LA ESTRATEGIA DE GOBIERNO EN LÍNEA: SEGURIDAD DE LA INFORMACIÓN EN COLOMBIA

Jeiffe Jubelly Muñoz Robayo
Universidad Piloto de Colombia
Jeiffe36@gmail.com

Abstract **- For Government on Line (GOL), information security is a transverse process and defines a set of guidelines that guarantee the integrity, availability and confidentiality of information assets, additionally is introduced the privacy of the information component in order to give guarantees on the data that can be shared and which must be booked, thus the Colombian Government aims to increase the participation of citizens in the State processes of agile way safe and above all promote transparency.**

Resumen **- Para Gobierno en Línea (GEL), la seguridad de la Información es un proceso transversal y define una serie de lineamientos que garantizan la integridad, disponibilidad y confidencialidad de los activos de información, adicionalmente se introduce el componente de privacidad de la información con el fin de dar garantías sobre los datos que se pueden compartir y cuales se deben reservar, de esta manera el Estado colombiano pretende incrementar la participación de los ciudadanos en los procesos estatales de manera ágil, segura y sobre todo fomentar la trasparencia.**

Palabras Clave: **información, seguridad, sistema integrado de gestión, riesgos, estrategias.**

I INTRODUCCIÓN

Los fenómenos crecientes y cambiantes de internacionalización como el internet la telefonía móvil y las redes de comunicación han traído consigo la desaparición de las fronteras que históricamente han acompañado al ser humano; estas nuevas herramientas de comunicación se han convertido en facilitadores y generadores expansivos de la información. Esta facilidad promueve el desarrollo social creando oportunidades transformado nuestra manera de interactuar en los nuevos entornos de globalización dando con resultado convenciones más eficientes y dinámicas para generar, compartir y transmitir todo tipo de datos. La información en sus más variadas formas es considerada en la actualidad uno de los activos más valiosos de cualquier tipo de organización ya que se reconoce como un recurso esencial para el logro y cumplimiento de sus objetivos, lo cual ha exigido una mayor responsabilidad y la búsqueda de herramientas que permitan su seguridad en cualquiera de sus ámbitos de manera organizada.

Conscientes de esta dinámica de globalización el Estado colombiano aborda el reto de la seguridad de la información en las entidades, incorporando en la política pública de Gobierno en Línea (GEL) el componente de seguridad de la información, está estrategia tiene sus inicios a principios de del siglo XXI, no obstante fue a partir de 2008 con la expedición del Decreto 1151 que definió los lineamientos generales de la estrategia GEL, adicionalmente la ley 1273 el 5 de enero de 2009 "por medio del cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – de la protección de la información y de los datos", el decreto 2693 de 2012 que define los componentes que contemplan temas y actividades transversales de la seguridad de la información que deben ser implementadas en las entidades del Estado a través de un Sistema Integrado de Gestión de Seguridad de la Información (SGSI). La implementación de esta herramienta permite identificar, atender y minimizar los riesgos que atenten contra la integridad, confiabilidad y disponibilidad de la información que pertenece a la organización, este sistema permitirá mejorar la oportunidad en la prestación de los servicios a la comunidad en general de forma amigable y organizada creando puentes de interacción que ayuden a generar en los usuarios confianza y apropiación de las entidades públicas.

De otro lado la entidad se beneficia con la protección de los activos de información, el cumplimiento de la ley, el mejoramiento de la imagen institucional y la reducción de los riesgos informáticos identificados.

II SITUACIÓN ACTUAL DE LA SEGURIDAD INFORMÁTICA EN COLOMBIA

El enfoque que le da la política pública de GEL a la seguridad de la información reconoce el rol del ciudadano en constante interacción con las entidades del estado a través del uso de las diferentes Tecnologías de la Información y la Comunicaciones (TIC), razón por la cual es necesario que la implementación de los sistemas integrados de información estén soportados por una intención clara de la administración en generar procesos y acciones concretas enmarcadas en los ciclos de mejora continua (planificar-hacer-verificar-actuar) que permitan a la organización el diseño, la implantación y el mantenimiento de procesos que gestionen en forma eficaz y eficiente la accesibilidad y la manipulación controlada y permitida de la información, con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de los mismo en cualquiera de sus formas. Es así como el éxito de la implementación de los SGSI es el conocimiento de los riesgos informáticos en un contexto de cambios, avances y sofisticación tecnológica permanente, es decir entender que la vertiginosa carrera de los avance tecnológicos se encuentra

cada vez más al alcance de quienes buscan el beneficio indebido de la información ya sea porque ellos mismos la generan o porque los SGSI no son lo suficientemente adaptables permitiendo espacios que son aprovechados por los delincuentes.

