiores de Monterrey, 2007)

4. TENDENCIAS EN EL USO DE TIC EN EL GOBIERNO

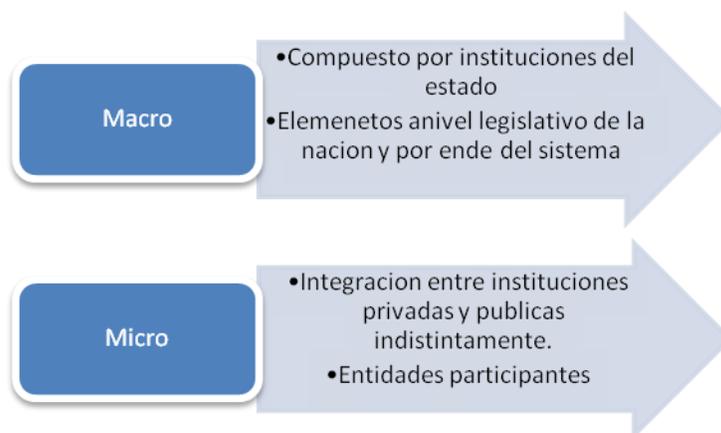
4.1 ESTRATEGIAS EN LA IMPLEMENTACION UNA INICIATIVA DE GOBIERNO EN LINEA

Dentro de las estrategias identificadas en la implementación de TIC en el gobierno, se identifica la necesidad de un marco institucional capaz de promover el desarrollo del E-Government, que posibilite la participación, integración a diversos agentes como protagonistas, permitiéndoles además participar en su continua construcción.

Parte de las estrategias vinculadas obliga una gestión que permita el estímulo y la regulación en el manejo de los contenidos que se generan.

Este marco institucional se caracteriza por dos niveles claramente diferenciables que se relacionan y condicionan entre sí. (Mestre, 2011)

Figura 10. Composición en el Sistema frente a la información.



Fuente: (Mestre, 2011)

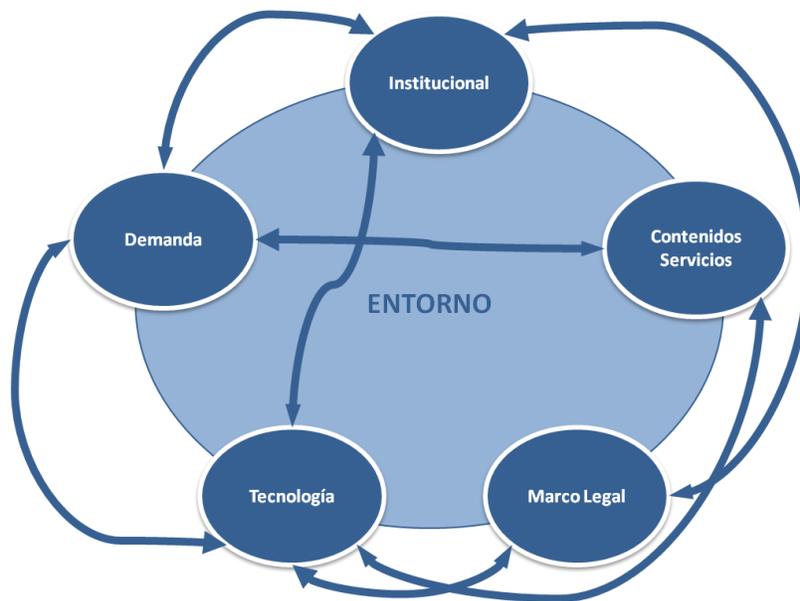
Dentro de estos dos elementos, macro y micro, relacionados con la regulación del sistema y de la participación de entidades públicas y privadas, respectivamente, se identifican elementos que se constituyen en análisis para la implementación de estrategias encaminadas a la implementación de este tipo de sistemas.

Estos elementos de análisis en el entorno son:

1. La demanda de servicios TI en una sociedad, ligada a la posibilidad de acceso, infraestructura de redes nacionales, cultura nacional frente al uso y aplicación tecnológica, capacidad técnica para el acceso y correcto uso de las plataformas online en todo el territorio. Este vínculo se fundamenta en la democratización de uso de las TIC.
2. La tecnología necesaria para la implementación de las plataformas, involucrando software y hardware necesario a nivel nacional e internacional.

3. Marco legal presente en la institucionalidad, carácter veraz y activo en el sistema, así como en la legislación e iniciativas gubernamentales ligadas al uso de la tecnología en un país, así como a la seguridad en la información a la que se accede y entrega por parte de un usuario.
4. Institucionalidad, referente a la regulación y participación de entidades privadas y públicas que se encuentran referidas como generadoras de información para y con el sistema.
5. Contenidos y servicios, este elemento se encuentra relacionado con la información, nivel de interacción de los diferentes usuarios con el sistema ante todo tipo de acciones, tales como trámites, consultas, accesos a subsistemas específicos, entre otros. Así como opciones de acceso y diseño visual del sistema.

Figura 11. Elementos de análisis en una estrategia de implementación E-Government



Fuente: (Mestre, 2011)

Estos elementos de análisis son identificados en cuatro aspectos, mostrados en la Figura 12

- **Entorno:** El desarrollo de una estrategia y la gestión del gobierno electrónico GE, dependen del escenario donde se genera, que en sí mismo está en función del alcance de las capacidades del mismo gobierno. El alcance se mide en dos dimensiones: alcance geográfico (nacional, regional o municipal) y alcance funcional (temática). Es necesario conocer y evaluar aquellos aspectos que condicionan y/o facilitan el diseño de capacidades de GE, que pueden ser de tipo social, cultural, político o económico.

Los elementos de análisis en el entorno se ven en la Tabla 1.

Figura 12. Elementos de análisis en la estrategia de implementación.



Fuente: CINTEL (2011)

Tabla 1: Análisis de entorno

ECONÓMICO
<ul style="list-style-type: none"> · Principales sectores productivos del país · El grado de asimilación de las tecnologías de la información y comunicación por parte del sector productivo · Grado de desarrollo del sector empresarial en tecnologías de la información y comunicación · Tarifas de los servicios básicos de telecomunicaciones son asequibles a los usuarios de ingreso promedio · Desarrollo de la infraestructura de las comunicaciones · Grado de acceso que tiene la población a los servicios básicos

Fuente: Hernando Mestre 2011.

Tabla 2: Análisis de gubernamental.

POLITICO – GUBERNAMENTAL
<ul style="list-style-type: none"> · Capacidad de ejecución y de gestión que tiene el Gobierno · Credibilidad que ofrece el Gobierno · Marco regulatorio de las telecomunicaciones · Una política nacional en Sociedad de la Información · Liderazgo de una estrategia nacional en Sociedad de la Información · Marco legal y político que de soporte al desarrollo de una estrategia hacia la Sociedad de la Información

Fuente: Hernando Mestre 2011.

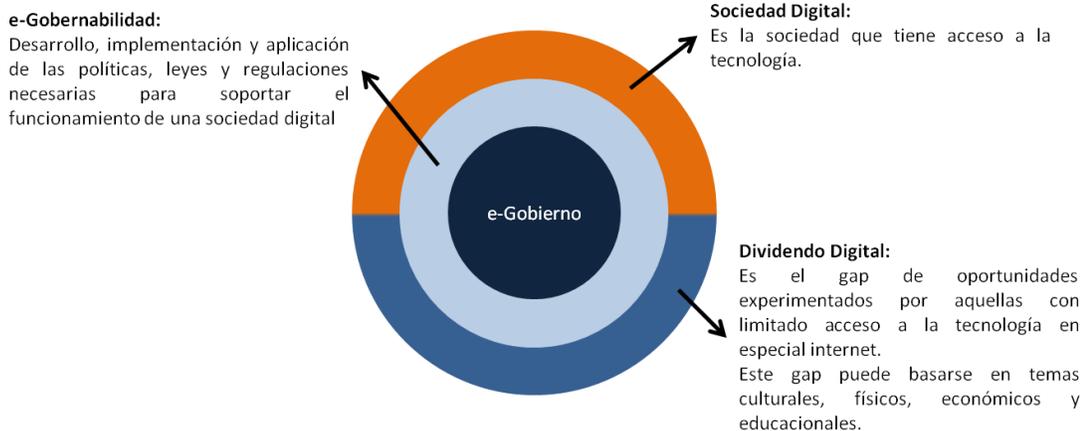
Tabla 3: Análisis de social y cultural.

SOCIAL – CULTURAL	
<ul style="list-style-type: none"> · · · · · · 	<p>Nivel cultural de los futuros usuarios</p> <p>Nivel de confianza que tienen los ciudadanos en el gobierno</p> <p>Índice de penetración de internet en la comunidad</p> <p>Edad media de la población</p> <p>Nivel de confianza de la sociedad en el gobierno y en la función de la administración pública</p> <p>Idiomas y dialectos</p>

Fuente: Hernando Mestre 2011.

De igual forma el análisis en la estrategia de implementación entra a considerar la sociedad actual bajo el paradigma de la digitalización, ejemplo caro se encuentra ligado a la conceptualización de ORACLE, presentada en la Figura 13.

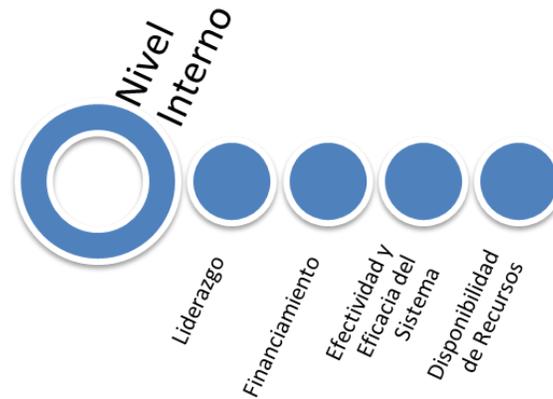
Figura 13. Interacción del e-Government con elementos externos y actuales paradigmas.



Fuente: (ORACLE, 2002)

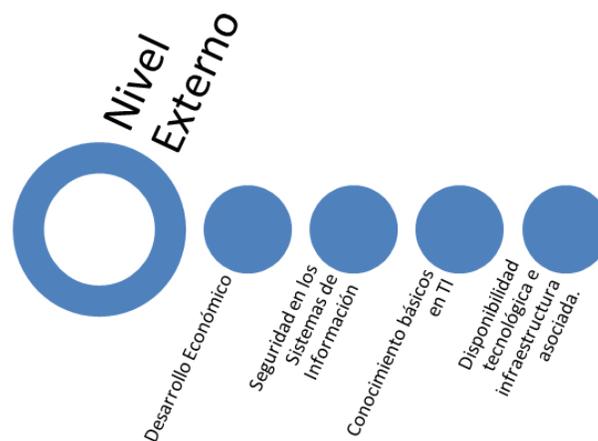
A nivel de participación de los factores que se encuentran en la estrategia, ORACLE (Figura 14 y Figura 15) reconoce dos niveles, conteniendo en cada uno acciones o actitudes a abordar para una estrategia exitosa.

Figura 14. Nivel interno en la estrategia de implementación.



Fuente: (ORACLE, 2002)

Figura 15. Nivel Externo en la estrategia de implementación.

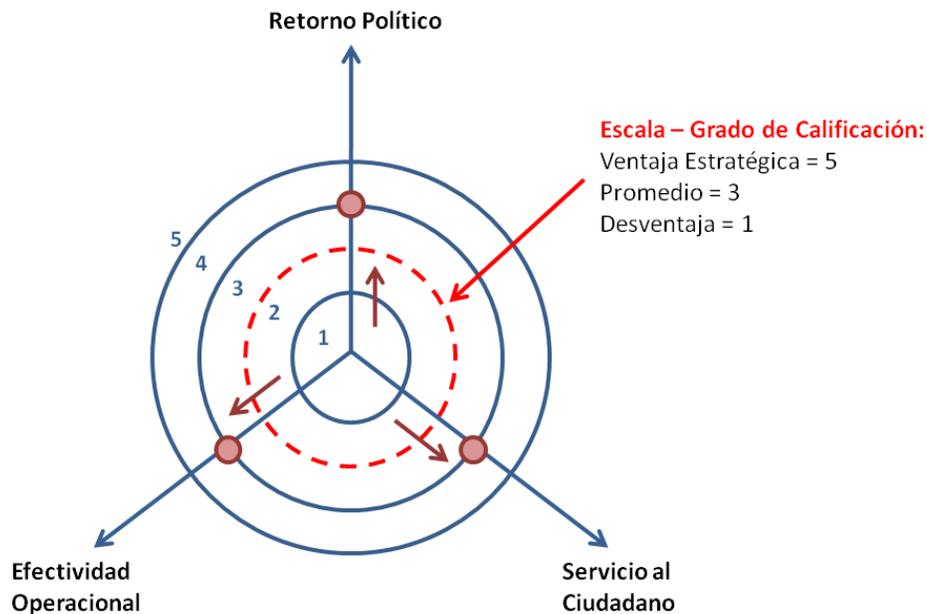


Fuente: (ORACLE, 2002)

4.2 ENFOQUE DE LA ESTRATEGIA

La estrategia en el sistema debe estar ligada a tres aspectos: el retorno político, el servicio al ciudadano y la efectividad operacional, tal como se observa en la Figura 16. Estos elementos miden el impacto de todo el sistema a nivel nacional.

Figura 16. Enfoque de estrategia en un sistema E-Government.



Fuente: (ORACLE, 2002)

En esta estrategia es necesario abordar de manera eficiente varios temas de importancia fundamental, los cuales pueden clasificarse del siguiente modo (Carmichae, 2010):

1. **Marco legislativo y limitaciones:** Como efecto de la existencia de un marco legislativo, se presenta la dependencia tradicional en las firmas manuscritas, en los trámites de legalización de documentos y en otros procesos jurídicos, que afectan el correcto funcionamiento del sistema.
2. **Protección de los derechos del ciudadano:**
 - Confidencialidad
 - Libertad de información
 - Función de las firmas
 - Autenticación y firmas electrónicas

Al mismo tiempo, han de protegerse los derechos del ciudadano y de otros clientes, como las empresas.

3. **Gestionar los riesgos del gobierno:**
 - Fraude
 - Otras actividades delictivas

El riesgo financiero, el fraude y el robo, afectan la interacción del sistema entre usuarios y servicios, participando en ello: pagos electrónicos y el envío de información cliente. Dada la cualidad de esta

información se deben realizar evaluaciones de carácter exhaustivo de los riesgos que se encuentren asociados a los procesos y elementos que conforman esta interacción como por ejemplo la identificación, localización, legalización y almacenamiento de los datos.

Algunos organismos estatales o privados responden a estas cuestiones implantando más soluciones tecnológicas, pero esto se constituye en una limitante que debe ser analizada a razón de la visión y la política para tratar estas cuestiones. En este sentido la tecnología puede tener su función, pero sin un marco de políticas adecuado, puede ser ineficiente. Es necesario que ante este esquema se planteen las siguientes opciones:

1. **Promover la aplicación de tecnologías:** El gobierno puede participar en la promoción del uso de estas tecnologías de varias maneras. Esta actuación debe articularse como un claro objetivo de política, con una clara estrategia de implantación.
2. **Trabajar en colaboración con el sector privado:** Los distintos programas políticos en relación con la participación del sector privado varían según los países y las regiones.

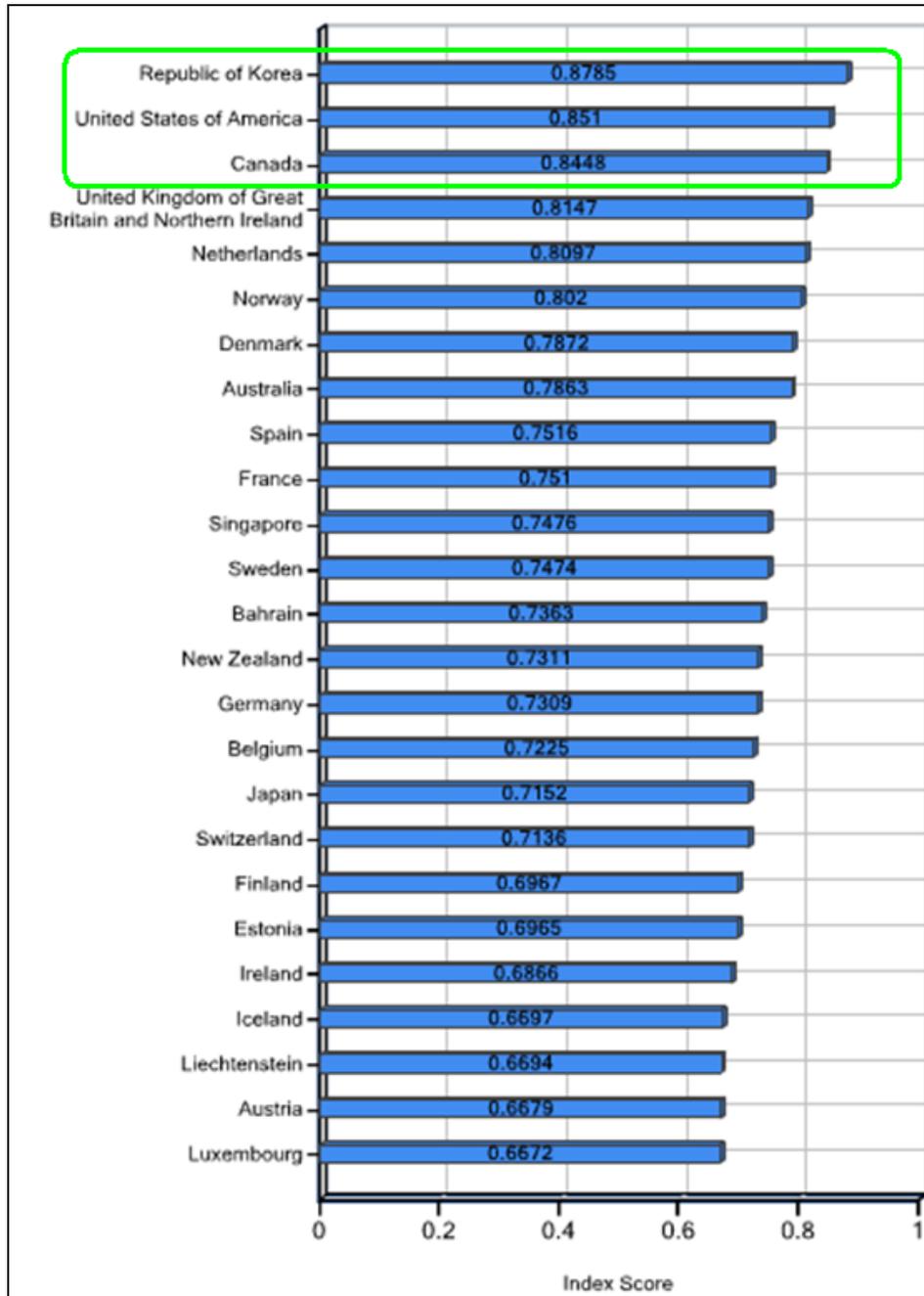
4.3 CASOS DE E-GOVERNMENT A NIVEL MUNDIAL

Se analizaron de forma particular las características de los países hispanoamericanos debido a las similares características sociales y culturales existentes, que facilitan los procesos de transferencia tecnológica. En este sentido, España es el país que presenta mayores índices de desarrollo de Clústers y E-Government, y por esta razón sus características de desarrollo se presentan en las secciones siguientes.

4.3.1 UN Public Administration Programme - UN E- Government Development Database

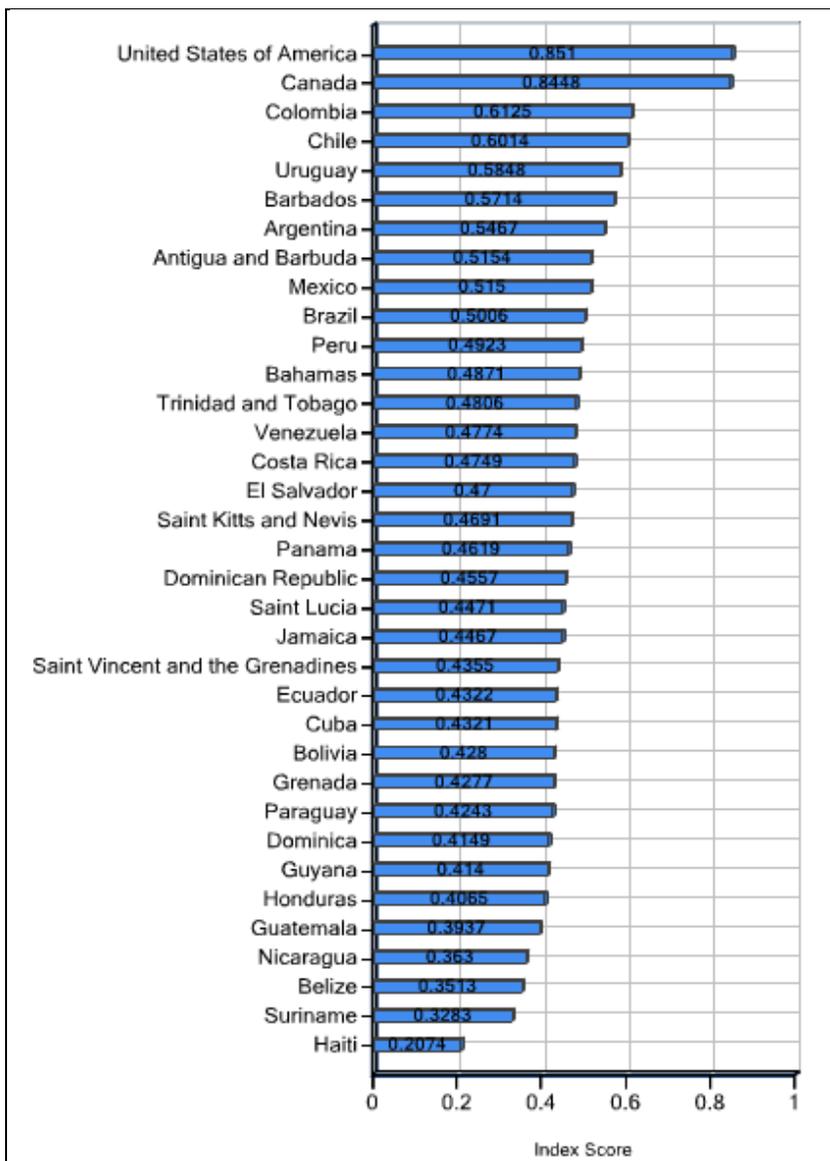
UNeGovDD es una base de datos que alberga las diversas propuestas a nivel mundial de E-Government, con datos de 193 países y, con la posibilidad de consultar los datos por continentes. La base de datos fue creada por la *División para la Administración Pública Y el Desarrollo de la Gestión del Departamento de Asuntos Económicos Y Sociales de las Naciones Unidas*. (UN, 2011)

Figura 17. Indexación a nivel mundial de sistemas E-Government.



Fuente: UN 2011

Figura 18. Indexación a nivel Américas de sistemas E-Government.



Fuente: UN 2011

A continuación se presenta un panorama de análisis sobre los criterios manejados por las Naciones Unidas, así como el posicionamiento de cuatro importantes países, en los primeros lugares del ranking de la plataforma UN con intención de comparar los datos: República de Corea, Estados Unidos, Canadá y Colombia.



Tabla 4: Comparación de Colombia contra tres países posicionados en el Ranking de sistemas E-Government.

Rank	Country Name	FACTORES DE ANALISIS					Rank
		2010 E-Government Index	2010 E-Participation Index	2010 Online Service Index	2010 Infrastructure Index	2010 Human Capital Index	2010 Online Service
1	Republic of Korea	0,8785	1	1	0,639	0,9929	1
2	United States of America	0,851	0,7571	0,9365	0,6449	0,9691	2
3	Canada	0,8448	0,7286	0,8825	0,6799	0,9708	3
31	Colombia	0,6125	0,4429	0,7111	0,2421	0,8813	9

Fuente: UN 2011

4.3.2 Análisis de los Factores de Selección

A continuación se presenta un análisis a los factores de indexación de los diversos Sistemas E-Government a nivel mundial, presentes en la base de datos de las acciones Unidas.

4.3.2.1 E-Government

El gobierno electrónico se define como el uso de las TIC y su aplicación por el gobierno para el suministro de información y los servicios públicos a la gente. El objetivo de E-Government por lo tanto, es proporcionar la gestión de gobierno eficaz de la información al ciudadano, una mejor prestación de servicios y el empoderamiento de las personas mediante el acceso a la información con la participación en las políticas públicas de toma de decisiones. (UN, 2011)

4.3.2.2 Participación Electrónica

La e-participación, o participación electrónica, abarca tanto la demanda como la oferta electrónica. Sin embargo, la e-participación determinada por las Naciones Unidas se limita a evaluar el aspecto de la participación de G2C, interacción gobierno y ciudadano.

4.3.2.3 Servicios Online - Web Measure

El Índice de Medición Web se basa en un modelo de cuatro etapas de desarrollo del gobierno electrónico de acuerdo a la escala de prestación de servicios al ciudadano, en base a estándares de las Naciones Unidas:

1. **Presencia emergente:** Representa la etapa I, donde la información es limitada y básica, presentándose principalmente en una página y/o un sitio web oficial. (UN, 2011)
Sin embargo, existen ligeras variantes que se fundamentan en los diversos enlaces asociados a los ministerios o departamentos de educación, salud, bienestar social, trabajo y finanzas; donde estas

uniones entre entidades regionales y/o locales pertenecientes al gobierno, se basa en la gestión de la información que soporta la página y/o la web oficial.

2. **Mayor presencia:** La calificación de “mayor presencia”, reconocido por las Naciones Unidas, corresponde a la etapa II, caracterizada por el ofrecimiento por parte del gobierno hacia la ciudadanía, de una mayor política pública y un incremento de las fuentes de información de gobernabilidad, tales como políticas, leyes, reglamentos, informes, boletines y bases de datos, disponibles en línea. (UN, 2011)

En esta etapa hay disponibilidad de una selección más amplia de documentos relacionados con la política pública, elementos en materia de educación o temas específicos de salud. Aunque más sofisticada, la interacción sigue siendo principalmente unidireccional con la información que fluye del gobierno a los ciudadanos. (UN, 2011)

3. **Presencia transaccional:** Corresponde a la etapa III, que permite la interacción bidireccional entre el ciudadano y su gobierno, incluyendo opciones para el pago de impuestos, solicitud de tarjetas de identidad, certificados de nacimiento / pasaporte, renovación de licencias y otras interacciones C2G de carácter similar. (UN, 2011)

Dentro de las operaciones que se presentan bajo este nivel, las Naciones Unidas en su base de datos de iniciativas de e-Government a lo largo del mundo, se destacan las siguientes:

- Transacciones económicas.
- Uso de tarjetas de crédito o débito.
- Acceso a información y gestión de los servicios públicos.
- Oferta en línea de contactos públicos a través de vínculos seguros.

4. **Presencia Conectada:** Corresponde al nivel más sofisticado de una iniciativa de gobierno electrónico, caracterizada por una integración de G2G, G2C y C2G. De esta forma el gobierno fomenta la deliberación participativa y la toma de decisiones, con disposición y capacidad para involucrar a la sociedad en un diálogo abierto de dos vías. (UN, 2011)

4.3.2.4 Infraestructura

El índice de infraestructura de telecomunicaciones es un índice compuesto promedio ponderado de los seis principales índices sobre la base de los indicadores básicos de infraestructura, que definen la capacidad de la infraestructura de TIC de un país. (UN, 2011)

Estos son: las personas que usan PC/1000, de Usuarios Internet/1000 personas; Líneas Telefónicas/1000 personas, la población en línea con el cálculo de Usuarios con Telefonía móvil /1000 personas y las personas con acceso a señal de TV/ 1000; según cálculos y apreciaciones de las Naciones Unidas en su base de iniciativas e-Government a nivel mundial.

Parte de los criterios en el análisis de la infraestructura, realizado por las Naciones Unidas, se basa en los datos de Estados miembros de la ONU, el cual fue tomado principalmente de la Unión Internacional de



Telecomunicaciones (UIT) y la División de Estadística de las Naciones Unidas, con complemento del Banco Mundial. Ello permitió la construcción de índices separados para la estandarización de los datos entre países.

Por otro lado las políticas de acceso a las TIC han tomado en cuenta los siguientes aspectos, desde la visión de las Naciones Unidas:

- La formulación de estrategias eficaces por parte del gobierno para facilitar una estructura de regulación capaz de gestionar una economía de mercado con las empresas que compiten por la participación en la infraestructura de telecomunicaciones. De igual forma la existencia de garantías de competencia leal entre empresas que compiten por bajar los precios y ahorrar los escasos fondos del gobierno en este aspecto, a través de organismos reguladores establecidos por el gobierno. (UN, 2011)
- Aplicación de conexiones inalámbricas a internet como mecanismo para la mejora de acceso y conectividad en las áreas remotas. Siendo estas además, una de las soluciones al robo de productos de cobre y alambre. (UN, 2011)
- Colaboración con otros gobiernos regionales para reducir las tasas de la tecnología satelital. La colaboración entre los estados vecinos pueden reforzar la investigación y también reducir los costos. (UN, 2011)
- Configuración de lugares para el acceso a internet y otros puntos de telecomunicaciones, con el objetivo de fortalecer la infraestructura de telecomunicaciones. (UN, 2011)

4.3.3 Capital Humano

Según las Naciones Unidas, uno de sus criterios en el análisis de sistemas e-government, es la existencia de una relación positiva entre el capital humano y el bajo desarrollo del gobierno electrónico. (UN, 2011)

Es importante concebir a partir de ello el impacto sobre el nivel de educación y cualificación de la población en general, logrando un mayor acceso a las TIC y una población más propensa a adoptar las tecnologías modernas de forma rápida y eficiente. Y a su vez, un aumento en la productividad económica y social. (UN, 2011).

4.4 PROGRAMA GOBIERNO EN LÍNEA

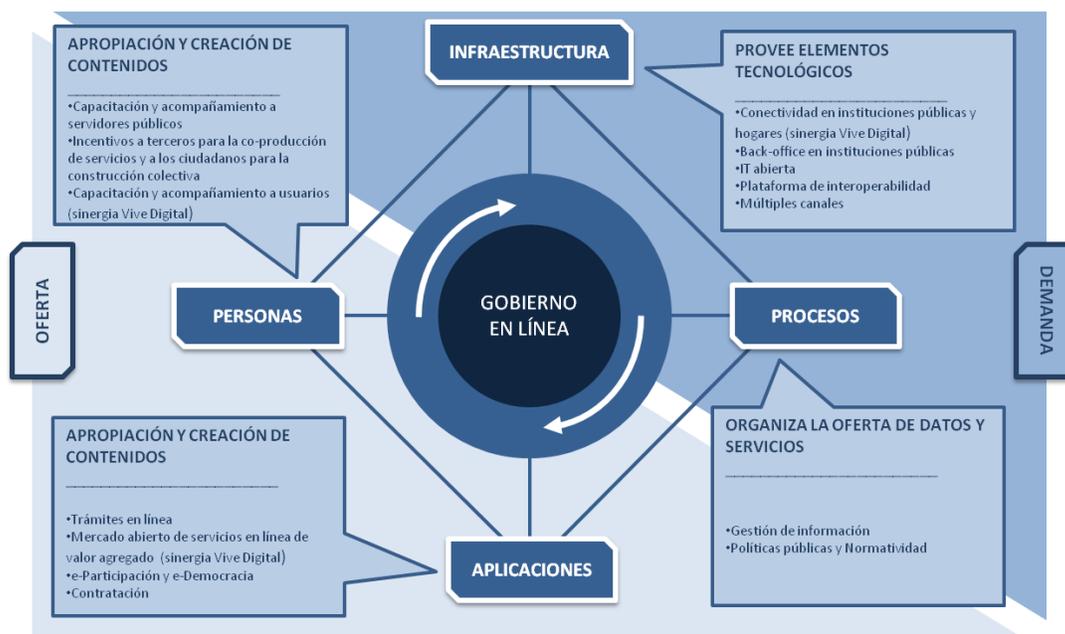
El Gobierno electrónico es más que tecnología, no se refiere únicamente a computadores e Internet, sino que hay una serie de aspectos normativos, sociales y culturales que inciden en el desarrollo del Programa de Gobierno en línea; implica un cambio organizacional para un Estado centrado en el ciudadano, enfocado en las necesidades de los clientes (que son de la Administración Pública) a quienes hay que prestarles un buen servicio. E igualmente implica un cambio cultural para los ciudadanos y las empresas en la forma en que se relacionan con el Estado.

Así mismo, el Programa Gobierno en línea impulsa una visión unificada del Estado, donde los colombianos no tienen que aprenderse la estructura del mismo, conocer cómo funciona cada institución para poder interactuar con éstas, ni acudir de un lugar a otro para resolver sus necesidades o cumplir con sus obligaciones, sino que el Estado es uno sólo con el que pueden relacionarse fácilmente. Con un Gobierno en línea que propende por la protección de la información del individuo y que adelanta acciones para estimular la credibilidad y confianza en el gobierno electrónico.

Desde luego, Gobierno en línea es una oportunidad para todos, está abierto para todos los colombianos al facilitar el acceso equitativo y multi-canal. Gran parte de las soluciones existentes actualmente se pueden acceder por Internet pero aun así, es necesario aprovechar las oportunidades de penetración por medio de otros canales, como el teléfono fijo, el teléfono móvil o los telecentros que ha venido instalando el Programa Compartel del Ministerio de Tecnologías de la Información y las Comunicaciones en las zonas más alejadas del país, y, en un futuro cercano, la televisión digital, para llegar fácilmente con los servicios de Gobierno en línea a toda la población.

Bajo estos principios se ha desarrollado el siguiente esquema o ecosistema que cuenta con cuatro componentes principales: personas, aplicaciones, procesos e Infraestructura.

Figura 19. Ecosistema de Gobierno en línea



Fuente: Programa de Gobierno el línea

Este ecosistema de Gobierno en línea en Colombia, se ha desarrollado para:

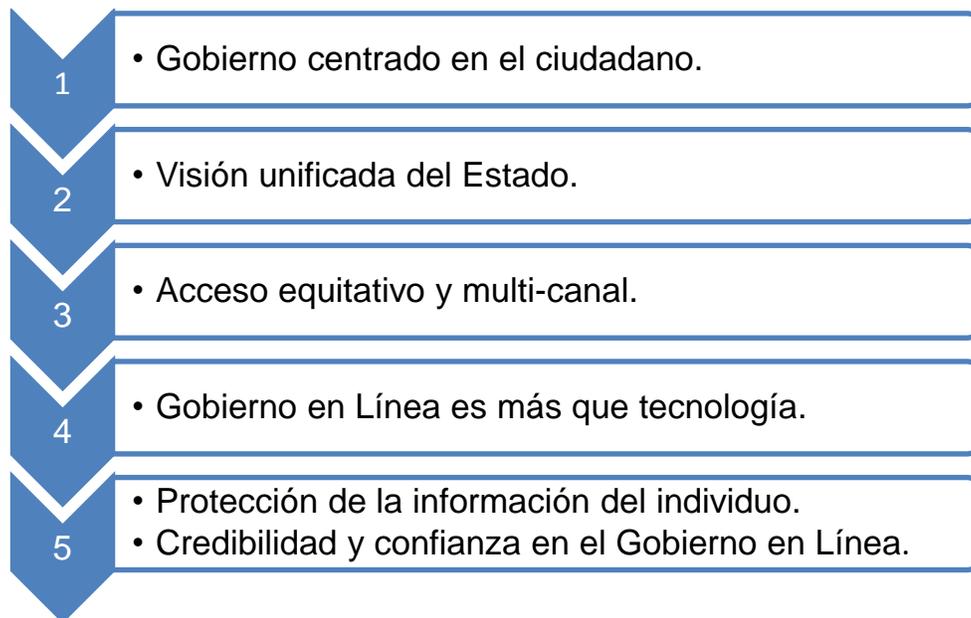
- Facilitar la eficiencia y colaboración en y entre las entidades del Estado, así como con la sociedad en su conjunto.
- Contribuir al incremento de la transparencia en la gestión pública
- Promover la participación ciudadana haciendo uso de los medios electrónicos

- Fortalecer la condiciones para el incremento de la competitividad y el mejoramiento de la calidad de vida

4.5 ESTADO ACTUAL

En la identificación de los principios básicos en la estrategia de Gobierno en línea (GEL) de Colombia, se hace mención de los siguientes principios que fundamentan su existencia en el territorio nacional encontrados en el Informe Final: Modelo de Seguridad de la Información Sistema SANSI - SGSI (Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea) del año 2008.

Figura 20. Principios básicos de la estrategia GEL



Fuente: (Equipo de Consultoría Digiware, 2008)

Como ejes de acción de la estrategia en GEL se reconocen tres conceptos generales: los servicios, la transparencia y la eficiencia. Como se puede ver a continuación.

Figura 21. Ejes de acción de GEL



Fuente: (Equipo Consultoría Digiware, 2008) Diagnostico de la Situación Actual - Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea



5. NODO DE INNOVACIÓN – CIBERSEGURIDAD

Este nodo se centra en la generación, adaptación, dominio y utilización⁶ de nuevas tecnologías que permitan minimizar y contrarrestar apropiadamente los riesgos e incidentes de naturaleza cibernética a los que está expuesto el Estado⁷. Este objetivo se enmarca en el Plan Nacional de Desarrollo 2010-2014 “Prosperidad para Todos”, el cual incluye la gestión de riesgos, protección al usuario y seguridad informática como lineamientos estratégicos para promover la competitividad y el crecimiento de la productividad en el país.

La conformación del nodo se da a través de las alianzas Estado – Academia y CDT – Empresa, con el propósito de realizar proyectos de innovación para mejorar la capacidad del estado en ciberseguridad y ciberdefensa.

A continuación se plantea una primera aproximación a los posibles integrantes para conformar el nodo.

Del sector Estado

Las instituciones del Estado son las receptoras de los procesos de implementación de las nuevas tecnologías que les permitirán protegerse de los riesgos y tratar adecuadamente cualquier incidente de ciberseguridad. Adicionalmente, varias de ellas son, por definición del CONPES 3701, responsables de procesos de liderar acciones concretas. En este sentido, son llamados a participar del Nodo:

- Entidades con responsabilidades específicas en ciberseguridad
 - Ministerio de Interior y de Justicia
 - Ministerio de Relaciones Exteriores
 - Ministerio de Defensa Nacional
 - Ministerio de Tecnologías de la Información y las Comunicaciones
 - Departamento Nacional de Planeación
 - Fiscalía General
- Entidades del estado:
 - Entidades líderes en la implementación de la norma ISO 27001
 - Entidades que han generado normativa de obligatorio cumplimiento en cuanto a seguridad de la información para sus entidades adscritas o vigiladas.

Del sector academia y CDT

- Universidades

⁶ COLCIENCIAS define como el propósito de la innovación tecnológica “generar o adaptar, dominar y utilizar una tecnología nueva en una región, sector productivo o aplicación específica y que permite a quienes lo desarrollen acumular conocimientos y las habilidades requeridas para explicar exitosamente la tecnología y posibilitar su mejora continua.”

⁷ El CONPES 3701 – Lineamientos de política para ciberseguridad y ciberdefensa definen estos dos términos como: a) Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética. b) Ciberdefensa: Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

- Grupos de investigación cuyo énfasis sea en la seguridad de la información, seguridad informática, comercio electrónico o recuperación de desastres.
- Asociaciones del sector
 - Asociaciones de especialistas que cuenten con líneas de trabajo en normalización, investigación, innovación o desarrollo en seguridad de la información, seguridad informática, comercio electrónico o recuperación de desastres.

Del sector empresa

Si bien en esta área se encuentran muchos actores importantes no institucionales sino trabajando a nombre propio, este listado se centra en las organizaciones que los pueden agrupar o que se convierten en contratantes usuales de estos expertos. Tal elección obedece a que el aseguramiento en el mediano plazo del mantenimiento de compromisos, suele ser más efectivo entre instituciones pares que entre instituciones a personas.

- *Clusters* de tecnología.
- Empresas consultoras en las líneas temáticas del nodo.
- Empresas proveedoras de software y *appliances* para la gestión de vulnerabilidades, gestión de amenazas y tratamiento de riesgo.

5.1 ESTADO ACTUAL EN EL MUNDO

5.1.1 Conceptualización de Ciberseguridad

La ciberdelincuencia traspasa las fronteras nacionales, bajo el mismo comportamiento que presenta la transmisión de un virus. Es así como, “la ciberdelincuencia se ha globalizado considerablemente porque esos delitos pueden cometerse contra usuarios de Internet en cualquier lugar del mundo”⁸.

Las infraestructuras de telecomunicaciones, los servicios y actividades relacionadas, deben plantearse, concebirse, instalarse y administrarse en términos de la seguridad. La seguridad es fundamental en toda actividad y debe contemplarse como un servicio gestionable, que permite el crecimiento de la infraestructura de los sistemas, con impacto sobre la generación de valor añadido (cibergobierno, ciberseguridad, ciberenseñanza, etc.) con independencia de las tecnologías⁹. A continuación se presentan los factores sobre los cuales se componen las actividades en la ciberdelincuencia.

⁸UIT, Crear un mundo en línea más seguro, 2011.

⁹UIT, Informe Tendencias en las Reformas de las Telecomunicaciones 2011

Figura 22. Factores que componen las actividades en Ciberdelincuencia.



Fuente: UIT, Guía de Ciberseguridad para los Países en Desarrollo, 2007

La UIT define la ciberseguridad como el conjunto de actividades gestionables y necesarias para garantizar que la identidad virtual y la información digital de tipo confidencial propia del cliente, pueda ser salvaguardada en las mejores condiciones, permitiendo un acceso seguro a los medios virtuales. Para el caso de e-Government, se aplica esta conceptualización en interacciones propias del sistema con sus múltiples usuarios. (UIT, 2011)

Al interior de las políticas de carácter nacional, se encuentra definida la ciberseguridad en las iniciativas de Gobierno en Línea, como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (DNP, 2011) Y se reconoce a la ciberdefensa como la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional. (DNP, 2011)

5.1.2 Objetivo de la Ciberseguridad

El objetivo de la Ciberseguridad es contribuir en la preservación de las fuerzas y medios organizativos, humanos, financieros, tecnológicos y de información, con las que cuentan las instituciones, con la intención de alcanzar sus objetivos. (UIT, 2007)

La finalidad de la seguridad informática es garantizar que ningún perjuicio pueda poner en peligro la vida de la organización ni de la información cliente. Esto equivale a reducir la probabilidad de materialización de las amenazas, limitar los ataques y los problemas de funcionamiento inducidos y permitir la vuelta a la normalidad de funcionamiento tras un siniestro, a un coste aceptable y en un plazo razonable. (UIT, 2007)

En la siguiente figura se identifican las características de seguridad asociadas a la existencia y mantenimiento de los servicios ofrecidos en un sistema e-government.

