SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO COLOMBIANO

Campos Ramírez, Jefferson Faruk
Especialización en Seguridad Informática, Universidad Piloto de Colombia
Bogotá, Colombia
Farcam.90@hotmail.com

Abstract* — *This article focuses on the Colombian public sector, describes the type of information the importance of your security and privacy challenges and challenges faced by the different entities to ensure its confidentiality, integrity and availability of information, changes in the regulations of Colombia in relation to the handling of information that defines the important implement the Colombian norms and standards aligned (ISMS) information security systems new safety requirements of security to comply with the requirements of the information privacy and security

Index Terms* — *ISMS, confidentiality, integrity, availability, security, privacy, Government online, information, open data, isms, SPI, asset, auditing, TIC, risks of security, public information, Government, State, effectiveness, transparency, policy, procedure and controls.

Resumen* — *Este artículo se centra en el sector público colombiano, describe su tipo de información, la importancia de su seguridad y privacidad, los retos y desafíos que afrontan las diferentes entidades para velar por confidencialidad, integridad y disponibilidad de la información, cambios en la normatividad de Colombia en lo referente al manejo de la información que definen nuevos requisitos de seguridad , lo importante de implementar sistemas de seguridad de la información (SGSI) alineados a la normatividad colombiana y estándares de seguridad para cumplir con los requisitos de seguridad y privacidad de la información.

***Índice de Términos* — *(SGSI), confidencialidad, integridad, disponibilidad, seguridad, privacidad, Gobierno en línea, información, datos abiertos, (SGSI), SPI, Activos, Auditoría, TIC, Riesgos de seguridad, información pública, Gobierno, Estado, eficacia, transparencia, política, procedimiento y controles*.**

I. INTRODUCCIÓN

El sector público en Colombia es el conjunto de entidades que pertenecen y son administradas por el Estado, entendiendo como Estado todo lo que forma parte de una sociedad, es decir que las entidades estatales por ser parte de una sociedad trabajan en beneficio de la Nación y de la ciudadanía colombiana. El gobierno tiene como objetivo desarrollar un estado más eficiente, transparente y participativo, para poder prestar los mejores servicios, lograr una excelente gestión generando confianza en los ciudadanos.

Las entidades del Estado necesitan hacer frente a las necesidades de la ciudadanía, mediante servicios electrónicos que permitan registrar, procesar y generar información pública, la cual se expone a diversas amenazas de seguridad comprometiendo su confidencialidad, integridad y disponibilidad. Por lo tanto el gobierno Colombiano ante los avances en la convergencia tecnológica y la demanda de servicios ha venido desarrollando medias y estrategias orientadas a la seguridad y privacidad de la información de la Nación y de la ciudadanía.

II. SECTOR PÚBLICO COLOMBIANO

El sector público está conformado por los organismos y/o entidades estatales que ejercen una función administrativa, buscando satisfacer las necesidades generales de los ciudadanos en conformidad con los principios y finalidades de las leyes y cometidos consagrados en la Constitución Política de Colombia. [1]

El sector público en Colombia está estructurado por el sector financiero y no financiero que se dedica a producir o suministrar bienes y servicios según sus funciones, de este subsector es propiedad y controlado por el gobierno, se clasifica en gobierno genera de la administración pública y empresas no financieras del Estado. [2]

A. Gobierno general de la administración pública

Son las instituciones de carácter público que suministran servicios de educación, justicia, defensa entre otros, financiadas por el cobro de impuestos y/o contribuciones obligatorias. [2]

B. Empresas no financieras del Estado.
Entidades que producen y venden bienes y servicios, son financiadas por sus ingresos de costos. [2]

III. INFORMACIÓN DEL SECTOR PÚBLICO

La información pública en Colombia es aquella que atañe a la Nación y la ciudadanía. La cual es registrada, procesada y generada, en beneficio del gobierno y de la ciudadanía. La cual tiene un valor de gran importancia ya que de ella se desarrollan servicios y se solucionan necesidades para la sociedad. La información del sector público es considerada como un bien público y en la constitución colombiana se establece el derecho a su acceso por parte de los ciudadanos.