Según comenta Andrés Velázquez, presidente y fundador de MaTTica, en [1], Colombia es el noveno país en el mundo generador de spam para fraudes. "En América Latina estábamos en el quinto lugar con creciente problemas de seguridad. No significa que somos inseguros, sino propensos de ataques. Brasil es de los países que mejor elevara los ataques en América Latina, le sigue Argentina, Chile y Colombia. Normalmente es casi igual a la capacidad tecnológica del país. La perfección con la que se logran los ataques está asociada a la capacidad del país. Colombia está creciendo mucho en tecnología, hay mayor cobertura en internet, hay más equipos económicos y eso incrementa la capacidad de ataques. Es sorprendente ver a Colombia en el noveno país en el mundo cerca de China y de Rusia que son los países con los mejores ataques de identificar y con impactos globales. En cuanto a estadísticas de seguridad, somos un país seguro en la región andina. Se puede decir que estamos en primer lugar en materia de desarrollo de seguridad. Respecto a América del sur, estamos en un tercer lugar. Los países más fuertes son Brasil, Chile y le sigue Colombia. Venezuela en la región es el más inseguro, basándonos en la seguridad de los portales. El 30% de los portales de este país son inseguros".

Bajo este contexto, es importante reiterar la necesidad de implementar en el marco de la política pública de GEL medidas que permitan proteger las entidades en coherencia con los esfuerzos de un Estado responsable de prevenir y contrarrestar toda amenaza que afecte su soberanía.

III LA ESTRATEGIA DE GEL COMO SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

La estrategia de gobierno en línea (GEL) busca que el Estado Colombiano interactúe de manera eficiente, transparente y participativa con los ciudadanos permitiendo hacer uso de las herramientas informáticas accediendo al interior de las organizaciones interactuando con la información que estas generan, sin embargo es importante hacernos entre otras las siguientes preguntas, ¿qué tan preparadas se encuentran las entidades del Estado para reaccionar a los ataques informáticos?, ¿Son las entidades del Estado blanco de los hackers en Colombia?, siendo conscientes de que las entidades del Estado poseen información que debe ser protegida, contempla dentro de sus componentes la implementación del SGSI, en donde cada entidad debe establecer tanto para sus procesos misionales como para los de apoyo el análisis juicioso de los riesgos informáticos y las medidas a implementar para contrarrestarlos, definiendo el estado actual de su nivel de seguridad y privacidad; elaborando un plan que organice y describa con claridad las acciones que se deberán realizar para su mitigación; verificando que estén alineadas con la política de seguridad de la entidad, de igual forma se deberán desarrollar actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información esta evaluación deberá buscar hacer las mediciones necesarias para calificar la operación y efectividad de los controles, estableciendo niveles de cumplimiento y de protección de los principios de seguridad y privacidad de la información.

Dentro de los delitos relacionados con las tecnologías de la información, podemos encontrar robos de información, fraude, espionaje, sabotaje o vandalismo y suplantación de identidad. Bajo este antecedente es importante recordar que las empresas del Estado manejan información sensible (información personal privada de un individuo) de la ciudadanía en general, es decir, la información de los usuarios ya sean individuos o empresas y organizaciones que debe protegerse de manos malintencionadas.

En una entrevista realizada a Andrés Velázquez forense digital, en reveló que la firma de seguridad informática Symantec en su reporte de amenazas a la seguridad en internet, "que los peligros potenciales en el ciberespacio van en aumento. En el 2011, la creación de nuevos virus y software malintencionado creció 41% en el 2011 respecto al año anterior con 403 millones de nuevas amenazas, publicado el año pasado. En los primeros meses del 2012, la filtración y robo de datos de empresas creció 41% respecto al año pasado. En el 2011, las pérdidas por este delito ascendieron a los a 5.5 millones de dólares en el 2011".