Figura 23. Características para la existencia y mantenimiento de servicios en un sistema de E-Government.



Fuente: UIT, Guía de Ciberseguridad para los Países en Desarrollo, 2007

El proceso de la ciberseguridad es un proyecto de la sociedad en la medida en que todos los individuos están afectados por su realización. Su validez quedará reforzada si se desarrolla una ciber-ética de utilización y de comportamiento en relación con las tecnologías de la información y si existe una verdadera política de seguridad que estipule sus exigencias de seguridad frente a los usuarios, agentes, asociados y proveedores de seguridad de las nuevas tecnologías. (UIT, 2007)

En la sociedad actual, bajo la interconexión de diversos procesos de comunicación, se han venido incrementando ciberataques como irrupción al canal compartido, surgiendo a partir de éstos, elementos de delicada consideración, como la propiedad, uso y disposición de la información. Ejemplo de ello se encuentra en las grandes empresas de tecnología cuya seguridad se ha visto afectada con la intromisión de los ciberdelincuentes en el espacio virtual (Google, Sony, Lockheed Martin, PBS, Epsilon, Citibank, entre muchas otras ¹⁰).

Acciones como la publicación de información falsa en el sitio web de la PBS, el robo de nombres, números de cuenta y direcciones de correo electrónico de 200.000 clientes de Citibank, ha impulsado la ciberseguridad como medida implícita en todo sistema informático. (UIT, 2007)

¹⁰ Ibid. Pág. 42.



5.1.3 Globalización de la ciberdelincuencia

Como se enunció anteriormente, la ciberdelincuencia suele traspasar las fronteras nacionales, se transmite como un virus a través de una serie de países por ejemplo durante la transferencia de un correo electrónico del remitente al destinatario.

Como ha señalado el Informe de Tendencias en las reformas de las telecomunicaciones 2010–2011, *“la ciberdelincuencia se ha globalizado considerablemente porque esos delitos pueden cometerse contra usuarios de Internet en cualquier lugar del mundo. Un ciberdelincuente puede obligar a los organismos de aplicación de la ley a realizar una caza virtual alrededor del mundo mediante diversas técnicas capaces de enmascarar su identidad y hacer difícil el seguimiento de las comunicaciones”*¹¹.

Un caso particular de esta globalización se evidencia en el reconocimiento de la debilidad o inexistencia de los marcos jurídicos en materia de ciberdelincuencia; aun así, como ha sido citado por UIT en su artículo de *“Crear un Mundo en Línea más Seguro”*, incluso en países con legislaciones rígidas respecto de la ciberdelincuencia, la velocidad a la que se han venido produciendo los robos y los fraudes electrónicos ha sido creciente.

En el informe *“tendencias en las reformas de las telecomunicaciones 2010–2011”* se subraya que *“la ciberdelincuencia seguirá ofreciendo altas recompensas y reducidos riesgos a los delincuentes hasta que exista una legislación nacional efectiva y marcos internacionales capaces de investigar, enjuiciar y castigar los ciberdelitos”*¹².

La seguridad es un bloque básico de toda actividad y debe contemplarse como un servicio que permite crear otros servicios y generar valor añadido (cibergobierno, ciberseguridad, ciberenseñanza, etc.) con independencia de las tecnologías. (UIT, 2011)

El control del patrimonio digital de la información, la distribución de los bienes intangibles, la valorización de los contenidos y la reducción de la brecha digital, por ejemplo, son problemas de orden económico y social cuya resolución no puede limitarse exclusivamente a la dimensión tecnológica de la seguridad informática. (UIT, 2011)

Frente a la existencia de iniciativas en los gobiernos, especialmente por el vínculo gobierno – sociedad con la democratización de las tecnologías, se ha identificado la necesidad por preservar y defender los contenidos y canales de comunicación, ante la existencia de ciberdelitos asociados a los siguientes elementos:

¹¹ *Ibíd.* Pág. 42.

¹² *Ibíd.* Pág. 42.

Figura 24. Elementos relacionados en la Seguridad Informática a nivel de gobierno

Elementos relacionados a la Seguridad Informática a nivel gobierno.	Control del patrimonio digital de la Información
	Distribución de los Bienes intangibles
	Valorización de los contenidos
	Reducción de la Brecha Digital

Fuente: CINTEL (2011)

5.1.4 Implementación de la Ciberseguridad

El proceso de la ciberseguridad es un proyecto de la sociedad en la medida en que todos los individuos están afectados por su realización más aún en la seguridad asociada a los Sistemas de E-Government. Su validez quedará reforzada si se desarrolla una estrategia de implementación, utilización y gestión; basado en relación a las TIC. (UIT, 2007)

En todo sistema basado en la aplicación TIC, se ha encontrado que la existencia de una política de seguridad que estipule sus exigencias de seguridad frente a los usuarios, agentes, asociados, tipologías de la ciberdelincuencia y proveedores de seguridad de las nuevas tecnologías; se hace necesaria no solo en su implementación sino en su evaluación en el tiempo, ya que las tecnologías no son estables.

Los objetivos son móviles y los conocimientos de los delincuentes evolucionan como también lo hacen las amenazas y los riesgos. Esto hace que la vigencia de las soluciones de seguridad, y el retorno de la inversión en las mismas, no estén nunca garantizados. (UIT, 2007)

A continuación se muestran las capacidades características de un sistema de gobierno digital, asociadas a objetivos y medios de seguridad necesarios.

Tabla 5: Capacidades de un sistema de gobierno en línea, objetivos y medios de seguridad

CAPACIDADES DE UN SISTEMA DE GOBIERNO EN LÍNEA	OBJETIVOS	MEDIOS DE SEGURIDAD
UTILIZACIÓN	Disponibilidad	Dimensionamiento
	Perdurabilidad	Redundancia
	Continuidad	Procedimiento de exploración y generación de copias de seguridad
	Confianza	
EJECUCIÓN	Seguridad de funcionamiento	Concepción
	Fiabilidad	Prestaciones
	Perdurabilidad	Ergonomía



CAPACIDADES DE UN SISTEMA DE GOBIERNO EN LÍNEA	OBJETIVOS	MEDIOS DE SEGURIDAD
	Continuidad	Calidad de Servicio
	Exactitud	Mantenimiento operacional
PERMISIBILIDAD DE ACCESO	Confidenciabilidad	Control de Acceso
	Integridad	Autenticación
		Control de errores
		Control de coherencia
		Encriptación
EVIDENCIA	No rechazo	Certificación
	Autenticidad	Grabación y Rastreo
	Ninguna contestación	Firma electrónica
		Mecanismos de prueba

Fuente: (UIT, 2007)

Se ha reconocido en muchos casos sobre sistemas basados en aplicación TIC como estrategia de seguridad cuya la limitante principal, en cuanto a la adopción de medidas de reducción de riesgos para la información de valor de las organizaciones, es normalmente la aplicación de una única solución tecnológica.

Sin embargo, bajo la depreciación tecnológica y la evolución de los sistemas, el planteamiento de la seguridad debe contemplarse en todas sus dimensiones y satisfacer igualmente las necesidades de seguridad de los individuos, especialmente en lo que se refiere a la protección de su vida privada y al respeto de sus derechos fundamentales¹³, elementos de mayor importancia aún en sistemas de E-Government.

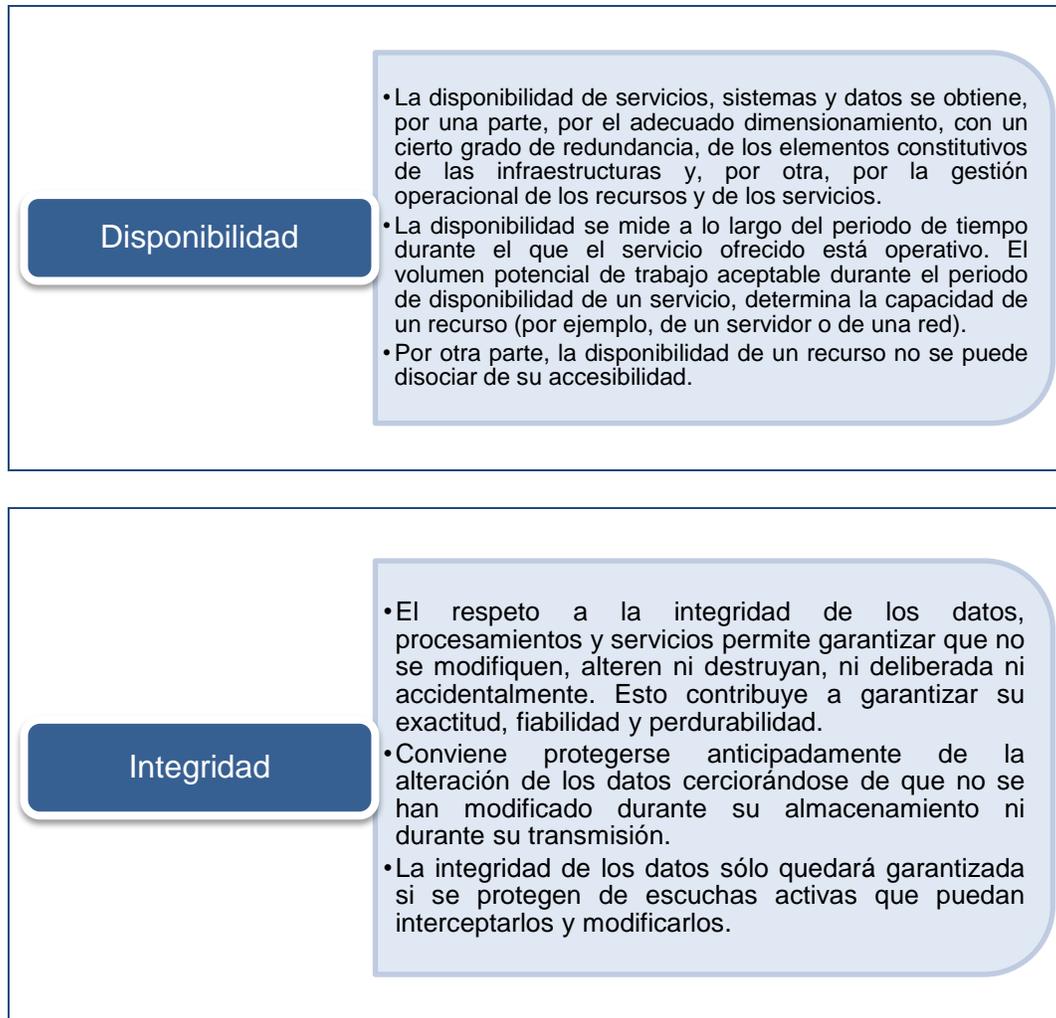
La Ciberseguridad debe estar disponible para todos y tener en cuenta la necesidad de protección de los datos de carácter personal. La identificación y gestión de los riesgos junto con la consideración del análisis de los riesgos vinculados a la informática, las telecomunicaciones y el ciberespacio, en un proceso de gestión de riesgos (*risk management*), inspira la estrategia de seguridad de las infraestructuras digitales como bien lo destaca UIT en su valoración de la seguridad en el ciberespacio.

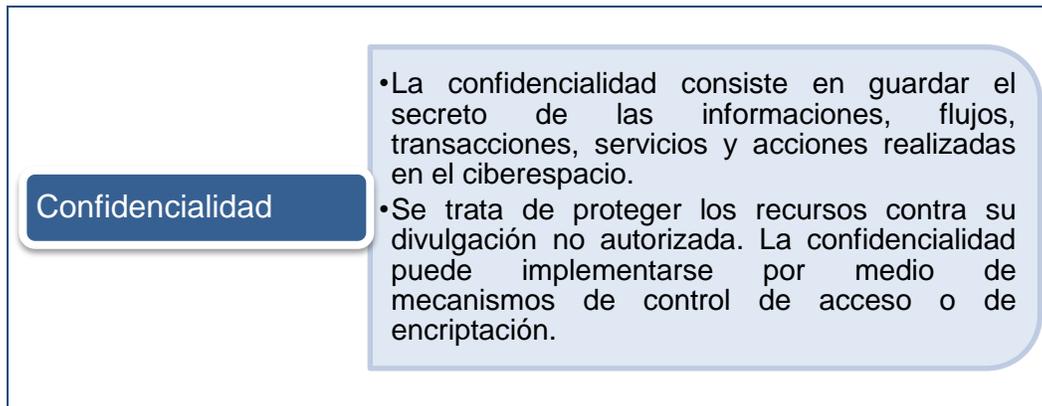
¹³ *Ibíd.* Pág. 42.

5.1.5 Fundamentos de la ciberseguridad

Las soluciones de seguridad deben contribuir a la satisfacción de los criterios básicos de la seguridad considerada planteada por UIT, estos tres criterios citados a continuación se añaden los que permiten demostrar la identidad de las entidades (concepto de autenticación) y las acciones o acontecimientos que han tenido lugar (conceptos de no rechazo, de imputabilidad y de rastreo).

Figura 25: Criterios básicos de seguridad en todo sistema.





Fuente: (UIT, 2007)

Según UIT esta protección puede realizarse por la implementación de los siguientes mecanismos de seguridad, centrados éstos en la gestión de integridad del sistema al cual se enfoca las iniciativas de protección:

Figura 26: Mecanismos de seguridad.



Fuente: (UIT, 2007)

5.1.6 Tecnologías

5.1.6.1 Tecnologías en la Ciberdelincuencia

A continuación se hace mención de las principales amenazas identificadas por Ministerio de Defensa de España en sus Cuadernos de Estrategia 149 nombrado como “*CIBERSEGURIDAD, RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO*” de año de 2010.

- **DDoS:** Los ataques DDoS (Distributed Denial of Service) son una forma relativamente sencilla y efectiva de bloquear el acceso a un recurso Web. Las acciones se pueden realizar de forma voluntaria siguiendo las instrucciones dadas para iniciar el ataque a una hora señalada en una convocatoria mediante foros en la Red o utilizando redes de ordenadores previamente infectados por virus (botnet) de forma que los usuarios ni siquiera son conscientes de que participan.
- **Botnets:** Las botnets (redes de robots) son redes de ordenadores zombis. se emplean para realizar ataques, envíos masivos de correo basura y espionaje contra empresas. Una botnet se crea infectando ordenadores sin que sus propietarios lo sepan.
- **Phishing:** Es la capacidad de duplicar una página web, con la intención de hacer creer al visitante su presencia en el sitio web original. Como principal elemento se destaca al engaño para la adquisición de información confidencial. (Segu-Info Seguridad de la Información, 2011)
- **Virus:** Es un programa de computador o conjunto de líneas de código que ataca al host de un programa dispuesto en otro ordenador. Una vez realizado esto se multiplica y realiza copias de si para infectar otros sistemas. No todos los virus son de carácter destructivo de programas o datos (University International Technology, 2011)
- **Worms:** Un “Gusano” es un programa que no necesita un host para multiplicarse, ya que se modifica el sistema operativo para convertirse en parte del boot process. A diferencia de la mayoría de virus los worms pueden desplegarse a través de redes de información. (University International Technology, 2011)
- **Trojan (trojan horse):** Un troyano es un programa de carácter malicioso que puede atacar resguardándose tras un programa legal. Este tipo de amenaza no se replica a sí mismo, pero puede llegar a activar o promover la presencia de otros virus. (University International Technology, 2011)
- **Ingeniería social:** Concerniente a la manipulación de formularios, llamadas no solicitadas, mensajes, entre otros.
- **Ataques multivectoriales:** Concerniente a la combinación de diferentes tipos de soporte como correo electrónico, mensajes en blogs, redes sociales, wikis, voz, vídeo, audio, etc.

Igualmente ISACA (como organización global independiente, sin ánimo de lucro, que participa en el desarrollo, adopción y utilización a lo largo del mundo, de conocimiento líder y prácticas en sistemas de información) ha reconocido en su interés por la generación de tecnologías y métodos para la seguridad de información en sistemas de TI, los siguientes elementos que conforman la tendencia en la consideración de vulnerabilidades:

Tabla 6: Tendencias de ataques
Incremento de profesionalismo y comercialización de actividades maliciosas
Incremento de las amenazas



Adaptación regional de la amenazas
Incremento en el número de etapas y/o niveles de los ataques
Los atacantes se dirigen a entidades de confianza
Convergencia de métodos de ataque
Migración de ataques por fama a los ataques por lucro.

Fuente: Fuente especificada no válida.

5.1.6.2 Tecnologías en la Ciberseguridad

- **Transmisión y Criptografía:** La encriptación de los datos (criptografía), contribuye a garantizar la confidencialidad de las informaciones durante su transmisión o almacenamiento, transformándolos de modo que resulten ininteligibles para las personas que no dispongan de los medios de descryptación adecuados. (UIT, 2007)
- **Identificación y Autenticación:** La autenticación debe permitir disipar cualquier duda sobre la identidad de un recurso. Esto supone la correcta identificación de todas las entidades (recursos materiales, programas informáticos y personas) y la posibilidad de que determinadas características sirvan de prueba para su identificación. Es necesario que todos los mecanismos de control de acceso lógico a los recursos informáticos efectúen la identificación y autenticación de las entidades. (UIT, 2007)
- Los procesos de identificación y autenticación tienen por objeto contribuir a:
 - **La confidencialidad e integridad de los datos:** sólo los agentes autenticados y autorizados pueden acceder a los recursos (control de acceso) y modificarlos si están habilitados para ello.
 - **El no rechazo y la imputabilidad:** es posible mantener un registro de que ciertas entidades identificadas y autenticadas han realizado determinada acción, la prueba de origen de un mensaje o de una transacción y la prueba de que cierta entidad identificada y autenticada es la destinataria de determinado mensaje.

El No rechazo se refiere a que el establecimiento de la responsabilidad exige la existencia de mecanismos de autenticación de los individuos y de imputabilidad de sus acciones. Es especialmente importante poder registrar la información a fin de «rastrear» la ejecución de acciones, cuando se trata de reconstruir un histórico de los acontecimientos, especialmente cuando se trata de investigaciones en medios informáticos para recuperar eventualmente, por ejemplo, la dirección del sistema desde el que se han enviado datos. (UIT, 2007)

Para ello se debe guardar (registro por diario) la información necesaria para un análisis posterior que permita realizar la auditoría de un sistema, bajo estas características se fundamenta la capacidad de un sistema para ser auditado (concepto de auditabilidad).

5.1.7 Modelo Ejemplo Republica De Corea del Sur

La ciberseguridad en el sistema de información en la República de Corea del Sur, se centra en la existencia del MIC – Ministerio de la Información y la Comunicación¹⁴. En este estamento se ve conformado por tres aspectos referidos a continuación (Heung Heung-Youl Youm Youm, 2007):

1. Actividades de promoción de las redes de información y comunicación: Se establece para la promoción de las redes de información y comunicación, así como de la protección asociada. Para estas actividades hacen uso y proveen entornos de forma segura. Además de promover en este aspecto la protección a usuarios, protección de redes y sanciones.
2. Actividades asociadas a la firma digital: provee los aspectos fundamentales para el uso digital de firmas para el incremento de la seguridad y confianza en los documentos electrónicos. De igual forma dimensiona la certificación de claves públicas y políticas de certificación electrónica, así como las autoridades frente al otorgamiento de licencias y certificados.
3. Actividades críticas en la protección de la infraestructura: contiene las actividades básicas para la protección de la infraestructura ante los ciberataques. En este conjunto de actividades se encuentran la identificación de las infraestructuras críticas, cuantificación y respuesta de incidentes, información compartida y responsables, compañías de consultoría en la seguridad sobre la información y las sanciones y responsabilidades legales.

5.1.7.1 Centro Coreano de Seguridad de Internet - Corea Internet Security Center (KISC)

Conocido como Kr-CERT/CC a nivel mundial, se establece como un departamento de KISA (Korea Information Security Agency) en diciembre de 2003; como resultado de un ciberataque masivo en el mismo año. Dentro de las actividades que desarrolla el KISC están la prevención contra ataques y todo tipo de daños a través de la red de internet de Corea del Sur, a través del análisis de información con diversos sensores en el ISP, industrias de antivirus, industrias de TI, entre otras. (Heung Heung-Youl Youm Youm, 2007)

Características de KISC

Dentro de las características que se han identificado se destacan: (Heung Heung-Youl Youm Youm, 2007)

- Identificación y Análisis de incidentes sobre la información a nivel doméstico e internacional en tiempo real.
- Actividades de monitoreo 24/7
- Respuesta a casos de emergencia

El KISK brinda información de los siguientes aspectos: (Heung Heung-Youl Youm Youm, 2007)

¹⁴ Desde la desintegración del Ministerio de Información y Comunicaciones de Corea el 2 de febrero de 2008; las funciones y programas de este referentes a Ciberseguridad fueron transferidos a la Comisión de Comunicaciones (KCC) y al KrCERT/CC.

Fuente: <http://www.itu.int/ITU-D/cyb/events/2009/hyderabad/docs/park-korean-cybersecurity-framework-sept-09.pdf>



- Los datos de mayor tráfico nacional ISP por puertos, protocolos y ataques.
- Información del estado de los servidores Web más importantes en el sector privado.
- Información sobre las estadísticas de consulta observada en la raíz DNS.
- Seguridad de las tendencias relacionadas con Anti-Virus, sistemas, software, y Compañías de Seguridad.
- Vulnerabilidades de seguridad recogidas y analizadas del honnypot establecido por KISA.
- Notificar a la empresa u organización víctima de los hechos cometidos.
- Generar y difundir una alerta de Hacking / Virus / advertencia.
- Solicitud de Análisis e Investigación de Incidentes.

De esta forma el Sistema KISC en Corea se fundamenta en la visión y priorización de políticas, la promoción de estrategias de I+D y el desarrollo tecnológico, el fortalecimiento de la competitividad a nivel mundial de las industrias coreanas y en la mejora en el sistema de regulación y legal. (Heung Heung-Youl Youm Youm, 2007)

5.1.7.2 Áreas y principios del KISC

A continuación se identifican las áreas sobre las cuales se ha estructurado la participación del Sistema KISC.

Figura 27: Áreas y principios del KISC.



Fuente: (Heung Heung-Youl Youm Youm, 2007)

5.1.8 Roadmap de las iniciativas en ciberseguridad en los Estados Unidos

La labor de Estados Unidos en la identificación de la evolución tecnológica asociada a la ciberseguridad se fundamenta en el reconocimiento de 11 problemas de alto impacto, estos son: (Homeland Security , 2009)

1. **Scalable trustworthy systems – Escalabilidad de Sistemas Confiables (Incluyendo arquitecturas y requisitos en las metodologías de desarrollo):** Este factor representa todas las amenazas a los sistemas en operación incluyendo todo aquello que puede evitar el funcionamiento de las aplicaciones críticas bajo el cumplimiento de sus requisitos, incluyendo el mal uso, malware, otras versiones, fallas de software, malfuncionamiento, errores humanos, daño físico e interrupciones en el entorno.
2. **Enterprise-level metrics – Métricas a nivel organizacional:** Este elemento de estudio está centrado en el desarrollo de métricas que permitan el entendimiento de los siguientes conceptos:

Tabla 7: Conceptos asociados al elemento de medición de nivel empresarial de ciberseguridad.

Seguridad en la organización
Antecedentes de la seguridad nacional
Nivel de confianza y respuesta a los retos de amenazas y tecnologías.
Seguridad en productos o software
Como interactúa el sistema o el producto con otros sistemas o redes
Fortalezas del sistema de seguridad en la respuesta a las amenazas

Fuente: (Homeland Security , 2009)

3. **System evaluation life cycle – Ciclo de vida de la evaluación de los sistemas (incluyendo las aproximaciones para una garantía de amplia cobertura):** Este elemento se encuentra ligado a la evaluación de seguridad integrada en el ciclo de vida del desarrollo de sistemas de información.
4. **Ataque por amenazas internas:** La gestión sobre la ciberseguridad se ha enfocado, en este caso, sobre las amenazas que se gestan al interior de las organizaciones, donde la experiencia ha demostrado la importancia en la identificación y tratamiento de amenazas relacionadas, por ejemplo, con *insiders* o ingeniería social
5. **Ataques en función de malware y botnets:** Este elemento se centra en el reconocimiento de los siguientes aspectos:
 - Alojamiento de malware al interior de una plataforma.
 - Detección de malware que ha sido instalado.
 - Limitar el daño que pudiera realizar el malware una vez instalado en una plataforma.
 - Operación efectiva y eficiente ante la presencia de malware
 - Determinar el nivel de riesgo a través de indicadores de detección malware.
 - Remoción de malware una vez haya sido instalado, así como el monitoreo e identificación de la fuente.
 - Inclusión de Honeypots como elemento tecnológico reconocible.



6. **Global-scale identity management – Gestión global de identidad:** Elemento enfocado directamente sobre las actividades comerciales y de gobierno de todo tipo de organizaciones que establecen lazos inter-organizacionales que actualmente son obstaculizados por la falta de credenciales de confianza para el acceso recursos.
7. **Supervivencia de los sistemas de misión crítica:** Este elemento se encuentra relacionado con la ausencia de requerimientos claros, de carácter fundamental, frente a la supervivencia de la seguridad informática y la adhesión de los sistemas a estos requerimientos.
8. **Entendimiento del entorno y de las atribuciones de los ciberataques:** Este elemento se centra en la búsqueda de soluciones en:
 - Valoración de amenazas.
 - Identificación de ataques.
 - Fuentes y atribución de los ataques.
 - Objetivos y comportamientos del ataque.
 - Impacto esperado del ataque.
 - Actividades de defensa.
 - Infraestructura de defensa.
 - Mitigación de ataques y posibles amenazas.
9. **Procedencia de información, sistemas y hardware:** Este elemento hace referencia a la cadena de la custodia que ejercen de manera consecutiva hardware, software, documentos, bases de datos, entre otros. (Homeland Security , 2009)
10. **Privacidad – Seguridad:** Reconocimiento de los siguientes aspectos sobre los cuales se centra la necesidad de la seguridad de la privacidad de la información.
 - Información de carácter personal.
 - Protección de la identidad en menores de edad sobre la web, protección de testigos y anonimato.
 - Límites en la divulgación de la información.
 - Gestión de la identidad.
 - Control de acceso múltiple.
11. **Usabilidad en la seguridad:** La usabilidad en la seguridad tiene como principio involucrar al diversos actores reconocidos dentro de los cuales se destacan los que se ven en la siguiente tabla.

Tabla 8: Usuarios reconocidos en la usabilidad de los elementos de seguridad por parte del Homeland Security para la proyección de las actividades en seguridad de la información en estados Unidos.

Usuarios no técnicos	- Terminologías y tecnologías no familiarizadas - Riesgos no claros en la seguridad
Usuarios ocasionales	- Transformación de todo el entorno de la seguridad - Gestión de la seguridad tratada de forma diferida
Usuarios frecuentes y expertos	- Restricción sobre los controles de seguridad para los usuarios no técnicos que pudieran obstruir los diálogos pop-up

Usuarios con necesidades especiales	- Sistema básico de la seguridad frente a un conjunto de usuarios similares pero con la adición de retos e interfaces en base a necesidades.
Sistema para los administradores:	- Configuración y mantenimiento de los sistemas que son transversales para diferentes usuarios envolviendo amenazas y políticas
Sistema de diseñadores:	- Fallas de seguridad y usabilidad mitigables a través de la educación y el entrenamiento
Sistemas de desarrolladores:	- Complejidad en la adición d seguridad y usabilidad de requerimiento en los procesos de desarrollo
Políticas de mercado:	- Dificultar en la captura y expresión de requerimiento de seguridad en vinculo con las líneas de trabajo organizacional

Fuente: (Homeland Security , 2009)

Para la proyección planteada por los Estados Unidos se ha reconocido a través del Departamento de Seguridad Interna como de vital importancia los elementos 1, 2, 4, 6, 7, 8, 9 y 10, numerados anteriormente. Mientras los elementos 3, 5 y 11, son la representación de la adición de áreas importantes como parte de la construcción futura.

Así mismo la estructura que estos elementos constituyentes se pueden estructurar de la siguiente manera: (Homeland Security , 2009)

- **Elementos 1 – 3:** Problemas generales.
- **Elementos 4 – 5:** Necesidades y amenazas de mayor consideración
- **Elementos 6 – 10:** Cualidades y conceptos del sistema que son requeridos para la implementación de los anteriores elementos.

5.2 ESTADO ACTUAL EN COLOMBIA

El Programa de Gobierno en línea fundamenta sus funciones en tres aspectos frente a la seguridad de la información, estos son: (Ministerio de Comunicaciones - República de Colombia, 2008)

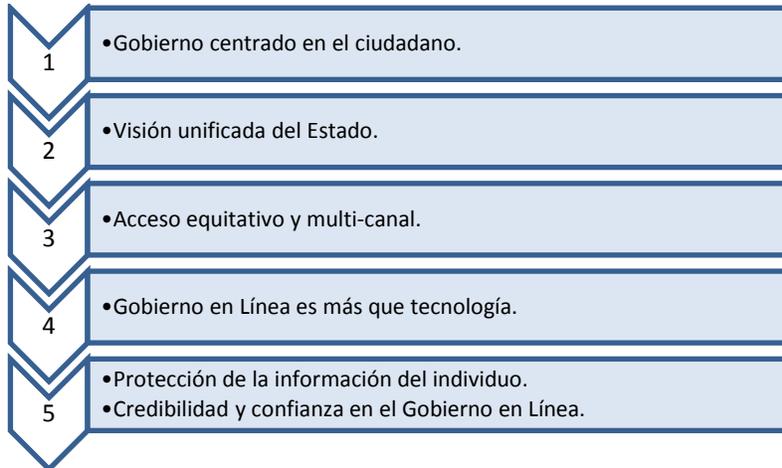
Figura 28 Aspectos de la seguridad en el GEL.



Fuente: (Ministerio de Comunicaciones - República de Colombia, 2008)

Así mismo se identifican los siguientes principios como básicos en la estrategia de Gobierno en línea de Colombia.

Figura 29 Principios básicos en el GEL.



Fuente: (Ministerio de Comunicaciones - República de Colombia, 2008)

En los ejes de acción sobre los cuales se fundamenta el Programa GEL se reconocen tres conceptos generales: los servicios, la transparencia y la eficiencia. Como se pueden ver a continuación: (es importante entender que el Gobierno nacional ha identificado estos ejes como principales en las iniciativas de gobierno en línea a nivel mundial, razón por la cual se decidió fundamentar la iniciativa GEL de Colombia sobre cada uno de éstos) (Ministerio de Comunicaciones - República de Colombia, 2008)

Figura 30 Ejes de acción GEL.



Fuente: (Ministerio de Comunicaciones - República de Colombia, 2008)

Para la respuesta eficiente en base a estos tres principios se ha estructurado como iniciativa presente la conformación del ColCERT, cuya planeación ha estado enfocada para los próximos años y se fundamenta en la construcción del entorno por una Comisión Intersectorial encargada de fijar la visión estratégica de la gestión de la información, así como de establecer los lineamientos de política respecto de la gestión de la infraestructura tecnológica (hardware, software y comunicaciones), información pública y ciberseguridad y ciberdefensa. (DNP, 2011)

Esta Comisión estaría encabezada por el Presidente de la República e integrada como mínimo por el Alto Asesor para la Seguridad Nacional, el Ministro de Defensa Nacional, el Ministro de Tecnologías de Información y Comunicaciones, el Director del Departamento Administrativo de Seguridad – DAS o quien haga sus veces, el Director de Planeación Nacional y el Coordinador del ColCERT. (DNP, 2011)

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT será el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa. Prestará su apoyo y colaboración a las demás instancias nacionales tales como el Centro Cibernético Policial - CCP y el Comando Conjunto Cibernético - CCOC. (DNP, 2011)

El Centro Cibernético Policial - CCP. Estará encargado de la ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos. Desarrollará labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país, informando en su página web sobre vulnerabilidades cibernéticas. Recibirá y atenderá los lineamientos nacionales en ciberseguridad y trabajará de forma coordinada con el ColCERT. (DNP, 2011)

Figura 31: Modelo de coordinación.



Fuente: Ministerio de Defensa Nacional 2011, tomado de Conpes 3701 de 2011

Objetivos de CoCIRT

- Coordinar con la comisión intersectorial el desarrollo y promoción de políticas, procedimientos, recomendaciones, protocolos y guías de ciberseguridad y ciberdefensa, en conjunto con los agentes correspondientes y velar por su implementación y cumplimiento.
- Promover el desarrollo de capacidades locales/sectoriales así como la creación de CSIRTs sectoriales para la gestión operativa de los incidentes de ciberseguridad en la infraestructura crítica nacional, el sector privado y la sociedad civil.
- Coordinar y asesorar a CSIRTs y entidades tanto del nivel público, privado y de la sociedad civil en la respuesta a incidentes informáticos.
- Ofrecer servicios de prevención ante amenazas informáticas, respuesta frente a incidentes informáticos, así como aquellos de información, sensibilización y formación en materia de seguridad informática a todas las entidades que así lo requieran.
- Coordinar la ejecución de políticas e iniciativas público-privadas de sensibilización y formación de talento humano especializado, relativas a la ciberseguridad y ciberdefensa.
- Apoyar a los organismos de seguridad e investigación del Estado en la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones.

- Fomentar un sistema de gestión de conocimiento relativo a la ciberseguridad y ciberdefensa, orientado a la mejora de los servicios prestados por el CoICERT.
- Proveer al CCP y al CCOC la información de inteligencia informática que sea requerida.
- Actuar como punto de contacto internacional con sus homólogos en otros países, así como con organismos internacionales involucrados en esta temática.

A continuación se presenta un diagrama que evidencia las interacciones que plantea la existencia de CoICERT.

Figura 32: Modelo Relacional CoICERT



Fuente: DNP 2011.

En la actual aplicación del sistema E- Government de Colombia: “Gobierno en Línea”, se han contemplado diversos lineamientos asociados a las siguientes reglamentaciones y normas de carácter internacional, no necesariamente aplicadas pero sí, comparables en el ejercicio de su implementación. Es importante aclarar que estas normas y estándares internacionales hacen parte de las iniciativas en la protección de los sistemas de información más populares a nivel mundial.

1. Normas de gestión de seguridad:

- ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems – Requirements. La norma equivalente en Colombia es la NTC ISO/ IEC 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI) Requisitos.



- ISM3 v2.00 Information Security Management Maturity Model. Fue desarrollada por el ISM3 Consortium. La versión 2.00 está vigente a partir del 2007. La nueva versión (2.10) sólo está disponible actualmente en forma impresa.
2. Mejores prácticas para Seguridad de Información:
 - ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management. La norma equivalente en Colombia es la NTC-ISO/IEC 17799 Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la gestión de la Seguridad de la Información, la cual corresponde a una traducción idéntica de la ISO/IEC 17799:2005.
 - The Standard of Good Practice for Information Security 2007. Ha sido desarrollada por el Information Security Forum, ISF. La versión disponible actualmente corresponde al año 2007.
 - NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems. Esta guía fue desarrollada por el National Institute of Standards and Technology, NIST y la fecha de su publicación corresponde a septiembre de 2006.
 3. Mejores prácticas de Gobierno y Control en Tecnología de Información:
 - Cobit 4.1 Control Objectives for Information and related Technology (COBIT®).
 - IT Control Objectives for Sarbanes Oxley
 - CONCT- Control Objectives for Net Centric Technologies.
 - NIST SP 800 – 53 Recommended Security Controls for Federal Information Systems
 4. Mejores prácticas para la prestación de servicios de TI:
 - Service Management - ITIL® Versión 3. Conjunto de mejores prácticas para la prestación del servicio de TI. Desarrollado por La Oficina de Gobierno de Comercio del Reino Unido.
 - ISO/IEC 20000-1:2005 Information technology -- Service management -- Part 1: Specification
 - ISO/IEC 20000-2:2005 Information technology -- Service management -- Part 2: Code of practice
 5. Normas de Administración de Riesgos:
 - AS/NZ 4360:2004 Risk Management, Standards Australia/Standards New Zealand.
 - ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management.
 - NIST SP 800-30 Risk Management Guide for Information Technology Systems.
 6. Metodologías de Administración de Riesgos:
 - MAGERIT
 - Octave
 - General Security Risk Assessment Guidelines, ASIS International.
 7. Normas para planeación de continuidad del negocio:
 - BS 25999-1:2006 Gestión de Continuidad de Negocio. Parte 1: Códigos de Práctica.
 - BS 25999-2:2007 Especificaciones para la continuidad del negocio.
 - NFPA 1600:2007 Standard on Disaster/Emergency Management and Business Continuity Program
 - ISO/IEC 24762:2008 Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services
 - NIST SP 800 – 34 Contingency Planning Guide For Information Technology Systems
 - GTC 176 Sistema de Planeación de Continuidad del Negocio

El Programa GEL, en Colombia, ha determinado varios criterios de selección de Estándares de Seguridad de la Información. Tomando en cuenta su propósito primario, el grado de reconocimiento a nivel mundial y la alineación con la estrategia de Gobierno en Línea.

A nivel nacional se estableció por parte del Ministerio TIC, con su Área de Investigación Y Planeación en el año 2008, los siguientes lineamientos como principales, debido al propósito y principios intrínsecos, que se alinean con la estrategia de Gobierno en Línea de manera general:

- NTC ISO/IEC 27001:2005
- ISM3 v 2.00
- The Standard of Good Practice for Information Security - ISF-SOGP
- COBIT 4.1
- ITIL v 3
- AS/NZ 4360 Risk Management

5.2.1 Antecedentes en Colombia

A continuación se presentan cuatro de las iniciativas de protección el ciberespacio con las cuales cuenta el Estado Colombiano; estas acciones han servido de soporte en la evolución por la ciberseguridad, cuyas funciones están actualmente están estructuradas en el ColCERT.

5.2.1.1 SANSI

El Sistema Administrativo de Seguridad de la Información (SANSI), junto con la conformación de la Comisión de Seguridad de la Información para Gobierno en línea¹⁵ son parte de la estructuración de un modelo de seguridad de la información para las entidades del Estado enfocado en la toma de decisiones estratégicas en torno a la ciberseguridad nacional, en el cual se llaman a participar el Departamento Nacional de Planeación, el Ministerio de Interior y de Justicia, el Ministerio de Relaciones Exteriores, el Ministerio de Defensa Nacional, el Ministerio TIC y el Departamento Administrativo de Seguridad, o quien haga sus veces. (DNP, 2011)

Parte de las iniciativas en la protección y defensa del ciberespacio se ha centrado en la definición de los lineamientos que permitan la implementación, seguimiento y mantenimiento del Modelo de Seguridad de la Información en cada una de las entidades públicas de orden nacional y territorial y en las entidades privadas que sean proveedoras de los servicios de Gobierno en línea¹⁶; así como en la actualidad con la conformación del ColCERT como organismo coordinador en los aspectos de ciberseguridad y ciberdefensa, en conjunto con el Centro Cibernético Policial (CCP) y el Comando Conjunto Cibernético (CCOC). (DNP, 2011)

¹⁵ Ministerio de Comunicaciones – República de Colombia, 2008.

¹⁶ OpCit.

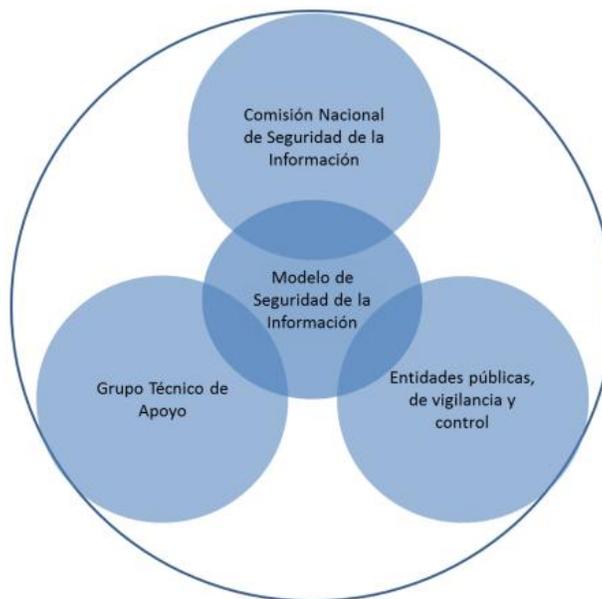


El SANSI es un sistema que se compone por la Comisión Nacional de Seguridad de la Información, Grupo Técnico de Apoyo y Entidades Públicas de Vigilancia Y Control, como se muestra a continuación: (DNP, 2011)

El SANSI busca coordinar las actividades relacionadas con la formulación, Ejecución, seguimiento y mantenimiento de las políticas y lineamientos necesarios para fortalecer la adecuada gestión de la seguridad de la información a nivel nacional; asesorado por la Comisión de Seguridad de la Información para Gobierno en línea (CSI) en temas relacionados con la seguridad de la información del país y de sus territorios, con el fin de generar credibilidad y confianza protegiendo la información de las entidades y de los ciudadanos.

A su vez, la Comisión de Seguridad de la Información para Gobierno en línea, es asesorada por el Grupo Técnico de Apoyo, cuya función principal es acotar, dentro de los parámetros establecidos en las normas pertinentes, el Modelo de Seguridad de la información a nivel táctico y técnico especificando las políticas, objetivos de control y controles propuestos para que sean implementados por cada una de las entidades objetivo. El Grupo Técnico de Apoyo somete a consideración de la Comisión, la aprobación del Modelo de Seguridad de la Información y sus ajustes posteriores.

Figura 33: Sistema Administrativo de Seguridad de la Información SASI.