En los esfuerzos del gobierno por estructurar la información, se generó el concepto de datos abiertos, donde se pone a disposición de los ciudadanos y de las empresas información pública que permita garantizar la transparencia y efectividad en la administración de las entidades, para mejorar la calidad de vida de los ciudadanos. [3]

IV. IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO

La información del sector público por estar ligada a la Nación y a la ciudadanía se convierte en un bien público que debe ser protegido. A esta información se le debe conservar su confidencialidad, integridad y disponibilidad. La información pública atañe a la Nación y la ciudadanía por lo tanto se ve expuesta a cualquier amenaza que represente un manejo antijurídico que puede afectar sus propiedades. Es de suma importancia la aplicación de la seguridad en la información pública ya que así se podrá preservar y proteger ante las diferentes amenazas y situaciones que puedan llegar afectarla, generando confianza en la ciudadanía y en las personas que proporcionan y/o usan este tipo de información, contribuyendo a mejorar la transparencia en el ejercicio de la administración pública de las entidades del Estado. La implementación de sistemas de gestión de seguridad de la información se hace importante ya que ayuda a preservar la seguridad y la privacidad de la información en el sector público, previniendo así que la información pública sea utilizada en ambientes inseguros que la puedan poner en riesgo frente amenazas, que puedan desestabilizar la continuidad de los procesos y el cumplimiento de objetivos en la gestión administrativa del sector público. [4]

V. ESTRATEGIA DEL GOBIERNO PARA LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO

El sector público pensando en adaptarse con facilidad y seguridad a las necesidades de la ciudadanía, diseño la estrategia de gobierno en línea en donde se contempla la seguridad y privacidad de los datos que hacen parte del sector público y de la ciudadanía. Buscando garantizar un gobierno más operativo, eficiente, transparente y seguro para los ciudadanos.

La estrategia de gobierno en línea del sector público colombiano tiene bases de la norma ISO/IEC 27001/2013, donde ofrece a las entidades del Estado asegurar la información y velar por su privacidad, mediante esquemas de sistemas de gestión de seguridad de la información, fortaleciendo las (TIC) en todas las entidades del estado que implementen la estrategia. [5]

VI. NORMATIVIDAD, LEGISLACIÓN Y ESTÁNDARES REFERENTES A LA SEGURIDAD DE LA INFORMACIÓN

A la hora de asegurar la información del sector público, se debe tener en cuenta el contexto en que se encuentra la seguridad de la información y al que hace parte cada entidad del estado, la normatividad y la legislación que rige el manejo de la información lo que define los requisitos de seguridad en la implementación de un sistema de gestión de seguridad de la información, lo que hace que se modifique las veces que sea necesarias y que se mantenga actualizado. Al tener en cuenta la normatividad, legislación y estándares para el manejo y aseguramiento de la información se logra tener un gobierno más eficiente y confiable para los ciudadanos, al cumplir con los requisitos legales que se generan para cubrir las necesidades de los ciudadanos en cuanto al uso de la información, desarrollando un nivel de madurez en cuanto a seguridad en la administración de las entidades. [6]

A continuación se describen Algunos de los ítems legales y recomendables a tener en cuenta a la hora de realizar el aseguramiento de la información:

A. Artículos de la constitución política de Colombia : [7]

1. Artículo 15: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

2. Artículo 20**:** Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

3. Artículo 23: Toda persona tiene derecho a presentar peticiones respetuosas a las autoridades por motivos de interés general o particular y a obtener pronta resolución. El legislador podrá reglamentar su ejercicio ante organizaciones privadas para garantizar los derechos fundamentales.

4. Artículo 74: Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley. El secreto profesional es inviolable.

B. Leyes relacionadas con el manejo de la información en Colombia

1. Ley de Habeas Data: Es el derecho que tiene toda persona para conocer, actualizar y rectificar toda aquella información que se relacione con ella y que se recopile o almacene en centrales de información. [8]

2. Ley 23 de 1982: Contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia. [9]

3. Ley 594 de 2000: La presente ley tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado [10]

4. Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [11]

5. Ley 1581: La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. [12]

6. Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. [13]

C. Estrategia de Gobierno en línea

Es la estrategia de gobierno electrónico que busca construir un buen gobierno a partir de las (TIC), en la cual se define un marco de la seguridad y privacidad de la información y de los sistemas de información. [5]

D. Norma ISO 27001

Esta norma contiene un estándar de seguridad de la información, la cual se publicó en el año 2005, con el objetivo de brindar un modelo para el establecimiento y administración de sistemas de gestión de seguridad de la información (SGSI). En la versión del año 2005 presenta una estructura enfocada a procesos y presenta una guía en la definición de un (SGSI), la realización de análisis de riesgos y definición de controles que permitan proteger los activos de las entidades.

En la actualización del manual de gobierno en línea del año 2015 se tuvo en cuenta los lineamientos de la nueva versión del año 2013 de la norma (ISO 27001), donde ya no se enfoca un sistema de gestión de seguridad basado en procesos, sino al cumplimiento de objetivos generarles de seguridad y donde se define el contexto que permita conocer el diagnóstico de la seguridad de la información. [14]

VII. SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL SECTOR PÚBLICO

Los sistemas de Gestión de Seguridad de la Información son las estructuras organizacionales de seguridad, los cuales están orientados a definir responsabilidades en cuanto a seguridad en la administración de las empresas, diseñar e implementar políticas, procesos y procedimientos que permitan establecer los objetivos de seguridad, conocer sus riesgos y la forma de asegurar la información frente a las posibles amenazas a la que se vea expuesta.

Los sistemas de gestión de la información en las entidades del Estado se implementan de acuerdo a la normatividad legal vigente de Colombia y a los estándares de seguridad de la información tales como la norma (ISO/IEC 27001/2013), contemplada en la estrategia de gobierno en línea y su nuevo manual de seguridad y privacidad de la información.

Mediante el programa "gobierno en línea" se busca generar una administración más eficiente y segura, mediante la implementación de sistemas de gestión de seguridad en las entidades del Estado, de orden nacional y territorial, llevando un acompañamiento a las entidades por parte del Ministerio de las Tecnológicas de la Información y las Comunicaciones (MINTIC) con el objetivo de orientar la implementación, seguimiento y mejora continua de los sistemas de gestión de seguridad de la información en el sector público Colombiano.

Investigaciones reflejan que varias de las entidades no han implementado sistemas de gestión de seguridad de la información, de las que están en el proceso de implementación, muy pocas tienen un avance notable en la fase del actuar después de una verificación al sistema y el resto están entre la planeación y ejecución. Lo que ha demostrado que con las nuevas políticas y estrategias desarrolladas por el gobierno en cuanto a seguridad de la información han generado un aumento en el nivel de conciencia sobre la importancia de proteger la información en las entidades. Con la implementación de sistemas de gestión de seguridad de la información en las entidades del Estado, se garantiza en el sector público el buen uso de la información asegurándola frente a escenarios no seguros. [15]

En la nueva versión del manual de gobierno en línea en el módulo de seguridad y privacidad de la información, se propone un modelo de (SGSI), que permita proteger la información y sus sistemas de acceso, manipulación, difusión, obstaculización o modificación no autorizada. [5]

En el nuevo modelo de seguridad y privacidad de la información de la estrategia de "gobierno en línea), el gobierno propone un nuevo esquema de sistema de gestión de la seguridad que está orientado por la norma (ISO/IEC 27001/2013). [5]

El modelo de sistema de gestión de seguridad de la información propuesto por el Estado en la estrategia de "gobierno en línea" tiene las bases para la implantación de un sistema de gestión de seguridad la información en cinco fases, las cuales permitirán a las entidades del sector público gestionar de forma eficiente la seguridad y privacidad de su información, con el objetivo de fortalecer la protección de la información y dar cumplimiento a los demás módulos de la estrategia de "gobierno en línea". En este modelo se tienen en cuenta niveles de madurez para tener una trazabilidad en la evolución continua de la seguridad de la información en las entidades del Estado [16].

El modelo propuesto por el gobierno en su operación y desarrollo de sus cinco fases, presenta objetivos, metas y herramientas que permiten que la seguridad y privacidad de la información sea sostenible en los sistemas de gestión de seguridad de la información dentro de las entidades del Estado. [16]

Fig. 1. Marco de seguridad y privacidad de la información de la estrategia de Gobierno en Línea[1].

A continuación se describe el marco operativo del modelo de seguridad y privacidad de la información en los sistemas de gestión de seguridad de la información del sector público: [16]

A. Diagnóstico de la seguridad y privacidad de la información

Esta fase busca definir el Estado de las entidades frente a los requerimientos de seguridad y privacidad de la información, determinando el contexto de la seguridad, teniendo en cuenta la infraestructura tecnológica con que cuenta, identificando el nivel de madurez de seguridad en la entidad mediante la ejecución de pruebas que permitan conocer la efectividad de las medidas de seguridad implementadas. [16]

Dicho diagnóstico se define en la norma (ISO/IEC 27001:2013) en su numeral cuatro, donde hace hincapié en la identificación de los problemas internos y externos, que rodean a las entidades en lo referente a seguridad y privacidad de la información. Es aquí donde se analizan los riesgos existentes asociados a la perdida de la confidencialidad, integridad y disponibilidad de la información, el análisis del contexto de seguridad en que se encuentra la entidad frente a sus objetivos. [14]

B. Planificación de la seguridad y privacidad de la información

Esta fase tiene como objetivo generar el plan de seguridad y privacidad de la información correlacionada con la misión de la entidad. Define el esquema metodológico que permite precisar el alcance, objetivos, políticas, procesos y procedimientos pertinentes para la gestión del riesgo y mejora de la seguridad de información, así como la toma de decisiones en la definición de controles de seguridad que permitan dar cumplimiento a las metas propuestas en el sistema de gestión de seguridad de la información. [16]

El modelo de seguridad y privacidad de la información de la estrategia de "gobierno en línea" en la fase de definición del plan de seguridad se ha basado en la norma (ISO/IEC 27001:2013) utilizando el numeral 4. Contexto de la información, 5. Liderazgo, 6.Planeación y 7. Soporte, generando la estructura organizacional de seguridad, estableciendo responsabilidades y compromiso desde la alta dirección, definiendo políticas, procesos y procedimientos que permitan establecer las mejores medidas de seguridad, con el objetivo de cumplir misión de seguridad de la información en la entidad establecida en el (SGSI). [14]

Esta fase genera entregables tales como, documentación del alcance y límites de la seguridad de la información, con aprobación y socialización por la alta dirección al interior de la entidad, resolución o acto administrativo por el cual se crea o se modifica las funciones del comité de gestión institucional en donde estén incluidos los temas de seguridad y privacidad de la información, políticas de seguridad y privacidad de la información, procesos y procedimientos integrados a los sistemas de gestión de la entidad y documentación de los inventarios de activos de información los cuales se van asegurar. [16]

C. Implementación de la seguridad y privacidad de la información

Después de haber realizado la debida planeación estratégica de seguridad y privacidad de la información, es en esta fase donde se procede con el

[1] Imagen tomada del modelo de seguridad y privacidad de la información publicado por el Ministerio de Tecnologías de la Información y las comunicaciones de Colombia, disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

plan de implementación, donde se busca ejecutar de manera específica la estrategia del sistema de gestión de la seguridad, llevando a cabo las actividades necesarias para el cumplimiento de las metas definidas. [16]

Del plan implementación se generan actividades de planificación y control operacional, implementación del plan de tratamiento de riesgo y controles de seguridad. [16]

Esta fase toma el numeral 8, denominado operación de la norma (ISO/IEC 27001:2013), donde se ejecuta la gestión de riesgos, identificando aquellos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, con el fin de cumplir con las expectativas de la entidad frente a la seguridad y privacidad de la información. [14]

Igualmente, dicha etapa genera la documentación de la estrategia de planificación y control operacional, informe de los resultados del plan de tratamiento de riesgos, el cual debe incluir la implementación de los controles definidos en una declaración de aplicabilidad, metas e indicadores de la gestión seguridad de la información. Toda la documentación que se genera esta fase debe estar revisada y aprobada por la alta dirección. [16]

D. Gestión de la seguridad y privacidad de la información

Esta fase tiene como finalidad realizar una trazabilidad al desempeño del sistema de gestión de seguridad de la información, realizando las calificaciones a su operatividad y eficiencia, definiendo los niveles de cumplimiento de los principios de la seguridad y privacidad de la información. Como resultado de este seguimiento se generan los cambios pertinentes y oportunos de la seguridad en los sistemas de gestión. [5]

La entidad en esta fase debe implementar acciones que promuevan una mejora continua, y que garanticen el cumplimento de las metas de seguridad y privacidad de la información en los (SGSI). [5]

En la fase de evaluación y desempeño se producen los planes de seguimiento y análisis de seguridad y privacidad de la información al (SGSI), auditorías internas y evaluación del plan de tratamiento de riegos. [16]

Como resultado de esta fase, se genera documentación de los registros del plan de seguimiento y evaluación del (SGSI), auditorías internas, seguimiento y monitoreo del plan de tratamientos de riegos, donde esta documentación debe estar revisada y aprobada por la alta dirección de la entidad. [16]

En cuanto a la evaluación de desempeño de la seguridad y privacidad de la información en los (SGSI) la norma (ISO/IEC 27001:2013) en su numeral 9, denominado evaluación del desempeño, se establece lo que se debe considerar para medir la efectividad y desempeño del (SGSI), donde es de vital importancia la realización de auditorías internas; para sus revisiones se debe tener en cuenta el estado de los planes de acción que permitan atender las no conformidades en cuanto a la seguridad y privacidad de la información. [14]

E. Mejora continua de la seguridad y privacidad de la información

Esta fase le permite a la entidad realizar mejoras continuas en la seguridad y privacidad de la información al (SGSI), implementando las acciones correctivas a los resultados de la fase de evaluación de desempeño. [16]

Dicha etapa genera el plan de seguimiento, evaluación y análisis en la seguridad de la información para el (SGSI). [16]

La norma (ISO/IEC 27001:2013) propone en su numeral 10 denominado mejora, que los principales elementos del proceso son las no conformidades identificadas, las cuales deben tener una trazabilidad, asegurando que no se repitan y que las acciones correctivas sean efectivas. [5]

VIII. INDICADORES DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

El gobierno en su estrategia de seguridad y privacidad de la información ha desarrollado la guía técnica de indicadores de gestión para medir el avance y el desempeño de la seguridad en los (SGSI), lo cual es de gran ayuda para la fase de mejora continua del modelo de seguridad y

privacidad en los (SGSI) propuesto en la estrategia de gobierno en línea. [17]

A continuación se nombra una serie de indicadores propuestos, que serán de gran ayuda para las entidades del Estado a la hora de realizar una trazabilidad a sus sistemas de gestión de la seguridad de la información:

- Organización de seguridad de la información.
- Cubrimiento del (SGSI) en los activos de información.
- Tratamientos de eventos relacionados en el marco de seguridad y privacidad de la información.
- Plan de Sensibilización.
- Cumplimiento de políticas de seguridad de la información.
- Identificación de lineamientos de seguridad
- Verificación de controles.
- Aseguramiento en la adquisición y mantenimiento de software.
- Implementación de los procesos de registro y auditoria.
- Políticas de privacidad y confidencialidad.
- Verificación de políticas de integridad de la información.
- Políticas de disponibilidad del servicio y de la información.
- Ataques informáticos a la entidad.
- Porcentaje de disponibilidad de los servicios de gobierno en línea que presta la entidad.
- Porcentaje de implementación de controles.

IX. RETOS DE LA SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO COLOMBIANO

El gobierno se enfrenta a obstáculos en cuanto a seguridad que se presentan en las entidades del Estado como los ataques a la seguridad, la baja capacidad de respuesta a incidentes de seguridad, una falta de conciencia y cultura en seguridad de la información, la poca articulación de las entidades, los avances en la convergencia tecnológica y las necesidades de servicios para los ciudadanos. El sector público afronta el reto de incrementar los niveles de madurez y fortalecer las capacidades en la apropiación de la seguridad y privacidad de la información en las entidades del Estado, buscando a través de estrategias como la de gobierno en línea y generando esquemas de seguridad y privacidad de la información, adquiriendo el uso seguro de la información y apropiación de las (TIC).

X. CONCLUSIONES

Con los avances en las tecnologías de la información y las comunicaciones en Colombia y la creciente demanda de servicios en línea ofrecidos a los ciudadanos se ha pensado en crear un mejor gobierno, eficiente y transparente, donde las entidades del Estado se deben esforzar por generar confianza en el uso de la información pública y apropiación de las (TIC), mejorando la privacidad y seguridad de la información.