Con estas cifras podemos precisar que el reto de los SGSI para proteger la información sensible debe ir más allá que el cumplimiento a la ley para convertirse en un cambio de cultura organizacional que permita la apropiación y transformación de los procesos que se ejecutan a diario en las empresas del Estado. Dentro del desarrollo de esta transformación debemos considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y/o fallos técnicos.

La implementación de los SGSI debe estar debidamente documentados no solo con el fin de que sirvan como consulta en las organizaciones, sino que contengan el enfoque que busca alcanzar la dirección de la entidad, razón por la cual el rol que deberá tener en la construcción y desarrollo de estos documentos es fundamental, ya que en estos deberá plasmarse de forma transversal y en coherencia con su plataforma estratégica sus objetivos y metas. A continuación se sugiere y se describe en forma detallada que debe contener un SGSI, de acuerdo con la norma técnica ISO 27001 esta guarda total relación con la estrategia, si tenemos en cuenta que está fue tomada como referencia. De acuerdo a la norma técnica ISO 27001 un SGSI, en [2] debe estar formado por los siguientes documentos:

1. *Manual de seguridad del SGSI*: debe describir las políticas y normas de seguridad de la información definidas por la entidad, está debe ser coherente con la plataforma estratégica al igual que la normatividad vigente relacionada con la finalidad de la entidad. Este documento debe basarse en un diagnóstico previo realizado de forma juiciosa de las necesidades que tiene la entidad, es importante no caer en el error de generalizar por el contrario el detallar los requerimientos a nivel de seguridad teniendo en cuenta los recursos tecnológicos existente, las características el recurso humano con el que se trabaja, los servicios que se prestan, y el grado de participación de los usuarios, son algunos de los criterios que se deberán tener en cuenta para definir la política de SGSI. Técnicamente el documento debe presentar el

alcance, objetivos, responsabilidades, políticas y directrices principales.

- Alcance del ámbito de la organización que queda sometido al SGSI.
- Política y objetivos de seguridad.
- Procedimientos y mecanismos de control que soportan al
- SGSI.
- Gestión del riesgo.

2. *Procedimientos*: los procedimientos y controles de calidad deben ser emitidos por la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, en alineación con el sistema de calidad de la entidad. Un procedimiento describe de forma más detallada lo que se hace en las actividades de un proceso, es decir es una descripción del paso a paso en el que se especifica cómo se deben desarrollar las actividades, cuáles son los recursos que se deben emplear, el método y el objetivo que se pretende lograr, el alcance que tiene dentro de la entidad.

El papel que desempeñan los jefes de área o dependencia es vital ya que estos se deben asegurar que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad se realicen correctamente para lograr el cumplimiento de las Políticas y estándares de seguridad de la información. Es recomendable no saturar de procedimientos las áreas, simplificar y hacer seguimiento de los resultados obtenidos en la ejecución de las actividades, permitirá la tomar decisiones que den paso a la mejora continua.

Teniendo en cuenta el rol de importancia que tiene la información como insumo de alto valor y su exposición contante ya que no es posible establecer un entorno totalmente seguro, la gestión del riesgo adquiere un papel protagónico dentro de las organizaciones. Este debe ser un proceso constante que permita a la dirección conocer los costos causados por la posible interrupción de las actividades o la pérdida de los activos de información, al igual que los costos en que se incurrirá al tomar las medidas de protección, reduciendo los riegos a niveles aceptables para la misma. A continuación se describen las cuatro actividades que se deben plantear para realizar la gestión del riesgo:

Fig. 1. Fuente: El autor, Agosto 2015. Ciclo de gestión de riesgos.

En el primer paso es importante mencionar que para la identificación de los activo de información está el rol de propietario de Información (generan, procesan, almacenan o transmiten información), quién es responsable de clasificar al activo de información de acuerdo con su grado de criticidad y de definir qué usuarios podrán acceder al mismo.

En el paso dos se debe valorar el nivel del riesgo, considera el impacto que se producirá al ver ejecutada la amenaza. En los términos de información la perdida de las características de confidencialidad, integridad y disponibilidad.

Para el paso tres, la determinación del riesgo se mide en conceptos de probabilidad e impacto, respondiendo:

- ¿cuándo podría pasar?
- ¿qué pasaría si sucede?