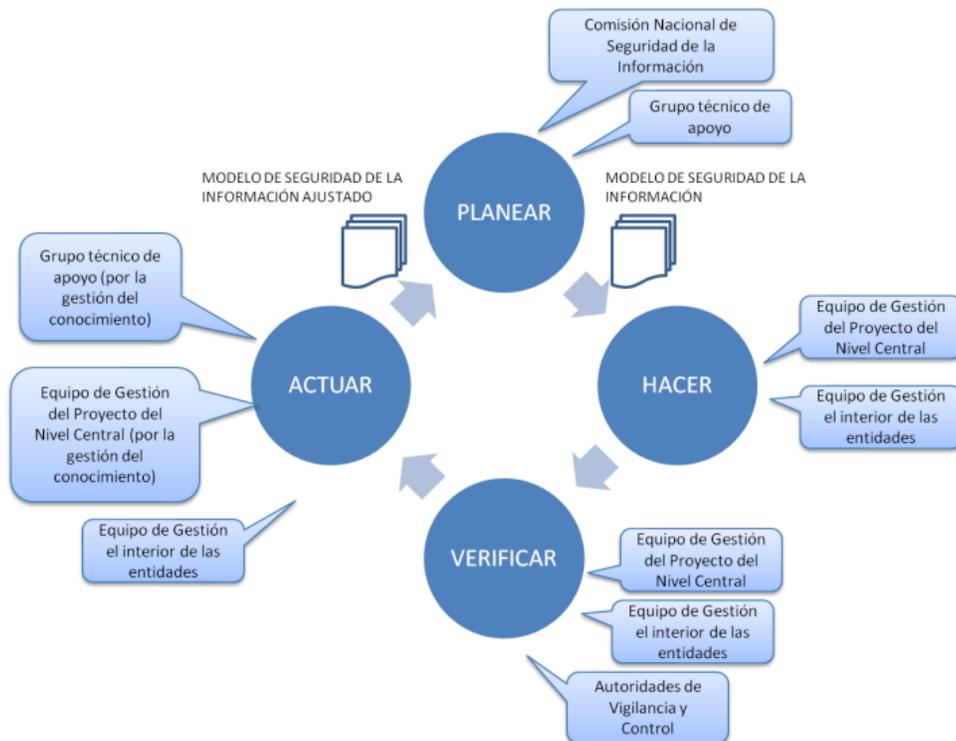


Fuente: (DNP, 2011)

Al interior de cada una de las entidades existe un equipo de gestión del proyecto que se encarga de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el Modelo de Seguridad de la Información al interior de su entidad, así como planear las actividades necesarias para una adecuada administración y sostenibilidad del mismo.

El comportamiento del SANSI y su respectiva gestión se fundamenta en la realización de las siguientes actividades:

Figura 34: Ciclo PHVA asociado al SANSI.



Fuente: (Fondo de Tecnologías de la Inforamción y las Comunicaciones, 2010)

5.2.1.2 CIRTISI – Colombia (Centro de Información y Respuesta Técnica a Incidentes de Seguridad Informática de Colombia)

En colaboración de varias entidades gubernamentales se desarrolló una primera propuesta para la constitución de un Centro de Información y Respuesta Técnica a Incidentes de Seguridad Informática de Colombia – CIRTISI.

Según esta propuesta, CIRTISI Colombia buscaría propender por la prevención, detección y reacción frente a incidentes de seguridad informática que amenacen y/o desestabilicen la normal operación de entidades gubernamentales e incluso la seguridad nacional, mediante apoyo tecnológico, entrenamiento y generación de una cultura global de manejo de la información. (Fondo de Tecnologías de la Inforamción y las Comunicaciones, 2010)

Sus objetivos generales habían sido:



- Brindar apoyo a las entidades gubernamentales para la prevención y rápida detección, identificación, manejo y recuperación frente a amenazas a la seguridad informática.
- Interactuar con los entes de policía judicial generando un espacio de consulta frente a las amenazas de seguridad e investigaciones informáticas.
- Proporcionar información especializada y conocimiento a las autoridades de policía judicial durante los procesos investigativos relacionados con la seguridad informática.
- Construir un laboratorio de detección e identificación, control y erradicación de amenazas informáticas para los diferentes organismos gubernamentales.
- Consolidar el capítulo HTCIA (High Technology Crime Investigation Association) Colombia y adelantar las actividades necesarias para su permanencia y crecimiento

Sus objetivos específicos habían sido:

- Proporcionar alertas tempranas frente a amenazas informáticas que puedan desestabilizar la tecnología y la seguridad nacional.
- Fomentar la investigación y desarrollo de estrategias de seguridad informática.
- Brindar una adecuada respuesta a incidentes de seguridad informática, con un enfoque metodológico que propenda por la eficiencia de las investigaciones realizadas.
- Establecer canales de comunicación nacionales expeditos de manera que sea posible ofrecer una atención a incidentes en forma efectiva.
- Generar redes de apoyo temáticas en materia de seguridad de la información.
- Promover la coordinación nacional con otras entidades pertinentes del orden regional
- Fortalecer la cooperación con organismos intergubernamentales en el ámbito subregional, regional e internacional.
- Impulsar la cooperación internacional con organismos de similar naturaleza y propósito.
- Participar en el Forum of Incident Response and Security Teams (FIRST)
- Consolidar, mantener y liderar el capítulo HTCIA Colombia
- Fomentar una conciencia global de seguridad informática
- Proveer un servicio especializado de asesoramiento en seguridad de redes.

Servicios Ofrecidos

- Investigación técnica de amenazas informáticas existentes e identificación de tendencias.
- Generación de alertas tempranas frente a las amenazas existentes, conocidas y potenciales.
- Entrenamiento local, nacional o internacional en materia de seguridad informática y procedimientos de computación forense para los organismos de policía judicial colombiana.
- Respuesta efectiva a incidentes de seguridad informática que se presenten en cualquier órgano gubernamental, brindando apoyo técnico para la recolección, análisis, preservación y presentación de evidencia digital en incidentes que den lugar a investigaciones informáticas.
- Promover la cultura de la seguridad informática y la estandarización de protocolos de seguridad.
- Establecer contactos con equipos de similar naturaleza o propósito y con organizaciones que agrupen estos equipos, tanto a nivel nacional como internacional.

El CIRTISI - Colombia propone desarrollar sus actividades dentro de los siguientes ejes estratégicos:

Tabla 9: Ejes estratégicos.

EJES ESTRATÉGICOS		
<p>Desarrollo de Políticas: Promover la formulación de políticas que contribuyan con la prevención, detección, identificación, manejo y recuperación frente a amenazas a la seguridad informática así como con la adopción de legislación para adecuar y actualizar la tipificación de las conductas conocidas por el CIRTISI.</p>	<p>Actividad Operacional: Obtener diagnósticos reales sobre las diferentes amenazas informáticas que se generan a partir de una cobertura de servicios y sectores definida y, de la permanente capacitación y optimización tecnológica.</p>	<p>Impacto Social: Generación de una cultura global de manejo de la información y fomento de la conciencia frente a la seguridad informática mediante la permanente socialización de las amenazas conocidas y nuevas y su impacto sobre la seguridad informática en Colombia.</p>

Fuente: (Ministerio de Comunicaciones - República de Colombia, 2008)

Frente a la estructura de CIRTISI se ven involucradas cinco áreas con liderazgo propio de manera que se puedan cubrir diversos aspectos de la seguridad informática nacional, como se puede identificar en el documento del Área de Investigación Y Planeación de Gobierno en Línea, titulado: Modelo de Seguridad de la Información para la Estrategia del Gobierno en línea del 2008.

1. **División de Infraestructura y Asesoría:** Encargada de todo el planeamiento logístico y estratégico necesario para la conformación y puesta en operación del CIRTISI - Colombia, apoyando directamente a la dirección general y junta directiva que se designe.
2. **División de Alertas Tempranas y Coordinación:** Encargada del monitoreo de amenazas y coordinación con CERT nacionales e internacionales, generando las alertas tempranas frente a amenazas potenciales. Además de mantener una base estadística de amenazas a la seguridad de la información.
3. **División de Investigación y Desarrollo:** Encargada del laboratorio de amenazas, proporcionadas por la división de alertas tempranas, con el fin de identificar riesgos efectivos. Generando además una base estadística de amenazas convirtiéndolas en riesgos y generando las alertas acerca de aquellos riesgos que podrían impactar de mayor manera la seguridad nacional.

Además esta división se encuentra ligada a todo lo relacionado con capacitación y entrenamiento tanto al interior del CIRTISI como hacia los diferentes entes del Gobierno.

4. **División de Respuesta a Incidentes:** Es la encargada de reaccionar ante cualquier incidente de seguridad de la información que se presente en el sector Gobierno. Esta división estará a cargo de los mecanismos de comunicación únicos nacionales que atenderían y manejarían los requerimientos de incidentes. Adicionalmente, los funcionarios de esta división podrán interactuar con las entidades con funciones de policía judicial en el desarrollo de investigaciones informáticas



ofreciendo apoyo técnico y especializado. Asimismo, el CIRTISI pondría a disposición de dichas entidades las estadísticas sobre investigaciones informáticas a nivel nacional.

5. **División de Divulgación y Concienciación:** Área encargada de proporcionar la información oficial que se derive de las actividades del CIRTISI hacia los medios de comunicación y la comunidad en general. Además de promover la generación de conciencia en el adecuado manejo de la seguridad de la información.

Las entidades involucradas en su constitución se muestran en la figura 35.

Figura 35: Entidades involucradas en CIRTISI.



Fuente: (Ministerio de Comunicaciones - República de Colombia, 2008)

5.2.1.3 COL-CSIRT

Un ejemplo de asociación en el desarrollo de entornos de seguridad de la información se encuentra representado por el COL-CSIRT, siendo este un grupo de investigación de la Universidad Distrital Francisco José de Caldas que pretende un marco de operación nacional y cuyo constituyente estará dado por entidades de educación superior y entidades oficiales del estado.

Cuyo principal objetivo es ofrecer un servicio de soporte a las entidades estatales y de educación superior, para la prevención, detección y corrección de los incidentes de seguridad informáticos, con los siguientes objetivos específicos:

- Desarrollar una Base de Datos que contenga la información concerniente a los diferentes incidentes de seguridad informáticos existentes y las preguntas más frecuentemente contestadas (FAQ).
- Prestar el soporte sobre Sistemas Operativos Windows y Linux (Unix).
- Utilizar la clasificación taxonómica de los incidentes y ataques con código malicioso propuesta en el proyecto de maestría en Teleinformática titulado "ANÁLISIS DE INCIDENTES RECIENTES DE SEGURIDAD EN INTERNET 1995 a 2003" para ofrecer una respuesta oportuna, eficaz y eficiente a los distintos reportes y alertas que se reciban diariamente en el centro de respuesta.
- Establecer detalladamente los servicios que prestará el centro de respuesta con respecto a los incidentes de seguridad informáticos.
- Integrar la base de datos del Centro de Respuesta a incidentes y ataques con código malicioso, al portal WEB del COL-CSIRT que está siendo desarrollado por el grupo de investigación ARQUISOFT de la Universidad Distrital Francisco José de Caldas.

5.2.1.4 Comité Interamericano contra el terrorismo de la OEA (CICTE)

A través del taller para practicantes en materia de seguridad cibernética del CICTE sobre la estrategia integral de seguridad cibernética de la OEA, en el 2004 se estableció un marco para una Red Interamericana de CSIRT para vigilancia y alerta.

El objetivo principal del CICTE era la creación de una red hemisférica de puntos nacionales de contacto entre equipos de respuesta a incidentes de seguridad en computadoras (Computer Security Incident Response Teams: CSIRT) con responsabilidad nacional (CSIRT nacionales), en los Estados Miembros de la OEA, con el mandato y la capacidad de responder debida y rápidamente a las crisis, incidentes y peligros relacionados con la seguridad cibernética.

Estos equipos podrían comenzar simplemente como puntos de contacto oficiales en cada uno de los Estados y estarían a cargo de recibir información sobre seguridad cibernética. En el futuro se convertirían en un CSIRT.

En complemento a ello, en mayo de 2008 se llevó a cabo en la ciudad de Bogotá una capacitación en "Fundamentos para creación y manejo de un CSIRT" organizada por la Secretaría del CICTE en coordinación con la Cancillería y la Policía Nacional de Colombia (DIJIN), con la participación de representantes de Bolivia, Chile, Ecuador, Paraguay, Perú, República Dominicana, y Colombia, con responsabilidades técnicas y/o políticas relativas al desarrollo de su infraestructura nacional de seguridad cibernética, incluida la creación y desarrollo de Computer Security Incident Response Teams (CSIRT).



5.2.2 Comparación con el Entorno Internacional

5.2.2.1 Modelos normativos

Con base en el estudio: Análisis de Situación Actual Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea elaborado por la Coordinación de Operación y Desarrollo en el año de 2011, se presenta como una de las debilidades frente a un análisis internacional, la escasa documentación que existe alrededor de los procesos, procedimientos, directrices o políticas de seguridad de la información en las entidades del Estado, debido básicamente a que no se ha liderado la actividad, ni existen los parámetros o estándares definidos y socializados que permitan su fácil implementación en las mismas.

Uno de los modelos de mayor aplicación alrededor de los temas que cubre la ISO27001:2005, sugiere el mantenimiento de la documentación para los sistemas de gestión de seguridad de la información en los siguientes niveles:

- Manual de Seguridad (incluyendo políticas y normas)
- Procedimientos
- Instrucciones, Listas de chequeo, Formularios y Registros.

5.2.2.2 Gestión del Riesgo

En lo que se refiere a la gestión del riesgo, a diferencia de los demás países que cuentan con entidades de gobierno, políticas y programas de seguridad que contemplan la gestión del riesgo como parte de las buenas prácticas de seguridad de la información, se reconoce a través del análisis realizado por Gobierno en línea del 2011 (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010), que Colombia sólo cuenta con instrumentos que no son de aplicación general, como la Circular 052 del 25 de Octubre de 2007 de la Superintendencia Financiera, e iniciativas aisladas como las del Instituto Colombiano de Normas Técnicas y Certificación – ICONTEC.

Estos gestionan todo tipo de información y presentan unos requisitos generales para el establecimiento e implementación del proceso de gestión del riesgo, involucrando la determinación del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y monitoreo regular de los riesgos.

Dentro de los estándares o directrices definidos alrededor del tema de la gestión del riesgo se deben comprender todos los aspectos relevantes a minimizar la probabilidad de materialización de riesgos de seguridad al interior del Estado y sus entidades. Dentro del mundo de los sistemas de gestión de seguridad de la información y de aplicación de la norma ISO27001:2005 es de amplio conocimiento y aplicación el modelo de gestión del riesgo, bajo las siguientes actividades:

1. Planificación
2. Identificar y analizar
3. Direccionar
 - a. Mitigar Riesgo
 - b. Transferir Riesgo

- c. Aceptar Riesgo
- d. Evitar Riesgo

5.2.2.3 Gestión de los incidentes

En Colombia no se evidencia la existencia de directrices o de mecanismos coordinados alrededor del tratamiento de Gestión de los Incidentes, a diferencia de países como España, donde la gestión de incidentes se encuentra considerada explícitamente en el “Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica” (Capítulo III – Requisitos Mínimos, Art. 24)¹⁷, o Estados Unidos, donde se encuentran presentes diversos centros de atención de incidentes, como el National Institute of Standards and Technology (NIST).

5.2.2.4 Mantenimiento y Sostenibilidad del modelo de seguridad de la información

En Colombia se observan acciones individuales para la implementación de sistemas de gestión de seguridad al interior de las entidades del Estado, al igual que de iniciativas para el mantenimiento y sostenibilidad de los mismos, visibles a través del estudio de contrataciones de servicios para tales fines publicados en el portal contratos.gov.co, sin embargo, no se evidencia la existencia de directrices o de mecanismos ya puestos en marcha alrededor del tema.

Frente a la existencia de control al interior de las entidades gubernamentales, se reconoce a Estados Unidos, donde el mantenimiento y sostenibilidad del modelo de seguridad de la información está a cargo de cada una de las entidades federales, el cual es verificado periódicamente a través de procesos de fiscalización y auditoría coordinados por la Oficina de Políticas Gubernamentales y la Oficina de Estrategia Tecnológica. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

También es de destacar el caso de España, donde a través del Real Decreto 3/2010 define lo que se puede considerar un modelo de seguridad de la información y los mecanismos de sostenimiento y robustecimiento del mismo.

Otro referente importante es el caso australiano donde se destaca la participación de la Oficina Nacional de Auditoría y la Dirección de Defensa como responsables de la implementación y monitoreo de los sistemas de gestión de seguridad. (Australian Government Information Management Office, 2011)

5.2.2.5 Infraestructura y activos críticos

Para el caso colombiano no existen procesos específicos en torno a las consideraciones mínimas para la adquisición, implementación y mantenimiento de infraestructura en el marco que define la seguridad de la información. Dentro del marco de operación del Programa Gobierno en Línea, se prevén algunas disposiciones tendientes a lograr el aseguramiento del transporte y comunicación de la información a

¹⁷ ANÁLISIS DE SITUACIÓN ACTUAL MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA, (Coordinación de Operación y Desarrollo - Gobierno en Línea, 2011)



través de RAVEC (Red de Alta Velocidad del Estado Colombiano) y el Centro de Datos del Estado Colombiano¹⁸.

Como casos internacionales destacables en elementos de infraestructura se encuentra a España, donde a través del Real Decreto 3/2010 en su capítulo III, Art. 28 y capítulo IX, Art. 42¹⁹, define la necesidad de contar con estándares en la adquisición, implementación y actualización de infraestructura, a pesar de dejar a elección de cada entidad la compra, montaje y renovación de la misma. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

La República de Corea del Sur, a través de La Ley de Promoción de la Red de Información y Comunicaciones utilización y protección de datos, ha definido las directrices para el montaje de infraestructura en general. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

Por su parte, Australia cuenta con directrices para la instalación de infraestructura de comunicaciones, equipos de procesamiento y sistemas de información, que son coordinadas desde la Dirección de Defensa y apoyadas por la Oficina Nacional de Auditoría. (Australian Government Information Management Office, 2011)

5.2.2.6 Custodia de la Información

Al interior de las entidades del Estado que han estado realizando la implementación de sistemas de gestión de seguridad de la información, existen políticas realizadas a la medida sobre procedimientos para realizar una adecuada custodia de la Información, sin embargo, todas están planteadas por gestión propia o provenientes de auditorías realizadas de las áreas de Tecnología, pero sin responder a directrices provenientes del Nivel Central²⁰, situación que podría ser integrable bajo los lineamientos de gestión del Archivo General de la Nación AGN, siendo esta una entidad del orden nacional adscrita al Ministerio de Cultura, que se encarga de la organización y dirección del Sistema Nacional de Archivos - SNA, que se vincula con la política archivista en Colombia y de custodiar, resguardar y proteger el patrimonio documental del país poniendo al servicio de la comunidad.

5.2.2.7 Seguridad Perimetral

Para poder prestar los servicios en el marco de la Estrategia de Gobierno en línea es evidente la existencia de centros de procesamiento al interior de las entidades, así como la disponibilidad de servicios de procesamiento centralizados puestos a disposición de las entidades del Estado por iniciativas

¹⁸ UIT, Guía de Ciberseguridad para Países en Desarrollo, 2007.

¹⁹ *Ibid.* Pág. 14

²⁰ *Ibid.* Pág. 14

planeadas desde el nivel central, como es el caso del Programa Gobierno en línea del Ministerio de Tecnologías de la Información y las Comunicaciones.

A nivel mundial es posible destacar los esfuerzos de Estados Unidos y España en términos de seguridad perimetral. Por un lado, Estados Unidos presenta esfuerzos importantes en la definición de estándares, procesos y procedimientos tendientes a la implementación de esquemas de aseguramiento perimetral y que son definidos y coordinados desde la Oficina de Estrategia Tecnológica y ejecutados por el Administrador de la Oficina de Gobierno y por el Jefe del Consejo de Servicios de Información. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

Por su parte España, con el Real Decreto 3/2010, genera las recomendaciones en la implementación de sistemas de seguridad perimetral, dejando a libre decisión de cada entidad la implementación de las mismas.

Por otra parte, es importante señalar a Canadá, que cuenta con iniciativas dedicadas exclusivamente a la seguridad física y perimetral en las entidades, brindando medidas para retrasar, prevenir e identificar intentos de acceso no autorizado a los activos de información del gobierno. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

5.2.2.8 Criptografía para la autenticación

Para el caso colombiano, al igual que en el punto anterior, debido a la cantidad de software desarrollado al interior de las entidades o adquirido en el mercado, es posible asegurar que existen múltiples implementaciones de esquemas de criptografía para la gestión de esquemas de autenticación y los passwords en los sistemas de las entidades²¹.

Entre los ejemplos más importantes a nivel internacional se tienen las gestiones realizadas al respecto por la Oficina de Estrategia tecnológica en Estados Unidos STO – Strategic Technology Office con el establecimiento de claves públicas de carácter estándar (Homeland Security, 2011)

5.2.2.9 Redes

Colombia no evidencia iniciativas en torno a la definición de parámetros y estándares para la adquisición e implementación de redes informáticas que garanticen la seguridad de la información, excepto en la Circular Externa 052 de 2007, en el numeral 3.1 de Seguridad y Calidad.

Actualmente los parámetros y estándares en las entidades del estado se dan gracias a la gestión o iniciativa propia de las áreas de Tecnología, pero no necesariamente por directrices emitidas por el

²¹ Ibid. Pág. 14



Gobierno Central. Ejemplo de ello a nivel nacional se encuentra en la Red de Alta Velocidad del Estado Colombiano – RAVEC, que interconecta a las instituciones públicas a altas velocidades, con altos niveles de disponibilidad y seguridad, proporcionando servicios seguros en la transferencia de la información entre organismos gubernamentales, además de ello cuenta con políticas a nivel interno y de licitación pública con la intención de apoyar la iniciativa en Gobierno en Línea Colombia.

En España, las directrices definidas alrededor de la implementación y mantenimiento de redes de comunicación se encuentran consignadas dentro del Esquema de Seguridad Nacional en el Capítulo II de Principios básicos y el Capítulo III de Requisitos Mínimos, sin embargo deja a encargo de las entidades del Estado su implementación y gestión²².

Dentro de la experiencia surcoreana, el Gobierno a través de “La Ley de Promoción de la Red de Información y Comunicaciones, utilización y protección de datos” ha definido las directrices para el montaje de infraestructura en general. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

Por otro lado, Canadá, a través del Departamento de Justicia, emitió leyes y políticas especializadas en el uso de redes electrónicas, a través de las cuales se definen los lineamientos para el buen uso de los recursos tecnológicos que conforman las redes.

5.2.2.10 Evaluaciones de Seguridad de la Información

Para Colombia, el Gobierno a través del Decreto 1599 de 2005 adopta el Modelo Estándar de Control Interno para el Estado Colombiano (MECI) que determina las generalidades y la estructura necesaria para establecer, documentar, implementar y mantener un Sistema de Control Interno en las entidades y agentes obligados conforme al artículo 5º de la Ley 87 de 1993. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

Es importante hacer mención en este punto del *ANÁLISIS DE SITUACIÓN ACTUAL MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA* (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010) cuyo análisis identificó un importante impacto bajo el alcance del MECI (Modelo Estándar de Control Interno) para todos los controles de tipo interno por parte del gobierno. Sin embargo, actualmente no existe parámetros o metodologías específicas para auditar sistemas de gestión de seguridad de la información”. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

Frente a este panorama, en el ámbito internacional se destaca la participación de España con el enfoque y alcance de las auditorías de seguridad de la información, definidas dentro del marco del Capítulo V -

²² UIT, Guía de Ciberseguridad para Países en Desarrollo, 2007.

Auditoría de Seguridad del Real Decreto 3/2010²³. Así como los Estados Unidos con las Oficinas de Estrategia de Tecnología y la Oficina de Políticas Gubernamentales. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

5.2.2.11 Liderazgo de iniciativas de Seguridad de la Información

En Colombia se pueden encontrar varias iniciativas al respecto, entre las que se cuentan las lideradas por el programa Gobierno en línea del Ministerio de Tecnologías de la Información y las Comunicaciones, y varias iniciativas orquestadas desde el Ministerio de Defensa. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

Internacionalmente, frente al liderazgo en iniciativas de Seguridad de la Información se pueden encontrar referentes importantes en Estados Unidos y en Australia. Es así como, Estados Unidos, a través de la Oficina de Estrategia Tecnológica y de la Oficina de Políticas Gubernamentales, ha demostrado un impulso en el nivel tecnológico que fundamenta la seguridad en el ciberespacio²⁴. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

En Australia, el liderazgo en cuanto a la implementación de medidas de Seguridad de la Información al interior de las entidades, lo tiene la Dirección de Defensa Australiana, apalancada por la ley de Seguridad Interna y apoyada por varios organismos, entre los que se encuentran la Organización de Inteligencia y Seguridad Australiana, el Departamento del Fiscal General, el Centro de Coordinación de Seguridad, la Oficina de Gestión de la Información del Gobierno y la Oficina Nacional de Auditoría. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

Por su parte, las iniciativas en Canadá, Corea y España están a cargo del Departamento de Justicia de Canadá, del Centro para la Democracia y la Tecnología de Corea y por el Ministerio de la Presidencia, respectivamente. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

5.3 RESULTADOS DEL EJERCICIO DE PROSPECTIVA

5.3.1 Caracterización de los actores

La naturaleza de la muestra de actores que diligenciaron los instrumentos para el nodo de ciberseguridad, estuvo compuesta en total por 7 profesionales, de los cuales 2 pertenecían a entidades del Estado: Policía Nacional y Ministerio de Defensa, 2 a empresas: Britel SAS y DAKYA (Nueva Generación) y 3 a la Academia: Universidad Manuela Beltrán, Universidad de Pamplona y Universidad Antonio Nariño. En relación con el nivel de formación de los participantes 3 de ellos cuentan con título de pregrado, uno de

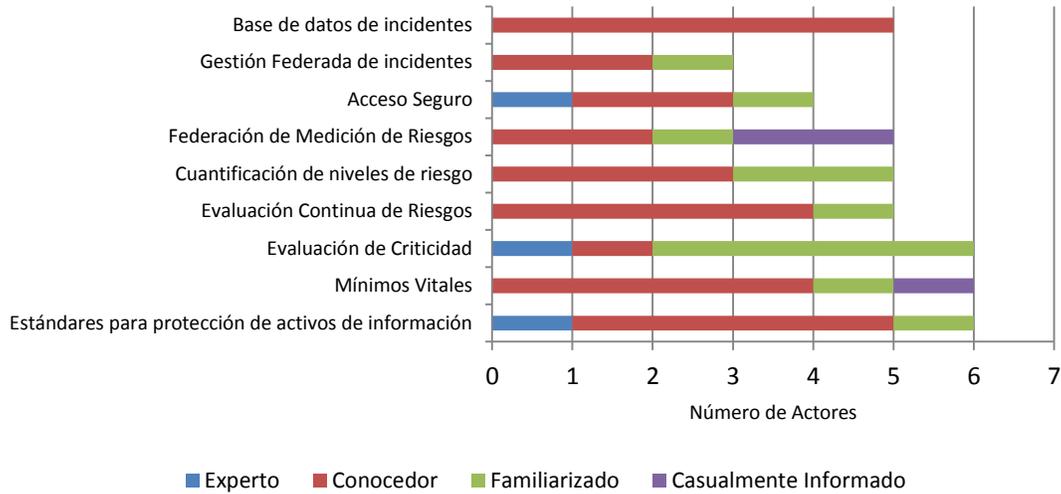
²³ Ibid. Pág. 8.

²⁴ Ibid. Pág. 8.



especialización y 3 de maestría. Por otro lado, la información suministrada por los expertos permitió determinar en un primer momento, el nivel de conocimiento de los participantes en relación a las 9 líneas estratégicas identificadas para el nodo de ciberseguridad, tal como se presenta en la Figura 36.

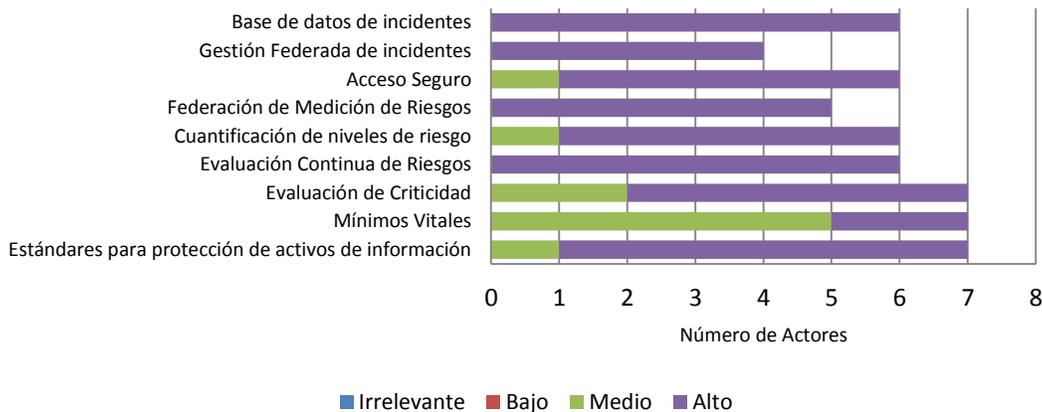
Figura 36. Nivel de Conocimiento de los Expertos con relación a las líneas estratégicas de Ciberseguridad



Fuente: CINTEL 2011

Se aprecia que todas las líneas estratégicas contaron con actores conocedores, es decir que cumplían alguna de las siguientes características: i) fue experto en el tema hace algún tiempo pero ahora se dedica a otras áreas, ii) está formándose como experto, pero considera que aun no tiene dominio total del tema y/o iii) trabaja en un campo muy relacionado y ocasionalmente aporta en el tema.

Figura 37: Nivel de Impacto de cada línea estratégica en el 2016



Fuente : CINTEL 2011

5.3.2 Análisis del Nivel de Impacto de cada línea estratégica

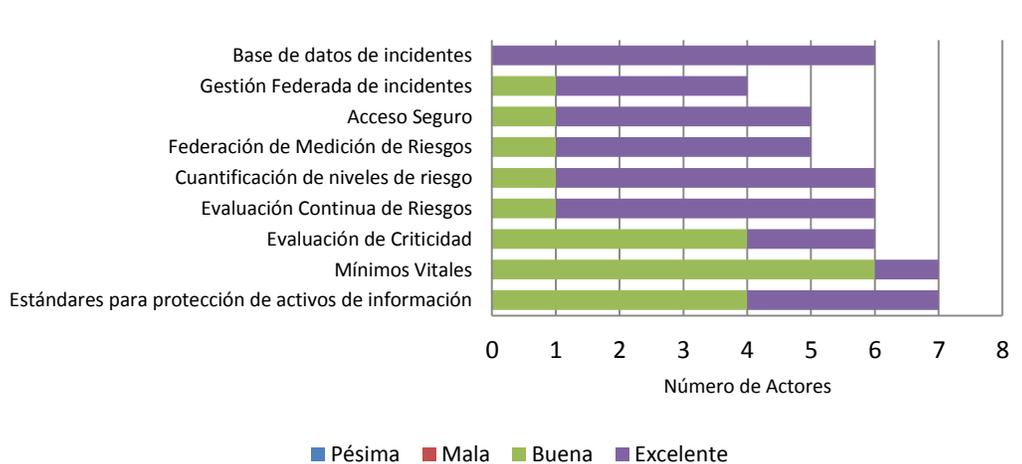
A través del instrumento se logró determinar la percepción de los actores sobre el nivel de impacto que cada línea estratégica tendrá en el 2016 en el desempeño de las entidades del gobierno colombiano (Figura 37).

Es relevante que las nueve líneas estratégicas obtuvieron una calificación entre un nivel de impacto alto y medio, sobresaliendo dentro de las de alto impacto: Base de datos de incidentes, evaluación continua de riesgos y estándares para protección de activos de información, mientras que la línea de mínimos vitales se considera tendrá un impacto medio.

5.3.3 Análisis de la Posición Competitiva del País

Igualmente se indagó a los participantes sobre la posición competitiva que Colombia podrá tener al 2016 frente a otros países en cada una de las líneas estratégicas, obteniéndose como se evidencia en la Figura 38 que en las líneas de Base de datos de incidentes, cuantificación de niveles de riesgo y evaluación continua de riesgo Colombia tendrá una posición excelente, mientras que en mínimos vitales, evaluación de la criticidad y estándares para protección de activos de información se considera que el país al 2016 tendrá una buena posición frente a otros países.

Figura 38 Posición Competitiva de Colombia en el 2016 en cada línea estratégica



Fuente: CINTEL 2011

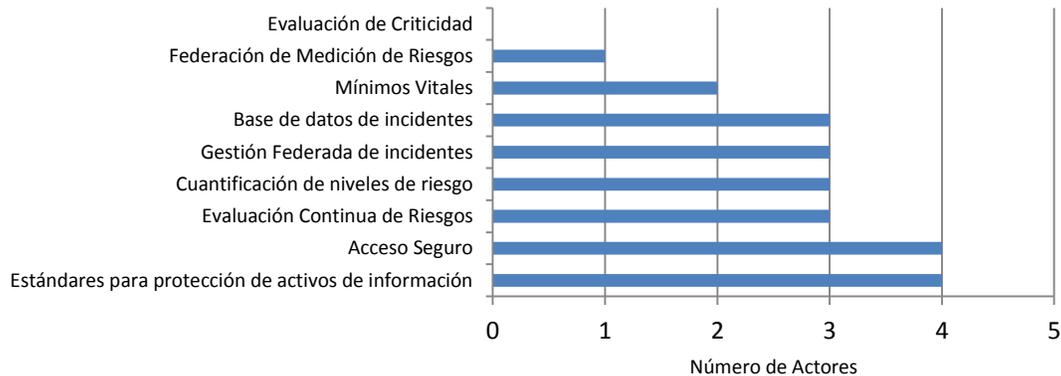
5.3.4 Priorización de Líneas de trabajo para el nodo

Con el objetivo de lograr identificar las líneas que resultan más estratégicas para focalizar el trabajo del nodo en los próximos cinco años, se le solicitó a los participantes que de las 9 líneas propuestas seleccionarán máximo 5, en la Figura 39 se presentan los resultados. A partir del análisis se observa que las líneas que los actores condensaron como prospectivas para iniciar el trabajo del nodo son: Estándares



para protección de activos de información, Acceso Seguro, Evaluación continua de Riesgos, Cuantificación de niveles de riesgo, Gestión Federada de incidentes y Base de datos de Incidentes.

Figura 39 Priorización de las líneas estratégicas del nodo



Fuente: CINTEL 2011

5.4 VISIÓN PROSPECTIVA DEL NODO

De acuerdo al ejercicio de prospectiva, se establece como visión inicial del nodo:

En el año 2016 el Nodo de Ciberseguridad será un referente nacional para el desarrollo de proyectos innovadores, de clase mundial, que permitan minimizar el riesgo y contrarrestar las amenazas e incidentes de naturaleza cibernética para las instituciones del estado.

5.4.1 Vectores de desarrollo del nodo

De acuerdo con las necesidades observadas en cuanto a las brechas existentes y a las mayores amenazas para la ciberseguridad del Estado colombiano, se proponen inicialmente los siguientes vectores de desarrollo del nodo, cada uno de los cuales presentará posteriormente líneas priorizadas de innovación.

5.4.1.1 Definiciones básicas, estándares y mínimos de protección vital

En el ámbito internacional, se observa que instituciones como NIST o SANS han desarrollado estándares específicos para el aseguramiento de su infraestructura crítica, creando guías que especifican de forma puntual las medidas requeridas para aumentar la seguridad de sus sistemas y activos de soporte. En el ámbito nacional, esta necesidad ha empezado a solventarse con iniciativas como el “Modelo de seguridad de la información para la estrategia de Gobierno en línea 2.0”, que establece una guía práctica sobre cómo establecer el sistema de gestión de seguridad de la información para las organizaciones del estado.

Para complementar el trabajo que se ha empezado a elaborar en el país y cerrar la brecha que genera dificultades en la implementación de buenas prácticas, es necesario contar con guías específicas que sean aplicables a las instituciones del Estado colombiano y en especial con aquellas que puedan no solamente establecer globalmente cómo gestionar un sistema de gestión de seguridad de la información, sino en específico, como definir y asegurar la infraestructura crítica, el mantenimiento de ambientes seguros, el aseguramiento de sistemas y los mínimos requeridos para minimizar los riesgos de naturaleza cibernética.

En este vector de desarrollo, se presentan tres líneas básicas a considerar:

- *Estándares para protección de activos de información* - Definición, implementación y valoración de la aplicación de estándares de seguridad apropiados para la protección de activos de naturaleza cibernética en el sector gobierno.
- *Mínimos vitales* - Definición, implementación y valoración de la aplicación de estándares mínimos basados en modelos de madurez, aplicables por tipo de sistema según su nivel de protección requerida.
- *Evaluación de criticidad* - Definición de esquemas de clasificación de entidades, sistemas y servicios y sus niveles de protección requeridos.

5.4.1.2 Gestión de riesgos

Más allá de la gestión de riesgos direccionada por normas como la ISO/IEC 27005 o por estándares específicos como OCTAVE, se ha observado la necesidad de establecer procesos que permitan mantener un conocimiento continuo de la seguridad de la información, amenazas y vulnerabilidades que permitan tomar decisiones apropiadas para la gestión del riesgo. En este sentido, existe una tendencia en tal campo y se ha generado normativa general como la NIST SP 800-237, para el caso específico de Estados Unidos (septiembre de 2011).

En este vector de desarrollo del nodo de ciberseguridad, se deberán trabajar por un lado, esquemas de gestión continua que permitan detectar y tratar apropiadamente los riesgos de ciberseguridad, y por otro, se deberá establecer e implementar una arquitectura que permita la estandarización de los niveles de riesgos, de forma que se hagan comparables las mediciones realizadas por diferentes entidades, y que se puedan manejar federaciones de los niveles de riesgo.

Las cuatro líneas de innovación que están dentro de este vector son:

- *Evaluación continua de riesgos* - Establecimiento de estrategias e implementación de mecanismos de medición automatizada y continua de los niveles de riesgo, amenazas y vulnerabilidades existentes en los sistemas gubernamentales y en aquellos considerados vitales fuera de este ámbito.
- *Cuantificación de niveles de riesgos* - Normalización y aplicación de los indicadores de riesgos para permitir resultados comparables entre entidades.
- *Federación de medición de riesgos* - Generación de esquemas agregados (federados) de medición de riesgos para medir el riesgo por Entidad, Entidades adscritas a un ente superior y otras agrupaciones de entidades para facilitar la toma de decisiones en cuanto a protección y detección temprana de puntos de fallo.



- Acceso seguro - Implementación de mecanismos de acceso seguro, doble autenticación u otros para ingreso a los sitios críticos, con el fin de minimizar riesgos de captura de contraseñas e información crítica.

5.4.1.3 Gestión de incidentes

Si bien el CONPES 3701 determina los lineamientos básicos para el establecimiento organizativo de la respuesta del Estado ante ciberataques, es necesario dotar a estos entes (COLCERT, en especial) de herramientas que le permitan contar con datos que faciliten su labor. Estas herramientas innovadoras deberán buscar recuperar información a partir de la integración de datos, siguiendo el intercambio de datos a través de esquemas federados como los que también se han tratado en el vector de desarrollo de gestión de riesgos.

Dentro de gestión de incidentes se presentan dos líneas de innovación:

- *Gestión federada de incidentes* - Puesta en funcionamiento de un sistema integrado (tecnología, procesos y personas) de gestión federada de Incidentes que permita informar, responder, alertar y tratar de forma apropiada ante la ocurrencia de incidentes de ciberseguridad.
- *Base de datos de incidentes* - Sistemas de centralización e intercambio de datos de detección/prevenición de intrusos y generación de mecanismos de alertas tempranas, al vuelo y análisis a posteriori.

5.5 AGENDA ESTRATÉGICA DE INNOVACIÓN - PRIORIDADES DE INNOVACIÓN EN CIBERSEGURIDAD

A continuación se presentan las líneas de innovación priorizadas de acuerdo a las calificaciones otorgadas en las secciones de prospectiva a los diferentes temas, tanto en el nivel de prelación de las líneas como en el de la ventaja competitiva a nivel país que cada una de ellas tendría.

5.5.1 Estándares para protección de activos de información

Esta línea de investigación trabajará en la definición, implementación y valoración de la aplicación de estándares de seguridad apropiados para la protección de activos de naturaleza cibernética en el sector gobierno, los cuales deberán ser complemento de las políticas determinadas en el modelo de seguridad de la información para la estrategia de gobierno en línea – 2010.

Como marco conceptual, se podrá tener en cuenta que Estados Unidos evidencia esfuerzos importantes en la definición de estándares, procesos y procedimientos tendientes a la implementación de esquemas de aseguramiento definidos y coordinados desde la Oficina de Estrategia Tecnológica y ejecutados por el Administrador de la Oficina de Gobierno y por el Jefe del Consejo de Servicios de Información. Igualmente, Australia Cuenta con directrices para la instalación de infraestructura de comunicaciones, equipos de procesamiento y sistemas de información, las cuales son coordinadas desde la Dirección de Defensa y apoyadas por la Oficina Nacional de Auditoría, mostrando una política clara del Estado en cuanto a este tema. (Fondo de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2010)

5.5.2 Acceso seguro a sistemas

Esta línea de innovación trabajará en la implementación de mecanismos de acceso seguro, doble autenticación, teclados virtuales u otros para ingreso a sistemas críticos, con el fin de minimizar riesgos de captura de contraseñas e información crítica. En Colombia, el sector financiero es un referente en este tema, pues varios de los sitios transaccionales de las entidades bancarias cuentan con mecanismos que minimizan amenazas como *keyloggers*, escuchas de comunicaciones y otros. En Francia, por ejemplo, como parte de la estrategia de ciberseguridad, se ha previsto la implementación de sistemas de autenticación fuerte basada, por ejemplo, en el uso de tarjetas inteligentes, como opción para mejorar la seguridad en el acceso a los sistemas de información del estado (Agence nationale de la sécurité des systèmes d'information, 2011).

5.5.3 Base de datos de incidentes

Esta línea trabajará en Sistemas de centralización e intercambio de datos de detección/prevención de intrusos y generación de mecanismos de alertas tempranas, en tiempo real y con posibilidad de análisis a posteriori. Los alcances iniciales, para el período 2012- 2016, deben centrarse en la recolección, correlación, análisis y divulgación (restringida) de datos de los sistemas de detección de intrusos. Temas como la prevención automatizada de ataques basado en la recolección temprana de datos, deben ser parte de una estrategia de investigación que no debe ser asumida inicialmente por el nodo pero que debe ser tenida en cuenta por otros actores del sistema de I+D+i, puesto que luego podría generar insumos para esta línea de innovación.

Como referencia para el desarrollo de la línea se puede tener en cuenta que el Instituto para la protección de la infraestructura informática (I3P), el cual en un estudio del año 2009, titulado “Retos de la investigación y el desarrollo de la ciberseguridad nacional”, menciona como una de sus necesidades el desarrollo de una base de datos confiable y actualizada de ataques e intrusiones sobre la tecnología. En específico se pueden tener en cuenta los programas EINSTEIN y EINSTEIN2²⁵, de la División de ciberseguridad del Departamento de seguridad doméstica de Estados Unidos. De igual forma, se debe tener en cuenta el Libro Blanco sobre defensa y seguridad nacional de Francia, que establece la capacidad de detectar ataques a los sistemas de la información.