El gobierno, pensando en mejorar la seguridad de las (TIC) y la información del sector público, desarrolló un marco de seguridad y privacidad en su estrategia de gobierno en línea, utilizando bases de la norma (ISO/IEC 27001:2013) estándar de seguridad de la información para la implementación de un (SGSI), enfrentándose a los diferentes obstáculos que se presentan al exterior e interior de las distintas entidades del Estado en lo referente a la seguridad de la información. A través de la trazabilidad que se la ha hecho a los (SGSI) de las entidades en el análisis de la seguridad es evidente que se deben aumentar los esfuerzos de articulación entre entidades y sus (TIC), implementando y alineando los (SGSI) de acuerdo a la normatividad colombiana que orienta el buen uso y de la información, de igual forma se recomienda a las entidades del Estado hacer uso del esquema de seguridad que presenta la estrategia de gobierno en línea así como también utilizar la norma (ISO/IEC 27001:2013) en la implementación de sus (SGSI), ya que permite orientar el diseño y desarrollo de una estructura organizacional de seguridad bajo políticas, procesos y procedimientos que ayuden a mejorar la seguridad en las entidades, permitiendo cumplir con el objetivo de crear un mejor gobierno, donde se genere confianza en el uso de la información y apropiación de (TIC) del Estado, aumentando así la participación ciudadana.

REFERENCIAS

[1]. Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, “LEY 489 DE 1998”, Disponible en:

http://www.mintic.gov.co/portal/604/articles-3676_documento.pdf

[2]. Universidad Santo Tomas de Villavicencio, Filosofía Política, "Sector público y privado en Colombia", Disponible en: http://es.slideshare.net/CarlosAJimenezC/sector-pblico-y-privado-en-colombia

[3]. "Lineamientos para la implementación de datos abiertos en Colombia", Disponible en: http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/Resumen_Ejecutivo_Datos_Abiertos.pdf

[4]. Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, "Modelo de Seguridad y privacidad de la información", Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

[5]. Gobierno en línea, "Manual de Gobierno en línea", Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf

[6]. Universidad del Norte - Catalogo de Publicaciones en línea, "El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma iso 27 001", Disponible en: http://rcientificas.uninorte.edu.co/index.php/derecho/article/download/2700/1811

[7]. Rama Judicial, "Constitución Política de Colombia de 1991", Disponible en: https://www.ramajudicial.gov.co/documents/10228/1547471/CONSTITUCION-Interiores.pdf/8b580886-d987-4668-a7a8-53f026f0f3a2

[8]. Súper Intendencia de Industria y Comercio, "Ley 1266 de 2008" Disponible en: http://www.sic.gov.co/drupal/sites/default/files/files/ley1266_31_12_2008(1).pdf

[9]. Ministerio de tecnologías de la información y las Comunicaciones de Colombia, "Ley 23 de 1982", Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3717.html

[10]. Ministerio de tecnologías de la información y las Comunicaciones de Colombia, "Ley 594 de 2000", Disponible en: http://www.mintic.gov.co/portal/604/w3-propertyvalue-594.html

[11]. Ministerio de tecnologías de la información y las Comunicaciones de Colombia, "Ley 1273 de 2009", Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html

[12]. Presidencia de la República de Colombia, "Ley 1581 de 2012", Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

[13]. Ministerio de tecnologías de la información y las Comunicaciones de Colombia, "Ley 527 de 1999", Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3679.html.

[14]. Magazcitum, ", Estructura del nuevo estándar ISO/IEC 27001:2013", Disponible en: http://www.magazcitum.com.mx/?p=2397#.VXdLPM9_NBc

[15]. Ministerio de tecnologías de la información y las Comunicaciones de Colombia, "Noticia Hora de implementar buenas prácticas de seguridad de información pública", Disponible en: http://www.mintic.gov.co/portal/604/w3-article-5414.html

[16]. Ministerio de tecnologías de la información y las Comunicaciones de Colombia, "Modelo de Seguridad y Privacidad de la Información", Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

[17]. Ministerio de tecnologías de la información y las Comunicaciones de Colombia, "Guía de indicadores de la gestión para la seguridad de la información", Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Indicadores.pdf