Por último en el paso cuatro, los controles son las alternativas de solución, estos son acciones que deben ser medibles y de impacto para lograr mitigar el riesgo a niveles tolerables por la organización.

IV EVOLUCIÓN DEL GOBIERNO EN LÍNEA EN COLOMBIA

El Gobierno en Línea (GEL) en Colombia ha venido siendo implementado de manera sistemática y coordinada en todas las entidades públicas, a partir de la aparición del decreto 1151 en el 2008, considerada a la fecha la norma más importante en esta materia en Colombia, ya que consolida los lineamientos generales en que la administración pública debe avanzar para la implementación de la estrategia. Pasados 7 años después de este significativo logro, se han realizado seguimientos con el fin de evidenciar los cambios y avances en el uso y apropiación de la TIC como herramientas que han permitido mejorar la gestión pública.

El objetivo de la estrategia de GEL, es colaborar con la construcción de un Estado más eficiente, integrando de manera transversal las diferentes entidades, mediante la utilización de las Tecnologías de la Información y las Comunicaciones – TIC para hacer un Estado más transparente, más participativo con mejores servicios a los ciudadanos, a las empresas y al mismo Estado. Para lograrlo la estrategia definió cuatro ejes de acción, en [4]

1. *Mejores Servicios* (TIC para servicios)
2. *Transparencia del Estado* (TIC para gobierno abierto)
3. *Participación ciudadana* (seguridad y privacidad de la información)
4. *Eficiencia del Estado* (TIC para la gestión)

Los fundamentos sobre los que se basa la estrategia es permitir la construcción colectiva, que involucra un conocimiento de las necesidades de la sociedad y la capacidad dentro de las propias entidades públicas y sus servidores a dar respuesta, con el fin de brindar mejores servicios, involucrando nuevas tecnologías que permitan un acercamiento entre el Estado y los ciudadanos concentrando sus funciones y deberes en ambientes idóneos que garanticen la integralidad, coherencia y confiabilidad de la información abriendo paso a una sociedad más eficiente y segura, de puertas abiertas a la transparencia y la participación de la ciudadanía. El modelo GEL está concebido como una construcción social progresiva con niveles de madurez que se ven reflejados en diversos ámbitos del contexto nacional.

Gracias a la estrategia GEL, los ciudadanos hoy en día cuentan con acceso a la información pública desde los sitios WEB del Estado, dando respuesta al eje de transparencia tanto de las entidades de todas las ramas del poder público del orden nacional y al 100% de los municipios y

departamentos de Colombia. Así mismo, el país ha mejorado en las mediciones internacionales, relacionadas con la implementación de servicios en línea y en participación electrónica. En un estudio de la Organización de las Naciones Unidas (ONU) realizado en 2012, se hace un reconocimiento a aquellos países que, con una población superior a los cien millones de personas, que han hecho un enorme esfuerzo por ofrecer servicios de gobierno electrónico a su gente, a pesar de los desafíos que tienen por delante. Colombia ocupa el mejor país en servicios en línea y en participación electrónica de América Latina y el Caribe (puestos 10 y 6 respectivamente a nivel mundial) y el No. 43 del mundo en gobierno electrónico, en [3]

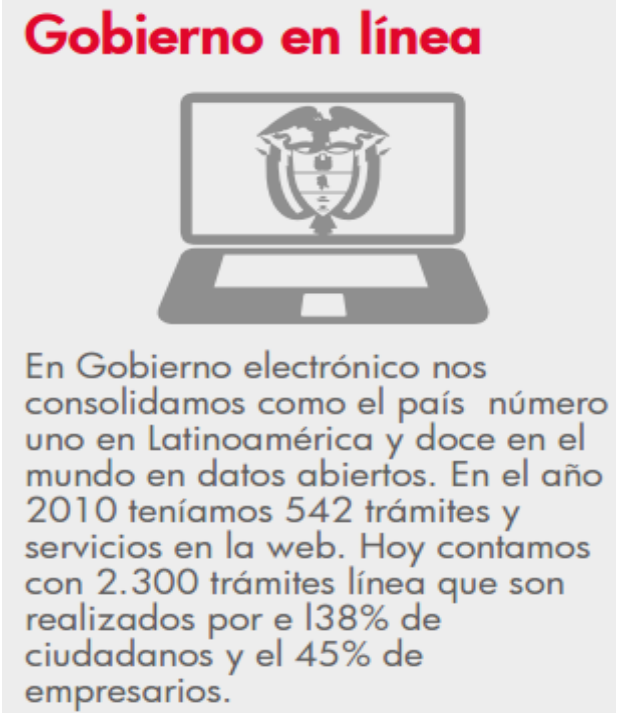

Fig. 2. Informe vive digital Colombia, Logros 2010-2015. Imagen tomada dehttp://www.mintic.gov.co/portal/604/articles-5193_recurso_3.pdf