5.5.4 Cuantificación de niveles de riesgos

El objetivo de esta línea es implementar proyectos de normalización y aplicación de los indicadores de riesgos para permitir contar con resultados comparables entre entidades.

Esta línea de trabajo se apoya en los resultados de investigación de la coordinación de Investigación, Políticas y Evaluación del programa Agenda de Conectividad. En específico, del “Modelo de seguridad de la información para la estrategia de Gobierno en línea”, en cuyo anexo 6 determina un Metodología de gestión del riesgo, la cual deberá ser adoptada y adaptada para permitir implementar métricas que

²⁵ Privacy Impact Assessment for Einstein 2, (Homeland Security, 2008).



permitan evaluar los niveles por entidad y agregarlos para generar un mapa nacional de riesgos de ciberseguridad, el cual facilitará la toma de decisiones y movimiento de recursos hacia puntos que pudieran estar más vulnerables dentro de la superficie expuesta en el ciberespacio.

5.5.5 Evaluación Continua de Riesgos

Esta línea abordará el establecimiento de estrategias e implementación de mecanismos de medición automatizada y continua de los niveles de riesgo, amenazas y vulnerabilidades existentes en los sistemas gubernamentales y en aquellos considerados vitales fuera de este ámbito.

Esta línea aparece como continuación de la visión inicial de Monitoreo continuo, el cual se aplicaba inicialmente para evaluar las dimensiones de riesgo y cumplimiento dentro del modelo GRC²⁶ para los ambientes financieros y operacionales, sin embargo, entidades como el Software Engineering Institute, del Carnegie Mellon, han expandido esta idea hasta la gestión de proyectos e instituciones como CISCO la han implementado descubriendo “sorpresas potenciales” y vulnerabilidades de alto riesgo que hubieran sido no detectadas de otra forma.

5.6 INICIATIVAS DE PROYECTOS POR PRIORIDAD

5.6.1 Estándares para protección de activos de información

Proyectos identificados:

- Definición e implementación modelo de una guía estandarizada para la identificación de activos relevantes
- Definición e implementación de estándares de seguridad en Desarrollo de Software
- Evaluación de estado de riesgo en el ciclo de vida de desarrollo de aplicaciones
- Creación de un modelo de normas políticas y procedimientos base para Colombia partiendo de las políticas del *Modelo de seguridad de la información para la estrategia de gobierno en línea*.

5.6.2 Acceso Seguro

- Definición e implementación de un modelo de llaves y restricciones con doble autenticación para el acceso a sistemas de información críticos

5.6.3 Base de datos de incidentes

- Implementación de un sistema centralizado para la detección de patrones de ataques, basada en aprendizaje automático en las entidades del estado.
- Implementación de un sistema de alertas tempranas, automáticas resultado de la correlación de datos de prevención de intrusos

²⁶ GRC Symposium, (ISACA, 2009).

5.6.4 Cuantificación de niveles de riesgos

- Diseño, desarrollo e implementación de un esquema para la evaluación y comparación de niveles (métricas) de riesgos en las entidades del estado
- Definición de mínimos evaluables para calificación de riesgos por cada entidad de cada sector

5.6.5 Evaluación Continua de Riesgos

- Implementación del centro de monitoreo y evaluación de riesgos a nivel nacional que permita generar información en tiempo real a las instituciones
- Desarrollo del modelo de evaluación continuo de riesgos e implementación modelo.

5.7 PERFILES DE PROYECTO

5.7.1 Proyecto 1

Entidad que presenta la iniciativa	Universidad Antonio Nariño Britel S.A.S. ColCERT ACIS
Entidades Participantes	<p><i>Del sector estado</i></p> <ul style="list-style-type: none"> • <i>Entidades con responsabilidades específicas en ciberseguridad (CONPES 3701)</i> • <i>Entidades líderes en la implementación de la norma ISO 27001</i> <p><i>Del sector Academia</i></p> <ul style="list-style-type: none"> • <i>Grupos de investigación cuyo énfasis sea en la seguridad de la información, en específico, con la gestión de modelos normativos, identificación de activos y clasificación de la información.</i> • <i>Asociaciones de especialistas que cuenten con líneas de trabajo en normalización o generación de modelos normativos, identificación de activos y clasificación de la información.</i> <p><i>Del sector Empresa</i></p> <ul style="list-style-type: none"> • <i>Empresas consultoras en la gestión de sistemas de seguridad de la información, en específico con desarrollo de modelos normativos, identificación de activos y clasificación de la información.</i>
Área de Interés (Debe corresponder a las líneas priorizadas en la AEI)	<i>Estándares para protección de activos de información</i>
Título de la iniciativa	<i>Definición e implementación modelo de una guía estandarizada para la identificación de activos relevantes (infraestructuras críticas para el estado)</i>



Descripción de la problemática	<i>La identificación y clasificación de activos de información se realiza normalmente siguiendo la norma ISO 27002, la cual, junto con otras normas de la serie 27000, ayudan a las instituciones a definir y calificar sus activos de información desde el punto de vista de cumplimiento de objetivos e impacto a sus variables críticas de negocio. Sin embargo, no existe una visión general que permita determinar cuáles son los activos críticos calificados contra raseros globales (a nivel de país). Contar con esta información será indispensable para generar mecanismos para la protección de los intereses no solo de las organizaciones sino de la ciberdefensa nacional, al enfocar los esfuerzos hacia esos activos de información que puedan ser de mayor impacto.</i>
Objetivo General	Definir un modelo general e implementar en una entidad piloto una guía específica que permita la identificación de activos críticos desde el punto de vista de la ciberseguridad en el ámbito nacional, expandiendo la visión actual de la ISO 27001/27002, que restringe la evaluación de los activos al cumplimiento de los objetivos de negocio.
Objetivos Específicos	<ul style="list-style-type: none">• Definir un modelo multidimensional específico para la identificación de activos críticos para las entidades estatales que evalúe impactos sobre la ciberseguridad nacional, expandiendo las fronteras requeridas por las normas actuales..• Definir los parámetros de evaluación y las reglas de calificación que deberán usar las entidades para permitir una calificación de activos desde el punto de vista de ciberseguridad nacional.• Aplicar los modelos desarrollados en un piloto para determinar las necesidades de inclusión de los activos dentro de las políticas de protección más allá de la frontera de la entidad.• Definir guías de aseguramiento para sistemas de infraestructura crítica de la nación.
Alcance	La iniciativa debe generar guías para la identificación y clasificación de los tipos de activos (ambientes, infraestructura, sistemas de información, <i>data</i> , medios de soporte, etc.) desde el punto de vista de la ciberseguridad nacional y deberá aplicarse para generar el inventario de las infraestructuras críticas de la nación.
Entidades Beneficiarias (Posible cliente)	Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT Ministerio de Tecnologías de Información y Comunicaciones
Impactos Esperados	<i>Con el conjunto de activos críticos identificados en el piloto y con la metodología que se podrá replicar, se espera que el colCERT pueda contar con información calificada para cumplir su objetivo de desarrollar y promover políticas, procedimientos, recomendaciones, protocolos y guías de ciberseguridad y ciberdefensa y que aumente la visibilidad interna en las instituciones sobre sus activos críticos, observados estos desde una visión global de la ciberdefensa y ciberseguridad de la nación.</i>
Duración estimada	Seis (6) meses.
Presupuesto estimado	El costo del proyecto, en un estimado del tipo orden de magnitud, es de COP 700,000,000.
Resultados Esperados de la iniciativa	<i>Guía replicable para la identificación de activos críticos (relevantes) desde el punto de vista de la ciberseguridad nacional, que le permita al colCERT contar con información calificada para cumplir su objetivo de desarrollar y promover políticas, procedimientos, recomendaciones, protocolos y guías de ciberseguridad y ciberdefensa. Contar con un conjunto de activos relevantes de las entidades piloto que deben ser protegidos y monitoreados por el ColCERT.</i>
Nivel de	Restringido

confidencialidad de
la iniciativa

5.7.2 Proyecto 2

Entidad que presenta la iniciativa	Universidad Manuela Beltrán
Entidades Participantes	<p><i>Del sector estado</i></p> <ul style="list-style-type: none"> • <i>Entidades con responsabilidades específicas en ciberseguridad (CONPES 3701)</i> • <i>Entidades líderes en la implementación de la norma ISO 27001</i> <p><i>Del sector Academia</i></p> <ul style="list-style-type: none"> • <i>Grupos de investigación cuyo énfasis sea en la seguridad de la información, en específico, con la seguridad en el desarrollo de software o desarrollo de aplicaciones de seguridad.</i> • <i>Asociaciones de especialistas que cuenten con líneas de trabajo en desarrollo de software seguro.</i> <p><i>Del sector Empresa</i></p> <ul style="list-style-type: none"> • <i>Empresas consultoras y proveedoras de software.</i>
Área de Interés (Debe corresponder a las líneas priorizadas en la AEI)	<i>Estándares para protección de activos de información</i>
Título de la iniciativa	<i>Definición e implementación de estándares de seguridad en Desarrollo de Software</i>
Descripción de la problemática	<i>La no inclusión de un proceso de gestión de la seguridad de los sistemas de información dentro del Ciclo de vida de desarrollo de sistemas (SDLC por sus siglas en Inglés) genera inconvenientes relacionados con problemas de vulnerabilidades no detectadas a tiempo en los sistemas, con costos mayores una vez estas son identificadas o incluso con la generación de riesgos durante el mismo desarrollo. Por ello, es necesario contar con un proceso que sea aplicable para el desarrollo de software para las entidades del estado que cubra todo el ciclo de vida y que tenga en cuenta los modelos usados en Colombia, que en general incluyen la tercerización de varias fases de ese ciclo.</i>
Objetivo General	Crear un conjunto integrado de guías de seguridad para el ciclo de vida del desarrollo de software que permita cubrir todos los procesos, desde la definición de requerimientos hasta la gestión de tercerización.
Objetivos	Desarrollar un conjunto de guías de seguridad para el SDLC que esté alineado con los estándares internacionales certificables de producto.



Específicos	<p>Desarrollar un método efectivo para especificar características de seguridad para cada fase del ciclo de vida, con sus indicadores correspondientes de confiabilidad.</p> <p>Establecer un mecanismo que le permita a las entidades especificar, evaluar y actualizar los requerimientos de seguridad en cada fase del ciclo de vida.</p> <p>Definir un esquema de evaluación que permita obtener valores de la confiabilidad de un sistema en el cumplimiento de los requisitos de seguridad generados en el ciclo de vida.</p>
Alcance	La iniciativa debe generar un estándar para el desarrollo de sistemas de información que cubra todo el ciclo de vida del software. No debe estar orientado a una tecnología específica y debe generar las métricas correspondientes para evaluar proceso y el producto y que estén alineados con el cumplimiento de requisitos internacionales certificables de producto.
Entidades Beneficiarias (Posible cliente)	Ministerio de Tecnologías de Información y Comunicaciones - Gobierno en Línea.
Impactos Esperados	<p><i>Mejora en la seguridad de los sistemas de información, disminuyendo el costo de aplicación de medidas de seguridad y facilitando la detección de amenazas como backdoors o vulnerabilidades existentes en el software.</i></p> <p><i>Mejor selección de sistemas o de proveedores a través de evaluaciones estandarizadas que generen características comparativas.</i></p>
Duración estimada	Seis (6) meses
Presupuesto estimado	El costo del proyecto, en un estimado del tipo orden de magnitud, es de COP 400,000,000.
Resultados Esperados de la iniciativa	<p>Guías integradas que comprendan metodología, herramientas y métricas para la gestión y evaluación de seguridad dentro del proceso de software.</p> <p>Implementación del estándar en una organización proveedora de software para la estrategia de gobierno en línea.</p> <p>Aplicación del estándar en el desarrollo de un proyecto modelo.</p>
Nivel de confidencialidad de la iniciativa	Restringido

5.7.3 Proyecto 3

Entidad que presenta la iniciativa	<p>DAKYA Ltda.</p> <p>ACIS</p> <p>ColCERT</p>
------------------------------------	---

<p>Entidades Participantes</p>	<p><i>Del sector estado</i></p> <ul style="list-style-type: none"> • <i>Entidades con responsabilidades específicas en ciberseguridad (CONPES 3701)</i> • <i>Entidades líderes en la implementación de la norma ISO 27001</i> <p><i>Del sector Academia</i></p> <ul style="list-style-type: none"> • <i>Grupos de investigación cuyo énfasis sea en la seguridad de la información, en específico, con la gestión de modelos normativos.</i> • <i>Asociaciones de especialistas que cuenten con líneas de trabajo en normalización o generación de modelos normativos.</i> <p><i>Del sector Empresa</i></p> <ul style="list-style-type: none"> • <i>Empresas consultoras en la gestión de sistemas de seguridad de la información, en específico con desarrollo de modelos normativos.</i>
<p>Área de Interés (Debe corresponder a las líneas priorizadas en la AEI)</p>	<p><i>Estándares para protección de activos de información</i></p>
<p>Título de la iniciativa</p>	<p><i>Creación de un marco normativo estándar - modelo de normas políticas y procedimientos base para Colombia como extensión del Modelo de seguridad de la información para la estrategia de gobierno en línea</i></p>
<p>Descripción de la problemática</p>	<p><i>Si bien existen normas como la ISO 27001 y esfuerzos para crear mecanismos de implementación en Colombia a través del modelo estándar de seguridad de la información, se requiere que, como ha sucedido en otros países, se cree un conjunto de estándares, procesos y procedimientos base tendientes a la implementación de esquemas de aseguramiento definidos y coordinados desde un punto central, los cuales guíen a las entidades en la definición de su propio modelo normativo para la ciberseguridad.</i></p>
<p>Objetivo General</p>	<p><i>Desarrollar una base sólida de políticas modelo que le permitan a las entidades del estado desarrollar, alrededor de ellas, su propio modelo normativo.</i></p>
<p>Objetivos Específicos</p>	<p><i>Desarrollar un marco normativo estándar de políticas, normas y procedimientos para la ciberseguridad de las organizaciones del Estado colombiano, que evolucione con el tiempo y recoja mejoras obtenidas durante su propia implementación y como resultado de otras iniciativas del nodo.</i></p> <p><i>Desarrollar las guías de adaptación (<i>tailoring</i>) del marco normativo estándar.</i></p>
<p>Alcance</p>	<p><i>El marco normativo estándar debe cumplir con los requisitos mínimos de políticas, normas y procedimientos requeridos por la ISO 27001 y debe estar enfocado a su aplicabilidad a las instituciones del estado colombiano.</i></p>
<p>Entidades Beneficiarias (Posible cliente)</p>	<p><i>Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT</i> <i>Ministerio de Defensa</i></p>
<p>Impactos Esperados</p>	<p><i>Una vez se cuente con los productos implementados en las entidades del estado, se tendrán los siguientes impactos:</i></p> <p><i>Aumento en la velocidad de desarrollo, implementación y evaluación de los modelos</i></p>



	<p><i>normativos de seguridad de la información de las entidades del Estado colombiano.</i></p> <p><i>Disminución de los costos de desarrollo de modelos normativos.</i></p> <p><i>Mejora en los controles procedimentales de seguridad de la información y todos los que se desprendan de ellos a través de la transferencia de tecnología explícita en las buenas prácticas incluidas en el modelo.</i></p>
Duración estimada	<i>Doce (12) meses.</i>
Presupuesto estimado	El costo del proyecto, en un estimado del tipo orden de magnitud, es de COP 1,000,000,000.
Resultados Esperados de la iniciativa	<p>Marco normativo estándar compuesto de políticas, normas y procedimientos base para la ciberseguridad de las entidades del Estado colombiano, creadas evolutiva y complementariamente a partir del Modelo de seguridad de la información para la estrategia de gobierno en línea.</p> <p>Guías de adaptación del modelo normativo de acuerdo a los diferentes tipos de entidades y alcances que se quiera dar a la aplicación del Marco.</p>
Nivel de confidencialidad de la iniciativa	Restringido

5.7.4 Proyecto 4

Entidad que presenta la iniciativa	Universidad de Pamplona Ministerio de Defensa
Entidades Participantes	<p><i>Del sector estado</i></p> <ul style="list-style-type: none"><i>Entidades con responsabilidades específicas en ciberseguridad (CONPES 3701)</i><i>Entidades líderes en la implementación de la norma ISO 27001</i> <p><i>Del sector Academia</i></p> <ul style="list-style-type: none"><i>Grupos de investigación cuyo énfasis sea en la seguridad de la información, seguridad informática o comercio electrónico.</i><i>Asociaciones de especialistas que cuenten con líneas de trabajo en normalización, investigación, innovación o desarrollo en seguridad informática, comercio electrónico y usabilidad de la seguridad.</i> <p><i>Del sector Empresa</i></p> <ul style="list-style-type: none"><i>Clusters de tecnología.</i><i>Empresas proveedoras de software y consultoras en controles para la autenticación.</i>

Área de Interés (Debe corresponder a las líneas priorizadas en la AEI)	<i>Acceso seguro</i>
Título de la iniciativa	<i>Definición e implementación de un modelo de llaves y restricciones con doble autenticación para el acceso a sistemas de información críticos</i>
Descripción de la problemática	<i>Si bien sectores como el financiero en Colombia cuentan ya con mecanismos relativamente sencillos, probados y operativos para la verificación de la autenticidad de quienes acceden a los sistemas de información, el sector público se encuentra rezagado y existe una brecha en el uso de estos mecanismos para autorizar el acceso de los usuarios y evitar ataques de man-in-the-middle, escuchas de telecomunicaciones y otros. Por lo anterior, se requiere contar con una revisión de las necesidades de los sistemas de información, para generar una taxonomía adecuada y contar con un nuevo modelo que le facilite a las entidades identificar y aplicar controles para la autorización.</i>
Objetivo General	Desarrollar un modelo de controles de diferentes niveles que, según el nivel de criticidad del sistema de información, sugiera los mecanismos de protección para el control de acceso a los sistemas de información.
Objetivos Específicos	<p>Determinar, conjuntamente con la iniciativa de identificación de activos, una taxonomía para los sistemas de información que permita distinguir los niveles de seguridad en el control de acceso requeridos.</p> <p>Desarrollar una guía que defina los diferentes mecanismos de control de acceso y su necesidad de aplicación según la taxonomía realizada.</p> <p>Implementar componentes de teclados virtuales, imágenes propias y otras que permitan mejorar el proceso de autenticación ante los sistemas de información.</p>
Alcance	El alcance de la guía será hasta la autenticación. No se cubrirá inicialmente la gestión de roles o autorización.
Entidades Beneficiarias (Posible cliente)	<p>El proyecto cuenta con todas las entidades del estado como posibles beneficiarias, a las cuales se sugiere llegar con los resultados del proyecto a través de dos entes que podrían promover y coordinar su implementación:</p> <p>Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT Ministro de Tecnologías de Información y Comunicaciones</p>
Impactos Esperados	<p><i>Mejora en la capacidad de defensa de los sistemas de información ante ataques contra el servicio de autenticación.</i></p> <p><i>Generación de mecanismos estándares que puedan ser aplicados de forma eficaz y efectiva, disminuyendo tiempos y costos.</i></p> <p><i>Creación de un modelo que mejore evolutivamente con el tiempo, con el conocimiento recogido a través de su propia aplicación, el descubrimiento de nuevos vectores de ataque y la aparición de nuevas vulnerabilidades.</i></p>
Duración estimada	El costo del proyecto, en un estimado del tipo orden de magnitud, es de COP 600,000,000.
Presupuesto	ND.



estimado	
Resultados Esperados de la iniciativa	Modelo de definición de los mecanismos de control de acceso y su necesidad de aplicación según una taxonomía definida para los sistemas de información según los niveles de seguridad requeridos para la protección del servicio de autenticación. Artefactos como teclados virtuales, imágenes propias y otras que puedan ser implementados como módulos para mejorar el proceso de autenticación ante los sistemas de información.
Nivel de confidencialidad de la iniciativa	Restringido

5.7.5 Proyecto 5

Entidad que presenta la iniciativa	Universidad Manuela Beltrán Ministerio de Defensa ACIS
Entidades Participantes	<i>Del sector estado</i> <ul style="list-style-type: none">• <i>Entidades con responsabilidades específicas en ciberseguridad (CONPES 3701)</i>• <i>Entidades líderes en la implementación de sistemas de detección y prevención de intrusos, tratamiento unificado de amenazas y similares.</i>• <i>Entidades que han generado normativa de obligatorio cumplimiento en cuanto a seguridad de la información para sus entidades adscritas o vigiladas.</i> <i>Del sector Academia</i> <ul style="list-style-type: none">• <i>Grupos de investigación cuyo énfasis sea la seguridad informática, en específico la correlación de eventos, detección, prevención de intrusos o similares.</i> <i>Del sector Empresa</i> <ul style="list-style-type: none">• <i>Clusters de tecnología.</i>• <i>Empresas proveedoras de software y appliances para la detección y prevención de intrusos, tratamiento unificado de amenazas, gestión de vulnerabilidades, gestión de amenazas y tratamiento de riesgo.</i>
Área de Interés (Debe corresponder a las líneas priorizadas en la AEI)	<i>Bases de datos de Incidentes</i> <i>Gestión federada de incidentes</i>
Título de la	<i>Implementación de un sistema centralizado para la recolección de datos y detección de patrones de ataques, basada en aprendizaje automático en las entidades del estado e</i>

iniciativa	<i>implementación de un sistema de alertas tempranas, automáticas resultado de la correlación de datos de prevención de intrusos</i>
Descripción de la problemática	<i>La falta de datos sobre intentos de intrusión, accesos no autorizados, ataques a la infraestructura y sus causas, consecuencias y evaluaciones de lecciones aprendidas, generan vacíos para la prevención de su repetición o la preparación para una respuesta adecuada cuando estos ocurran. Por ello, se requiere de una base de conocimiento que recoja las experiencias en este tema y que pueda ayudar a prevenir, responder y mitigar posibles ataques basado en el estudio de intentos de intrusión previos.</i>
Objetivo General	Desarrollar un sistema centralizado para la detección de ataques y la evaluación de sus medios, causas, consecuencias y respuestas para permitir generar acciones anticipadas ante posibles nuevas ocurrencias del mismo tipo de incidentes.
Objetivos Específicos	Determinar los principales mecanismos instalados en las entidades del estado para la detección de ataques. Crear mecanismos para el intercambio de información con el nivel central, que permita recopilar datos de ataques y realizar la correlación de información para generar. Socializar y poner en marcha los mecanismos de comunicación y tratamiento coordinado de incidentes.
Alcance	El alcance de la iniciativa debe ser establecido de acuerdo a las entidades finalmente participantes. Se sugiere que inicialmente se incluyan entidades que tienen disponibles sistemas de IDS en una etapa madura de implementación.
Entidades Beneficiarias (Posible cliente)	Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT Centro Cibernético Policial - CCP Comando Conjunto Cibernético de las Fuerzas Militares – CCOC
Impactos Esperados	<i>Mejora en la detección de ataques y en la preparación para la prevención y respuesta ante situaciones similares.</i> <i>Mejora en la comunicación interinstitucional para la gestión de incidentes.</i>
Duración estimada	<i>Doce (12) meses.</i>
Presupuesto estimado	El costo del proyecto, en un estimado del tipo orden de magnitud, es de COP 1,200,000,000.
Resultados Esperados de la iniciativa	Sistema central de recopilación de datos, correlación y análisis de información. Sistema de integración de bases de datos de detección de intrusos, incluyendo sus respectivos colectores. Proceso comunicativo de alerta temprana, escalamiento de informes de ataques y de gestión de respuestas a incidentes.
Nivel de confidencialidad de la iniciativa	Restringido

5.7.6 Proyecto 6

Entidad que presenta la	Universidad Manuela Beltrán Universidad de Pamplona
-------------------------	--



iniciativa	Britel S.A.S. DAKYA Ltda. ColCERT
Entidades Participantes	<i>Del sector estado</i> <ul style="list-style-type: none">• <i>Entidades con responsabilidades específicas en ciberseguridad (CONPES 3701)</i>• <i>Entidades líderes en la implementación de la norma ISO 27001</i>• <i>Entidades que han generado normativa de obligatorio cumplimiento en cuanto a seguridad de la información para sus entidades adscritas o vigiladas.</i> <i>Del sector Academia</i> <ul style="list-style-type: none">• <i>Grupos de investigación cuyo énfasis sea en gestión de riesgos.</i>• <i>Asociaciones de especialistas que cuenten con líneas de trabajo en normalización, investigación, innovación o desarrollo en seguridad de la información y gestión de riesgos.</i> <i>Del sector Empresa</i> <ul style="list-style-type: none">• <i>Clusters de tecnología.</i>• <i>Empresas consultoras en la identificación y valoración de riesgos.</i>• <i>Empresas proveedoras de software y appliances para la gestión de vulnerabilidades, gestión de amenazas y tratamiento de riesgo.</i>
Área de Interés (Debe corresponder a las líneas priorizadas en la AEI)	<i>Cuantificación de niveles de riesgos</i> <i>Gestión continua de riesgos</i>
Título de la iniciativa	<i>Diseño, desarrollo e implementación de un esquema para la evaluación y comparación de niveles (métricas) de riesgos en las entidades del estado</i>
Descripción de la problemática	<i>Colombia cuenta con mapas de riesgo del territorio nacional en niveles tan diferentes como la relacionada con temas electorales hasta la directamente aplicable a grupos ilegales. Estos mapas de riesgos ayudan a tener una visión global de la situación país y enfocar los esfuerzos en áreas que lo requieren, además de permitir evaluar la evolución de las situaciones desde diferentes puntos de vista. Se requiere que este tipo de mapas de riesgos existan para la ciberseguridad, con dimensiones que no necesariamente sean geográficas pero que sí permitan evaluar el estado general del estado en ciberseguridad y permita enfocar esfuerzos, hacer seguimientos y ver cambios de situaciones en el tiempo.</i>
Objetivo General	Crear un esquema completo para la evaluación de niveles de riesgos y generación de mapas de riesgos de ciberseguridad a nivel nacional.
Objetivos Específicos	Crear un esquema de evaluación de riesgos que contemple el desarrollo de medidas que permitan la comparabilidad interinstitucional de los niveles de riesgos de acuerdo al posible impacto a nivel de la ciberseguridad nacional. Implementar un esquema de integración de datos que permita generar mapas de riesgos multidimensionales, que permita la toma de decisiones informadas para la gestión de amenazas y vulnerabilidades.

Alcance	El alcance de la iniciativa debe ser establecido de acuerdo a las entidades finalmente participantes. Se sugiere que inicialmente se incluyan entidades que pertenezcan inicialmente a uno o dos sectores, de forma que una de las dimensiones a evaluar sea la de sector institucional (dentro del estado).
Entidades Beneficiarias (Posible cliente)	Comisión intersectorial de Ciberseguridad y Ciberdefensa
Impactos Esperados	<i>Mejora de la información existente para la toma de decisiones para la gestión de riesgos desde el ColCERT.</i> <i>Mejora de las estrategias de ciberdefensa al contar con datos integrados de riesgos bajo un esquema apropiado de federación.</i>
Duración estimada	<i>Nueve (9) meses.</i>
Presupuesto estimado	El costo del proyecto, en un estimado del tipo orden de magnitud, es de COP 1,300,000,000.
Resultados Esperados de la iniciativa	Esquema de identificación y evaluación de riesgos de ciberseguridad enfocados a la comparabilidad interinstitucional de los niveles de riesgos de acuerdo al posible impacto a nivel de nacional. Mapas multidimensionales de riesgos de ciberseguridad.
Nivel de confidencialidad de la iniciativa	Restringido



6. NODO DE INNOVACIÓN EN ARQUITECTURA TI

La arquitectura de tecnologías de información en el marco del Subsistema de Innovación, es fundamental para lograr que las TIC en uso del gobierno, soporten de manera eficiente los procesos y las operaciones de las entidades. De esta manera, el objetivo fundamental es alinear las estrategias con la infraestructura de comunicación, la tecnología y los servicios de información que las apoyan.

El Nudo de Innovación de Arquitectura TI, como un escenario para el punto de encuentro y de desarrollo de proyectos conjuntos de la industria, gobierno, academia enfocados en los usuarios, tiene como objetivo general definir el entorno y las condiciones de los modelos de negocio²⁷ y de TI, tanto actuales como deseados, para establecer un camino de transición que permita:

- Optimizar las interdependencias entre los procesos de las entidades y las TI que las soportan.
- Optimizar la interacción entre las diferentes entidades públicas y de estas con la ciudadanía, las empresas y demás entidades privadas.

Estos modelos permitirán interacciones entre entidades del gobierno con un interés común en segmentos específicos, donde podrán generarse incrementos de eficiencias y economías de escala. De esta forma las entidades y los sectores tendrán un marco único de referencia para definir las arquitecturas de los negocios, los sistemas de información y la apropiación de TIC con mejor desempeño para el cumplimiento de las metas.

Al implementar una arquitectura de TI soportado en modelos de arquitectura empresarial se tiene como objetivo lograr que los procesos de negocio de las entidades de gobierno sean más efectivos en su misión, que logren las metas estratégicas propuestas y que puedan responder de forma apropiada a los cambios del entorno.

6.1 IDENTIFICACIÓN DE BRECHAS

Tomando como base las iniciativas de proyectos planteadas en el programa de Gobierno en línea (Gobierno en Línea, 2010), se establecieron los marcos de referencia que permitan desarrollar, mantener y facilitar la implementación de las arquitecturas empresariales para cada una de aquellas iniciativas (que se recogen en la Tabla 3). Estos marcos se utilizarán para realizar el análisis de brechas en Arquitecturas de TI y Arquitecturas Empresariales que se creen o implementen a nivel de los procesos de gobierno.

²⁷ Entendiendo como modelos de negocio en el caso de gobierno los procesos operacionales y de servicio que se realizan para el desarrollo de la misión en las entidades

Tabla 10: Iniciativas de proyecto de gobierno en línea y su relación con arquitectura empresariales.

INICIATIVA DE PROYECTOS DE GOBIERNO EN LINEA	MARCOS DE REFERENCIA PARA ARQUITECTURAS EMPRESARIALES
Definición de un modelo colaborativo y participativo que incentive la participación ciudadana, a través de los canales y medios disponibles, tales como las redes sociales	Modelo de Colaboración y participación ciudadana
Optimización de los procesos en las entidades apoyados en el uso de la tecnología en su gestión documental.	Modelo para optimización de procesos
Interoperabilidad para facilitar el intercambio de información en y entre entidades.	Modelo de interoperabilidad
Una estrategia para la apertura de datos que permita el desarrollo de nuevos servicios y la participación de otros actores en el desarrollo económico del país.	Modelo de Datos abiertos
Definición de estándares de seguridad para la gestión de información por parte de las entidades.	Modelo de seguridad de la información
Computación por demanda que permita el aprovechamiento de los recursos.	Modelos de servicios computacionales
Adecuación de la metodología de monitoreo y evaluación del Programa GEL que refleje el grado de avance de las entidades frente al modelo de madurez propuesto en la versión 3 del Manual de Gobierno en línea.	Modelo de Inteligencia competitiva país

Fuente: CINTEL (2011)

6.1.1 Estado Actual en el mundo

A nivel mundial existe un amplio consenso sobre la construcción de e-gobierno, no obstante, la definición de la arquitectura del e-gobierno no ha sido claramente definida y frecuentemente ésta se relaciona con los términos “Marco de interoperabilidad” y “Arquitectura de referencia”. Sin embargo la modernización de las estructuras de gobierno, los marcos de gobernanza y los procesos, requieren de una arquitectura extensiva que evolucione y que evite la duplicación innecesaria de infraestructura, que aumente los componentes y que integre procesos, servicios y actividades dispares (Escobar Moreno & Et.Al, 2007).

El primer aspecto fundamental en la concepción de la arquitectura para gobierno es distinguir entre dos dimensiones de la incorporación de TIC en el gobierno: vertical en términos del nivel de gobierno (regional,



local o por industria) y horizontal en términos de los procesos internos y externos del gobierno. (Beynon-Davies, 2004). En este aspecto la arquitectura debe contemplar que (Song & Hee, 2006):

1. El sistema de e-gobierno en su totalidad consiste en múltiples partes (subsistemas) organizadas en forma vertical y en jerarquía
2. En este sistema el flujo de recursos entre las partes del gobierno tanto a nivel vertical como horizontal tiene entradas, proceso, resultados y retroalimentación. Los recursos que se mueven en el sistema, no sólo los físicos (como personas o información), sino también los intangibles (como demandas, soporte, y expectativas de las personas).
3. El sistema es abierto al entorno externo e interactúa activamente con éste. La flexibilidad de la interacción con el entorno permite al sistema mejorar sus habilidades de adaptación.

Por otra parte, una arquitectura de e-gobierno debe representar como las entidades públicas con varios sistemas TI y elementos de gestión trabajan juntas como un todo en el marco de:

- Procesos de negocios
- Información/datos,
- Aplicaciones e Infraestructura tecnológica.

En este sentido cobran relevancia los marcos de interoperabilidad que se refieren a un set de estándares adoptados por una organización y los cuales deben ser implementados para aplicaciones o sistemas en miras a intercambiar datos bajo un mismo formato (Escobar Moreno & Et.Al, 2007). Consecuente con lo anterior, la interoperabilidad de los sistemas es la base de la construcción de una plataforma adecuada de gobierno y TIC, en este sentido la interoperabilidad debe ser abordada sobre la base de estándares de comunicación con cuatro dimensiones (Papazoglou & Ribbers, 2006):

- **Estándares de tecnología:** Concerniente a middleware, protocolos de red, protocolos de seguridad entre otros
- **Estándares de Sintaxis:** Se refiere a qué redes de organización se agregan y cómo integrar aplicaciones heterogéneas basadas en una estructura de lenguaje para el intercambio de mensajes.
- **Estándares de Semántica:** Constituyen un acuerdo adicional a los acuerdos de sintaxis ya establecidos, el cual contiene los términos usados por un sistema de información de una entidad para comunicarse y entender los mensajes de otro sistema de información. La interoperabilidad de la semántica es el activo principal en la integración.
- **Estándares de practicidad:** son acuerdos en prácticas y protocolos direccionados por mensajes, tales como especificaciones de órdenes y entregas.

6.1.1.1 Modelos de Arquitectura Empresarial para Gobierno a Nivel Mundial

Una arquitectura empresarial explica cómo los sistemas de información, los procesos, las unidades organizacionales y las personas en una organización funcionan como un todo. La arquitectura empresarial puede funcionar como una sombrilla, la cual describe y explica la relación entre proyectos, tanto en adquisiciones de sistemas como en la gestión del cambio. Los modelos de arquitectura, los principios y los

estándares forman el contenido de una Arquitectura Empresarial (Finish Enterprise Architecture Research Project, 2007).

En el contexto del gobierno, la arquitectura empresarial es referenciada como Arquitecturas Empresariales Nacionales (NEA) o Arquitecturas Empresariales Federales (FEA)²⁸, en estas la administración pública es vista como una colección de organizaciones heterogéneas que tienen diferentes procesos de negocio y sistemas de información. La arquitectura sirve especialmente para asegurar la interoperabilidad de estos sistemas sin alterar el campo específico de administración. La necesidad de una arquitectura empresarial se hace imperativa cuando el número de sistemas de información se incrementa y los procesos de servicio comienzan a requerir el intercambio de información entre autoridades (Finish Enterprise Architecture Research Project, 2007).

Tomando como base el trabajo realizado por el proyecto de investigación en arquitecturas empresariales del gobierno de Finlandia se presenta²⁹ una comparación de diferentes NEA de gobiernos líderes en e-gobierno, bajo los siguientes criterios (Finish Enterprise Architecture Research Project, 2007):

1. **Políticas, actores y estructura:** Directrices y entorno político de cada NEA. Los objetivos estratégicos para arquitectura son provistos por actores políticos y consecuentes con las estructuras democráticas.
2. **Gobernanza:** Modelo de gobernanza y prácticas que son necesarias para mantener la arquitectura actualizada. Las guías de gobernanza también puede motivar un comportamiento deseado en la arquitectura.
3. **Framework de arquitectura y metodologías:** Definición de NEA, el Framework usado y los procesos de arquitectura
4. **Principios y estándares de arquitectura:** Estándares, principios y guías usadas para implementación y gestión del cambio.
5. **Implementaciones:** Implementación de NEA a través de proyectos transversales al sector público
6. **Ventajas/Desventajas:** Beneficios en operación y su medición, experiencias y utilidad, o características especiales a resaltar de cada NEA en operación.

Los países considerados en la revisión se encuentran entre los 20 países líderes en desarrollo de e-gobierno, estos son:

1. República de Corea
2. Estados Unidos de América
3. Canadá
4. Reino Unido
5. Holanda
6. Noruega
7. Dinamarca

²⁸ Específicamente para el caso del gobierno de Estados Unidos.

²⁹ Ver Tabla 8, Tabla 9 y Tabla 10



8. Suecia
9. Nueva Zelanda
10. Alemania
11. Bélgica
12. Japón
13. Suiza
14. Finlandia
15. Estonia

La comparativa entre Arquitecturas Empresariales Nacionales de los países líderes se presenta a continuación³⁰:

REPUBLICA DE COREA

Políticas, actores y estructuras: La política ha sido definida por la oficina presidencial y desarrollada por el Ministerio de Comunicaciones, y la agenda de implementación es controlada por un comité de proyectos dependientes de la presidencia. El presidente lidera proyectos estratégicos e incluso responde por las modificaciones y el mejoramiento del sistema. (Song & Hee, 2006)

Gobernanza: Debido a que el proyecto es liderado por el presidente el sistema reduce las dificultades para motivar el uso. La secretaria de estado también recibe reportes y provee directrices para todos los tomadores de decisión a través del sistema. (Song & Hee, 2006)

Frameworks de arquitecturas y metodologías: NEA está definida para cubrir los siguientes aspectos fundamentales (MOGAHA, 2005):

1. Procedimientos de digitalización de documental
2. Exhaustiva informatización de las finanzas públicas y nacionales
3. Realización de e-gobierno local
4. Construcción de un sistema de e-auditoria
5. Realización de las e-asamblea nacional
6. Construcción integrada del sistema de justicia criminal
7. Exhaustiva informatización de la gestión de recursos humanos
8. Sistema de diplomacia electrónica
9. Gestión de la agenda nacional en tiempo real
10. Expansión de información administrativa compartida

³⁰ Fuente: CINTEL. 2011. Adaptado de: (Finish Enterprise Architecture Research Project, 2007)

11. Desarrollo del modelo de referencia para negocios de gobierno

Principios de arquitectura y estándares: Se plantearon tres objetivos de gobierno (MOGAHA, 2005):

1. Democracia para el pueblo,
2. Desarrollo Social Balanceado, y
3. Era de paz y prosperidad en el norte de Asia.

Sobre estos, los siguientes principios:

1. Confianza y principios,
2. Justicia y Transparencia,
3. Diálogo y compromiso,
4. Descentralización del poder y autonomía

Implementaciones: Los hitos claves de implementación fueron (MOGAHA, 2005):

- Construir una agencia nacional de computación e información a nivel de gobierno
- Fortalecer las redes de comunicación para e-gobierno
- Establecer una agencia nacional de tecnologías de la información a nivel nacional
- Construcción de un sistema de seguridad informática
- Restructuración de la informatización de organizaciones y personal
- Restructuración de la gestión de los recursos de información centrados en un entorno digital integrado,
- Restructuración de los roles y funciones del portal de gobierno electrónico
- Mejorar la accesibilidad de los servicios públicos
- Unir y coordinar información compartida para tareas relacionadas

Ventajas/ Desventajas: La larga historia de implementación de e-gobierno en Corea ha derivado en sus fortalezas. Asimismo la gobernanza favorecida por el liderazgo que en este proceso ejerce la presidencia también ha influido en su consolidación. La creación de una infraestructura común para los órganos de gobierno (incluyendo grandes centros de datos únicos) ha facilitado la interoperabilidad y la operación de la arquitectura de gobierno.

ESTADOS UNIDOS

Políticas, actores y estructuras: La política fue definida por el congreso y la implementación es controlada por un programa operacional configurado por el presidente. El programa operacional federal es implementado por la Oficina de Gestión y Presupuesto. Cada ministerio implementa el programa bajo el control de la Oficina de Contabilidad Gubernamental. Las iniciativas de orden local vienen de los gobernadores.

Gobernanza: Existe una legislación en adquisiciones públicas de TI. El modelo de gobernanza está basado en un Framework de Evaluación llamado Enterprise Architecture Management Maturity Framework (EAMMF), usado para evaluar la madurez administrativa desde una perspectiva de arquitectura.



La oficina de contabilidad gubernamental (GAO) evalúa el progreso del programa de arquitectura cada dos años. La oficina de gestión y presupuesto (OMB) reporte el logro de beneficios y provee instrucciones. Además el Consejo responsables de oficinas de información (CIOCI) da recomendaciones al Grupo de Trabajo de Arquitectura Federal (FAWG)

Frameworks de arquitecturas y metodologías: NEA está definida para cubrir tanto tecnologías como negocio. Contiene modelos que son usados para modelar las operaciones de las organizaciones. La descripción incluye el estado presente, los estados objetivos y una estrategia. El Framework usado incluye aspectos de TOGAF, FEAF y FEA. Con el Modelo de Referencia de Datos v 2.0, el Instituto Nacional de Estándares y Tecnología (NIST) ha formulado una directriz de estándar, la cual combina indicadores de desempeño para una agencia orientados a los resultados de operación y la seguridad. La descripción completa está en el Modelo de Referencia Consolidado (CRM) el cual incluye:

- Modelo de referencia para el desempeño
- Modelo de referencia de negocio
- Modelo de referencia de componentes de servicio
- Modelos de referencia técnica
- Modelos de referencia de datos

Principios de arquitectura y estándares: La legislación controla la operación de NEA. La resolución de Resultados y Desempeño del Gobierno (GPRA), conecta los procesos presupuestales de ramas administrativas y agencias, y las obliga a seguir indicadores de desempeño. La resolución Clinger-Cohen obliga procesos de reforma para implementarse antes de los sistemas de adquisiciones. La resolución de e-gov define los principios de e-gobierno, incluyendo prácticas de seguridad en las agencias, responsabilidades de reporte y el control federal. Un portal web define los componentes universales usados en arquitectura, así como las responsabilidades en su mantenimiento.

Implementaciones: Cada rama administrativa puede llevar sus propios proyectos en conformidad con los modelos de NEA y los principios de las resoluciones GPRA y Clinger-Cohen. La implementación es monitoreada por la OMB la cual tiene autoridad presupuestaria. Las recomendaciones de implementación de cada rama administrativa provienen de la OMB.

Las guías del Framework Federal de Transición (FTF) han sido desarrolladas para los proyectos transversales del sector público.

Ventajas/ Desventajas: El análisis costo-beneficio es comúnmente usado

Los indicadores clave de desempeño son cada vez más comunes y permiten ahorrar costos.

Esta arquitectura es considerada la más avanzada. Enfocada a ramas administrativas específicas, aunque no motiva directamente los proyectos transversales del sector público. A nivel federal su implementación ha sido rigurosa, pero a nivel local aún es baja y bastante dispersa.

CANADÁ

Políticas, actores y estructuras: La División de Arquitectura Empresarial y Estándares, la cual esta subordinando al Departamento del Tesoro es la encargada de la operación de NEA. El objetivo es incrementar la unidad del gobierno.

Gobernanza: El programa no es obligatorio para las partes, razón por la cual son las regiones las que deciden acogerse a este.

Frameworks de arquitecturas y metodologías: Canadá aplica un modelo de referencia en línea con la Arquitectura Orientada a Servicios – SOA. La división de arquitectura empresarial y estándares es responsable por el diseño, desarrollo e implementación de arquitectura empresarial y estándares.

Principios de arquitectura y estándares: El kit de herramientas de la arquitectura empresarial consiste en dos partes: 1) Modelos de referencia estratégicos del gobierno de Canadá, y 2) Metodología de transformación.

Implementaciones: Énfasis en el uso de la arquitectura orientada a servicios.

Ventajas/ Desventajas: No están definidos indicadores para la evaluación de la arquitectura en operación.

El problema con la NEA en operación es la carencia de autorización, y la ausencia de una visión holística en colaboración entre diferentes organizaciones gubernamentales

REINO UNIDO

Políticas, actores y estructuras: La unidad de eGobierno (eGov) es responsable por la implementación y desarrollo de la estrategia. El consejo de jefes de oficinas técnicas es la organización transversal de gobierno responsable por incrementar la cooperación a nivel tecnológico.

Gobernanza: El seguimiento total de las prácticas y especificaciones del e-Government Interoperability Framework (e-GIF) es obligatorio.

Frameworks de arquitecturas y metodologías: e-GIF define las políticas técnicas de gobierno y las especificaciones para lograr la interoperabilidad y la coherencia entre los sistemas TIC a través del sector público. e-GIF contiene un Framework y un registro. La primera versión de una Arquitectura Empresarial Transversal de Gobierno (xGEA) ha sido recientemente publicada.

Principios de arquitectura y estándares: El catálogo de estándares técnicos define un grupo mínimo de especificaciones que conforman las políticas técnicas definidas en el e-GIF.

Implementaciones: e-GIF está en uso, pero la adopción de xGEA está iniciando. Las ramas administrativas tienen sus propios programas de arquitectura empresarial que son parcialmente compatibles.



Ventajas/ Desventajas: Algunos objetivos no han sido alcanzados (en participación, democracia e incremento de la inclusión).

e-GIF se ha propagado a varios países. La operación extensiva de la arquitectura está comenzando.

HOLANDA

Políticas, actores y estructuras: El ministerio de modernización e innovación del gobierno está a cargo de la operación de NEA. El objetivo principal es reducir la burocracia para compañías y agencias.

Gobernanza: El uso de NEA no es obligatorio y las agencias son libres de diseñar su propia arquitectura siguiendo cualquier modelo. No obstante, equipos de soporte al cambio han sido creados para ayudar a las agencias en su adopción de AE.

Frameworks de arquitecturas y metodologías: Una versión simplificada del modelo de Zachman es usado para estructurar los principios de arquitectura. El programa NEA no usa un modelo de arquitectura, pero a nivel de agencias públicas locales han adoptado una variedad de modelos de arquitectura

Principios de arquitectura y estándares: NEA contienen un grupo de principios y guías de alto nivel. Los esfuerzos son principalmente basados en consensos. El uso de estándares abiertos es promovido en algunas áreas.

Implementaciones: La arquitectura orientada a servicios SOA es el paradigma dominante. Componentes de software estandarizados son desarrollados y usados en la operación de NEA.

Ventajas/ Desventajas: La interoperabilidad entre las agencias depende altamente de los sistemas de información diseñados con SOA. Programa de arquitectura no exhaustivo. La arquitectura no considera objetivo de largo plazo.

A continuación se presenta la comparación de Arquitecturas Empresariales Nacionales de Noruega, Dinamarca, Suecia, Nueva Zelanda, Alemania:

NORUEGA

Políticas, actores y estructuras: El Ministerio de Administración y Reforma del Gobierno es el responsable del desarrollo y estrategia de TIC.

Gobernanza: Está en construcción un modelo de gobernanza como parte de NEA.

Frameworks de arquitecturas y metodologías: La arquitectura está basada en un modelo por capas compuesto por una capa de presentación, una capa de componentes comunes y una capa de negocio.

Principios de arquitectura y estándares: Fuerte énfasis en estándares abiertos y software abierto. NEA incluye estándares técnicos, conceptuales, organizacionales y procedimentales.

Incluye además una librería de componentes compartida.

Implementaciones: Inicio su implementación en 2008 por lo que su valoración aún no está determinada.

Ventajas/ Desventajas: Inicio su implementación en 2008 por lo que su valoración aún no está determinada.

Inicio su implementación en 2008 por lo que su valoración aún no está determinada.

DINAMARCA

Políticas, actores y estructuras: El ministerio de ciencia, tecnología e innovación es el responsables de las iniciativas de NEA en colaboración directa con las municipalidades danesas y el ministerio de finanzas. El enfoque está en la interoperabilidad así como la seguridad, apertura, flexibilidad y escalabilidad.

Gobernanza: El modelo de gobernanza de NEA está basado en iniciativas. Las agencias son libres de planear su propia arquitectura. La adopción de NEA no está obligada por ley o regulación alguna.

Frameworks de arquitecturas y metodologías: La arquitectura incluye Frameworks de: principios, métodos, herramientas y control. Esta arquitectura está basada en el Framework de Zachman.

Principios de arquitectura y estándares: NEA incluye una selección de estándares, el diseño de un modelo de referencia y los principios para establecer unos elementos comunes de infraestructura.

Fuerte énfasis en estándares abiertos disponibles públicamente.

El Framework de interoperabilidad ha sido creado en concordancia con el European Interoperability Framework.

Implementaciones: Dominada orientación a SOA.

Desarrollo e implementación de componentes de software estandarizados es incidental.

Ventajas/ Desventajas: Metas conceptuales han sido reportadas, pero no se ha reportado el logro real de las mismas. Solo un limitado grupo de indicadores ha sido usado.

La mayor ventaja del programa de NEA es que toma la interoperabilidad como punto central. Desafortunadamente no existe un modelo fuerte de gobernanza lo que ha implicado problemas en la implementación de NEA.

SUECIA

Políticas, actores y estructuras: La agencia sueca para el desarrollo administrativo es la responsable de coordinar el desarrollo del gobierno central.

Gobernanza: La gobernanza es descentralizada y cada cuerpo administrativo es responsable de sus propios proyectos de e-gobierno.



Frameworks de arquitecturas y metodologías: No existe en concreto un modelo de arquitectura específico, no obstante existe bastantes adelantos en la arquitectura para e-health.

Principios de arquitectura y estándares: Estos corresponden a los dictados por la agencia sueca para el desarrollo, pero no corresponden a un modelo de arquitectura como tal (Gotze & Christiansen, 2009)

Implementaciones: No existe una medición concreta del éxito de los proyecto de e-gobierno.

Ventajas/ Desventajas: Actualmente los proyectos de e-gobierno se encuentran desconectados sin facilidades del gobierno central.

Los beneficios de una arquitectura nacional no han sido logrados por la carencia de un modelo de arquitectura y gobernanza propiamente dichos.

NUEVA ZELANDA

Políticas, actores y estructuras: El departamento de tecnologías de la información y las comunicaciones operando bajo la comisión de servicios estatales está a cargo de la implementación de la estrategia de e-gobierno. Las metas incluyen: a) apropiación y satisfacción, b) integración y eficiencia, c) confianza y participación.

Gobernanza: La arquitectura empresarial incluye una arquitectura a nivel nacional y arquitecturas propias por agencia. Al tiempo nuevas responsabilidades son nombradas y la gobernanza y las finanzas incrementan. Varios comités han sido configurados para apoyar a las ramas administrativas transversales de gobierno.

El uso del e-Government Interoperability Framework (e-GIF) es obligatorio para algunas partes del gobierno y recomendadas para otros.

Frameworks de arquitecturas y metodologías: La arquitectura empresarial está definida como la utilización de una práctica y un método extensivo para modelar la estructura de procesos, sistemas de información, personal y unidades organizacionales actuales y futuros de una organización, en una forma que estos se alineen con los objetivos centrales y las estrategias de la organización.

El e-GIF es una colección de prácticas, estándares y fuentes de información que soportan los sistemas TI de Nueva Zelanda.

Principios de arquitectura y estándares: NEA está basado en una arquitectura empresarial federada. e-GIF motiva el uso de estándares abiertos.

Implementaciones: Inicio su implementación en 2007 por lo que su valoración aún no está determinada.

Ventajas/ Desventajas: La evaluación ha sido llevada a cabo, descubriendo el cumplimiento con las metas.

Un exhaustivo enfoque de NEA y una documentación extensiva ha sido positivo.

ALEMANIA

Políticas, actores y estructuras: La responsabilidad de e-gobierno recae en el Ministerio Federal del Interior. El ministerio ha configurado una oficina de dirección TI.

El programa NEA (SAGA - Standards and Architectures for eGovernment Applications) se enfoca en la reducción de costes y el mejoramiento de la eficiencia. Se ha propuesto la importancia de los servicios federales de e-gobierno para negocios y ciudadanos en términos de cantidad y calidad.

Gobernanza: El programa de arquitectura nacional está centrado y coordinado por el Ministerio Federal del Interior. SAGA es una guía obligatoria para las agencias federales.

Frameworks de arquitecturas y metodologías: El programa de arquitectura está basado en el modelo de referencia ISO para sistemas para procesamiento abierto distribuido (RM-ODP) y considera empresa, información, computación, ingeniería, y perspectivas de tecnología.

Principios de arquitectura y estándares: NEA guía el uso de estándares conceptuales y técnicos en diseño e implementación. Los objetivos son interoperabilidad, reusabilidad, apertura, escalabilidad, y reducción de costos y riesgos. El uso de estándares y software abierto es enfatizado. NEA cumple con los requerimientos del European Interoperability Framework.

Implementaciones: SAGA sigue el uso de paradigmas basados en componentes y arquitecturas orientadas a servicios.

Ventajas/ Desventajas: Las metas son documentadas y los beneficios son calculados, esto ha permitido conocer el trabajo de arquitecturas previas. Se busca evaluar las metas financieras anualmente con un cálculo de costo – beneficio. SAGA se enfoca particularmente en la arquitectura técnica.

BELGICA

Políticas, actores y estructuras: Los actores clave en e-gobierno son: FEDICT (Servicio público federal de TIC) Ministerio del Interior y la Secretaria de Estado para la Simplificación de la Administración. FEDICT tiene el rol de coordinador. La estrategia de e-gobierno busca crear una administración pública virtual simple. Los objetivos son la diseminación de la información y al redefinición de los procesos de negocio.

Gobernanza: El modelo de gobernanza federal es descentralizado.

Frameworks de arquitecturas y metodologías: Formalmente no existe un modelo de arquitectura específico para implementación en las agencias.

Principios de arquitectura y estándares: Un catálogo de servicios, el cual es una lista de productos y servicios de FEDICT.



El uso de estándares abiertos y/o especificaciones comunes es obligatorio y el uso de software de código abierto es aconsejado en el gobierno.

Implementaciones: La implementación se hace a través de proyectos individuales de e-gobierno.

Ventajas/ Desventajas: Un Framework para la evaluación de progreso en e-gobierno es usado. Esto permite evaluar el grado de contribución estratégica, los beneficios potenciales y el grado de urgencia de inversiones en ICT.

No existe una arquitectura empresarial nacional formal, esto implica que la evaluación se realiza con la poca información común disponible.

JAPÓN

Políticas, actores y estructuras: El objetivo de la estrategia de e-Japón es hacer al país más avanzado en el mundo en el estado de TI. Además, se busca mejorar la calidad de los servicios públicos y la eficiencia del trabajo administrativo. Un plan estratégico de cinco años es publicado lanzando en 2006 un programa NEA que busca renovar los procesos de negocio y los sistemas en la administración pública.

Gobernanza: Un proyecto para una oficina de gestión gobierno y un proyecto para una oficina de control han sido establecidos para ayudar la gobernanza. El propósito de estas oficinas es soportar la eficiencia de las iniciativas IT a través del sector público. El uso de los Framework de arquitectura y procesos es obligatorio.

Frameworks de arquitecturas y metodologías: El programa de NEA contiene un Framework de arquitectura tecnológica y un Framework de procesos.

Principios de arquitectura y estándares: Las reformas deben estar acompañadas por un plan de optimización, el cual describe los retos y metas del uso de TI, así como una evaluación de los ahorros en tiempo y costo logrados con las reformas. Las metas incluyen, por ejemplo, transición a sistemas abiertos y subcontratación de procesos de negocio.

Implementaciones: La implementación se hace a través de proyectos individuales en cada agencia de gobierno.

Ventajas/ Desventajas: Un comité de evaluación gubernamental compuesto por expertos de TI evalúa los procesos de negocio y los proyectos de optimización de sistemas ministeriales. El comité mejora la evaluación del costo-beneficio y si es necesario, aconseja la planeación, desarrollo, uso y evaluación de los sistemas.

La evaluación de arquitectura es difícil debido a la poca información específica disponible.

SUIZA

Políticas, actores y estructuras: El Departamento de Finanzas es el responsable por la planeación e implementación de la estrategia de e-gobierno.

El Consejo Federal de TI tiene la responsabilidad sobre la estrategia general de uso de TIC en la administración federal y la Unidad Estratégica Federal para TI crea la estrategia, los programas, la arquitectura y los estándares.

La Arquitectura Empresarial Nacional (denominada SAGA.CH) se enfoca en hacer las actividades administrativa tanto eficientes, económicas y centradas en las personas les sea posible en toda de Suiza.

Gobernanza: La responsabilidad de NEA se encuentra en el Departamento de Finanzas, y debe ser usado tanto en administraciones federales como locales.

Frameworks de arquitecturas y metodologías: El programa está basado en el Framework TOGAF para el desarrollo de arquitectura. NEA contiene los principios, estándares, herramientas, criterios de evaluación, consideraciones de procesos y vistas estructurales.

Principios de arquitectura y estándares: El uso de estándares abiertos y software abierto es promovido. NEA cumple con los requerimientos del European Interoperability Framework y los principios del programa i2010.

Implementaciones: SAGA.CH sugiere el paradigma de arquitectura orientada a servicios para la implementación de aplicaciones de e-gobierno.

Ventajas/ Desventajas: La arquitectura define criterios y medidas para evaluar la calidad de las soluciones de e-gobierno. La medición está relacionada al desempeño, la eficiencia y los costos.

Se cuenta con un programa de arquitectura bastante extenso.

FINLANDIA

Políticas, actores y estructuras: NEA es desarrollado por el Ministerio de Finanzas. El Consejo de Estado reconoce los sistemas de información compartida, la tecnología común básica, los servicios compartidos, y los procesos transversales en el sector público como áreas claves de enfoque.

Gobernanza: El modelo de arquitectura incluye un modelo de gobernanza.

Frameworks de arquitecturas y metodologías: El Framework cubre cuatro puntos de vista comunes (negocios, información, aplicaciones y tecnología) los cuales son soportado en varias maneras usando Frameworks (FEA, TOGAF, IEF y E2AF). Aunque el método de arquitectura esta en concordancia con los procesos de TOGAF.

Principios de arquitectura y estándares: La arquitectura incluye un modelo de madurez basado en los modelos CMM y NASCIO. A nivel de gobierno la arquitectura esta en concordancia con el EIF. El modelo de referencia de desempeño es adaptado del Framework de rentabilidad de la administración en el análisis de costo –beneficios.

Implementaciones: La implementación del plan se inició a finales de 2007, los proyectos piloto iniciaron ese año.



Ventajas/ Desventajas: Un modelo de análisis de costo – beneficios está incluido como parte de la arquitectura.

El éxito depende del éxito en cada una de las fases de implementación.

ESTONIA

Políticas, actores y estructuras: La responsabilidad principal es llevada por el Departamento de Estado para Sistemas de Información y el Centro de Informática de Estonia, los cuales funcionan bajo el Ministerio de Asuntos Económicos y de Comunicación. Los ministerios y las municipalidades tienen sus propios consejos. La Sociedad Estratégica de Información tiene tres objetivos: 1) desarrollo de sociedad inclusiva centrada en el ciudadano, 2) desarrollo de economía basada en el conocimiento, y 3) desarrollo de administración pública centrada en el ciudadano, transparente e eficiente.

Gobernanza: La coordinación del sistema no es jerárquica. El seguimiento del Framework de interoperabilidad y sus documentos relacionados es obligatorio, pero no forzado por alguna ley.

Frameworks de arquitecturas y metodologías: No existe formalmente una arquitectura empresarial nacional. No obstante el Framework de Interoperabilidad cubre tres perspectivas: Organizacional, Semántica y Técnica.

Principios de arquitectura y estándares: El proyecto X-Road, el cual está basado en una arquitectura orientada a servicios, dan forma a la creación de un espacio común de servicios. Para asegurara la interoperabilidad, los estándares abiertos y especificaciones son usadas en los sistemas de información. De acuerdo a las posibilidades son aplicadas soluciones de código abierto.

Implementaciones: El rol de X-Road en el desarrollo de e-servicios ha sido significativo para la implementación del GIF.

Ventajas/ Desventajas: Se han definido indicadores en la estrategia para cada objetivo. Además cada objetivo es analizado y evaluado anualmente por un grupo experto.

Sistemas de coordinación no jerárquicos y descentralizados reta el desarrollo de una arquitectura a nivel nacional.

La siguiente tabla presenta un análisis comparativo entre los países considerados en la revisión (hallados entre los líderes en desarrollo de e-gobierno, de acuerdo con el estudio de Overview of Enterprise Architecture work in 15 countries (Ministry of Finance- Finland Research reports 6b/2007) e incluida la República de Corea por su avance en el tema de aplicación de arquitecturas de tecnología en gobierno. Para efectos del análisis, la primera fila identifica los modelos y programas implementados en primeras fases de los programas de gobierno en la mayoría de ellos previo a la implementación de programas de Arquitectura Empresarial Nacional. La segunda fila identifica el avance en el desarrollo de las National Entreprices Architecture (NEA).

Las filas identifican las temáticas relevantes sobre las cuales fueron proyectadas como objetivos estratégicos en la implementación de sus NEA. El esquema de puntos ubicados en los cuadros indica que el modelo se prioriza por las temáticas marcadas.

Tabla 11. Relación entre países que están aplicando Arquitectura Empresarial Nacional (NEA) desde gobierno y las principales temáticas abordadas

	NORUEGA	SUECIA	DINAMARCA	HOLANDA	INGLATERRA	ALEMANIA	CANADA	EU	NUEVA ZELANDA	KOREA
Metodología preelminares		Service Oriented Architecture (SOA)	Danish Interoperability Framework		e-Government Interoperability Framework (e-GIF)	SAGA (Standards and Architectures for eGovernment Applications)	The Government of Canada Service-Oriented Architecture Strategy		interoperability framework for e-government e-GIF	Technical Standard on interoperability for public IT project (2002)
Desarrollo de National Enterprise Architecture- NEA	NEA basado modelo de capas: presentación, componentes comunes y de negocio	No hay iniciativas para NEA	OIO (Offentlig Information Architecture NEA)	Version simplificada del modelo Zachman	Version publicada de Cross-Government Enterprise Architecture (xGEA)	German National Enterprise Architecture (NEA)	in diseño por The Enterprise Architecture and Standards Division	TOGAF, FEAF and FEA With the Data Reference Model v 2.0, the NIST (National Institute of Standards and Technology)	En diseño NEA will be based obasado en Federated Enterprise architecture.	NEA- Government-wide enterprise architecture framework
PRIORIZACIÓN TEMÁTICA										
Interoperabilidad	*	*	*		*	*	*		*	*
Calidad de servicios ciudadano (confianza, participación)		*							*	
Eficiencia de uso TIC pública			*		*	*	*			
Estandares abiertos	*		*	*						*
Promision desarrollo arquitecturas comunes					*					
Adquisición TI (reducción de riesgos y presupuestos)					*	*		*		
Operaciones y seguridad								*		
Justicia y transparencia										*

Fuente: Finnish Enterprise Architecture Research Project- Finlandia - CINETEL. 2011

6.2 ESTADO ACTUAL EN COLOMBIA

Específicamente en arquitectura de TI, Colombia no ha establecido un marco para el diseño e implementación de Arquitecturas Empresariales (AE) en las entidades de gobierno, y no existe una Arquitectura Empresarial Nacional que contenga modelos de referencia. No obstante, como se evidenció en la revisión de países líderes en e-gobierno, la primera fase de la construcción de una NEA está fundamentada en la creación de un marco de interoperabilidad. En este aspecto Colombia ya cuenta con un marco inicial publicado en el año 2009 (Ministerio de Tecnologías de Información y las Comunicaciones, 2010), el cual aún requiere de su fortalecimiento, específicamente en la creación de modelos complementarios de administración y medición que, aunque están contemplados en la agenda de Gobierno en línea, no se ha adelantado su construcción.

Por otra parte uno de los avances ha sido la elaboración de una guía metodológica para la implementación del marco de interoperabilidad que permite a las agencias de gobierno lograr mejores niveles de interoperabilidad medidos bajo un modelo de madurez ya definido. El marco de interoperabilidad actual para Colombia tiene las siguientes características directamente relacionadas con arquitectura empresarial

- **Objetivos y políticas:** Aunque incluidas en el Marco de Interoperabilidad de Gobierno, éstas definen los lineamientos sobre los cuales las entidades locales y nacionales implementan sistemas de TI y



sobre las cuales se genera su articulación. Estos aspectos constituyen un avance para el inicio de la construcción de una Arquitectura Empresarial Nacional.

- **Modelo de gestión en tres pasos:**

- **Modelo de madurez para interoperabilidad:** Este modelo es importante para la medición del avance en la consolidación de interoperabilidad, y en este sentido la evaluación y el conocimiento de los estados actuales de las entidades facilita la implementación de arquitectura empresarial a nivel vertical.
 - **Modelo de administración:** No está aún construido, sin embargo en el marco de arquitectura empresarial la construcción de este modelo debe ser articulado para contemplar la administración para interoperabilidad y adicionalmente para estar inmerso un marco de referencia de negocio y componentes de servicio.
 - **Modelo de medición:** No está aún construido, sin embargo su construcción debe estar inspirada en un marco de referencia para la medición del desempeño de arquitectura empresarial de forma integral.
- **Lineamiento de estándares:** Estos lineamientos ya desarrollados por el programa Gobierno en línea son insumos clave para la construcción del marco de arquitectura tecnológica.
 - **Lineamientos de selección de estándares:** Estos lineamientos ya desarrollados por el programa Gobierno en línea son insumos clave para la construcción del marco de arquitectura tecnológica.
 - **Catálogo de estándares por aspectos semánticos y técnicos:** Este catálogo que ya cuenta con una base (es necesario mencionar que estos catálogos deben ser revisados y actualizados periódicamente) son insumos clave para la construcción del marco de arquitectura tecnológica y de aplicaciones.

6.3 CONCLUSIONES

De acuerdo con los resultados de la observación del estado actual de aplicación de arquitecturas en gobiernos, se hace evidente la tendencia hacia la construcción de modelos de arquitectura de orden nacional.

Según las características encontradas en los diferentes modelos investigados y cruzándolos con los modelos identificados en la sección 6.1.1.1. (basados en las iniciativas e-gobierno), se evidenció que algunos de ellos se encuentran incorporados en la estructura general de las arquitecturas en el cual la interoperabilidad es un objetivo fundamental de su adopción, siendo el segundo de mayor cubrimiento el de la apertura de datos y eficiencia de TIC públicas. Estos modelos permiten el desarrollo de nuevos servicios y la participación de otros actores, entre los que se encuentran:

- **Gobierno:** Tanto a nivel central, donde se juega el rol principal al diseñar e implementar e-gobierno, como a nivel local (regional) donde es requerida la coordinación total de los proyectos para garantizar la conexión horizontal y vertical, los gobiernos locales son quienes reciben las solicitudes de servicios de los usuarios y a su vez demandan servicios al gobierno central, por este motivo se requiere gestionar las tensiones generadas entre el gobierno local que considera los aspectos locales más importantes y el gobierno central cuya prioridad es la provisión de modelos de servicio comunes.
- **Empresas:** Entidades que se convierten en un actor principal del mercado proveedor de soluciones (de TI, Outsourcing, Comunicaciones, etc.) y a su vez son beneficiarios de los servicios de las entidades públicas.

- **Ciudadanos y sociedad civil:** Estos juegan múltiples roles, ya que pueden ser vistos como receptores de servicios, aliados en la provisión de servicios, supervisores de desempeño, y pagadores de impuestos (por lo que esperan eficiencia y calidad en los servicios que demandan al estado). En estos roles la ciudadanía demandara: Valor agregado, Eficiencia, Responsabilidad, Control de Finanzas y Efectividad.

Las interacciones entre estos actores deben estar marcadas por los siguientes modelos:

Tabla 12: Interacciones Electrónicas de e-Gobierno.

	Destino			
		G (Gobierno)	B (Business)	C (Ciudadanos)
Origen	G	G2G Back Office	G2B Resultados de Front Office	G2C Resultados de Front Office
	B	B2G Insumos para el Front Office	B2B e-business	B2C e-business
	C	C2G Insumos para el Front Office	C2B e-business	C2C e-community

Fuente: (Song & Hee, 2006)

Respecto a la implementación o apropiación de estos modelos, en el análisis para Colombia se concluye que aunque varias entidades gubernamentales nacionales o locales pueden haber adelantado procesos de arquitectura empresarial, su no articulación, la falta de comunicación y la carencia de un modelo de referencia para la medición del desempeño a nivel nacional, impiden que se reconozcan sus experiencias como ejemplos de éxito que apoyen la construcción de una Arquitectura Empresarial Nacional.

Por otra parte, Gobierno en línea ha iniciado el proceso de fortalecimiento de su arquitectura empresarial interna, sin embargo aún se requiere establecer y desarrollar los marcos de aplicación de negocios, tecnología, aplicaciones, y desempeño que permitan a las entidades de índole local iniciar acciones de mejoramiento bajo un Framework común que asegure la coherencia general entre los sistemas TI, y que, al mismo tiempo, el sistema sea optimizado en términos de necesidades locales pero con la posibilidad de articularse a nivel nacional. La creación de este Framework de arquitectura común debe mantener una visión de mejoramiento de la calidad, optimización de los recursos y reducción de costos.

Algunos de los gobiernos de los países evaluados presentan estructuración y adaptación de arquitecturas empresariales, mientras que otros lo hacen por medio de *frameworks* para los procesos que inter-operan. La adopción de los *framework*, (estándares, guías o técnicas) identificados en algunos países, no necesariamente establecen que el gobierno posea arquitecturas empresariales y de TI estructuradas, sin embargo, al estar implementadas, facilitan lenguajes y procesos comunes que servirán de insumos fundamentales al momento de la construcción de una Arquitectura de TI de alto nivel.



Para el caso de los países que están soportando sus TI y procesos en una Arquitectura Empresarial estructurada para gobierno, se encuentran establecidos varios modelos y marcos de referencia que definen las condiciones y características de la arquitectura adoptada (Escobar Moreno & Et.Al, 2007).

En este sentido, y en el ámbito de la creación de proyectos innovadores que permitan seguir posicionando a Colombia en el reconocimiento de los avances del programa de Gobierno en línea, el enfoque dado a las temáticas y sub-temáticas de la agenda de innovación, está enmarcada en el diseño y construcción de un Arquitectura Empresarial de gobierno, cuyas características serán descritas en los Vectores de desarrollo de los Nodos de este documento.

Una arquitectura para la interoperabilidad y open-government, representa una ventaja competitiva para el país, no solo por la organización de sus componentes de negocio, tecnología y sistema de información, propios de cada modelo, sino además por que genera nuevos compromisos, nuevos niveles de actuación y sistemas de decisión, y compenetra a todas las entidades del gobierno bajo un lineamiento común. En este sentido la experiencia de Dinamarca (Ministry of Science, Technology and Innovation, 2007) resalta las siguientes características de cambio generados en su desarrollo de la Arquitectura Empresarial para su gobierno:

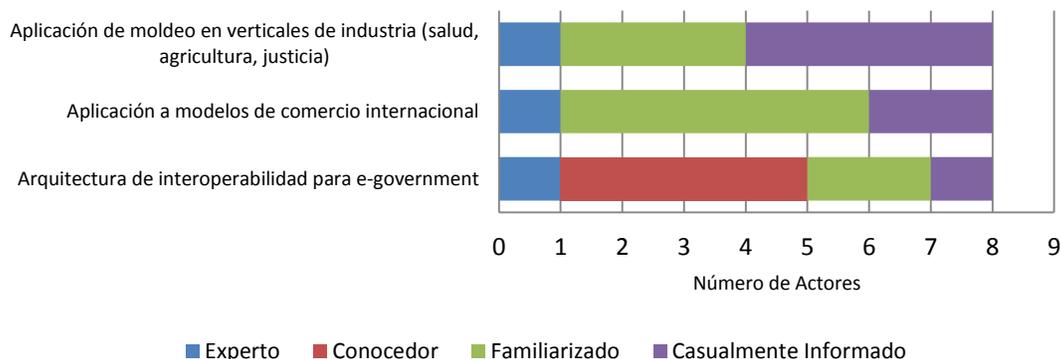
- “El sector público (...) ha tomado mayor responsabilidad activa para su propia Arquitectura Empresarial”.
- Un *framework* común de Arquitectura Empresarial deberá ser establecido para la planificación de los sistemas de TI del sector público, con especial atención en el aseguramiento de la interoperabilidad.
- Esta Arquitectura empresarial deberá ser un esfuerzo concertado para difundir el conocimiento y desarrollar competencias en la Arquitectura Empresarial, especialmente en lo relacionado a la unión de las iniciativas del sector público”.

6.4 RESULTADOS DEL EJERCICIO DE PROSPECTIVA

6.4.1 Caracterización de los actores

La naturaleza de la muestra de actores que diligenciaron los instrumentos para el nodo de Arquitectura TI, estuvo compuesta en total por 8 profesionales, de los cuales 1 pertenecía a entidades del Estado: Ministerio de las Tecnologías de la Información y Comunicaciones, 2 a empresas: Ethos Soluciones de Software y un Consultor en IT Strategy y 5 a la Academia: Universidad de los Andes, Universidad Antonio Nariño, Universidad Nacional sede Medellín, Politécnico Gran Colombiano y Centro de Investigación I2DCorp. En relación con el nivel de formación de los participantes uno de ellos cuenta con título de pregrado, 2 de especialización y 5 de maestría. Por otro lado, la información suministrada por los expertos permitió determinar en un primer momento, el nivel de conocimiento de los participantes en relación a las 3 líneas estratégicas identificadas para el nodo de Arquitectura TI, tal como se presenta en la Figura 40.

Figura 40 Nivel de Conocimiento de los Expertos con relación a las líneas estratégicas de Arquitectura IT



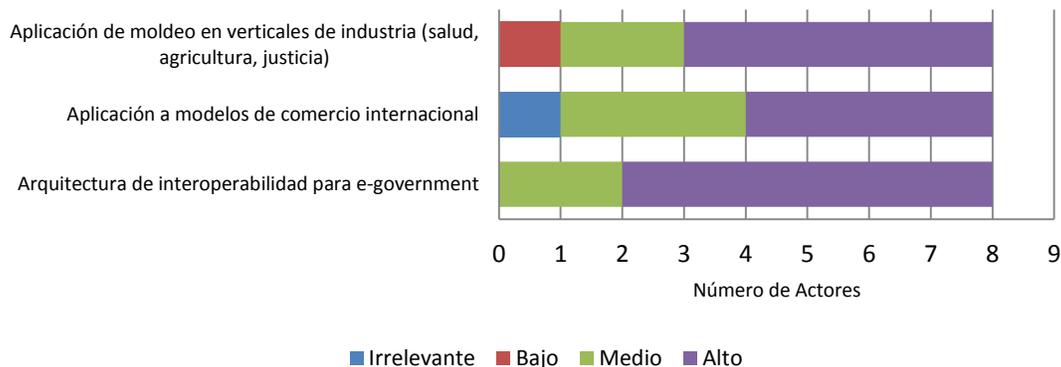
Fuente: CINTEL 2011

Se aprecia que la línea estratégica de arquitectura de interoperabilidad para e-government, fue la que contó con el mayor número de actores que se identificaron como conocedores del tema, mientras que para las líneas de aplicación a modelos de comercio internacional y aplicación de modelo en verticales de industria, la mayoría de actores se encuentran entre familiarizados con el tema, es decir que han leído sobre el tema y se han formado una opinión sobre él o casualmente informados, que son aquellos actores que reconocen solamente han escuchado sobre el tema.

6.4.2 Análisis del Nivel de Impacto de cada línea estratégica

A través del instrumento se logró determinar la percepción de los actores sobre el nivel de impacto que cada línea estratégica tendrá en el 2016 en el desempeño de las entidades del gobierno colombiano (Figura 41).

Figura 41 Nivel de Impacto de cada línea estratégica en el 2016



Fuente: CINTEL 2011

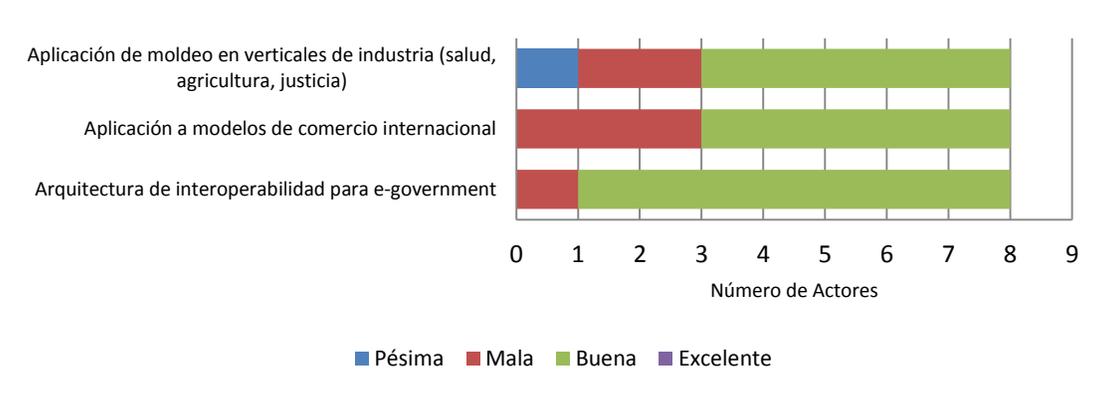


Los actores consideran que la línea de arquitectura de interoperabilidad para e-government, es la que mayor impacto puede tener en el futuro en el desempeño de las entidades del gobierno, seguido por aplicación de moldeo en verticales de industria y tras de esta aplicación a modelos de comercio internacional.

6.4.3 Análisis de la Posición Competitiva del País

Igualmente se indagó a los participantes sobre la posición competitiva que Colombia podrá tener al 2016 frente a otros países en cada una de las líneas estratégicas, obteniéndose como se evidencia en la Figura 42, que en arquitectura de interoperabilidad para e-government Colombia tendrá una posición buena. Se resalta que los actores participantes no identifican una posición competitiva excelente del país en ninguna de las líneas propuestas.

Figura 42 Posición Competitiva de Colombia en el 2016 en cada línea estratégica

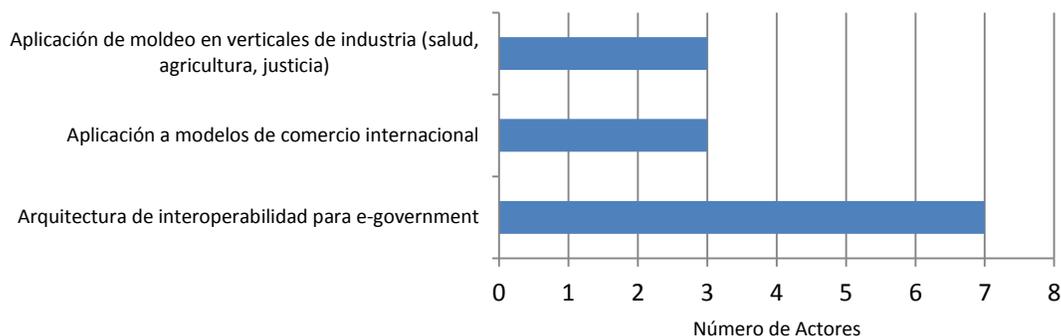


Fuente: CINTEL 2011

6.4.4 Priorización de Líneas de trabajo para el nodo

Con el objetivo de lograr identificar las líneas que resultan más estratégicas para focalizar el trabajo del nodo en los próximos cinco años, se le solicitó a los participantes que de las 3 líneas propuestas seleccionarán máximo 2, en la Figura 43 se presentan los resultados. A partir del análisis se observa que la línea que los actores condensaron como prospectiva para iniciar el trabajo del nodo es Arquitectura de interoperabilidad para e-government.

Figura 43 Priorización de las líneas estratégicas del nodo



Fuente: CINTEL 2011

6.5 VISIÓN PROSPECTIVA DEL NODO

El nodo de arquitectura TI en el 2016 debe contar con un marco de referencia que proporcionará los mecanismos para el desarrollo y apropiación de las capacidades de TI bajo una Arquitectura estructurada e innovadora aplicada para el gobierno de Colombia y fundamentada en el principio de la interoperabilidad y de estándares abiertos, a través de una dinámica de trabajo efectiva entre Estado, Empresas y Academia; que responda a los retos del proceso de desarrollo de la política de Gobierno en línea y consolide a Colombia como un país líder en la región, cualidad que se reflejen en los indicadores de la eficiencia de los servicios a la ciudadanía apoyados por TI, la dinámica de las apropiaciones y del uso de TIC en el gobierno, y la transparencia de los procesos; logrando a través de sus proyectos la sinergia lograda entre la industria y la academia, junto a la generación del conocimiento, un nivel de autonomía sobre la estrategia del sub-sistema de innovación.

6.5.1 Objetivo de la innovación

Desarrollar un modelo de referencia único de Arquitectura de TI para el gobierno de Colombia, alineado a las mejores prácticas nacionales e internacionales y fundamentados en los modelos de referencia de Arquitectura Empresarial mundiales aplicados en gobierno, que le permitan a las entidades la alineación de las tecnologías de información que requieren para cumplir las metas estratégicas del gobierno en línea y las misiones institucionales.

6.5.2 Vectores de Desarrollo del Nodo

De los análisis anteriores se define como proyecto marco de innovación para este nodo, el **diseño, desarrollo y consolidación de una Arquitectura de TI para la interoperabilidad y el Open-government.**



Los vectores de desarrollo que se desprenden de esta temática de innovación propuesta, obedecen al resultado de la investigación de las experiencias de implementación en otros países, y de diferentes hallazgos y conclusiones de estudios nacionales, así como también de la identificación de la brecha existente en cuanto a la aplicación de la arquitectura de TI en el gobierno.

Estos vectores de desarrollo darán la ruta para la formulación de los proyectos y corresponden a las siguientes sub-temáticas:

- Arquitectura para la interoperabilidad y el *Open-government*
- Marcos de referencia de Arquitectura para la interoperabilidad en comercio internacional bajo el marco de *Open-government*
- Marcos de referencia para la interoperabilidad en modelos de negocio en sectores específicos bajo el marco de *Open-government*

En la propuesta de innovación, la Arquitectura TI para la Interoperabilidad y *Open- Government* debe construirse a partir de las experiencias y el trabajo que diferentes países han realizado teniendo como fundamento los marcos de referencia de arquitecturas creados desde los años 80 y adaptados por cada país de acuerdo con las condiciones específicas del contexto político, social, cultural, organizacional, semántico y técnico. Esto implica en las primeras fases del programa de desarrollo de la arquitectura, recoger y consolidar los marcos de referencias y los dominios existentes en de cada una de las temáticas propuesta de interoperabilidad y Open - Government.

6.5.2.1 Innovación aplicada

La construcción de un modelo de arquitectura que responda estas necesidades, el cual incluya una guía para implementación y un modelo de medición del desempeño, que permita mejorar significativamente, tanto los procesos de negocio de las entidades intervenidas como los procesos administrativos a nivel nacional.

Es notable que a nivel mundial este tipo de arquitecturas aún están en construcción en algunos países considerados líderes en este aspecto, en consecuencia, el marco de desarrollo propuesto permitirá a Colombia ser un referente a nivel regional por la construcción e implementación de nuevos modelos para la generación de un gobierno TIC con una visión holística e integral.

6.5.2.2 Interoperabilidad como principal componente del modelo

La guía para la interoperabilidad de e-government de las Naciones Unidas (United Nations Development Programme, 2007) establece de acuerdo con las prácticas realizadas en los diferentes países este sentido: “*Así como la interoperabilidad, los estándares abiertos son la columna vertebral de un enfoque basado en servicios. Son ellos los que aseguran la flexibilidad, por lo que los criterios y las decisiones estarán orientadas a servicios y a tecnologías neutrales.*”

Los vectores de desarrollo que corresponden a los subcomponentes del Nodo para la Arquitectura TI de gobierno, se han desarrollado sobre estos principios rectores: la interoperabilidad y los estándares

abiertos, los cuales se evidenciaron como destacados en las investigaciones sobre experiencias de otros gobiernos.

Este direccionamiento apoya el desarrollo de la estrategia de Gobierno en línea, la cual define interoperabilidad como: “*El ejercicio de colaboración entre organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio, con el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades*”. (Ministerio de Tecnologías de Información y las Comunicaciones, 2010)

6.5.2.3 Open Government como componente del modelo

Un objetivo rector de la Estrategia de Gobierno en línea, se fundamenta en un modelo de gobierno abierto (open Government) basado en fomentar la transparencia en la actividad de los Gobiernos, así como la colaboración y la apertura de la participación de las diferentes grupos y sectores de la sociedad sobre todos los procesos de decisión y control. Este objetivo y sus principios de transparencia, participación y colaboración sobre los cuales el uso y la apropiación de las TIC en entidades de gobierno son imprescindibles, definen un marco en el cual debe estar soportada la arquitectura y desde el que se direccionarán modelos y proyectos específicos para su aplicación y cumplimiento.

6.5.2.4 Principios rectores para la arquitectura

De acuerdo con la e-Government Interoperability: Guide. De la Naciones Unidas (United Nations Development Programme, 2007), las arquitecturas están desarrolladas y sus medidas están basadas en los siguientes principios críticos comunes, los cuales tomamos como referentes para la primera aproximación al desarrollo de las Arquitectura de TI para open-government: Escalabilidad, reusabilidad, flexibilidad, apertura y seguridad.

6.5.2.5 Modelos de arquitectura de negocios

La arquitectura de TI para open- government deben generarse alrededor de los modelos de negocios que articulan los sectores de gobierno, industria y academia, los que dan el sustento para la generación de proyectos con impacto a cada grupo y hacen efectiva la participación activa de los mismos en el desarrollo de este nodo y de la agenda de innovación. Se tienen en cuenta los siguientes modelos de negocio:

- **G2G:** Focalizado en la interoperabilidad gobierno a gobierno
- **G2B:** Focalizado en la interoperabilidad gobierno a Empresas
- **G2C:** Focalizado en la interoperabilidad gobierno a ciudadano

Otros dos modelos son referenciados para ser incorporados en arquitecturas de gobierno por el orden y la magnitud de sus interoperaciones:

- **G2Org:** Focalizado en la interoperabilidad Gobierno a Organizaciones
- **G2OG:** Focalizado en la interoperabilidad Gobierno a Otros Gobiernos



6.5.2.6 Marcos de referencia de Arquitectura para la interoperabilidad y Open-government para modelos de negocio en las verticales de industria y segmentos especializados

Consiste en focalizar los esfuerzos en áreas de negocio de mayor impacto en las operaciones del gobierno, las que manejan sistemas administrativos comunes y programas a varios sectores y/o a la ciudadanía. En este campo un tema planteado es el *Marcos de referencia de Arquitectura para la interoperabilidad en comercio internacional*.

Otros grupos están conformados por sectores específicos de servicios y programas que tienen un alto impacto en la sociedad e integran los grupos de empresa, gobierno y academia en su desarrollo, conforman modelos de negocios de verticales planteados para salud, justicia y agricultura.

Estos grupos representan segmentos especializados dentro de la globalidad de la arquitectura de TI de y son considerados como una empresa (sobre la cual se plantea una Arquitectura empresarial) dentro del marco de la arquitectura empresarial de alto nivel para el gobierno.

6.6 AGENDA ESTRATÉGICA DE INNOVACIÓN - PRIORIDADES DE INNOVACIÓN EN ARQUITECTURA TI

Por la misma característica y amplitud del diseño y montaje de la arquitectura empresarial planteada como proyecto de innovación para el uso y apropiación de las TIC en el gobierno, las prioridades están determinadas por la arquitectura de más alto nivel, seguidas de las sub-arquitecturas planteadas como modelos de negocios en los sectores especializados y en segmentos transversales. El orden para los modelos de sectores estratégicos del gobierno no está determinado inicialmente y será parte de una valoración en el transcurso del desarrollo del nodo.

6.6.1 Prioridad 1

Diseño e implementación de Arquitectura de TI para la interoperabilidad y el Open-government.

6.6.2 Prioridad 2

Adopción e incorporación de marcos de referencia en la Arquitectura de TI para interoperabilidad y open. Government en ***modelos de negocio de sectores de salud, justicia y agricultura***.

6.6.3 Prioridad 3

Adopción e incorporación de marcos de referencia en la Arquitectura de TI para interoperabilidad y open. Government ***en comercio internacional***.

6.7 INICIATIVAS DE PROYECTOS POR PRIORIDAD

Para la identificación de proyectos así como sus fases, alcances y metas, se han tenido en cuenta las experiencias y mejores prácticas en el proceso de implementación de otros países. Se plantean los siguientes temas claves (FEAR project 2007, Finnish Enterprise Architecture, Ministry of Finance –

Finland), que han sido considerados en la definición de proyectos de innovación para la implementación de arquitectura de TI para la estrategia de gobierno en línea:

6.7.1 Fases del trabajo de implementación

Los procesos identificados en experiencias de otros países demostraron los siguientes patrones:

1. El desarrollo de frameworks a nivel nacional y modelos de referencias. (en este sentido en Colombia y a través de programas de gobierno en línea, se cuenta con avances importantes que soportarán el proceso de implementación de arquitecturas de TI).
2. La siguiente fase en la creación de un modelo de gobernanza para la integración e implementación de de arquitectura empresarial nacional.
3. Después de esto se focalizaron en el aseguramiento que la interoperabilidad esté adicionada al modelo de gobernanza.

6.7.2 Medición y priorización de metas

El éxito de un programa de arquitectura TI soportado en mejores prácticas de NEA, está relacionado con la definición clara y específica de objetivos.

Las metas deben ser priorizadas a nivel de proyectos de administración de gobierno en línea y de las organizaciones que den inicio al trabajo de arquitectura. Estas deben decidir cuáles temas deberán ser tratados de forma inmediata para su desarrollo. La priorización de temas deben ser realizadas desde la perspectiva de negocios, y estos requieren la cooperación de la administración, personal especializado y las funciones de TI requeridas.

6.7.3 Incremento del entendimiento y del desarrollo de interacciones

Un proceso clave que necesita un trabajo de arquitectura empresarial nacional en el gobierno, es el desarrollo de interacciones, las cuales deben ser llevadas para el aseguramiento del éxito en la implementación. Ejemplo de estas son las comunicaciones, la generación de documentación y entrenamiento para estar acorde con especialidades de arquitectura empresarial (negocios, información y tecnología) para personal de administración pública, empresas y sociedad en general.

6.7.4 Implementación de un modelo de gobernanza

Con un modelo de gobernanza, una autorización de alto nivel para el lanzamiento de cierto tipo de proyectos de impacto transversal o nacional, pueden ser mantenidos. Esto garantizaría que desarrollo de proyectos similares no estén en vía de ejecución, o sean redundantes en algunas localizaciones al mismo tiempo. Un modelo de gobernanza es una forma de promover la creación de procedimientos uniformes en entidades de gobierno.



6.8 PERFILES DE LOS PROYECTOS

6.8.1 Proyecto 1

Entidad que presenta la iniciativa	Iniciativa creada por el Nodo, con la participación de entidades y expertos temáticos.
Entidades Participantes	<p>ACADEMIA – CDT</p> <ul style="list-style-type: none">• Universidades (temática arquitectura empresarial y de TI)• Universidades (temática innovación)• Centro de investigación• <p>EMPRESA</p> <ul style="list-style-type: none">• Gestión de arquitecturas de TI (a seleccionar)• Consultoría experta en framework de Arquitectura Nacional (a seleccionar)• Empresas multinacionales del sector TIC, con líneas de negocio de Arquitectura empresarial para gobierno (IBM, ORACLE)• Proveedora software para Arquitectura empresarial ((a seleccionar)• Otras entidades comprometidas con el nodo <p>ESTADO</p> <ul style="list-style-type: none">• De acuerdo con las fases de desarrollo de la innovación:• Entidades de gobierno que firmaron compromiso para acompañar en las primeras fases (Gobierno en línea. Min Hacienda, Planeación Nacional)• En las fases de innovación de aplicación del desarrollo, se estima la participación de mínimo 10 entidades de gobierno de orden nacional y tres Departamental participantes de los nodos o que por su misión es estratégico en el área de interoperabilidad. <p>CIUDADANO</p> <ul style="list-style-type: none">• Participación del Nodo de servicio al ciudadano en el aporte al reconocimiento de la visión.• Participación del nodo
Area de Interés	Diseño e implementación de Arquitectura TI en el marco de la interoperabilidad para e-government
Título de la iniciativa	Proyecto de innovación ARQUITECTURA TI PROGRAMA DE ARQUITECTURA EMPRESARIAL PARA TIC DE GOBIERNO
Descripción de la problemática	<p>No se tiene una visión holística de las capacidades utilizadas , modelos y procesos que se implementados en los servicios a ciudadanos, por lo que no pueden visualizar y realizar propuestas de innovación para mejorar los procesos que requieran de interoperabilidad.</p> <p>Las entidades que intervienen en proceso de trámites resuelven sus tecnologías y estándares, sin evidenciar la capacidades de TIC compartidas en su entorno o de otros recursos que puedan integrarse para hacer sinergias.</p> <p>Un estado eficiente debe actuar a través de redes de organizaciones interdependientes más que mediante organizaciones autónomas que se limitan a buscar sus propios objetivos y que</p>

	<p>ello reflejaría en toda su amplitud la necesidad de contar con marcos interpretativos propios (y no prestados de la gestión privada) para mejorar e innovar en el sector público.</p> <p>Las organizaciones cuentan con estándares y arquitecturas básicas que aplican a modelos de forma independiente, pero no se cuenta con un claro modelo integrado que articule arquitecturas de negocios, aplicaciones y tecnologías de información y controlen el efecto de cambios entre sus dependencias e interrelaciones, por lo que ni cuentan con un modelo que mapee constantemente su articulación y pueda realizar una rendición de cuentas, alineado con metas de gobierno.</p> <p>Algunas organizaciones pueden identificar los costos individuales de un activo. Sin embargo, muchos no evidencian el costo real de los activos con todo sus inter-relaciones e interdependencias, para la oferta de un servicio.</p>
<p>Objetivo General</p>	<p>Innovación de tecnología blanda, para el desarrollo de un modelo nacional de arquitectura de TIC, elaborado partir de modelos de arquitectura empresarial reconocidos internacionalmente y adaptados a las condiciones para la aplicación en entidades del gobierno de Colombia y gobiernos de la región.</p> <p>A partir de este modelo de Arquitectura Empresarial para TIC de gobierno desarrollado, permitir que las entidades hagan innovación en la organización pública, mediante sus redefinición de procesos internos, procesos de uso y apropiación de TIC que apoyan la interacción con ciudadanía en general y con otras instituciones de gobierno.</p>
<p>Objetivos Específicos</p>	<p>Crear innovación aplicada a través de la adopción de frameworks de arquitectura empresarial para gobierno, en uso en otros países y su adaptación a las estrategias y condiciones de la arquitectura actual del gobierno en línea</p> <p>Incrementar la colaboración, soportada por la identificación de tecnologías duplicadas, reusables y capacidades que puedan ser compartidas, a partir de proyectos de innovación generadas en entidades de gobierno con la apropiación del modelo de arquitectura de TIC desarrollado.</p>
<p>Alcance</p>	<p>Innovar en los procesos organizacionales, el uso y apropiación de TIC, en las entidades de gobierno en el cumplimiento de la atención a ciudadanos y a las entidades públicas y privadas, y en la relación con otras entidades, a través de la implementación del modelo de Arquitectura empresarial.</p> <p>Para logra este alcance, debe ser desarrollados los procesos que enmarcan la innovación, cada uno con los siguientes alcances específicos:</p> <p>Investigación aplicada: Se debe realizar una evaluación y adopción de los diferentes frameworks usados por gobiernos en el mundo adaptados a sus características y necesidades a partir de los principales frameworks de arquitectura empresarial como Zachman, TOGAF, que para el contexto de gobierno se han referenciado como National Enterprise Architecture (NEA), federal enterprise architecture (FEA) en el caso de los Estados Unidos o llamados también Governance enterprise architecture (GEA).</p> <p>Desarrollo: A partir de los resultados de evaluación y teniendo en cuenta las mejores prácticas de casos internacionales y las perspectivas generalmente aceptadas (Janssen and Hjort-Madsen - 2007) y que han sido consideradas en el análisis del benchmark de este documento, que son:</p> <ol style="list-style-type: none"> 1) Políticas, actores y estructuras



	<ol style="list-style-type: none">2) Gobernanza3) Frameworks de architecture y metodologías4) Principios de arquitectura y estándares5) Implementación. <p>Se estructura un nuevo modelo acondicionado, práctico y usable que será el framework de arquitectura empresarial de TIC para el gobierno de Colombia. En el desarrollo de la innovación, se tendrá en cuenta los lineamientos y estrategias de gobierno en línea, que han venido definiendo un conjunto de principios y políticas que orientan los esfuerzos políticos, legales y organizacionales de las entidades, con el fin de facilitar el intercambio de información.</p> <p>innovación:</p> <p>Se aplicará el desarrollo del modelo nacional, en las entidades de gobierno. Inicialmente en las entidades que manifestaron su interés en la participación del nodo, como un escenario de piloto de innovación, como el caso de Planeación Nacional, Ministerio de TIC, Ministerio de Hacienda.</p> <p>Por su característica el framework desarrollado para Colombia, debe cumplir con las condiciones y características para ser adaptados a nivel de gobiernos de países de la región.</p> <p>Finalmente el producto pasa a la etapa de industrialización que se desarrollará con todas las entidades de gobierno mediante de mecanismos de transferencias.</p>
Entidades Beneficiarias	<p>Durante este proyecto las entidades beneficiarias serán entidades de gobierno que acompañan el proceso de desarrollo del modelo de arquitectura para TIC (se han identificada 5 que firmaron su intención de participación) y entidades que por su característica y tipos de trámite se vinculan a la implementación de la innovación.</p> <p>Se estiman en la primera fase (anterior al desarrollo comercial) un número de 10 entidades de orden Nacional y 5 de orden Departamental.</p>
Impactos Esperados	<ul style="list-style-type: none">• Involucramiento de un número masivo de entidades que quieren participar en el desarrollo, por la connotación de la temática y por ser una disciplina que se está imponiendo en las instituciones.• Recopilación y organización bajo el framework propuesto para Colombia, de cada una de los modelos vigentes y/o en construcción por parte de las entidades competentes, especialmente de gobierno en línea, para integrarlo a la innovación planteada.• Alineamiento de expectativas y visión, con respecto a las iniciativas de proyectos de investigación especialmente con temas relacionados con arquitectura para gobierno en línea e interoperabilidad.
Duración estimada	36 meses
Presupuesto estimado	Innovación aplicada: \$ 900.000.000 Desarrollo: \$ 2.100.000.000 Innovación en entidades: \$ 5.000.000.000

<p>Resultados Esperados de la iniciativa</p>	<p>El resultado de los proyectos debe propender por el uso de prácticas de Arquitectura Empresarial para TIC de clase mundial adaptadas a las necesidades de las diferentes entidades de gobierno que les permita través de su implementación innovar en:</p> <ul style="list-style-type: none"> • La transformación de procesos internos que mejoren los trámites ofrecidos a la ciudadanía de acuerdo con la misión de la entidad. • Mejora de los resultados en desarrollo de proyectos de tecnología articulados con la estrategia de la entidad y de programas de gobierno. • Aprovecha todo el potencial de las tecnologías e información comunicaciones (TIC). <p>los beneficios obtenidos por la entidades con la innovación se categorizan en dos grupos:</p> <p>En procesos de negocio (servicios y trámites)</p> <ul style="list-style-type: none"> • Ayuda a mejorar las estrategias de cada entidad involucrada, permitir que las inversiones en TI están trazadas en las metas y desempeño del servicios; asegurar que los negocios (servicios y trámites) puedan ser adaptados con nuevas innovaciones y no estancados por TI. • Agiliza el “time to market” de nuevas innovaciones que requieran TIC y desarrollo de capacidades. • Desarrollar o adaptar procesos innovadores de oportunidades identificadas para integración o re-uso de información y procesos inconsistentes. • Mayor confiabilidad, seguridad y disminuir los riesgos del servicio y de la interoperabilidad, al proveer una clara trazabilidad entre proceso de negocios, datos, roles de los usuarios, aplicaciones e infraestructura. • Debe proveer usabilidad tanto en nivel colombiano como regional. <p>En TIC</p> <ul style="list-style-type: none"> • Mejor trazabilidad de costos de TI. • Bajar los costos de TIC en diseños, compras, operación y soportes • Menor complejidad en desarrollos e implementación de TIC. La Arquitectura empresarial, provee herramientas para identificar procesos y servicios duplicados.
<p>Nivel de confidencialidad de la iniciativa</p>	<p>N.A.</p>

6.8.2 Proyecto 2

<p>Entidad que presenta la iniciativa</p>	<p>Iniciativa creada por el Nodo, con la participación de entidades y expertos temáticos.</p>
<p>Entidades Participantes</p>	<p><i>ACADEMIA – CDT</i></p> <ul style="list-style-type: none"> • <i>Universidades (temática arquitectura empresarial y de TI)</i> • <i>Universidades (temática innovación)</i> • <i>Centro de investigación</i>



	<ul style="list-style-type: none">• EMPRESA<ul style="list-style-type: none">• <i>Gestión de arquitecturas de TI (a seleccionar)</i>• <i>Consultoría experta en framework de Arquitectura Nacional (a seleccionar)</i>• <i>Empresas multinacionales del sector TIC, con líneas de negocio de Arquitectura empresarial para gobierno (IBM, ORACLE)</i>• <i>Proveedora software para Arquitectura empresarial ((a seleccionar)</i>• <i>Otras entidades comprometidas con el nodo</i>• ESTADO<ul style="list-style-type: none">• <i>De acuerdo con las fases de desarrollo de la innovación:</i>• <i>Ministerio de TIC</i>• <i>Ministerio de Comercio Industria y Turismo</i>• <i>Entidades de gobierno involucradas en el proceso de acuerdo con el desarrollo de las fases. (ver lista en capítulo entidades beneficiarias)</i>• CIUDADANO<ul style="list-style-type: none">• <i>Participación entidades representantes de empresas que utilizan comercio internacional</i>• <i>Gremios</i>• <i>Participación del nodo Servicio al Ciudadano</i>
Area de Interés	Diseño e implementación de Arquitectura TI en el marco de la interoperabilidad para e-government
Título de la iniciativa	Proyecto de innovación ARQUITECTURA TI ARQUITECTURA EMPRESARIAL PARA TIC PARA EL COMERCIO INTERNACIONAL
Descripción de la problemática	<p>En el escenario del comercio internacional, en Colombia las entidades involucradas en los procesos y trámites de importaciones y exportaciones, no utilizan al máximo el potencial de sus tecnologías de Información y comunicaciones (TIC) para generar mayores beneficios e eficiencias en un entorno en el cual múltiples empresas privadas se verían beneficiadas en sus procesos de comercio con el exterior.</p> <p>La arquitectura actual del sistema de Ventanilla Única de Comercio Exterior (VUCE), ha planteado unos avances significativos en procesos de interoperabilidad y de agilidad en los trámites internos, sin embargo debe propenderse por generar nuevos y mejorados procesos e innovar en los temas de interoperabilidad apoyada por la TIC de las entidades que interviene en los trámites y del modelo colombiano con otros sistema de comercio internacional de otros países.</p> <p>Existen múltiples desafíos para desarrollar la interoperabilidad en la implementación de ventanillas únicas para la región, las cuales pueden ser abordadas desde proyectos innovadores con arquitectura de TI.</p>
Objetivo General	Innovación de tecnología blanda, para el desarrollo de un modelo nacional de arquitectura de TIC para el comercio internacional, elaborado partir de modelos de arquitectura empresarial reconocidos internacionalmente y adaptados a las condiciones para la aplicación en entidades del gobierno de Colombia y gobiernos de la región.
Objetivos Específicos	Crear innovación aplicada a través de la adopción de frameworks de arquitectura empresarial para gobierno, en uso en otros países y su adaptación a las estrategias y condiciones de la arquitectura actual que poseen el Ministerio de Comercio, Industria y Turismo y de la

	<p>arquitectura de interoperabilidad que rige al gobierno desde el programa de gobierno en línea.</p> <p>Aportar innovación para el uso y adopción de TIC de las entidades involucradas para mejorar sus capacidades tecnológicas y reducir la brecha en función de la interoperabilidad de proceso de comercio internacional para empresas nacionales y su coordinación con pares de gobierno a nivel internacional, a partir del desarrollo de la arquitectura empresarial para TIC, en su alcance de cierre de brechas tecnológica.</p>
<p>Alcance</p>	<p>Innovar en los procesos organizacionales, el uso y apropiación de TIC, en las entidades de gobierno en el cumplimiento de los proceso de comercio internacional, en la eficiencia de servicios a la ciudadanía, a través de la implementación del modelo de Arquitectura empresarial.</p> <p>Este proceso estará enmarcado y utilizará frameworks adoptados por la arquitectura de interoperabilidad habilitada desde el proyecto anterior, teniendo en cuenta la adopción de nuevos modelos utilizados en otros países en proceso de comercio e internacionalización.</p> <p>Para logra este alcance, debe ser desarrollados los procesos que enmarcan la innovación, cada uno con los siguientes alcances específicos:</p> <p>Investigación aplicada: Hacer un estudio y determinar los framework ya construidos en el mundo y especializados en el tema de comercio internacional, que serán adoptados para el caso colombiano.</p> <p>Desarrollo: A partir de los resultados de evaluación y teniendo en cuenta las mejores prácticas de casos internacionales, se estructura un nuevo modelo acondicionado, práctico y usable que será el framework de arquitectura empresarial de TIC para el gobierno de Colombia para el comercio internacional.</p> <p>En el desarrollo de la innovación, se tendrá en cuenta los lineamientos y estrategias de gobierno en línea, y los estándares y arquitectura actual del modelo VUCE, que han venido definiendo un conjunto de principios y políticas que orientan los esfuerzos políticos, legales y organizacionales de las entidades, con el fin de facilitar el intercambio de información. El framework desarrollado para Colombia, debe tener una visión para cumplir con procesos de coordinación regional sobre plataformas de interoperabilidad las condiciones y características para ser adaptados a nivel de gobiernos de países de la región, atendiendo propuestas como la de Plataforma de Interoperabilidad para América Latina y el Caribe (PiLAC).</p> <p>innovación: Se aplicará el desarrollo del modelo nacional, en las entidades de gobierno involucradas en los procesos y trámites del estado en este tema de comercio.</p>
<p>Entidades Beneficiarias</p>	<p>Las entidades beneficiarias serán las que intervienen en el proceso de trámites de comercio que son:</p> <ul style="list-style-type: none"> Ministerio de Comercio Industria y Turismo DIAN Ministerio de Agricultura Ministerio de Protección Social Instituto Colombiano Agropecuario – ICA Instituto Colombiano de Desarrollo Rural – INCODER Instituto de Vigilancia de Medicamentos y Alimentos . INVIMA Dirección nacional de Estupefacientes Ministerio de Minas y Energía Ingeominas Ministerio de Medio Ambiente, Vivienda y Desarrollo Territorial



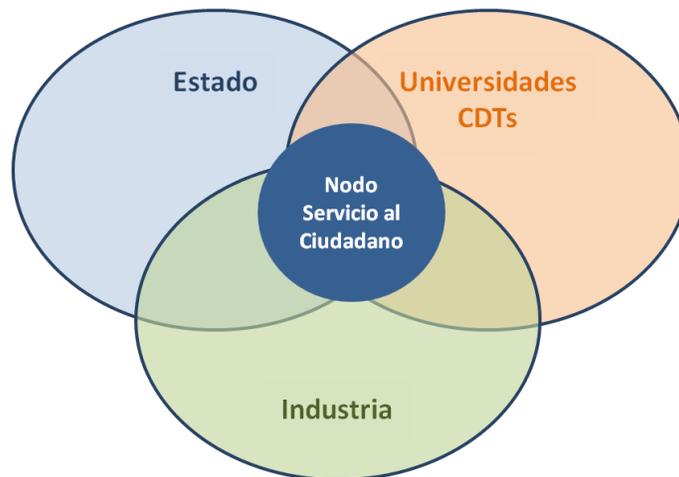
	<p>Ministerio de Defensa Nacional Industria Militar- INDUMIL Ministerio de Transporte Superintendencia de Industria y Comercio Superintendencia e Vigilancia y Seguridad Privada</p> <p>Las múltiples empresas privadas y entidades del estado que utilizan los servicios de comercio internacional, serán también beneficiadas a través de la implementación de la innovación en los nuevos procesos y mejoras de servicios integrados ofrecidos en la actualidad.</p>
Impactos Esperados	<ul style="list-style-type: none">• Involucramiento de un número masivo de entidades que quieren participar en el desarrollo, por la connotación de la temática y por ser una disciplina que se está imponiendo en las instituciones.• Recopilación y organización bajo el framework propuesto para Colombia, de cada una de los modelos vigentes y/o en construcción por parte de las entidades competentes, especialmente de gobierno en línea, para integrarlo a la innovación planteada.• Alineamiento de expectativas y visión, con respecto a las iniciativas de proyectos de investigación e innovación especialmente con temas relacionados con arquitectura para gobierno en línea e interoperabilidad.
Duración estimada	24 meses
Presupuesto estimado	Innovación aplicada: \$ 700.000.000 Desarrollo: \$ 2.000.000.000 Innovación en entidades: \$ 5.000.000.000
Resultados Esperados de la iniciativa	<p>El resultado de los proyectos debe propender por el uso de prácticas de Arquitectura Empresarial para TIC de clase mundial adaptadas a las necesidades de las diferentes entidades de gobierno involucradas en trámites de comercio internacional, que les permita a través de su implementación innovar en:</p> <ul style="list-style-type: none">• La transformación y mejora de los procesos internos ofrecidos a las múltiples empresas.• Nuevos modelos de integración con tecnologías aplicadas de comercio en la región.• Aprovecha todo el potencial de las tecnologías e información comunicaciones (TIC). <p>los beneficios obtenidos por las entidades con la innovación se categorizan en dos grupos:</p> <p>En procesos de negocio (servicios y trámites)</p> <ul style="list-style-type: none">• Asegurar que los negocios (servicios y trámites) puedan ser adaptados con nuevas innovaciones y no estancados por TI.• Agiliza el “time to market” de nuevas innovaciones que requieran TIC y desarrollo de capacidades.• Mayor confiabilidad, seguridad y disminuir los riesgos del servicio y de la interoperabilidad, al proveer una clara trazabilidad entre proceso de negocios, datos, roles de los usuarios, aplicaciones e infraestructura, para los modelos de negocio comercio internacional.• Modelo replicable que recoja: mejores prácticas, problemáticas, una visión para Colombia y la región.

	<p>En TIC</p> <ul style="list-style-type: none">• Mejor trazabilidad de costos de TI.• Bajar los costos de TIC en diseños, compras, operación y soportes• Menor complejidad en desarrollos e implementación de TIC. La Arquitectura empresarial, provee herramientas para identificar procesos y servicios duplicados, ,
Nivel de confidencialidad de la iniciativa	<p>Media.</p>

7. NODO DE INNOVACIÓN – SERVICIOS AL CIUDADANO

El Nodo de Innovación de Servicios al Ciudadano es una instancia de gestión suscrita al programa de Gobierno en Línea y conformada mediante alianzas entre Estado-Academia/CDTs³¹ y Empresas (ver Figura 44). Este Nodo se dedicará fundamentalmente a la innovación para ofrecer servicios a la ciudadanía (ciudadanos, servidores públicos y empresas) dentro del marco de la Estrategia de Gobierno en línea (GEL), cuyo propósito es contribuir con la construcción de un Estado más eficiente, más transparente, más participativo y que preste mejores servicios a los ciudadanos y las empresas, mediante el aprovechamiento de las TIC³² y la colaboración de la sociedad.

Figura 44. Conformación del nodo de servicios a la ciudadanía, vista a través de la interacción de los principales actores



Fuente: CINTEL. 2011.

La Estrategia de Gobierno en línea fomenta la mejora de los servicios, de la participación y la democracia haciendo uso de las TIC. La implementación de esta estrategia, que ya de por sí constituye una innovación, ha permitido a muchas entidades superar exitosamente los componentes de información en línea, interacción en línea y transacción en línea, y a algunas entidades avanzar en los componentes de transformación en línea y de democracia en línea.

Las fuentes principales de información de este Nodo en cuanto a posibilidades/necesidades de innovación son dos: (i) Las entidades que se convierten en la principal fuente de información sobre los retos y necesidades de innovación en la implementación de la estrategia y (ii) La ciudadanía (ciudadanos, empleados públicos y empresas) que pueden identificar en su interacción diaria con el Estado

³¹Centros de Desarrollo Tecnológico

³²Tecnologías de la Información y las Comunicaciones

posibilidades de mejoras y simplificación de trámites, procesos y mecanismos de participación y democracia con TIC.

Con el fin de que el Nodo constituya un punto de encuentro efectivo entre los actores clave, se ha planteado una primera aproximación de los posibles integrantes para su conformación.

Del sector gobierno

Si bien la gran parte de las entidades del Estado se encuentran implementando la estrategia de GEL, guiados por el Manual de Gobierno en línea, es indispensable nutrir estos procesos con componentes de innovación que permitan por una parte resolver de manera creativa e innovadora los problemas inherentes a la implantación y por otra asumir desde la misma perspectiva los retos que han surgido durante estos años y los derivados de la evolución permanente de la tecnología. Por esta razón, la propuesta es que la participación del gobierno en este Nodo se dé a través del programa encargado de la ejecución y monitoreo de la estrategia y de las entidades que han participado activamente en la misma.

- Ministerio TIC
 - Programa Gobierno en Línea
 - Centro de Innovación en Gobierno (actualmente en proceso de definición y creación)
- Departamento Nacional de Planeación
 - Programa Nacional de Servicio al Ciudadano
- Entidades del Estado:
 - Entidades líderes en la implementación de la estrategia, con retos que requieran innovación
 - Entidades líderes en alguna de las líneas propuestas a continuación

La selección de estas entidades se debe realizar con colaboración del Programa GEL, que es la fuente principal de información de los avances de las entidades en la implementación de la estrategia.

De las universidades y centros de desarrollo tecnológico

- Grupos de investigación de Universidades y/o Centros de desarrollo tecnológico cuyas líneas de investigación puedan contribuir a lograr los objetivos específicos planteados por la Estrategia GEL. A continuación se mencionan algunos temas:
 - Tecnologías que faciliten múltiples canales (Ej. plataformas móviles, TV digital, etc.)
 - Plataformas de colaboración / Redes Sociales
 - Optimización de procesos
 - Integración/Calidad de datos
 - Ingeniería de software

Igualmente se podrán considerar temas que contribuyan a resolver problemas puntuales en la implantación de la estrategia o a implementar retos específicos.



De la industria

- Clústeres de tecnología
- Fabricantes de dispositivos
- Prestadores de servicios de datos/telefonía/TV digital

Empresas de desarrollo de software y tecnología involucradas en los proyectos sectoriales que ha realizado el Programa GEL.

7.1 IDENTIFICACIÓN DE BRECHAS

7.1.1 Estado actual en el Mundo

En el ámbito global, la adopción de TIC por parte del sector público es una tendencia que va en aumento, y por lo tanto, es un factor que ha incidido notablemente en que los ciudadanos cuenten cada vez con mejores servicios electrónicos de gobierno, mayor acceso a información, una gestión pública más eficiente y por lo tanto, mejoras en la interacción con instituciones de gobierno.

En este proceso evolutivo frente a la adopción de prácticas e impulso de iniciativas de gobierno electrónico, existe un amplio conjunto de países desarrollados y en vía de desarrollo, que ha invertido de una manera importante en el desarrollo de sus estrategias y canales de interacción con la ciudadanía, y por otra parte, hay algunos que deben realizar esfuerzos cada vez mayores para brindar a sus ciudadanos la posibilidad de involucrarse con los entes de gobierno a través de medios electrónicos. (Organización de las Naciones Unidas, 2010)

Colombia es uno de los países que en los últimos años ha mostrado un progreso notorio en el desarrollo de servicios de gobierno electrónico a la ciudadanía a través de su Estrategia de Gobierno en línea. Este esfuerzo le ha permitido posicionarse en el noveno (9º) puesto a nivel mundial en provisión de servicios gubernamentales en línea, y en el puesto veintiséis (26º) entre los países con mejor indicador de e-participación. Este mismo esfuerzo a nivel gobierno lo ha convertido en el líder en gobierno electrónico en Suramérica. (Organización de las Naciones Unidas, 2010)

Con miras a continuar con el liderazgo en la región, y con la prestación de cada vez mejores servicios a la ciudadanía para un gobierno más eficiente, transparente y participativo, es necesario tomar como ejemplo a países como la República de Corea, Estados Unidos, Reino Unido, España, Australia y Baréin, que son referentes muy importantes en los dos criterios previamente mencionados, y que pueden aportar elementos clave para orientar las iniciativas de innovación a nivel nacional, en pro de servicios a la ciudadanía de mejor calidad, útiles y al alcance de la ciudadanía.

Para establecer las áreas prioritarias de trabajo que han permitido a estos países lograr el liderazgo a nivel mundial en provisión de servicios a la ciudadanía, se realizó un inventario de las principales iniciativas de gobierno electrónico a nivel nacional en cada uno de ellos, cuya categorización se presenta en la Tabla 13.

Tabla 13: Iniciativas de gobierno electrónico en servicios a la ciudadanía en los países líderes a nivel mundial

PAÍS	INICIATIVA	BENEFICIARIO	TEMAS DE E-GOVERNMENT
República de Corea	On-Nara-BPS	Gobierno	Servicios electrónicos para la ciudadanía, Intercambio de información
	Home-Tax	Empresas, Personas	Servicios electrónicos para la ciudadanía, Recaudo Electrónico de Impuestos, Intercambio de Información
	Servicio de adquisiciones electrónico	Gobierno, Empresas	Gestión Electrónica de Contrataciones
	Agencia nacional de recursos de cómputo e información (NCIRA)	Gobierno	Intercambio de información, Acceso a la información
	Sistema de Intercambio de información gubernamental	Gobierno	Intercambio de información
	Servicio de aduanas de clase mundial (UNI-PASS)	Empresas	Gestión electrónica de Aduanas
	Public I-Pin	Gobierno, Personas	Servicios electrónicos para la ciudadanía
	Servicio Civil en Línea (G4C)	Personas	Portal gubernamental, Servicios electrónicos para la ciudadanía, Acceso a la información
	Participación pública en línea	Personas	Participación ciudadana en línea
	Information Network Village	Personas	Servicios electrónicos para educación, Inclusión digital, Acceso a la información
	E-hanaro	Personas	Servicios electrónicos para la ciudadanía
	Sistema de verificación de documentos electrónicos	Gobierno, Empresas, Personas	Acceso a la información
Sistema de administración de documentos electrónicos oficiales para peticiones civiles	Personas	Acceso a la información, Servicios electrónicos para la ciudadanía	



PAÍS	INICIATIVA	BENEFICIARIO	TEMAS DE E-GOVERNMENT
	Definición de paquetes de servicios electrónicos	Personas	Servicios electrónicos para la ciudadanía
	Promoción y educación pública	Personas, Gobierno	Servicios electrónicos para la ciudadanía, Inclusión digital, Servicios electrónicos para educación, Acceso a la información
Estados Unidos	Benefits.gov	Personas	Portal gubernamental, Acceso a la información, Participación ciudadana en línea
	Disaster Assistance Improvement Program	Personas	Servicios electrónicos para la ciudadanía, Servicios electrónicos de medio ambiente, Acceso a la información
	IRS Free File	Empresas, Personas	Recaudo Electrónico de Impuestos
	Recreation One Stop	Empresas, Personas	Servicios electrónicos para la ciudadanía, Acceso a la información, Intercambio de información
	USA Services	Personas	Acceso a la información, Inclusión digital
	Business Gateway	Empresas	Servicios electrónicos para la ciudadanía, Acceso a la información
	E-Rulemaking	Personas	Participación ciudadana en línea, Acceso a la información, Intercambio de información
	Federal Asset Sales	Gobierno, Empresas, Personas	Servicios electrónicos para la ciudadanía, Gestión presupuestal electrónica, Comercio electrónico, Acceso a la información
	International Trade Data System (ITDS)	Empresas	Gestión electrónica de Aduanas
	International Trade Process Streamlining (ITPS)	Empresas	Acceso a la Información

PAÍS	INICIATIVA	BENEFICIARIO	TEMAS DE E-GOVERNMENT
	Disaster Management	Gobierno, Empresas, Personas	Servicios electrónicos para la ciudadanía, Servicios electrónicos de medio ambiente, Acceso a la Información, Intercambio de información
	Geospatial One Stop (GOS)	Gobierno	Intercambio de información, Servicios electrónicos de medio ambiente
	Grants.gov	Empresas	Portal gubernamental, Servicios electrónicos para la ciudadanía, Acceso a la información
	SAFECOM	Gobierno	Intercambio de información
Reino Unido	Government Gateway	Gobierno, Empresas, Personas	Portal gubernamental, Servicios electrónicos para la ciudadanía
	Participación e integración con medios sociales	Personas	Participación ciudadana en línea, Acceso a la información
	Manejo de tierras y propiedad	Empresas, Personas	Servicios electrónicos para la ciudadanía
	Servicios para habitantes de zonas rurales y negocios agrícolas	Empresas, Personas	Servicios electrónicos para la ciudadanía, Inclusión digital
	Trabajo y pensiones	Empresas, Personas	Servicios electrónicos para la ciudadanía, Acceso a la información
	Movilidad	Gobierno, Personas	Servicios electrónicos para la ciudadanía
	Medio Ambiente	Gobierno, Empresas	Servicios electrónicos de medio ambiente, Servicios electrónicos para la ciudadanía
	Renta y Aduanas	Empresas	Gestión electrónica de Aduanas, Recaudo Electrónico de Impuestos
	Servicios de gobierno electrónico en distritos municipales	Gobierno, Empresas, Personas	Portal gubernamental
	Conciliación y cobros	Empresas, Personas	Servicios electrónicos para la justicia



PAÍS	INICIATIVA	BENEFICIARIO	TEMAS DE E-GOVERNMENT
	WEFO Online	Empresas	Servicios electrónicos para la ciudadanía
España	Red integrada 060 de atención al ciudadano	Personas	Portal gubernamental, Servicios electrónicos para la ciudadanía
	Ventanilla única de directiva de servicios	Empresas	Servicios electrónicos para la ciudadanía
	Forja del Centro de Transferencia Tecnológica (Forja-CTT)	Gobierno, Empresas, Personas	Participación ciudadana en línea, Acceso a la información
	Centro de referencia en accesibilidad y estándares web para gobierno electrónico	Gobierno	Inclusión digital, Servicios electrónicos para educación
	Gobierno Abierto	Gobierno, Empresas, Personas	Acceso a la información, Participación ciudadana en línea
	Jornadas TECNIMAP	Gobierno, Empresas, Personas	Participación ciudadana en línea, Servicios electrónicos para educación
	SOROLLA	Gobierno	Gestión presupuestal electrónica
	HARPA	Gobierno	Servicios electrónicos para la ciudadanía
	Proyecto avanzado de telemedicina (Gobierno de la Rioja)	Personas	Servicios electrónicos para salud
	Plataforma para la gestión del sistema educativo Andaluz	Gobierno	Servicios electrónicos para educación
Plataforma de tramitación y notificación telemática (Islas Baleares)	Personas	Servicios electrónicos para la ciudadanía, Recaudo Electrónico de Impuestos, Acceso a la información	
Red SARA	Gobierno	Intercambio de información	
Australia	Programa AGOSP	Personas	Portal gubernamental, Acceso a la información
	Blog de Consulta del Gobierno Australiano	Empresas, Personas	Participación ciudadana en línea

PAÍS	INICIATIVA	BENEFICIARIO	TEMAS DE E-GOVERNMENT
	Estrategia nacional de intercambio de información de gobierno	Gobierno	Intercambio de información
	Marco de trabajo de gestión de direcciones	Gobierno	Intercambio de información
	Sitios Web del gobierno australiano	Empresas, Personas	Portal gubernamental
	Publicación de información del gobierno australiano	Empresas, Personas	Acceso a la información
	Entorno de servicios de gobierno	Gobierno, Empresas, Personas	Servicios electrónicos para la ciudadanía
Baréin	Sistema de gestión de casos	Gobierno, Personas	Servicios electrónicos para la justicia, Acceso a la información
	Aduanas y puertos	Gobierno, Empresas	Gestión electrónica de Aduanas
	Educación	Personas	Servicios electrónicos para educación, Acceso a la información
	e-Health	Personas	Servicios electrónicos para salud, Servicios electrónicos para la ciudadanía, Acceso a la información
	e-Office	Gobierno	Acceso a la información
	e-Procurement	Gobierno, Empresas	Gestión Electrónica de Contrataciones
	Portal G2B	Empresas	Portal gubernamental, Acceso a la información
	Portal G2E	Gobierno	Portal gubernamental
	Programa Nacional del Empleo	Personas	Servicios electrónicos para educación
	Dataset Nacional	Gobierno	Intercambio de información
Finca Raíz	Empresas, Personas	Servicios electrónicos para la ciudadanía	

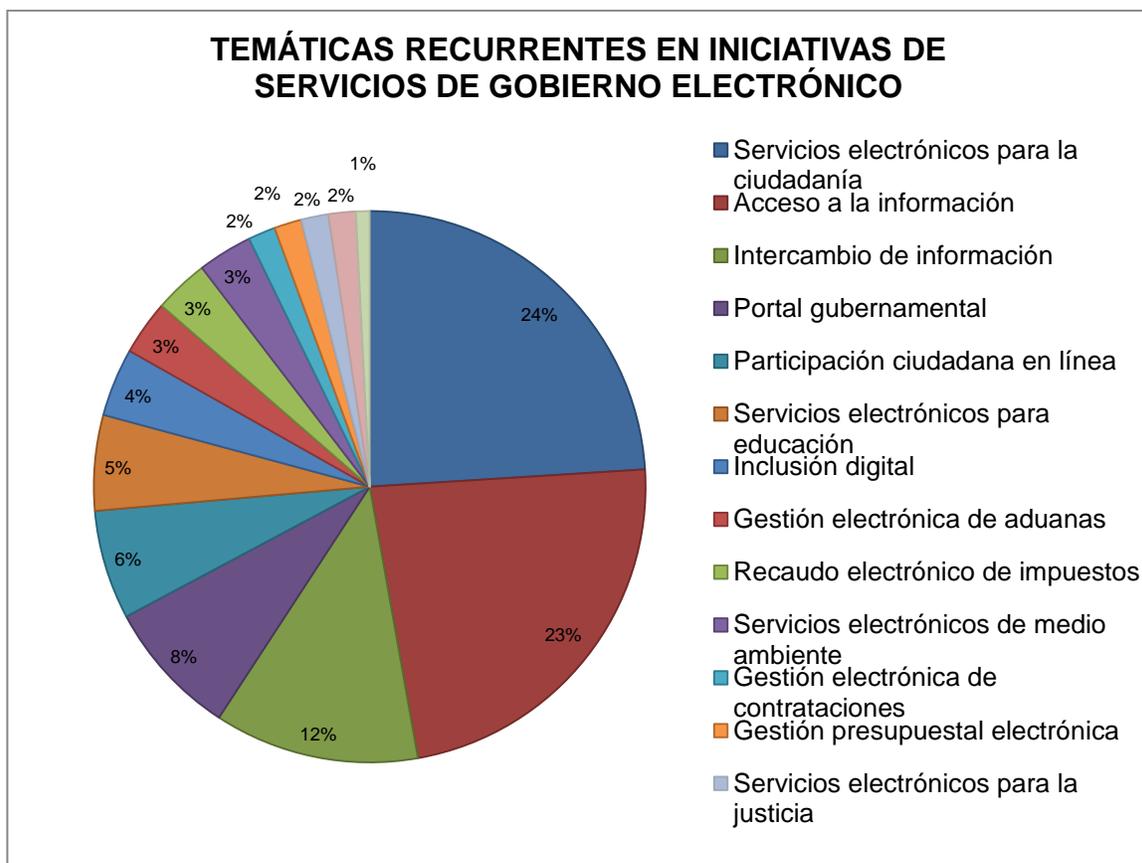


PAÍS	INICIATIVA	BENEFICIARIO	TEMAS DE E-GOVERNMENT
	Sistema de información social	Personas	Servicios electrónicos para la ciudadanía, Intercambio de información
	Servicios de turismo	Empresas, Personas	Servicios electrónicos para la ciudadanía, Acceso a la información

Fuente: CINTEL. Datos: ESICenter SinerTIC Andino, 2011

Las temáticas de gobierno electrónico más recurrentes en las iniciativas inventariadas se presentan en la Figura 45.

Figura 45. Temáticas de gobierno electrónico recurrentes entre las iniciativas de los países líderes en servicios electrónicos a la ciudadanía



Fuente: CINTEL.

Por su parte, la relación de países y temáticas de gobierno electrónico se presenta en la Tabla 17.

Tabla 14: Relación entre los países líderes en servicios electrónicos de gobierno y las principales temáticas de gobierno electrónico en sus iniciativas de orden nacional

TEMÁTICA	Australia	Baréin	España	Estados Unidos	Reino Unido	República de Corea
Acceso a la información	2	6	3	10	2	6
Comercio electrónico				1		
Gestión electrónica de aduanas		1		1	1	1
Gestión electrónica de contrataciones		1				1
Gestión presupuestal electrónica			1	1		
Inclusión digital			1	1	1	2
Intercambio de información	3	2	1	5		4
Participación ciudadana en línea	1		3	2	1	1
Portal gubernamental	2	2	1	2	2	1
Recaudo electrónico de impuestos			1	1	1	1
Servicios electrónicos de medio ambiente				3	1	
Servicios electrónicos para educación		2	3			2
Servicios electrónicos para la ciudadanía	2	4	4	6	6	8
Servicios electrónicos para la justicia		1			1	
Servicios electrónicos para salud		1	1			

Fuente: CINTEL

Mediante el análisis del contenido de las iniciativas inventariadas que se relacionan en la Tabla 14, se hizo una clasificación preliminar, a modo de posibles líneas de trabajo en los países considerados, con potencial de innovación en el contexto colombiano. Los resultados de dicha clasificación se presentan en la Tabla 15.



Tabla 15: Relación entre líneas de trabajo con potencial de innovación en el contexto colombiano, y su relación con el trabajo de los países líderes en servicios de gobierno electrónico

LÍNEAS		AUSTRALIA	BARÉIN	ESPAÑA	ESTADOS UNIDOS	REINO UNIDO	REPÚBLICA DE COREA
PARTICIPACIÓN, COLABORACIÓN Y DEMOCRACIA	Interacción en Web 2.0 y Web 3.0	●		●	●	●	
	Juventud y democracia		●				
	Mecanismos de participación ciudadana en línea			●	●		●
MEJORES SERVICIOS PARA CIUDADANOS, EMPRESAS Y ESTADO	Accesibilidad Web Inclusiva	●		●			
	Información y procesos de servicio	●	●	●	●	●	●
	Generación de capacidades en talento humano		●		●		●
	Legalidad y autenticidad						●
TRANSPARENCIA	Justicia		●			●	
	Veeduría ciudadana en línea	●	●		●		●
	Adquisiciones y contratación		●		●		●

Fuente: CINTEL. (2011)

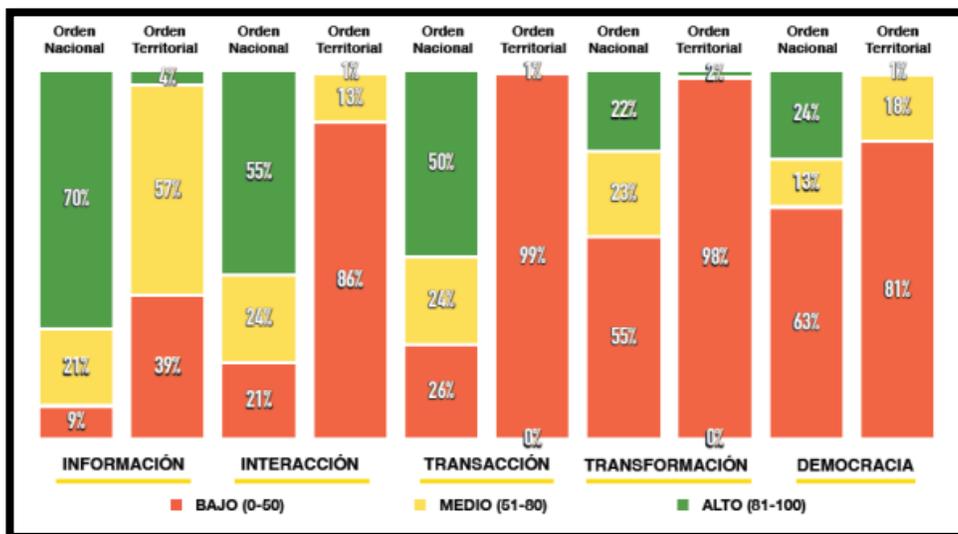
7.1.2 ESTADO ACTUAL EN COLOMBIA

En el marco del desarrollo de la Estrategia de GEL desde su definición y puesta en marcha, se ha venido avanzando en la implementación de un conjunto de iniciativas con amplia incidencia en servicios a la ciudadanía (personas, empresas y entidades del Estado), que han permitido a Colombia posicionarse en el 9º lugar en el ámbito global, en la provisión de servicios de gobierno electrónico accesibles y de calidad, siendo el No. 1 en Suramérica. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2010)

El modelo de desarrollo de Gobierno en línea en Colombia está formulado en términos de 5 componentes: Información, interacción, transacción, transformación y democracia. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011). El esfuerzo realizado por las entidades de gobierno en su conjunto para la adopción de buenas prácticas de gobierno electrónico ha permitido avanzar satisfactoriamente en los primeros tres componentes mencionados, con algunos aspectos a mejorar en el tema de transacción, (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011) que sin embargo, pueden abordarse en su mayoría mediante alternativas tecnológicas existentes, acompañadas del respectivo apoyo de las diferentes instituciones públicas.

Por su parte, las prácticas correspondientes a los componentes de transformación y democracia aún se encuentran en un estado de implementación bajo tanto a nivel nacional como territorial (ver Figura 46), e implican esfuerzos mucho más relacionados con la redefinición de procesos y políticas del Estado a diferentes niveles, así como con el acercamiento de la ciudadanía a la administración pública, que ameritan llevar a cabo actividades de innovación enfocadas y de alto impacto, con el propósito de que Colombia se convierta en un referente más notorio en la prestación de servicios a la ciudadanía en el mundo, y continúe con su liderazgo en el ámbito Suramericano.

Figura 46. Estado de la implementación de la Estrategia de Gobierno en Línea en entidades de orden nacional y territorial



Fuente: Ministerio TIC, 2011

7.1.2.1 Oportunidades de Mejora de Tipo Transversal

De acuerdo con la evaluación realizada el 31 de enero 2011 por el Ministerio TIC, en términos de la adopción de la Estrategia de Gobierno en Línea a nivel nacional, las organizaciones que mayor esfuerzo deben hacer para avanzar en la implementación de los cinco componentes son: (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)

- Instituciones de Organización Electoral
- Universidades e Institutos
- Rama Legislativa

Esto deja ver que algunos de los principales retos para el país en los próximos años respecto a la evolución de los servicios a la ciudadanía, en el marco de la Estrategia de Gobierno en línea, están enfocados en temas de democracia electoral, servicios electrónicos en instituciones de educación pública; principalmente en aquellas ubicadas fuera de las ciudades principales, y participación ciudadana en temas normativos y de construcción de políticas.

7.1.2.2 Oportunidades de Mejora en el Componente de Transformación

En el marco del servicio a la ciudadanía, el componente de transformación del modelo colombiano para la adopción de la Estrategia de Gobierno en Línea se centra en la prestación de servicios conforme a las necesidades de los usuarios. Dentro de este componente, que es otro de los puntos a mejorar a nivel



nacional, se encuentran aspectos como: (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)

- La optimización, automatización y personalización de trámites y servicios, y la creación de procesos adaptables a las necesidades de los usuarios, por múltiples canales, bajo enfoques de inclusión para que las personas puedan aprovechar los servicios electrónicos de gobierno, independientemente de su situación física, económica, nivel de escolaridad o ubicación geográfica.
- La promoción y divulgación de servicios electrónicos de gobierno al interior de las instituciones públicas y la capacitación en temas de gobierno electrónico a los funcionarios responsables de dichos servicios, así como en temas de interoperabilidad, cultura de cero papel y otros tópicos clave para la adecuada adopción e incorporación de la Estrategia de Gobierno en Línea.
- El ajuste normativo requerido para dotar a los trámites, procesos y servicios electrónicos de validez legal dentro del marco regulatorio colombiano.
- La retroalimentación de usuarios, monitoreo, evaluación y mejora de los servicios, al lado de una apropiada gestión del conocimiento en servicios y trámites, haciendo posible de este modo el desarrollo de una cultura de innovación a nivel institucional, centralizada y apalancada en el nodo de servicios al ciudadano.

Las organizaciones que deben enfocar mayores esfuerzos en la incorporación de prácticas correspondientes al elemento de transformación son: (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)

- Instituciones de Ambiente, Vivienda y Desarrollo Territorial
- Rama Judicial
- Corporaciones Autónomas Regionales
- Instituciones de Cultura

7.1.2.3 Oportunidades de Mejora en el Componente de Democracia

En relación al quehacer del NDI en servicios al ciudadano, el componente de democracia se centra en la participación activa de toda la sociedad en la definición y mejora de servicios para la ciudadanía. Entre sus principales elementos se encuentran:

- Veeduría ciudadana y rendición de cuentas sobre las acciones de la administración pública.
- Disponibilidad de mecanismos e instancias de participación ciudadana por medios electrónicos en:
 - Toma de decisiones de gobierno
 - Proyectos de normatividad y construcción de políticas
 - Control social
 - Solución de problemas
- Información pública sobre mecanismos, instancias e insumos para la participación ciudadana.
- Capacitación del talento humano de instituciones públicas responsable de los procesos de participación ciudadana.
- Realimentación de parte de la sociedad, monitoreo, evaluación y mejora de los mecanismos de participación ciudadana por medios electrónicos, al lado de una apropiada gestión del conocimiento, convirtiendo a la participación en un elemento clave dentro de la gestión de la calidad de las

instituciones, haciendo posible de este modo el desarrollo de una cultura de innovación a nivel institucional, centralizada y apalancada en el nodo de servicios al ciudadano.

7.1.2.4 Temáticas Estratégicas de Gobierno Electrónico en Colombia

Dentro del modelo de madurez planteado como base para la implementación de la Estrategia de Gobierno en Línea se planteó una serie de temáticas clave, que constituyen factores habilitantes de tipo político, normativo, de monitoreo y evaluación; con una amplia incidencia en cada nivel de adopción de la estrategia. La conceptualización de las temáticas más pertinentes al quehacer del NDIdServicios al ciudadano se presenta a continuación:

- **Datos Abiertos de Gobierno:** Es un enfoque de gestión de datos gubernamentales que contribuye con la efectividad y transparencia de la gestión pública a través del libre acceso de los mismos y su reutilización por parte de la ciudadanía (personas, empresas y entidades de gobierno). El concepto de datos abiertos de gobierno se fundamenta en ocho principios base, definidos por el Equipo de Trabajo de Datos Abiertos de Gobierno en el año 2007, en Sebastopol California³³. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)
- **Interoperabilidad:** En el marco de la estrategia de gobierno electrónico para Colombia, se define como el ejercicio de colaboración entre organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio, con el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)
- **Prestación de servicios por múltiples canales:** Es una práctica tendiente a incrementar la satisfacción de la ciudadanía, mediante la provisión de los servicios electrónicos de gobierno a través de diferentes canales, de modo que estos sean accesibles por los usuarios conforme a sus posibilidades y a su necesidad.
- **Implementación de procedimientos administrativos electrónicos:** Es una práctica de la Estrategia de Gobierno en Línea que contribuye con el establecimiento unificado de un enfoque genérico para la automatización de los procesos las entidades de gobierno, de modo que se garantice el cumplimiento de sus metas institucionales, con base en esfuerzos previos documentados y alineándolos con las nuevas tecnologías. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)
- **Gobierno en redes sociales:** Es un conjunto de prácticas enfocadas a reforzar la presencia de las instituciones de gobierno en la Web 2.0, utilizando los medios sociales como canal para la interacción con la ciudadanía en doble vía y para un mayor acercamiento con las personas, habilitando así nuevas alternativas para la participación ciudadana. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)

³³https://public.resource.org/open_government_meeting.html



Conforme se han logrado avances en el despliegue de la Estrategia de Gobierno en línea, se ha profundizado en conocimiento de dichas temáticas clave y se han identificado además algunas brechas importantes respecto a los principales referentes internacionales. Esta identificación de brechas es un insumo clave para orientar las actuaciones del programa de Gobierno en Línea en relación a estas temáticas, y por lo tanto, focos potenciales de innovación dentro las actuaciones del NDI de Servicios al ciudadano.

La identificación de brechas de las temáticas descritas anteriormente se resume en la Tabla 16.

Tabla 16: Resumen de la identificación de brechas en las temáticas estratégicas de gobierno electrónico en Colombia.

TEMÁTICA ESTRATÉGICA	ESTADO EN COLOMBIA	ESTADO EN EL MUNDO
Datos abiertos de gobierno	Colombia se encuentra aún en un estado inmaduro en cuanto a la implementación de datos abiertos en gobierno, considerando las perspectivas organizacional, político-legal, presupuestal, sociocultural y tecnológica. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)	Países como Estados Unidos, Reino Unido y Australia que han tenido un desarrollo destacado en iniciativas de datos abiertos, aún no han llegado a un nivel suficientemente maduro en todas las perspectivas ³⁴ . La mejor explicación es el desarrollo naciente de este tipo de iniciativas en el ámbito global. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)
Interoperabilidad	Colombia cuenta con un marco de interoperabilidad para Gobierno en Línea que ha venido evolucionando en los últimos años. Las dimensiones planteadas en dicho marco han demostrado su utilidad y pertinencia, y corresponden con enfoques internacionalmente reconocidos y aceptados. No obstante, en cuanto a principios y políticas, el modelo de entrega de servicios, los actores involucrados y su interacción, los tipos de servicio que contempla y el contexto en el que se desarrolla la interoperabilidad pueden requerirse algunos ajustes de acuerdo con algunos estudios que aún se encuentran en progreso. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)	Cada uno de los países analizados aplica prácticas que pueden enriquecer los planteamientos de la estrategia colombiana en el tema de interoperabilidad. El enfoque australiano está alineado con prácticas que apoyan los principios de gobierno abierto y emplea además directrices de colaboración en su marco de interoperabilidad, que pueden ser muy útiles para la articulación de iniciativas de colaboración y participación impulsadas a nivel nacional. En España se destaca el tema de regulación en torno a la definición de normas asociadas a la implementación de marcos de interoperabilidad. Respecto al caso Canadiense el principal punto de interés está en establecer buenas prácticas aplicables al

³⁴Se refiere a las perspectivas evaluadas en el estudio de benchmarking en datos abiertos realizado por Cintel. Dichas perspectivas son: Organizacional, Político-Legal, Presupuestal, Socio-Cultural y Tecnológica.

TEMÁTICA ESTRATÉGICA	ESTADO EN COLOMBIA	ESTADO EN EL MUNDO
		contexto colombiano en descubrimiento, definición, diseño, desarrollo y publicación de información entre entidades. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)
Prestación de servicios por múltiples canales	La prestación de servicios por múltiples canales para un gobierno inclusivo y equitativo es un punto importante de interés dentro de la Estrategia de Gobierno en Línea. Como uno de los primeros pasos, se cuenta inicialmente con una guía para la caracterización de usuarios de las entidades públicas, así como con los avances en las demás iniciativas tendientes al acercamiento a la ciudadanía, de modo que los canales anteriormente mencionados contribuyan eficazmente con la inclusión social para la que están siendo progresivamente implementados. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)	Existen experiencias internacionales notables en España, Países Bajos, Bélgica en los que la prestación de servicios multicanales constituye un ejemplo de buenas prácticas para otros países. De acuerdo con la Unión Europea en su reporte, el gobierno electrónico inclusivo beneficia a la población susceptible de exclusión mediante el establecimiento de redes en las que el gobierno así como intermediarios cercanos a los beneficiarios unen esfuerzos, para que a través de los canales dispuestos, la población socialmente excluida logre acceso a los servicios de gobierno. Esto se debe a la compleja variedad de necesidades, la amplia variedad de servicios y la cantidad de recursos requeridos para conectar dichos servicios a la población excluida. La prestación de servicios es posible gracias a la habilitación de múltiples canales, principalmente mediante el uso de Tecnologías de la Información y las Comunicaciones (TIC), en una combinación de sistemas, tecnologías y multimedia. En este escenario, el uso de TIC es un catalizador en la creación de valor para población vulnerable a través de nuevos modelos de servicio. (Comisión Europea, 2009)
Implementación de procedimientos administrativos electrónicos	Colombia cuenta con un marco normativo que permite la implementación de sistemas administrativos por medios electrónicos. Las normas se encuentran dispersas, y aunque se pueden aplicar integralmente, se dificulta la implementación uniforme al nivel de procedimientos. Es importante contar con una normatividad integral que contemple	En el ámbito de aplicación de procedimientos administrativos electrónicos, las experiencias internacionales de Estados Unidos, Canadá y España muestran que han incorporado en su normatividad disposiciones específicas para la utilización de herramientas de las tecnologías de la información dentro de los procedimientos de la administración pública.



TEMÁTICA ESTRATÉGICA	ESTADO EN COLOMBIA	ESTADO EN EL MUNDO
	<p>elementos que a su vez permitan una implementación uniforme a nivel de procedimientos en las entidades del Estado. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)</p>	<p>Este hecho facilita que el desarrollo de los procedimientos sea uniforme y permita certeza sobre la utilización de sistemas como el documento electrónico, situación que redundaría en el ciudadano al contar con reglas claras de interoperabilidad. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)</p>
<p>Gobierno en redes sociales</p>	<p>A pesar de no tener una ley específica para Gobierno en Línea, Colombia ha desarrollado una serie de normas entre leyes y decretos que se complementan armónicamente y que permiten la utilización de las redes sociales. Sin embargo, se observa la ausencia de lineamientos legales uniformes que faciliten el uso de estas redes a pesar de contar con una buena introducción a las redes sociales destinada a las entidades estatales. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)</p>	<p>Los casos más evolucionados en términos de regulación normativa para el empleo de redes sociales, así como en la elaboración de guías para la adopción de herramientas para participación ciudadana en el ámbito del gobierno electrónico, son los de Estados Unidos y Canadá.</p> <p>España, por su parte, dispone de una regulación que garantiza el acceso y participación de los ciudadanos a la gestión estatal. No obstante, el aterrizaje de normativas a lineamientos normativos específicos es escaso en el ámbito nacional, con excepciones en la Generalidad de Cataluña y el Gobierno Vasco, que han desarrollado guías de usos y estilo en las redes sociales para facilitar el uso de estas herramientas en las entidades de cada comunidad. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)</p>

Fuente: Cintel, 2011

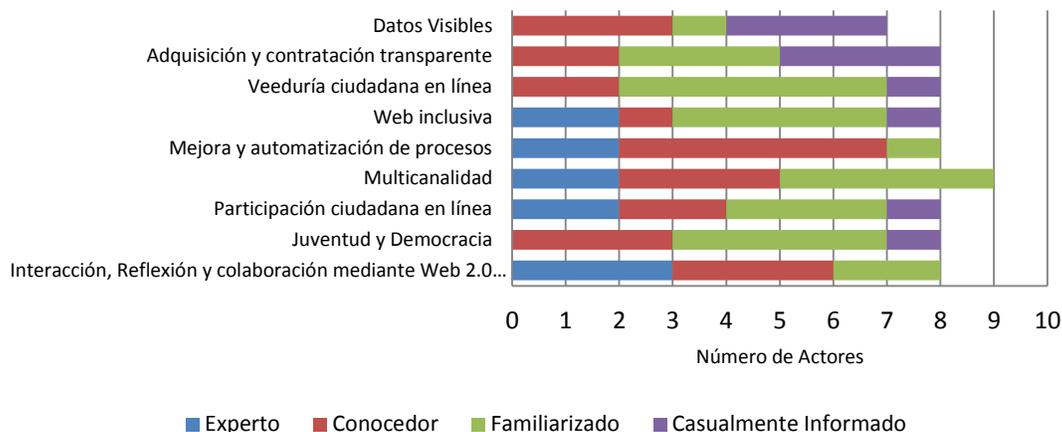
7.2 RESULTADOS DEL EJERCICIO DE PROSPECTIVA

7.2.1 Caracterización de los actores

La naturaleza de la muestra de actores que diligenciaron los instrumentos para el nodo de servicio ciudadano, estuvo compuesta en total por 9 profesionales, de los cuales 5 pertenecían a empresas: Focused Management Colombia, Seven4N Ltda, Eventic LTDA, CINTEL y un asesor en TIC's y 4 a la Academia: Universidad Antonio Nariño, Fundación para el desarrollo regional FEDERAL, Centro de Investigación I2DCorp y Centro Internacional de Física. En relación con el nivel de formación de los

participantes 2 de ellos cuentan con título de pregrado, 4 de especialización y 3 de maestría. Por otro lado, la información suministrada por los expertos permitió determinar en un primer momento, el nivel de conocimiento de los participantes en relación a las 9 líneas estratégicas identificadas para el nodo de servicio ciudadano, tal como se presenta en la Figura 47.

Figura 47 Nivel de Conocimiento de los Expertos con relación a las líneas estratégicas de Servicio Ciudadano



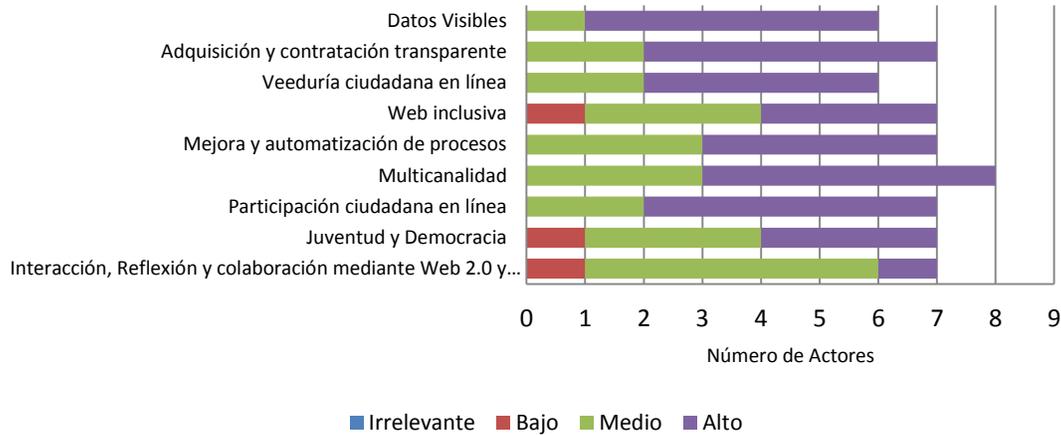
Fuente: CINTEL 2011

Se aprecia que cinco de las líneas contaron con al menos dos expertos, es decir con profesionales que actualmente dedican la mayor parte de su tiempo a este tema y probablemente tienen producción académica relacionada, dichas líneas fueron: i) Interacción, reflexión y colaboración mediante Web 2.0 y 3.0, ii) Participación Ciudadana en línea, iii) Multicanalidad, iv) Mejora y automatización de procesos y v) Web Inclusiva.

7.2.2 Análisis del Nivel de Impacto de cada línea estratégica

A través del instrumento se logró determinar la percepción de los actores sobre el nivel de impacto que cada línea estratégica tendrá en el 2016 en el desempeño de las entidades del gobierno colombiano (Figura 48). Se observa que las líneas de Datos visibles, adquisición y contratación transparente, multicanalidad y participación ciudadana en línea, fueron consideradas como de alto impacto.

Figura 48 Nivel de Impacto de cada línea estratégica en el 2016

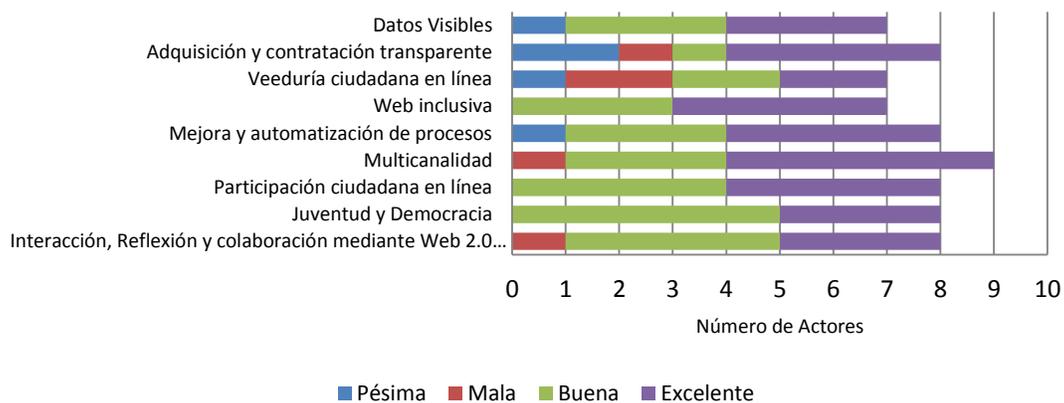


Fuente: CINTEL 2011

7.2.3 Análisis de la Posición Competitiva del País

Igualmente se indagó a los participantes sobre la posición competitiva que Colombia podrá tener al 2016 frente a otros países en cada una de las líneas estratégicas, obteniéndose como se evidencia en la Figura 49 que en en multicanalidad, web inclusiva, mejora y automatización de procesos y participación ciudadana, Colombia tendrá una posición excelente, mientras que en Juventud y Democracia y Interacción, reflexión y colaboración mediante Web 2.0 y 3.0 se considera que el país al 2016 tendrá una buena posición frente a otros países.

Figura 49 Posición Competitiva de Colombia en el 2016 en cada línea estratégica

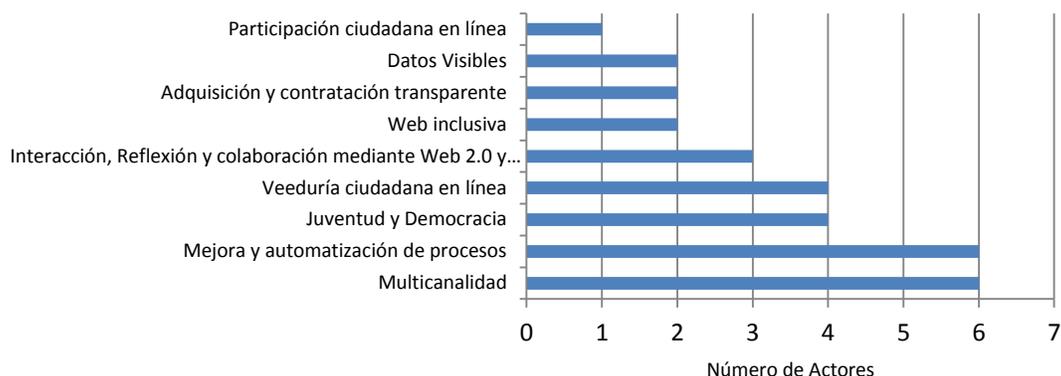


Fuente: CINTEL 2011

7.2.4 Priorización de Líneas de trabajo para el nodo

Con el objetivo de lograr identificar las líneas que resultan más estratégicas para focalizar el trabajo del nodo en los próximos cinco años, se le solicitó a los participantes que de las 9 líneas propuestas seleccionarían máximo 5, en la Figura 50 se presentan los resultados. A partir del análisis se observa que las líneas que los actores condensaron como prospectivas para iniciar el trabajo del nodo son: Multicanalidad, Mejora y automatización de procesos, Juventud y Democracia, Veeduría ciudadana en línea e Interacción, Reflexión y colaboración mediante Web 2.0 y 3.0.

Figura 50 Priorización de las líneas estratégicas del nodo



Fuente: CINTEL 2011

7.3 VISIÓN PROSPECTIVA DEL NODO DE SERVICIOS AL CIUDADANO

De acuerdo con el ejercicio de prospectiva realizado, la visión inicial del nodo se establece:

En el 2016 el nodo será reconocido a nivel nacional e internacional como el punto de encuentro de la academia, los centros de investigación, la empresa y el estado, que actúa como un catalizador para la innovación de servicios al ciudadano con TIC a través de la promoción de proyectos innovadores y de alto impacto.

Se retoma dentro de esta visión el concepto de innovación presentado al inicio de este documento como “la aplicación de una nueva o significativa mejora en un producto (bien y/o servicio) o proceso, un nuevo método de comercialización, o un nuevo método de organización en las prácticas de negocio, lugar de trabajo o en las relaciones externas”. Un proyecto innovador debe proponer claramente un beneficio claro y evidente en la mejora propuesta, en otras palabras debe generar valor para el receptor de la mejora, es decir la ciudadanía (ciudadanos, empresas, estado). Para generar valor en el receptor es necesario



centrarse en resolverle una necesidad y/o disminuirle una incomodidad y aumentar la confianza en la mejora propuesta.

7.3.1 Vectores de Desarrollo del Nodo

Considerando los principales hallazgos en relación con las iniciativas de los países líderes en prestación de servicios de gobierno en línea, así como las principales oportunidades de mejora en cuanto a la implementación de la Estrategia de Gobierno en línea a nivel nacional, y las temáticas estratégicas relacionadas con los servicios al ciudadano lideradas por el programa, se plantean a continuación los vectores en los cuales se pueden enmarcar las prioridades del nodo de innovación en servicio al ciudadano.

Los tres vectores propuestos están alineados por un lado con el objetivo del Programa Gobierno en línea de “contribuir a la construcción de un Estado más eficiente, más transparente y participativo y que presta mejores servicios con la colaboración de toda la sociedad, mediante el aprovechamiento de las TIC”, y por otro con el propósito de contribuir a mejorar el estado de la implementación del Programa Gobierno en línea, a través de proyectos innovadores que coadyuven a las entidades a alcanzar las metas todavía no logradas. En particular, en los componentes de transformación y democracia que requieren de un gran impulso tanto en el orden nacional como territorial y en los otros tres componentes en el orden territorial.

Las innovaciones propuestas en este nodo requerirán que se consideren procesos paralelos de gestión de cambio y de empoderamiento para la innovación de los actores principales, es decir de los funcionarios públicos, de los ciudadanos y de los empresarios. Es necesario generar una cultura de innovación continua en las entidades para que los proyectos de innovación tengan un marco adecuado para su ejecución. Las universidades se convierten entonces en catalizadores indispensables en el logro de estas condiciones.

7.3.1.1 Participación, colaboración y democracia

Este vector tiene como objetivo realizar proyectos de innovación que permitan a las entidades del Estado prestar servicios que favorezcan la participación y la colaboración ciudadana y la democracia. Las innovaciones propuestas deben propender por:

- Crear mecanismos y estrategias que conlleven a la colaboración efectiva entre las entidades, ciudadanos y las empresas en la construcción colectiva de un Estado incluyente y con mejores oportunidades para todos.
- Favorecer la participación ciudadana para la construcción colectiva de políticas públicas, resolución de problemas, toma de decisiones y control social, desde el orden local hasta el orden nacional.
- Empoderamiento de los ciudadanos, empresarios y servidores públicos para participar y expresar de manera segura su opinión.
- Generar mecanismos de esquemas de participación al interior de las entidades, esto para obtener ideas primero de los funcionarios y después de la ciudadanía para optimizar sus procesos.
- Generar mecanismos de esquemas de participación para que los ciudadanos participen en la identificación y definición de servicios de alto impacto en las entidades a ser creados o mejorados con uso de TIC.

Dentro de esta línea se consideran desde formas innovadoras de utilizar las tecnologías existentes, hasta desarrollo de herramientas particulares para cubrir necesidades específicas.

7.3.1.2 Mejores servicios

Este vector tiene como propósito ir más allá de los servicios y trámites en línea y realizar proyectos de innovación y alto impacto que implementen servicios a la ciudadanía, integrales e integrantes (involucrando varias entidades). Estas acciones deben estar totalmente coordinadas con los proyectos de optimización de trámites que actualmente tienen las entidades identificando los obstáculos que impiden lograr la simplificación y la prestación de mejores servicios.

Las innovaciones en cuanto a mejoramiento de servicios pueden considerar los siguientes aspectos:

- Lograr una transformación de los servicios que las entidades prestan para que sean servicios centrados en el ciudadano, fortaleciendo el desarrollo de las ventanillas únicas, que permiten la visualización del Estado como uno solo.
- Concebir servicios integrales e integrantes que mejoren la calidad de vida de los ciudadanos, a través de la simplificación de los trámites, la posibilidad de seguimiento de los mismos, su facilidad de uso y su disponibilidad por diferentes canales. Si es necesario, involucrar terceros que generen valor agregado a los servicios.
- Mejorar la eficiencia y costos de los servicios incorporando soluciones de digitalización de documentos, contribuyendo de esta manera a la iniciativa Cero papel de gobierno nacional.
- Incorporar en las mejoras modelos de autoservicio que permitan mejorar la eficacia y la eficiencia, generando ahorros en costos y tiempos.
- Garantizar la accesibilidad a los servicios para grupos vulnerables.

7.3.1.3 Transparencia (Información, gestión, visión de lo público)

Esta línea tiene como objetivo abordar proyectos para ofrecer servicios que hagan visible la información y la gestión del Estado a la ciudadanía. Los esfuerzos en este tema redundarán en generación de confianza en el Estado. Las TIC facilitan y hacen posible poner a disposición de la ciudadanía de manera efectiva y oportuna datos e información que le permitan ejercer vigilancia y control sobre las actuaciones del Estado, promoviendo de esta forma la transparencia.

Las innovaciones que se propongan en este vector, deben considerar incorporar uno o varios de los siguientes aspectos:

- Visibilidad de la información, de acuerdo a las propuestas que se han realizado en el proyecto de Open Data del Programa Gobierno en línea.
- Permitir la participación y la colaboración de la ciudadanía para ejercer la veeduría, el control y seguimiento de la gestión realizada por las entidades.
- Hacer del Estado un elemento observable y rastreado.
- Brindar calidad y efectividad a las peticiones ciudadanas a través de sistemas PQR que se integren a nivel local, regional y nacional.



- Lograr la disponibilidad de la información a todas las poblaciones incluyendo las vulnerables, lo que exige asegurar la accesibilidad, la utilización de múltiples medios y la multicanalidad.
- Hacer visible y accesible, la información de rendición de cuentas de las entidades.
- Generar relaciones semánticas en la información publicada que permita búsquedas y navegación más eficiente.

Empoderar a la ciudadanía (ciudadanos, empresas y funcionarios públicos) para utilizar la información publicada.

7.4 AGENDA ESTRATÉGICA DE INNOVACIÓN (SERVICIO AL CIUDADANO)

Dentro de las líneas propuestas se han identificado y priorizado, de acuerdo al ejercicio de prospectiva realizado, las siguientes sublíneas, que constituyen inicialmente la agenda del nodo.

7.4.1. Línea: Mejores servicios

7.4.1.1 Sublínea: Multicanalidad

Iniciativas que fomenten y mejoren la prestación de servicios de las entidades públicas, por medio de múltiples canales para facilitar el acceso de los ciudadanos.

7.4.1.2 Sublínea: Automatización y mejora de procesos

Iniciativas que promuevan la mejora de los servicios ofrecidos a los ciudadanos a través de la mejora de procesos de las entidades y/o interinstitucionales y/o con intervención de terceros, a través de su redefinición y automatización, cumpliendo con estándares internacionales para documentar procesos y usando tecnologías que faciliten la interoperabilidad.

7.4.2 Línea: Participación, colaboración y democracia

7.4.2.1 Sublínea: Interacción, reflexión y colaboración mediante Web 2.0

Iniciativas enfocadas en el aprovechamiento de redes sociales y nuevas tecnologías de Internet para promover espacios de reflexión, colaboración e interacción para promover la participación, colaboración y democracia, involucrando a la ciudadanía y al Estado.

7.4.2.2 Sublínea: Juventud y democracia

Iniciativas que hagan uso eficiente de las TIC en pro de la inclusión de la juventud en la realidad política del país, y para incentivar la formación y participación democrática desde temprana edad.

7.4.3 Línea: Transparencia

7.4.3.1 Sublínea: Veeduría y control ciudadano en línea

Iniciativas enfocadas a la provisión de herramientas para la veeduría y el control ciudadano, a nivel nacional, departamental, municipal y distrital, en cuanto a la gestión presupuestal, seguimiento de planes de gobierno, acciones legislativas y demás aspectos de interés para la ciudadanía en general.

7.4.4 Otras sublíneas

Las siguientes sublíneas se consideraron en los ejercicios de prospectiva pero no fueron consideradas como prioritarias para el Nodo de innovación.

- **Línea: Participación, colaboración y democracia**
Sublínea: Participación ciudadana en línea:
Iniciativas orientadas a implementar canales de comunicación basados en el uso de las Tecnologías de la Información, para habilitar mecanismos formales de participación ciudadana contemplados en el marco legislativo colombiano, incluyendo iniciativas para el aseguramiento de su viabilidad técnica, regulatoria y metodológica.
- **Línea: Mejores servicios**
Sublínea: Web Inclusiva
Iniciativas dirigidas al desarrollo de directrices de servicio y adopción de estándares técnicos para habilitar la interacción de personas con algún tipo de discapacidad física, que podría limitarlas para aprovechar los servicios de Gobierno en línea.
- **Línea: Transparencia**
Sublínea: Adquisiciones y contratación transparentes:
Iniciativas que permitan asegurar y procesos de contratación pública completamente transparentes y eficientes en todas sus etapas de ejecución, habilitando y mejorando una gestión perfectamente asistida por tecnologías de la información en beneficio de una ejecución más ágil, con todas las garantías exigidas por el marco legal colombiano.
- **Línea: Transparencia**
Sublínea: Datos visibles:
Iniciativas que promuevan la apertura de datos de las entidades públicas, priorizando la información que se va a publicar, y considerando su impacto y relevancia para la ciudadanía e incentive la publicación con la calidad, oportunidad y completitud requerida.

7.5 INICIATIVAS DE PROYECTOS POR PRIORIDAD

La construcción de iniciativas para este Nodo se fundamenta en la información provista por las entidades en las diferentes reuniones desarrolladas y en los resultados obtenidos del ejercicio de perspectiva. Inicialmente se presenta una lista de iniciativas propuestas, y luego se detallan fichas para los proyectos



para los que se contó con información suficiente para plantear una propuesta. Sin embargo, es de notar que el ejercicio de construcción de fichas debería continuar para especificar los proyectos que fueron mencionados por las entidades que participaron en las reuniones e identificar otros proyectos de las entidades que manifestaron su interés en participar en el Nodo.

7.5.1 Línea: Mejores servicios

7.5.1.1 Sublínea: Multicanalidad

- Construcción de servicios por móviles con seguridad
- Construcción de servicios por TDT (Información)
- Construcción de servicios de transacción por TDT

7.5.1.2 Sublínea: Automatización y mejora de procesos

- Construcción de servicios que incluyan a varias entidades
- Construcción de plataforma de pago para no bancarizados
- Consulta Georeferenciada de la red de servicios de las entidades prestadoras de salud
- Solución para el manejo en línea de las Juntas Técnico Científicas y de la Defensoría del usuario de la Superintendencia Nacional de salud.
- Fortalecimiento de la cultura sobre trámites y servicios en línea para generar confianza en la ciudadanía

7.5.2 Línea: Participación, colaboración y democracia

7.5.2.1 Sublínea: Interacción, reflexión y colaboración mediante Web 2.0

- Desarrollar plataforma para recolectar en línea ideas de los funcionarios/ciudadanos para mejorar servicios y procesos.
- Establecer incentivos. Abrir foros. "Plan sugerencias en línea"
- Construcción de módulos de participación en portales territoriales
- Construcción de ontología para el Estado

7.5.2.2 Sublínea: Juventud y democracia

- Plataforma web en la que se identifiquen las necesidades de la juventud y sus intereses
- Portales que promuevan la participación colectiva de los jóvenes
- Red de jóvenes interesados en dar a conocer sobre las problemáticas de sus lugares de origen
- Juego colaborativo para niños de participación democrática

7.5.3 Línea: Transparencia

7.5.3.1 Sublínea: Veeduría y control ciudadano en línea

- Sistema unificado para peticiones, quejas y reclamos de la ciudadanía con interacción con los entes de control³⁵
- Publicación de los presupuestos oficiales en formatos unificados con programación de ejecución y seguimiento on-line

7.6 PERFILES DE PROYECTO

Para realizar este portafolio no se contó con la información suficiente para completar las fichas de proyectos, por lo tanto sería necesario realizar un acercamiento más puntual y profundo entidad por entidad para poder proyectar esta información. Se lograron realizar reuniones informativas con algunas entidades, pero debido al periodo de finalización de año en las entidades, no se lograron realizar mesas de trabajo para completar y precisar con más detalle los proyectos. A continuación se presenta una primera versión de las fichas de proyectos que se vislumbraron de los ejercicios realizados, de aquellos de los que no se cuenta con suficiente información se dejan mencionados.

7.6.1 Proyecto 1

Entidad que presenta la iniciativa	Iniciativa creada por el Nodo, con la participación de entidades y expertos temáticos
Entidades Participantes	<ul style="list-style-type: none"> • CDT o Universidad con especialidad en TDT • Entidad(es) con interés de proveer servicios en TDT • Proveedor de tecnología TDT
Area de Interés (Debe corresponder a las líneas priorizadas en la AEI)	Multicanalidad
Título de la iniciativa	Construcción de Servicios para TDT
Descripción de la problemática	<i>La adopción de la TDT en Colombia, va a permitir a las entidades poner a disposición de sus usuarios servicios para ser utilizados en este tipo de canales. La TDT permitirá la incorporación de servicios de una vía y de doble vía, es decir que el usuario reciba contenido y que pueda interactuar con él. En términos de Gobierno en línea se podrán ofrecer servicios de carácter informativo hasta servicios que requieran transacciones. Es necesario que las</i>

³⁵ La oficina de atención al ciudadano del IDU manifestó interés en participar en la definición de este proyecto, sin embargo al momento de cierre de este informe no se pudo concretar una mesa de trabajo con ellos para determinar la ficha del proyecto.



	<i>entidades asuman el reto de utilizar este nuevo canal en la prestación de sus servicios.</i>
Objetivo General	Diseñar y poner en funcionamiento aplicaciones para ofrecer servicios al ciudadano a través TDT.
Objetivos Específicos	<ol style="list-style-type: none">1. <i>Definir una metodología para construcción de servicios para TDT partiendo de servicios que ya se ofrezcan en línea.</i>2. <i>Definir una arquitectura de software referencia para la implementación de servicios para TDT, para el programa GEL.</i>3. <i>Diseñar e implementar aplicaciones para TDT para varias entidades</i>
Alcance	La iniciativa debe generar al menos dos aplicaciones a través de las cuales se agrupen varios servicios a la ciudadanía. Se seleccionarán un conjunto de servicios en línea que sean propicios para prestar también por TDT. El proyecto desarrollará, una metodología y una arquitectura de referencia que podrán ser utilizados por otras entidades para la implementación de servicios para TDT.
Impactos Esperados	<i>Impulsar el uso de TDT para prestación de servicios al ciudadano Fomento del uso de los servicios por parte de la ciudadanía Mejorar los índices de inclusión para los servicios GEL</i>
Tiempo estimado de duración	<i>1 año</i>
Valor Estimado	<i>\$ 1.200.000.000³⁶</i>
Resultados Esperados de la iniciativa	<i>Tener disposición de los ciudadanos un conjunto de servicios a través de TDT y contar con guías para la implementación (metodología y arquitectura de referencia) para las entidades.</i>

7.6.2 Proyecto 2

Entidad que presenta la iniciativa	Superintendencia Nacional de Salud / Nodo
Entidades Participantes	<i>Empresa de desarrollo de software o Grupo de Investigación en Información Geográfica SuperSalud (Probablemente IGAC)</i>

³⁶ Se tomó como referencia el costo aproximado para este tipo de servicios reportado en Perspectives of Digital TV applications development in Russia, [Software Engineering Conference in Russia \(CEE-SECR\), 2009 5th Central and Eastern European](#), IEEE, 173 – 176, Octubre 2009. Se tomo como precio referencia 10 años hombre por aplicación, con un costo promedio de ingeniero senior a precios del mercado de 2011-

Area de Interés (Debe corresponder a las líneas prioritizadas en la AEI)	Mejora de servicios / Multicanalidad
Título de la iniciativa	<i>Consulta de red de Servicios de las entidades Prestadoras de Salud</i>
Descripción de la problemática	<i>Dificultad para el ciudadano para consultar la red de servicios de salud, de acuerdo a su EPS.</i>
Objetivo General	Diseñar, implementar y poner en funcionamiento una aplicación que permita al ciudadano identificar su red de servicios de salud a través de una aplicación, que pueda ser consultada por diferentes canales, WEB, dispositivos móviles, IVR, etc. De ser posible se debe presentar información en mapas interactivos.
Alcance	<ol style="list-style-type: none"> 1. <i>Diseñar y levantar la información geográfica de las redes de salud de las EPS</i> 2. <i>Diseñar e implementar un sistema web para que se pueda mantener actualizada la información de las redes de servicio de salud de las EPS</i> 3. <i>Diseñar y desarrollar las aplicaciones para web, dispositivos móviles e ivr.</i> 4. <i>Implementar el sistema web y colocar a disposición de los usuarios las aplicaciones en los mercados de aplicaciones de dispositivos móviles.</i>
Impactos Esperados	<p><i>Mejorar la disponibilidad de la información para los usuarios del sistema de salud</i> <i>Tener una fuente de consulta única y confiable de la información de las redes de servicio de salud</i> <i>Garantizar el acceso a esta información para todos los ciudadanos</i></p>
Tiempo estimado de duración	6 meses
Valor Estimado	\$320.000.000.00
Resultados Esperados de la iniciativa	<p><i>Sistema WEB de consulta de redes de servicios de salud</i> <i>Aplicaciones de consulta para dispositivos móviles</i></p>

7.6.3 Proyecto 3

Entidad que presenta la iniciativa	IDU / Supersalud / Nodo
Entidades Participantes	<p><i>Empresa de desarrollo de software y/o CDT con capacidad de construcción de software</i> <i>Entidades interesadas (inicialmente IDU, Supersalud, ...)</i> <i>Programa Nacional de Servicio al Ciudadano</i></p>
Area de Interés (Debe	Transparencia



corresponder a las líneas priorizadas en la AEI)	
Título de la iniciativa	<i>Sistema de peticiones, quejas y reclamos unificado</i>
Descripción de la problemática	<p><i>Actualmente las entidades del estado se encuentran implementando los lineamientos del programa nacional de servicio al ciudadano. Uno de las líneas de acción de este programa es establecer procesos y procedimientos relacionados con PQR's para definir responsables, responsabilidades, tiempo de respuesta y contenidos que brinden calidad y efectividad a las peticiones ciudadanas. Es necesario contar con un sistema que pueda ser implementado en diferentes entidades para gestionar y responder con oportunidad, que pueda ser "personalizado" para cada entidad pero que igualmente permita consolidar estadísticas de servicios agrupadas por diferentes conceptos como por ejemplo el sector, entidad, etc. Este tipo de problemática, que corresponde a producir aplicaciones que comparten un conjunto de características comunes y que se diferencian en otras (conocida como variabilidad), se puede resolver desde el punto de vista de Ingeniería de software con técnicas de líneas de producto de software. Según el Instituto de Ingeniería de Software (SEI) una LPS se define de como: "Una LPS es un conjunto de sistemas de software que comparten características comunes y administradas que satisfacen las necesidades específicas de un segmento de mercado particular y que son desarrolladas de forma preescrita a partir de un conjunto común de elementos clave".</i></p> <p><i>En los talleres y reuniones de perspectiva se detecto la necesidad de contar con sistemas de PQR que si bien deben responder a los lineamientos generales del PNSC también deben responder a las necesidades específicas de los servicios que presta cada entidad.</i></p>
Objetivo General	Diseñar e implementar una línea de producto de software para producir sistemas de PQR para gobierno, utilizando técnicas de líneas de producto de software y modelos.
Objetivos Específicos	Aplicar las metodologías de desarrollo de software basadas en líneas de productos y desarrollo basado en modelos para construir varias aplicaciones de PQR, que respondan a los requerimiento generales del PNSC y adaptadas a las necesidades de cada entidad. Utilizar la línea de producto para definir y crear aplicaciones para conjuntos de entidades que comparten necesidades específicas, como por ejemplo, PQR para entidades territoriales, PQR para entidades de vigilancia y control, PQR para gobernaciones, etc.
Alcance	<ol style="list-style-type: none"><i>1. Realizar la ingeniería de dominio para la familia de aplicaciones de PQR para gobierno.</i><i>2. Diseñar e implementar los artefactos de la LPS</i><i>3. Diseñar e implementar las herramientas basadas en modelos para la generación de código para la LPS dos</i><i>4. Definir al menos dos aplicaciones para entidades específicas y producirlas utilizando la LSP.</i><i>5. Definir al menos una aplicación que responda a las necesidades de un conjunto de entidades que comparten necesidades específicas)</i>
Impactos Esperados	<ul style="list-style-type: none"><i>• Aumentar la satisfacción de los ciudadanos en la atención de sus PQR en las entidades que se implemente.</i>

	<ul style="list-style-type: none"> • Reducir tiempos requeridos para la atención de PQR en las entidades que se implemente. • Mejorar la capacidad de control de los entes de vigilancias respecto a la atención de PQR. • Proveer de manera ágil sistemas de PQR a entidades del estado, de acuerdo a sus necesidades, con reducción de costos de producción.
Tiempo estimado de duración	<p>Fase 1: Ingeniería de dominio (de 3 a 6 meses)</p> <p>Fase 2: Creación de la LPS y herramientas (de 4 a 8 meses)</p> <p>Fase 3: Generación de aplicaciones (de 2 a 4 meses)</p>
Valor Estimado	Entre \$800.000.000.00 y \$1.300.000.000.00
Resultados Esperados de la iniciativa	<p>Una línea de producto de software para PQR de gobierno con todos los artefactos y herramientas de generación que permiten la creación ágil de sistemas de PQR para las entidades del gobierno</p> <p>Al menos tres aplicaciones de PQR, dos particulares y una genérica producidas a través de la LPS.</p>

7.6.4 Proyecto 4

Entidad que presenta la iniciativa	Nodo de Innovación en Servicios al Ciudadano 10 Instituciones de gobierno de orden nacional
Entidades Participantes	<p>ACADEMIA – CDT</p> <ul style="list-style-type: none"> • Universidades (Grupos de investigación en temáticas relacionadas con BPM) • Centro de Desarrollo Tecnológico <p>EMPRESA</p> <ul style="list-style-type: none"> • Empresas de desarrollo de soluciones de BPM con experiencia en sector gobierno. • Empresas de desarrollo de soluciones XaaS. • Empresas especializadas en desarrollo de aplicaciones para dispositivos móviles. • Empresas multinacionales del sector TIC, con líneas de negocio de BPM (MICROSOFT, IBM, ORACLE). • Empresas de desarrollo organizacional para ejecución de programas de gestión del cambio en entidades de gobierno. • Cámaras de Comercio • Otras entidades comprometidas con el nodo <p>ESTADO</p> <ul style="list-style-type: none"> • Programa Gobierno en Línea • Registraduría Nacional • Entidades de gobierno que lideran la prestación de servicios a la ciudadanía. • En las fases de implementación y prueba piloto se estima la participación de mínimo 10 entidades de gobierno de orden nacional. <p>CIUDADANÍA</p> <ul style="list-style-type: none"> • Aporte y retroalimentación de la ciudadanía (personas, empresas y entidades de gobierno) durante la fase de implementación del proyecto.
Área de Interés	Mejora y automatización de procesos de prestación de servicios a la ciudadanía, Multicanalidad, Interacción y colaboración mediante Web 2.0, Veeduría ciudadana en



	<i>línea.</i>
Título de la iniciativa	Sistema para la optimización de trámites en línea basado en Web 2.0
Descripción de la problemática	<p><i>El avance en la implementación de la Estrategia Gobierno En línea y los esfuerzos de orden nacional en materia de simplificación de trámites han dado importantes pasos en torno a las bases de mejora de los procesos para el servicio a la ciudadanía. Hoy en día la ciudadanía cuenta con una amplia base de información de trámites, alternativas de participación en torno a la mejora de dichos procesos, ventanillas únicas de trámites, y cuenta además con los beneficios del programa nacional de servicio al ciudadano y la ley antitrámites (962 de 2005).</i></p> <p><i>Aunque en términos de información de procesos y trámites se ha logrado un importante avance, la evolución de los procesos de prestación de servicios a la ciudadanía sigue estando supeditada a la organización, sistematización y procesamiento de retroalimentación individual y aislada, con lo que difícilmente se podría captar el beneficio que se obtendría mediante la interacción de dicha retroalimentación en un entorno que promueva el esfuerzo colaborativo de la ciudadanía.</i></p> <p><i>Si bien algunos de los trámites actuales proporcionan resultados inmediatos, los que por su naturaleza están asociados a procesos en varias etapas, no proporcionan información de su estado y evolución en tiempo real, para la supervisión por parte de los solicitantes, y para la vigilancia por parte de las entidades de control.</i></p> <p><i>La interacción colaborativa entre personas, empresas y entidades de gobierno en torno a la creación, evaluación y mejora de procesos para prestación de servicios a la ciudadanía, así como los respectivos mecanismos de seguimiento permitirían una ágil, eficaz y permanente mejora de los procesos de prestación de servicios de gobierno.</i></p>
Objetivo General	<i>Diseño e implementación de un sistema para la creación, puesta en marcha, seguimiento, evaluación y mejora de procesos de prestación de servicios gubernamentales a la ciudadanía.</i>
Objetivos Específicos	<p><i>Diseño de una plataforma colaborativa de BPM para servicios de gobierno, accesible mediante la Web y que cuente con funcionalidades de interacción social para realización de propuestas y diagramación de procesos bajo la noción de comunidad.</i></p> <p><i>Incorporar a la plataforma de BPM los procesos actuales de prestación de servicios a la ciudadanía de las entidades de gobierno participantes.</i></p> <p><i>Realizar procesos de difusión de la plataforma entre la ciudadanía a través de diferentes medios masivos y canales de comunicación.</i></p> <p><i>Llevar a cabo una prueba piloto del sistema, incluyendo la documentación de las lecciones aprendidas y oportunidades de mejora para las siguientes etapas de implementación.</i></p>
Alcance	<p><i>Sistema BPM para procesos de prestación de servicios a la ciudadanía:</i></p> <ul style="list-style-type: none"><i>• Debe ser accesible mediante Web, con parámetros de independencia tecnológica que promuevan la inclusividad de toda la población.</i><i>• Debe manejar registro y autenticación de usuarios por rol (ciudadanos, empresas y entidades de gobierno)</i><i>• Debe contener una interfaz amigable para el diseño visual de procesos de prestación de servicios a la ciudadanía, así como opciones de diseño detallado para usuarios avanzados.</i>

<ul style="list-style-type: none"> • <i>Debe manejar una interfaz abierta que permita a los usuarios publicar propuestas de procesos, así como visualizar y comentar propuestas de otros usuarios.</i> • <i>Debe contar con un sistema de puntuación de alternativas de procesos actuales que permitan a las entidades responsables de los procesos clasificar por prioridad los cambios a evaluar en el marco institucional.</i> • <i>Debe contarse con personal de entidades de gobierno para su mantenimiento, así como con consultores especializados en BPM, que se encarguen de orientar el esfuerzo de la ciudadanía en la propuesta de procesos.</i> • <i>Debe permitir hacer seguimiento en tiempo real a los procesos de servicios de gobierno a la ciudadanía que se encuentren en curso.</i> • <i>Debe contar con un sistema de reputación de usuarios, así como de control y sanción contra malas prácticas y conductas no apropiadas.</i> • <i>Debe contar con Wikis y contenidos especializados sobre estándares para planteamiento de servicios de gobierno, información general sobre los trámites y demás información relevante para proponer procesos consistentes y útiles en el marco institucional.</i> <p><i>Incorporación de procesos actuales:</i></p> <ul style="list-style-type: none"> • <i>Se prevé la participación de 10 instituciones de gobierno de orden nacional para la inclusión de los procesos.</i> • <i>Por cada institución se debe contar con una persona de contacto, con capacidad de gestión de la iniciativa en la respectiva entidad.</i> <p><i>Difusión de la iniciativa:</i></p> <ul style="list-style-type: none"> • <i>Se sugiere hacer uso de espacios en medios masivos de comunicación para llamar la atención de la ciudadanía, y lograr que se vinculen a la iniciativa.</i> • <i>Se propone la creación de incentivos tributarios para las personas y empresas que se comprometan con la iniciativa, frente a resultados previamente acordados.</i> • <i>Se propone la realización de eventos, conversatorios, desayunos de trabajo y jornadas de capacitación para captar la atención de diferentes grupos objetivo, y para brindar herramientas y conocimiento básico para la participación en el piloto.</i> <p><i>Prueba piloto:</i></p> <ul style="list-style-type: none"> • <i>Se debe establecer un límite de tiempo dependiendo del número de participantes, no inferior a 6 meses.</i> 	<ul style="list-style-type: none"> • <i>Debe manejar una interfaz abierta que permita a los usuarios publicar propuestas de procesos, así como visualizar y comentar propuestas de otros usuarios.</i> • <i>Debe contar con un sistema de puntuación de alternativas de procesos actuales que permitan a las entidades responsables de los procesos clasificar por prioridad los cambios a evaluar en el marco institucional.</i> • <i>Debe contarse con personal de entidades de gobierno para su mantenimiento, así como con consultores especializados en BPM, que se encarguen de orientar el esfuerzo de la ciudadanía en la propuesta de procesos.</i> • <i>Debe permitir hacer seguimiento en tiempo real a los procesos de servicios de gobierno a la ciudadanía que se encuentren en curso.</i> • <i>Debe contar con un sistema de reputación de usuarios, así como de control y sanción contra malas prácticas y conductas no apropiadas.</i> • <i>Debe contar con Wikis y contenidos especializados sobre estándares para planteamiento de servicios de gobierno, información general sobre los trámites y demás información relevante para proponer procesos consistentes y útiles en el marco institucional.</i> <p><i>Incorporación de procesos actuales:</i></p> <ul style="list-style-type: none"> • <i>Se prevé la participación de 10 instituciones de gobierno de orden nacional para la inclusión de los procesos.</i> • <i>Por cada institución se debe contar con una persona de contacto, con capacidad de gestión de la iniciativa en la respectiva entidad.</i> <p><i>Difusión de la iniciativa:</i></p> <ul style="list-style-type: none"> • <i>Se sugiere hacer uso de espacios en medios masivos de comunicación para llamar la atención de la ciudadanía, y lograr que se vinculen a la iniciativa.</i> • <i>Se propone la creación de incentivos tributarios para las personas y empresas que se comprometan con la iniciativa, frente a resultados previamente acordados.</i> • <i>Se propone la realización de eventos, conversatorios, desayunos de trabajo y jornadas de capacitación para captar la atención de diferentes grupos objetivo, y para brindar herramientas y conocimiento básico para la participación en el piloto.</i> <p><i>Prueba piloto:</i></p> <ul style="list-style-type: none"> • <i>Se debe establecer un límite de tiempo dependiendo del número de participantes, no inferior a 6 meses.</i>
Entidades Beneficiarias	<p><i>Las entidades beneficiarias directas serán entidades de gobierno que participen en el proyecto, mediante la inclusión de sus procesos para mejora, evaluación y seguimiento.</i></p> <p><i>Se estima un número de 10 entidades de orden nacional.</i></p>
Impactos Esperados	<ul style="list-style-type: none"> • <i>Mejora continuada de procesos de servicios de gobierno a la ciudadanía bajo paradigmas de comunidad, a niveles nacional, regional y local.</i> • <i>Surgimiento de nuevas herramientas para la veeduría ciudadana, la vigilancia y el control de procesos de servicios a la ciudadanía.</i> • <i>Integración más eficiente entre organizaciones de gobierno con procesos en común.</i> • <i>Procesos con menores tiempos de ejecución, más eficientes y retroalimentación rápida.</i> • <i>Participación ciudadana en materia de trámites más consciente, efectiva, proactiva y con mayor confianza en la gestión pública.</i>
Duración estimada	24 meses



Presupuesto estimado	<i>Innovación aplicada:</i> COP\$ 2.000'000.000
Resultados Esperados de la iniciativa	<ul style="list-style-type: none">• <i>Plataforma de procesos de negocio en línea para la propuesta, evaluación, seguimiento y mejora de procesos para prestación de servicios a la ciudadanía.</i>• <i>Procesos de servicio de 10 organizaciones de orden nacional incorporados para evaluación y seguimiento por parte de la ciudadanía.</i>• <i>Participación de personas, empresas y agencias de gobierno en la evaluación, seguimiento y mejora de los procesos de las 10 organizaciones gubernamentales participantes.</i>• <i>Documento con las lecciones aprendidas de la prueba piloto del sistema.</i>
Nivel de confidencialidad de la iniciativa	N.A.

7.6.5 Proyecto 5

Entidad que presenta la iniciativa	Nodo de Innovación en Servicios al Ciudadano
Entidades Participantes	<p>ACADEMIA – CDT</p> <ul style="list-style-type: none">• <i>Universidades (Grupos de investigación en temáticas relacionadas con e-learning/b-learning y Web 2.0)</i>• <i>Centro de Desarrollo Tecnológico</i> <p>EMPRESA</p> <ul style="list-style-type: none">• <i>Empresas de desarrollo de soluciones de trabajo colaborativo basdas en Web.</i>• <i>Empresas especializadas en soluciones de e-learning/b-learning y en apoyos pedagógicos.</i>• <i>Empresas de la industria gráfica especializadas en el desarrollo de contenidos educativos virtuales.</i>• <i>Organizaciones y conferencistas especializados en ciencias políticas, democracia y comunicación social.</i>• <i>Otras entidades comprometidas con el nodo</i> <p>ESTADO</p> <ul style="list-style-type: none">• <i>Programa Gobierno en Línea</i>• <i>SENA</i>• <i>Ministerio de Educación Nacional</i>• <i>Alcaldías Locales</i>• <i>Juntas Administradoras Locales</i> <p>CIUDADANÍA</p>

	<ul style="list-style-type: none"> Aporte y retroalimentación de la ciudadanía sobre los contenidos de formación y en los temas de discusión de la plataforma.
Área de Interés	Juventud y democracia, Interacción y colaboración mediante Web 2.0, Participación ciudadana.
Título de la iniciativa	Plataforma para la promoción de la cultura democrática a través de medios sociales
Descripción de la problemática	<p>La construcción de la democracia es responsabilidad de todos los ciudadanos, y por ende es también responsabilidad de la ciudadanía cumplir con sus deberes y hacer ejercicio de sus derechos, tomando decisiones a plena conciencia.</p> <p>Son destacables los esfuerzos realizados por el gobierno nacional en su acercamiento hacia la ciudadanía, la mejora del servicio y la implementación de estrategia de gobierno en línea, con el fin de facilitar para la ciudadanía el acceso a los servicios de gobierno, y para incrementar su eficiencia y transparencia.</p> <p>Con el fin de asegurar que la participación democrática a mediano y largo plazo corresponda con el esfuerzo de gobierno por acercarse a la ciudadanía y lograr un estado más igualitario, equitativo e inclusivo, es necesario que se promuevan de forma paralela a las iniciativas actuales, estrategias de formación y promoción de la cultura democrática con especial énfasis en la juventud. Para ello, la tecnología puede desempeñar un papel fundamental.</p>
Objetivo General	Diseño e implementación de una plataforma informativa, educativa y promotora de la cultura democrática en el país, orientada a niños y adolescentes, y de utilidad para la población adulta con poca o ningún tipo de formación en democracia.
Objetivos Específicos	<p>Identificación de las principales brechas de conocimiento en temas de gobierno, democracia y participación ciudadana entre los niños y adolescentes del territorio nacional.</p> <p>Creación de un portal informativo, bajo el concepto de Wiki, para la construcción colectiva de contenidos relacionados con cultura democrática y participación ciudadana, acorde con las brechas identificadas.</p> <p>Diseño y desarrollo de la plataforma de formación virtual en cultura democrática, incluyendo el diseño curricular y la creación y publicación de contenidos digitales.</p> <p>Jornadas de sensibilización, vinculación y formación de jóvenes colombianos en cultura democrática y apertura de canales de interacción con líderes comunitarios, apoyados en redes sociales y uso de dispositivos móviles.</p>
Alcance	<p>Brechas de conocimiento en cultura democrática:</p> <ul style="list-style-type: none"> Deben realizarse valoraciones en escuelas y colegios privados y públicos a nivel nacional, tanto en zonas rurales como en ciudades. Debe realizarse un estudio previo que permita seleccionar una muestra representativa de calidad a nivel nacional. Debe valorarse dentro de los criterios de evaluación el perfil de los docentes encargados de impartir las cátedras de democracia en las instituciones educativas. <p>Portal informativo sobre democracia:</p> <ul style="list-style-type: none"> Se contará con un sistema de autenticación compartido para todo el sistema que permita la autenticación de usuarios por rol.



	<ul style="list-style-type: none">• Se contará con personal especializado en docencia, en ciencias políticas y en comunicación social para la revisión y evaluación de la calidad de los contenidos del Wiki.• Se permitirá participación abierta y retroalimentación en relación con contribuciones de la ciudadanía, tanto respecto a información general como respecto a noticias y seguimiento de temas de actualidad en el ámbito nacional. <p><i>Plataforma de formación virtual:</i></p> <ul style="list-style-type: none">• Debe contener el diseño curricular de las temáticas prioritarias establecidas mediante el diagnóstico inicial.• Debe incluir contenidos virtuales de formación que se actualicen periódicamente.• Debe contemplar espacios de discusión formativa de temáticas de actualidad en el ámbito nacional y local, así como con canales de retroalimentación de líderes y representantes políticos locales.• Debe incluir un módulo de evaluación que mida el progreso logrado por los participantes mediante el uso de la plataforma. <p><i>Jornadas de sensibilización, vinculación y formación:</i></p> <ul style="list-style-type: none">• Se debe poner en marcha la plataforma y considerar un tiempo de funcionamiento no inferior a 12 meses, sujeto a las necesidades establecidas en el diagnóstico.
Entidades Beneficiarias	<p>Los beneficiarios directos son las personas que participen en los procesos de formación y capacitación.</p> <p>Como beneficiarios indirectos están las entidades de gobierno que puedan contar con retroalimentación de calidad sobre temáticas de interés discutidas en los espacios formativos.</p>
Impactos Esperados	<ul style="list-style-type: none">• Mejora de la visibilidad de las actuaciones de gobierno entre la juventud.• Mejora de los índices de participación ciudadana en el largo plazo.• Disponibilidad de una herramienta adicional de retroalimentación sobre temas de actualidad política del país, asistido por especialistas en ciencias políticas y democracia, así como por comunicadores sociales especializados en temas de opinión pública.• Surgimiento de un mayor número de líderes políticos juveniles en el largo plazo.• Mayor conocimiento de las problemáticas de orden político en diferentes comunidades y regiones del país, por parte de los jóvenes y líderes comunitarios.
Duración estimada	24 meses
Presupuesto estimado	Innovación aplicada: COP\$ 2.500'000.000
Resultados Esperados de la iniciativa	<ul style="list-style-type: none">• Diagnóstico sobre las principales brechas de conocimiento entre los jóvenes, frente a la cultura democrática y participación ciudadana en el marco colombiano.• Plataforma informativa abierta especializada en cultura democrática y participación ciudadana, así como en información de actualidad política del país.• Plataforma educativa e-learning / b-learning especializada en temas de democracia, orientada a niños y jóvenes, de utilidad para adultos con poca o ninguna formación en cultura democrática.• Formación de 600 jóvenes en temas de democracia y participación ciudadana, entre todos

	<i>los departamentos del país.</i>
Nivel de confidencialidad de la iniciativa	N.A.



8. ANEXO 1

EJERCICIO PROSPECTIVO EJEMPLO

SUBSISTEMA DE INNOVACIÓN PARA USO Y APLICACIÓN DE TIC EN EL GOBIERNO

NODO XXX

IDENTIFICACIÓN DEL PARTICIPANTE

Nombre: _____

Correo Electrónico: _____

Teléfono: _____ Profesión: _____

Entidad: _____ Cargo: _____

Seleccione el Nivel de Formación Académica que posee:

Último académico obtenido:	Pregrado	Especialización	Maestría	Doctorado	Posdoctorado	título

Años de Experiencia en la Temática: _____

Seleccione conjunto actores del usted hace parte:	Estado	Empresa	Academia	el de cual

II. PRESENTACIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones junto con CINTEL se encuentra realizando la conceptualización, diseño, desarrollo, implementación y ejecución de la primera fase del "Subsistema de Innovación para el uso y apropiación de TIC en el Gobierno", enmarcado dentro del Sistema de I+D+i de TIC definido por el Ministerio TIC, con el objetivo de fomentar el desarrollo de la industria, fortalecer la estrategia de Gobierno en Línea y contribuir al desarrollo económico, social y político del país.



2) Pensando en el nodo de XXXXX a un horizonte de cinco años, es decir en el **2016**, proponga un enunciado que refleje el estado del nodo en dicho año.

VISIÓN DEL NODO AL 2016

En el 2016 el nodo de XXXXX

IV. IDENTIFICACIÓN DE LAS LÍNEAS ESTRATÉGICAS DE INNOVACIÓN PARA EL NODO

A continuación se presentan algunas de las líneas estratégicas de innovación que desde la ciberseguridad pueden impactar el desempeño de las entidades del gobierno colombiano en el futuro. Por favor si usted considera que existe otra adiciónela.

- 1) Lea cada una de las líneas estratégicas propuestas y su definición. La definición se presenta en el documento anexo al instrumento.
- 2) Marque con una X el nivel de experticia que tiene frente a cada línea. Utilice la siguiente escala:

Experto	Conocedor	Familiarizado con el tema	Casualmente Informado
Actualmente dedica la mayor parte de su tiempo a este tema y probablemente tiene producción académica relacionada.	Cumple al menos una de las siguientes condiciones: i) fue experto en el tema hace algún tiempo pero ahora se dedica a otras áreas, ii) está formándose como experto, pero considera que aun no tiene dominio total del tema, iii) Trabaja en un campo muy relacionado y ocasionalmente aporta en el tema.	Ha leído sobre el tema y se ha formado una opinión sobre él.	Ha escuchado sobre el tema.

- 3) Marque con una X el nivel de impacto que usted considera que cada línea estratégica tendrá en el 2016 en el desempeño de las entidades del gobierno colombiano. Justifique su respuesta.

- 4) Marque con una X la posición competitiva que usted considera tendrá Colombia al 2016 frente a otros países, en cada una de las líneas estratégicas. Justifique su respuesta.
- 5) Marque con una X el tipo de entidad del gobierno que usted identifique podrá ser el principal cliente de los resultados obtenidos del trabajo de innovación desarrollado en cada una de las líneas estratégicas. Considere la siguiente tipología de entidades:

Entidades del gobierno del orden nacional	Entidades del Gobierno del orden territorial
<ul style="list-style-type: none"> - Entidades correspondientes a la rama ejecutiva según los siguientes sectores: Cultura, Protección Social, Función Pública, Defensa Nacional, Comercio Industria y Turismo, Transporte, Minas y Energía, Ambiente Vivienda y desarrollo Territorial, Agricultura y desarrollo Rural, Seguridad, Relaciones Exteriores, Hacienda y Crédito Público, Interior y de Justicia, Educación Nacional, Comunicaciones, Planeación, Presidencia, Economía Solidaria, Estadística. - Entidades correspondientes a la rama Legislativa y Judicial. - Organización electoral y organismos de control. 	<ul style="list-style-type: none"> - Departamentos con todas las entidades de cada uno ellos. - Organismos de control de orden territorial.

Líneas Estratégicas de Innovación en XXXX	Nivel de Experticia				Nivel de Impacto				Justificación del Impacto	Posición Competitiva				Justificación de la Posición	Tipo de Entidad Gubernamental		Si el tipo de entidad seleccionado fue de orden nacional, por favor mencione los tres principales sectores de acuerdo a la tipología
	Experto	Conocedor	Familiarizado	Casualmente Informado	Irrelevante	Bajo	Mediano	Alto		Pésima	Mala	Buena	Excelente		Entidades del orden nacional	Entidades del Orden Territorial	
Línea 1																	
Línea 2.																	

V. IDENTIFICACIÓN DE POSIBLES PROYECTOS DE INNOVACIÓN PARA EL NODO

De la totalidad de las líneas de innovación valoradas en el ítem anterior:



- 1) Seleccione las **cinco** que usted considera resultan más estratégicas para focalizar el trabajo del nodo en los próximos cinco años y ubíquelas en la tabla.
- 2) Si usted se identificó en el componente I como **actor de la academia o de la empresa**, para cada una de las líneas proponga tres posibles proyectos de innovación en los cuales usted considera se debería invertir recursos para generar impactos relevantes en las entidades del gobierno.
Si usted se identificó en el componente I como **actor del gobierno**, para cada una de las líneas identifique tres necesidades reales que tengan las entidades del gobierno en relación con la línea.
- 3) Si usted propuso proyectos mencione el resultado tangible de dicha iniciativa. Si identificó necesidades continúe con el siguiente paso.
- 4) Para cada proyecto propuesto o necesidad identificada seleccione el año en el cual usted considera el nodo debe empezar a trabajar.

Líneas Estratégicas de Innovación en Ciberseguridad Priorizadas	Posibles Proyectos de Innovación ó necesidad real	Resultado Tangible	Año en el cual el nodo debe empezar a trabajar				
			2012	2013	2014	2015	2016
	1.						
	2.						
	3.						

9. BIBLIOGRAFÍA

Australian Government Information Management Office. (2011). Australian Government Internet Gateway Reduction Program.

Bannister, F., & Remenyi, D. (2005). The societal value of ICT: First steps towards an evaluation framework. <http://www.ejise.com/volume6-issue2/issue2-art21.htm>. Reading, England: Academic Conferences Limited.

Beynon-Davies, P. (2004). Constructing electronic government: the case of UK inland revenue. Swansea, Wales: European Business Management School.

Carmichae, G. (2010). eGovernment - Los retos principales. Cuarto congreso de economía de Navarra.

Castellanos, O. (2007). Gestión Tecnológica: de un enfoque tradicional a la Inteligencia. Bogotá, Colombia: Facultad de Ingeniería, Universidad Nacional de Colombia.

Castellanos, O., Torres, L. M., & Domínguez, K. (2009). Manual Metodológico para la definición de Agendas Prospectivas de Investigación y Desarrollo Tecnológico en cadenas productivas agroindustriales. Bogotá: Ministerio de Agricultura y Desarrollo Rural.

Castro, A., Jonhson, B., D Ápice, M., & Filho, A. (2002). Análise Prospectiva de Cadeias Productivas.

CINTEL. (2010). Analisis de Situación Actual - Diseño del Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.

CINTEL. (2010). Anexo 2: Metodología de Gestión del riesgo - Modelo de Seguridad de la Información para la estrategia de Gobierno en Línea.

Comision Europea. (10 de 05 de 2011). CORDIS. Recuperado el 11 de 11 de 2011, de European Technology Platforms: <http://cordis.europa.eu/technology-platforms/>

Comisión Europea. (Junio de 2009). MC-eGov: Study on Multi-channel Delivery Strategies and Sustainable Business Models for Public Services addressing Socially disadvantaged Groups. Birmingham, West Midlands, Reino Unido.

Coordinación de Operación Y Desarrollo - Gobierno en Línea. (2011). ANÁLISIS DE SITUACIÓN ACTUAL MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA.

D.R. Instituto Tecnológico y de Estudios Superiores de Monterrey. (2007). Diplomado en estrategias básicas de Government electrónico, Módulo 7. Futuro de las tecnologías de información y comunicación en el sector público en el mundo . Monterrey, Mexico.

Dijk, J. v. (9 de 9 de 2010). Own research program - ICT and government organizations. Recuperado el 23 de 12 de 2011, de University of Twente:



http://www.utwente.nl/gw/vandijk/research/e_government/e_government_plaatje/a_digital_divide_own_research.doc/

DNP. (2011). Conpes 3701 - Lineamientos de Política para Ciberseguridad Y Ciberdefensa.

Equipo Consultoría Digiware. (2008). Diagnostico de la Situación Actual - Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.

Equipo de Consultoria Digiware. (2008). Informe Final - Modelo de Seguridad de la Información Sistema SANSI - SGSI (Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea).

Erazo, S. C. (2009). El Gobierno Electrónico como estrategia de participación ciudadana en la Administración pública a nivel de Suramérica - Casos Colombia Y Uruguay.

Escobar Moreno, H., & Et.Al. (2007). e-Government architectures, technical and political situation in Latin America. Santiago, Chile: United Nations Publication.

Euskadi+Innova. (s.f). Agenda de Innovación.

Finish Enterprise Architecture Research Project. (2007). Overview of Enterprise Architecture work in 15 countries. Helsinki. Finland: Finland Ministry of Finance.

Fondo de Tecnologías de la Información y las Comunicaciones – República de Colombia. (2010). Análisis de Situación Actual - Diseño del Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea.

Fondo de Tecnologías de la Información y las Comunicaciones. (2010). Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea.

Gichoya, D. (2005). Factors affecting the successful implementation of ICT projects in government. The Electronic Journal of e-government Volume 3 Issue 4 , 175-184.

Gobierno Digital México. (2011). Agenda de Gobierno Digital México.

Gobierno en línea. (2010). Componentes Estratégicos. Recuperado el 30 de Noviembre de 2010, de Programa Gobierno en Línea:
[http://programa.gobiernoenlinea.gov.co/componentes.shtml?apc=&s=d&m=a&cmd\[25\]=c-1-002-2-002D&als\[MIGA\]=Componentes](http://programa.gobiernoenlinea.gov.co/componentes.shtml?apc=&s=d&m=a&cmd[25]=c-1-002-2-002D&als[MIGA]=Componentes)

Gobierno en línea (2011). Principios y objetivos. Recuperado el 25 de diciembre de 2010, de Programa Gobierno en línea:
<http://programa.gobiernoenlinea.gov.co/componentes.shtml?apc=&s=d&m=a&cmd%5b25%5d=c-1-002-2-002A&als%5bMIGA%5d=Principios%20y%20objetivos>

Gotze, J., & Christiansen, P. E. (2009). Cross-National Interoperability and Enterprise Architecture. Informatics Vol. 20. Institute of Mathematics and Informatics, Vilnius , 369-396.

- Heung Heung-Youl Youm Youm, P. (2007). Countermeasures for Combating Cyber Attacks in Korea. Homeland Security . (2009). Cybersecurity Research.
- Homeland Security. (2011). blue print for a secure cyber future .
- ISACA. (2009). GRC Symposium.
- Kreizman, G., Baum, C., & Fraga, E. (2003). Detailed view of e-government conceptual architecture - Gartner Enterprise Architecture: A Home for E-Government. United States: Gartner.
- Mestre, H. (2011). Gobierno Efectividad Y Transparencia: E-Government.
- Miklos, T., & Tello, M. E. (1997). Planeación Prospectiva: una estrategia para el diseño del futuro. México: Limusa.
- Ministerio de Comunicaciones - Republica de Colombia. (2008). Diagnóstico de la Situación Actual - Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
- Ministerio de Comunicaciones - Republica de Colombia. (2008). Informe Final - Modelo de Seguridad de la Información Sistema SANSI - SGSI (Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea).
- Ministerio de Defensa de España. (2010). Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio - cuaderno de estrategia 149.
- Ministerio de Tecnologías de Información y las Comunicaciones. (2010). Marco para la Interoperabilidad del Gobierno en Línea - Versión 2010. Bogotá, Colombia: Ministerio de Tecnologías de información y las Comunicaciones. Programa Gobierno en Línea.
- Ministerio de Tecnologías de Información y las Comunicaciones. (30 de Septiembre de 2011). Análisis de Prospectiva en Interoperabilidad y Estándares GEL. Bogotá, Distrito Capital, Colombia.
- Ministerio de Tecnologías de Información y las Comunicaciones. (30 de Septiembre de 2011). Documento de avance del diagnóstico de presencia Web 2.0 en entidades públicas. Bogotá, Distrito Capital, Colombia.
- Ministerio de Tecnologías de Información y las Comunicaciones. (31 de Enero de 2011). Estrategia de Gobierno en línea, estado de implementación a nivel nacional. Bogotá, Distrito Capital, Colombia.
- Ministerio de Tecnologías de Información y las Comunicaciones. (30 de Septiembre de 2011). Estudio de Entorno Actual y Mejores Prácticas - Lineamientos para la implementación de datos abiertos en Colombia. Bogotá, Distrito Capital, Colombia.
- Ministerio de Tecnologías de Información y las Comunicaciones. (4 de Diciembre de 2010). Evolución del gobierno en línea 2011-2019. Bogotá, Distrito Capital, Colombia.



Ministerio de Tecnologías de Información y las Comunicaciones. (30 de Septiembre de 2011). Guía para la caracterización de usuarios de las entidades públicas - Lineamientos para la prestación de servicios de GEL por múltiples canales. Bogotá, Distrito Capital, Colombia.

Ministerio de Tecnologías de Información y las Comunicaciones. (30 de Septiembre de 2011). Lineamientos para la implementación de procedimientos administrativos electrónicos. Bogotá, Distrito Capital, Colombia.

Ministerio de Tecnologías de Información y las Comunicaciones. (15 de Junio de 2011). Manual 3.0 para la implementación de la estrategia de gobierno en línea en las entidades del orden nacional en la república de Colombia. Bogotá, Distrito Capital, Colombia.

Ministry of Science, Technology and Innovation. (2007). Danish White Paper on Enterprise Architecture . Copenhagen, Denmark: <http://www.oio.dk/files/whitepaper.pdf>.

MOGAHA. (2005). Anual Report for e-Government. Seoul, South Korea: Ministry of Government Administration and Home Affairs.

Nagji, B., & Quinn, B. (2010). Una Agenda de la innovación para asegurar el éxito. Harvard Deusto Business Review , 53-58.

Ndou, V. (2004). E-government for developing countries: Opportunities and challenges. <http://www.is.cityu.edu.hk/research/ejisd/vol18/v18r1.pdf> edn (pág. 19). Hong Kong, China: University of Hong Kong, Erasmus University of Rotterdam, University of Nebraska at Omaha.

NIST . (1999). NIST Enterprise Architecture Model / Federal Enterprise Architecture Framework V1.1. New York, US: NITS.

NIST (2008). Security Considerations in the System Development Life Cycle. NIST Special Publications 800.64 Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2008

Obi, T. (2011). e-Government in Korea.

ORACLE. (2002). E-Government: Conectando Ciudadanos, Empleados Y Proveedores.

Organización de las Naciones Unidas. (13 de Abril de 2010). United Nations E-Government Survey 2010. Nueva York, Nueva York, Estados Unidos.

Papazoglou, M., & Ribbers, P. (2006). e-Business Organizational and Technical Foundations. Chichester, United Kingdom: Wiley & Sons.

Secretaria de la función Pública de México. (2005). Modelo de Arquitectura Gubernamental de TI. - Recomendación de un Modelo de Referencia de Arquitectura Gubernamental de Tecnologías de Información. México D.F., México: Secretaria de la función Pública de México.

Segu-Info Seguridad de la Información. (2011). Phishing.

Song, J., & Hee. (2006). e-Government in Developing Countries. Lessons Learned From Republic of Korea. Bangkok, Thailand: United Nations Educational, Scientific and Cultural Organisation.

UIT. (2007). Guia de Ciberseguridad para los Países en Desarrollo.

UIT. (2007). Guía de Ciberseguridad para Países en Desarrollo.

UN. (2011). Public Administration Programme: Overview.

UN. (2011). UN E-Government Development Database. Obtenido de UNeGovDD:
<http://www2.unpan.org/egovkb/>

United Nations Development Programme. (2007). e.-Government Interoperability: Guide. New York, Unites States: United Nations Development Programme with the support of IBM Oracle .

University International Technology. (2011). Preventing Viruses, Worms, and Trojans. Obtenido de <http://uit.tufts.edu/?pid=540>