En junio del 2014, el ministerio de la las comunicaciones publica en su página WEB el documento "Gobierno en Línea presentará balance de resultados en todos los departamentos del país" en donde cita textualmente "el ministerio de las TIC ha logrado masificar el uso de tecnología en la administración pública para que las entidades del Estado y las privadas que ejercen funciones públicas provean información de calidad, generen espacios de comunicación en doble vía y participación con sus ciudadanos, implementen más y mejores trámites y servicios en línea para que los ciudadanos no tengan que hacer filas y gastar tiempo y dinero haciendo sus vueltas en las entidades. Ya se cumplió la meta establecida para 2013, 52% entidades territoriales y 78% de entidades del orden nacional con altos índices de GEL, lo cual evidencia las capacidades para la innovación y la transformación de la gestión pública gracias a la tecnología y el mejoramiento continuo de la calidad de los servicios electrónicos y la interacción con los ciudadanos.

Actualmente, se pueden realizar más de 2.000 trámites usando medios electrónicos, de los cuales 1.533 son de entidades territoriales. Entre otros, se destacan, el impuesto predial, el impuesto de vehículos y el impuesto de industria y comercio" en [5]

En el marco del cumplimiento al decreto 2573 del 2014, que en el artículo quinto, precisa que: "TIC para la gestión comprende la planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información. Igualmente, la gestión y aprovechamiento de la información para el análisis, toma de decisiones y el mejoramiento permanente, con un enfoque integral para una respuesta articulada de gobierno y para hacer más eficaz la gestión administrativa entre instituciones de gobierno". El ministerio de tecnologías de la información y las comunicaciones estructuró un equipo de acompañamiento que trabajará directamente con las entidades para desarrollar, de acuerdo con sus necesidades, los cuatro componentes de la estrategia GEL en [6] por medio de cuatro momentos o fases:

- *Difundir*: dar a conocer el contenido del nuevo decreto GEL, sus componentes, y el marco de referencia de arquitectura Tecnología de Información (TI) entre las entidades.
- *Informar*: cada entidad profundizará en los contenidos, guiada por el equipo de acompañamiento del ministerio.
- *Entender*: es el punto en el que las entidades se apropian de los contenidos y herramientas, con ejemplos concretos que les permitan estructurar sus planes y proyectos según sus contextos y de forma articulada con la estrategia GEL.
- *Ubicar*: a partir de un diagnóstico que harán las mismas entidades, identificarán el nivel y estado respecto al cumplimiento de los logros del nuevo Decreto GEL.

Como resultado de la implementación de la estrategia en las entidades públicas de orden nacional en el 2014 se publicaron en la página de GEL los siguientes índices de resultados:

Fig. 3. Informe vive digital Colombia, Logros 2010-2015. Imagen tomada de http://es.slideshare.net/vivegobiernoenlinea/indice-de-gobierno-en-lnea

Fig. 4. Informe vive digital Colombia, Logros 2010-2015. Imagen tomada de http://es.slideshare.net/vivegobiernoenlinea/indice-de-gobierno-en-lnea

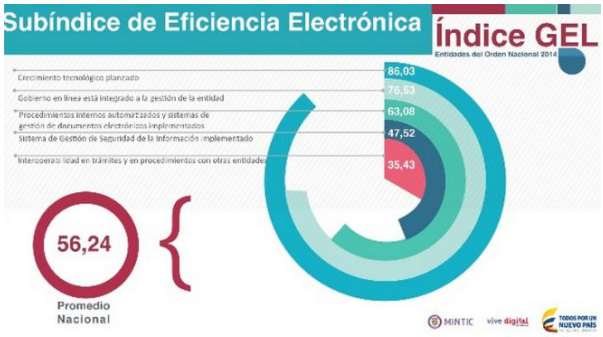

Fig. 5. Informe vive digital Colombia, Logros 2010-2015. Imagen tomada de http://es.slideshare.net/vivegobiernoenlinea/indice-de-gobierno-en-lnea

Fig. 6. Informe vive digital Colombia, Logros 2010-2015. Imagen tomada de http://es.slideshare.net/vivegobiernoenlinea/indice-de-gobierno-en-lnea

Es así como el fortalecimiento de las dinámicas de interacción con la ciudadanía y las empresas públicas como estrategia para mejorar la calidad de vida de los ciudadanos, los avances legislativos y los alcances logrados en su implementación pone a la vanguardia al Estado colombiano el proceso del gobierno electrónico, han permitiendo asumir los retos de un mundo cambiante y en medio de la globalización trayendo beneficios internos como el aumento en los niveles de eficiencia en la gestión pública, disminución en los costos de transacción y coordinación entre las diferentes entidades públicas, mejora la utilización de los recursos, aporta agilidad y transparencia a la gestión administrativa, apoyar a eliminar la corrupción. Sin embargo es claro que el reto de GEL debe continuar y que con el tiempo debe fortalecerse con la integración de otros gobiernos con el fin de mitigar y enfrentar los ataques a la seguridad de la información.

V CONCLUSIONES

La Seguridad y privacidad de la Información comprende acciones tendientes a garantizar la confidencialidad, la integridad y la disponibilidad de la información, así como la responsabilidad, la finalidad y el consentimiento relacionado con los datos personales.

Con la implementación de las estrategia GEL en Colombia, pretende garantizar a la ciudadanía una mejor comunicación, participación en interacción con las entidades estatales, lo mismo que el establecimiento de procesos transparentes, con servicios eficientes y optimizando los recursos públicos.

Uno de los principales obstáculos para la utilización de GEL es la percepción que se tiene de inseguridad en la utilización de canales electrónicos, por lo tanto es necesario fortalecer los procesos de seguridad de la información y difundirlos generando confianza en los ciudadanos.

El sistema de gestión de seguridad de la información para GEL está alineado con la familia de estándares ISO/IEC 27000 y COBIT.

Uno de los factores de éxito para la implantación del modelo de seguridad de la información en las entidades es contar con el compromiso por parte de directores y alta gerencia de la entidad para promover y soportar la implementación, la operación y los recursos del SGSI.

REFERENCIAS

[1] El Economista, Julio Sánchez Sep-2012 “Cómputo forense: los CSI de la informática” [Online]. Disponible: http://eleconomista.com.mx/tecnociencia/2012/09/20/computo-forense-csi-informatica

[2] Norma Técnica NTC-ISO-IEC Colombiana 27001-2013, (2013, Dic 11). Tecnología de la información: Técnicas de seguridad. Sistemas de gestión de seguridad de la información: Requisitos

[3] Reporte Global de las Naciones Unidas (2012, [Online]. Disponible: http://workspace.unpan.org/sites/Internet/Documents/EGovSurvey2012_Spanish.pdf

[4] Evolución del Gobierno en línea en Colombia. Disponible: [Online]. Disponible: http://viejoprograma.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/Documento_de_evoluci_n_de_la_pol_tica_GEL_20110630_1.pdf

[5] Gobierno en Línea presentará balance de resultados en todos los departamentos del país [Online]. Disponible: http://www.mintic.gov.co/portal/604/w3-article-6322.html

[6] Nuevo Decreto GEL, una nueva estrategia para Gobierno en línea 5/05/2015, [Online]. Disponible: http://www.mintic.gov.co/portal/604/w3-article-8651.html

[7] El Gobierno Electrónico como estrategia de participación ciudadana en la Administración pública a nivel de Suramérica -Casos Colombia y Uruguay” [Online]. Disponible: http://gyepro.univalle.edu.co/documentos/linc1.pdf

[8] Modelo De Seguridad De La Información Para La Estrategia De Gobierno En Línea 2.0 [Online]. Disponible: http://css.mintic.gov.co/ap/gel4/images/Modelo_Seguridad_Informacion_2_01.pdf

[9] Modelo De Seguridad De La Información Para La Estrategia De Gobierno En Línea 3.1 [Online]. Disponible: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf