REALITY OF THE IMPLEMENTATION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM ON MUNICIPAL MAYORALTY CATEGORY 6

Article Information:

Received: October 5, 2013
Accepted: December 19, 2013

Keywords: Government Online, Management system of information security, Information technology, Information security, Models and standards

Abstract: The Colombian State seeking to be a world leader on the use of information technology and communications (TIC) to improve management processes and management in all areas. For this reason, the Government has created Online program (GEL), where the general guidelines of the GEL strategy is established and its performance is guaranteed by implementing manual GEL v3.1, which contains the component "cross members" related to the implementation of a Management System of Information Security (SGSI). Since it is government policy to deploy the SGSI throughout the national territory, this document details the ISMS and describes the reality of its implementation, particularly those municipalities category 6, because the municipalities with less population and income (Law 1551, July 6, 2012, Congress of Colombia).

REALIDAD DE LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LAS ALCALDÍAS MUNICIPALES CATEGORÍA 6

Ángela Indira Suárez Casas[1], Esp., Pablo Fernando Páez Cely[2], Esp., John A. Bohada[3], Ph.D.

Grupo de Investigación Muisca, Facultad de Ingeniería, Fundación Universitaria Juan de Castellanos, Tunja, Colombia.

[1]aindirasc@gmail.com, [2]pfpc98@hotmail.com, [3]jbohada@jdc.edu.co

Información del artículo:

Recibido: 05 de octubre de 2013
Aceptado: 19 de diciembre de 2013

Palabras Clave: Gobierno en Línea (GEL), Sistema de Gestión de Seguridad de la Información (SGSI), Tecnologías de la Información (TI), Seguridad de la información, Modelos y estándares internacionales.

El Estado Colombiano buscando estar a la vanguardia mundial respecto al uso de las Tecnologías de la Información y las Comunicaciones (TIC) para mejorar los procesos de gestión y administración en todas sus áreas. Por esta razón, ha creado el programa Gobierno en Línea (GEL), donde se establecen los lineamientos generales de la estrategia GEL y cuyo cumplimiento se garantiza mediante la implementación del manual GEL v3.1, el cual contiene el componente "elementos transversales" relacionado con la ejecución de un Sistema de Gestión de Seguridad de la Información (SGSI). Dado que es política del gobierno realizar la implementación de los SGSI en todo el territorio nacional; este documento detalla el SGSI y describe la realidad de su implementación, particularmente aquellos municipios de categoría 6, por cuanto son los municipios con menor cantidad poblacional y de ingresos (ley 1551, 6 de julio de 2012, Congreso de Colombia).

1. INTRODUCCIÓN

El presente artículo tiene por objeto dar a conocer a las entidades territoriales (Alcaldías y Gobernaciones), en su definición de Alcaldías Categoría 6 [1], la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) [2], reconociendo la seguridad como un factor primordial para la apropiación de las Tecnologías de la Información (TI) en la prestación de servicios a través de medios electrónicos que debe ser respaldado por un sistema de gestión de políticas y procedimientos adecuados, orientados a proteger el activo más importante de cualquier entidad, preservando los principios básicos de la información que se describen a continuación:

- **Confidencialidad:** Garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma [3].
- **Integridad:** Se refiere a la exactitud, totalidad y consistencia de los elementos de la información y los métodos de almacenamiento y procesamiento [4].
- **Disponibilidad:** Garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, al momento que se requiera [5].

Las alcaldías municipales categoría 6 deben asegurar la sostenibilidad del SGSI mediante la ejecución de los recursos ofrecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC) como son lineamientos, metodologías, guías o anexos y estándares indicados en el manual 3.1 Gobierno en Línea GEL [6], componente de elementos transversales, que ofrece unas herramientas de apoyo para el establecimiento del SGSI contemplando el análisis de riesgos (ISO 27000 [7]) y las medidas a establecer en la entidad.

En el Manual GEL 3.1 para la implementación del SGSI, los lineamientos comprenden el establecimiento de la política, implementación del modelo, operación, monitoreo, revisión, mantenimiento y mejoramiento. Por lo tanto, es importante conocer los requisitos y etapas para la implementación del modelo de seguridad abordando aspectos que involucran la preparación de la entidad mediante el desarrollo de actividades de sensibilización, apropiación, apoyo y participación a través de sus funcionarios y contando con el compromiso de la alta gerencia para gestionar y soportar la implementación, la operación y los recursos necesarios del SGSI. Estos lineamientos tienen en cuenta una serie de prerrequisitos donde se hace necesario que la entidad cuente con la estructura organizacional de GEL, el compromiso de la alta gerencia da continuidad al sistema frente a posibles cambios en la dirección, así como la integración y unificación de los sistemas de gestión con sistemas comunes; se resalta además, que la responsabilidad sobre el sistema no debe recaer de manera exclusiva sobre el encargado del departamento de tecnologías de información y comunicaciones, puesto que en la coordinación local de seguridad [8] se indica como medida o control, la asignación de las responsabilidades a cada Jefe de departamento.

De igual forma, dentro de los lineamientos se toman en cuenta los factores críticos de éxito, que son componentes incluidos dentro del SGSI, los cuales deben ser estimados y contenidos para ver su alcance en la entidad. Dichos factores consideran los siguientes elementos:

- El interés de la administración se muestra vinculando activamente a cada miembro de la entidad, mostrando la importancia de proteger la información a través de políticas que respaldan el SGSI.
- Se deben definir los requerimientos de seguridad mediante la identificación y clasificación de sus activos de información de acuerdo con las necesidades de la entidad.
- La entidad debe contar con una política de seguridad (**ISO/IEC 27001:2005**) [9], que se articule con todas las áreas para garantizar su aplicación, asegurando los procesos y servi-

cios ofrecidos a través de las tecnologías de la información.

- Realizar análisis de riesgos, identificando y evaluando cada uno de los activos, respecto a los principios de la información, estableciendo controles que mitiguen, acepten o transfieran el riesgo.
- Aceptación de la alta gerencia respecto a la implementación del SGSI.
- Definir perfiles, roles y responsabilidades, de los funcionarios participantes en la implantación SGSI.
- Realizar jornadas de sensibilización: concientización, entrenamiento, educación y retroalimentación.
- Medir el desempeño del SGSI aplicando herramientas de evaluación, que generen reportes del estado actual.

Además, los lineamientos establecen unos requisitos de seguridad que la entidad debe cumplir; estos a su vez establecen el plan de seguridad para los diferentes niveles (nivel inicial, nivel básico, nivel avanzado y nivel de mejoramiento permanente), que según el manual GEL 3.1 se resaltan tres aspectos importantes: el nivel del plan de seguridad, el detalle del requisito y el recurso necesario.

2. METODOLOGÍA

El Sistema de Gestión de Seguridad de la información es tal vez un término poco común entre las entidades públicas, y seguramente la inclusión dentro de los procesos y procedimientos en cada una de las Alcaldías es casi nulo; pero su implementación se debe cumplir mediante el acatamiento del decreto 2693 de 21 de diciembre 2012 [10], donde invita a cada alcalde o alcaldesa, a ceñirse a las indicaciones dadas por la misma.

Para poder identificar el avance en el desarrollo de los SGSI en cada Administración Municipal, el MINTIC, junto al Centro de Ciencia y Tecnología de Antioquia (CTA [11]), adelantaron una autoevaluación denominado autoevaluación - definición de brecha - modelo de seguridad de la información para la estrategia de Gobierno en Línea 2.0 [12], documento propio del programa GEL. Esta Autoevaluación consiste en una encuesta básicamente estructurada en dos partes: La primera diseñada para obtener información sobre el uso de algunas medidas de protección, indagando sobre posibles pérdidas de información y por qué se han dado [13]. La segunda parte se incluyó, para determinar la forma en que el SGSI, se integra con otros sistemas de Gestión y qué tanta importancia recibe por parte de los directivos de la administración municipal [14].

Así mismo, es importante mencionar que la encuesta o autoevaluación se desarrolló junto al webmaster, o el encargado del área de Sistemas, o al líder de GEL asignado en cada alcaldía; la encuesta fue aplicada por parte de un funcionario, llamado delegado Territorial Gobierno en Línea del CTA, quien a su vez orientó a los funcionarios y despejó las dudas para que los resultados fueran lo más precisos posibles. Luego de realizado el acompañamiento en cada uno de los municipios, se procedió a tabular la información de cada entidad haciendo uso de herramientas ofimáticas, encontrándose que todos los municipios están ubicados en nivel inicial para la implementación del sistema de gestión de seguridad de la información.

3. ANTECEDENTES

Gobierno en Línea [15], ha surgido como una necesidad en Colombia, debido a las grandes transformaciones que el planeta ha venido afrontando en la forma en que operan los estados y la responsabilidad frente a las exigencias de la sociedad, llevando al Gobierno a tomar medidas que permitan fortalecer la eficiencia, eficacia, visibilidad y publicidad; para los ciudadanos que con más fuerza piden soluciones a situaciones críticas como, el desempleo, la pobreza, la salud, el

medio ambiente y otros más, cuyo fin último es mejorar la calidad de vida de los mismos.

Luego de un camino recorrido previamente por el decreto 1151 del 14 de abril de 2008 [16], que estableció los lineamientos generales de la estrategia GEL, donde las entidades del orden Territorial (Alcaldías y Gobernaciones), debían cumplir con la implementación de cinco fases (información, interacción, transacción. transformación, participación y democracia), en unos tiempos establecidos. Este decreto no fue cumplido a cabalidad en los tiempos de ejecución, ni en el cumplimiento de los lineamientos fijados en cada fase, razón por la cual, el Gobierno nacional mediante decreto 2693 del 21 de diciembre de 2012 [10], conmina a las entidades territoriales al cumplimiento de 6 componentes; de los cuales hacen parte los cinco componentes del decreto 1151 de 2008 [16], (Norma derogada), y además se crea el componente elementos trasversales, donde se invita a las entidades territoriales, a implementar las siguientes actividades: 1. Institucionalizar la estrategia de Gobierno en Línea; 2. Centrar la atención en el usuario; 3. Implementar un Sistema de Gestión de Tecnologías de Información; 4. Implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

En el Manual 3.1 de GEL se dan las pautas sobre el abordaje para SGSI, donde se indica la forma en que se deben desarrollar cada una de estas actividades, y para el caso del SGSI, se realiza mediante la herramienta de mejora continua, ciclo PHVA [17], presentada por Deming luego del año 1950, compuesta de 4 pasos: Planear (Plan), Hacer (Do), Verificar (Check) y Actuar (Act); de ahí que derive su nombre PHVA. La cual está relacionada directamente con los niveles de madurez descritos en los lineamientos de implementación del modelo de seguridad de la información 2.0, propuestos por Gobierno en Línea, que se exponen en la Tabla 1:

Tabla 1. Relación entre PHVA y los lineamientos de implementación del modelo de seguridad de la información 2.0

Etapas PHVA	**Lineamientos de implementación del modelo de seguridad de la información 2.0** ***(Grados de madurez)***
Planear (Plan)	Nivel inicial
Hacer (Do)	Nivel básico
Verificar (Check)	Nivel avanzado
Actuar (Act)	Nivel de mejoramiento continuo

Fuente: Los autores, 2016

Para cada una de las etapas mencionadas en la Tabla 1, se proponen una serie de actividades que deben realizarse de acuerdo con el nivel de madurez en el cual se ubique la Entidad Territorial, cumpliendo con los tiempos sugeridos en el documento, ajustados a los lineamientos de implementación del modelo de seguridad de la información 2.0 definido por el MINTIC.

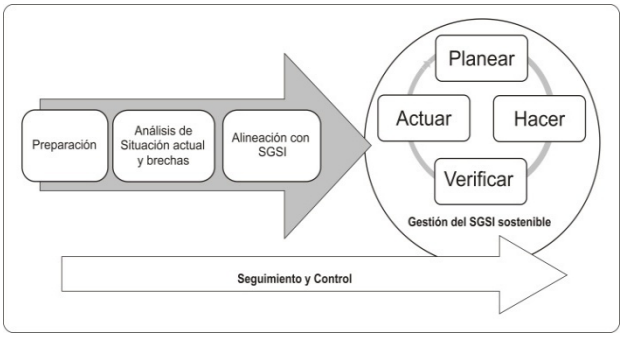
4. IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN NIVEL INICIAL

El Estado en procura de asegurar que se lleve a cabo la estrategia Gobierno En Línea [18] en cada uno de sus componentes, incorpora a través del decreto 2693 de 2012 y manual GEL 3.1, el componente de elementos transversales, el cual define una serie de actividades que se interrelacionan con las demás áreas temáticas, la protección de las relaciones del Estado con los usuarios, y a su vez permite que las entidades identifiquen en la información un activo de gran importancia que debe ser protegido a través de la implementación del SGSI. Para lo cual se plantea una estrategia de trabajo divida en una serie de lineamientos básicos ("Sistema de atención de seguridad de la in-

formación de GEL, Estratificación de entidades, Control de seguridad, Indicadores de Seguridad y Lineamientos para la implementación del modelo de seguridad de la Información" [19]), los cuales están alineados con los niveles de madurez indicados en el manual GEL 3.1, que los define como "un estado de evolución de la implementación de la estrategia y sirven como referente para establecer el avance en términos generales en cada uno de los componentes" [20] de la estrategia GEL. Los niveles mencionados se clasifican en: Plan de seguridad nivel inicial, Plan de seguridad nivel básico, Plan de seguridad nivel avanzado y Plan de seguridad nivel de mejoramiento permanente [21]. Para nuestro caso atenderemos las consideraciones necesarias para la implementación del plan nivel inicial.

El plan tiene como objeto identificar el estado actual de la entidad y medir el grado de madurez que ha desarrollado en cuanto a la seguridad de la información y, a partir de esta identificación, iniciar un ciclo PHVA [22]-[23]-[24] (Planear-Hacer-Verificar-Actuar) como un modelo de mejora continua y sostenible (ver Figura 1), para lo cual las entidades deben definir los objetivos, actividades y duración, soportados en el modelo de gestión.

Figura 1. Plan de Implementación del Sistema de Gestión de Seguridad de la Información en las entidades [25]



Fuente: Gobierno en Línea 2.0, 2011

Es importante aclarar que antes de vincular las actividades que se indican en la Figura 1, se deben definir los objetivos orientados a concientizar a la alta gerencia y funcionarios acerca de la importancia de proteger la información e incluir en la construcción del SGSI los factores críticos de éxito.

Posteriormente, se establecen una serie de actividades como se muestran en la Figura 1 que corresponden a: 1. Preparación, 2. Análisis de la situación actual y brechas, 3. Alineación con el SGSI, actividades tenidas en cuenta para determinar el nivel actual de madurez al que pertenece la entidad. Dentro de estas actividades se debe dar cumplimiento a una serie de etapas previas a la implementación del sistema de gestión que deben ser consideradas para lograr compromiso por parte de la alta gerencia y sus funcionarios dentro de la entidad.

La etapa de preparación sugiere, que la entidad se comprometa en implementar a cabalidad las actividades definidas para esta fase: "formación de capacitadores, campaña de sensibilización a las entidades públicas y privadas y plan de capacitación para las entidades públicas" [26]

Luego, las siguientes actividades deben partir del hecho que la entidad haya completado el proceso de formación, sensibilización y capacitación de sus funcionarios para la correcta implementación del SGSI, las cuales corresponden a: involucrar y sensibilizar la alta dirección, identificar los responsables, y caracterizar los perfiles y responsabilidad.

El segundo ítem define el análisis de la situación actual y la definición de brechas. Se define brecha como "la ausencia total o parcial en la estructura, las políticas, los controles, directrices, procesos y/o procedimientos existentes al interior de la entidad, al ser comparadas con las requeridas por el Manual GEL 3.1, para cada etapa de madurez" [27], esta actividad se enfoca en la adquisición de conocimiento que tiene la entidad frente al modelo de seguridad y los lineamientos establecidos en el manual.

La definición del alcance del sistema de gestión, está soportada con base en las características que

identifican a cada entidad; las sedes, los activos de información, las funciones claves del negocio, procesos, procedimientos y las tecnologías que estarán cubiertas por el sistema. Así mismo, se establecen las políticas de seguridad. "La política del SGSI es un documento de alto nivel que aborda la necesidad de un sistema de gestión para la seguridad de la información." [28], este documento debe ajustarse a las condiciones específicas y particulares de la Administración Municipal, y para garantizar su cumplimiento requiere la firma del mandatario local, quien respalda la política y permite el debido cumplimiento del contenido allí plasmado.

Además, se sugiere llevar a cabo un análisis del riesgo mediante una aproximación a través de la selección y aplicación de una metodología (**OCTAVE** [29] [30]**, MEHARI** [31] [32]**, MARGERIT** [33] [34]**, CRAMM** [35]**, ISO 27005:2008** [36]) clara, sistemática y objetiva; que reconozca el riesgo frente a los activos de información. Para lo cual, se considera importante evaluar el riesgo de cada activo frente a la integridad, disponibilidad y confidencialidad, de esta manera se fijarán los controles respectivos que conllevan reducir este a un nivel de riesgo aceptable, evaluando las diferentes opciones de tratamiento, para esto se asignan valores que permitan determinar los riesgos más relevantes, críticos, prioritarios y cuáles se pueden aceptar de acuerdo con su impacto en la organización.

La selección de controles establece las bases para el plan del tratamiento del riesgo aprobando los controles a implementar para tratar los riesgos identificados. El producto de esta fase es un documento en el que se indique el método aplicable para cada riesgo (aceptar, reducir, transferir), los controles que actualmente se tienen implementados, controles adicionales propuestos y estimación del tiempo en el cual los controles propuestos serán puestos en ejecución.

Se debe poner en conocimiento de la dirección y alta gerencia que el tiempo establecido para reducir la brecha de acuerdo con el manual GEL 3.1 es de un período no mayor a 4 meses. Por último, se tiene en cuenta la alineación con el SGSI, esta actividad debe estar orientada a la aplicación y cumplimiento de la estrategia de seguridad de la entidad para la implementación de un SGSI, que dependiendo del nivel de madurez identificado, serán validados y homologados o deberán ser trabajados para cubrir la brecha y alinearse con el estándar. Una vez la entidad ha sido alineada con los requisitos exigidos por el Manual GEL 3.1, pasa a la aplicación al ciclo PHVA del SGSI, identificado el grado de madurez en el que está ubicado.

Estas fases se indican con más detalle en el manual GEL 3.1, en el criterio Sistema de Gestión de Seguridad de la Información, indicando que "las entidades deben establecer un sistema de gestión de seguridad de la información para sus procesos misionales y de apoyo, además, el sistema debe tener en cuenta el análisis de riesgos y las medidas de control para el modelo de apertura de datos" [37].

Es importante recordar que existe una relación de corresponsabilidad directa, entre las fases del ciclo PHVA y los niveles de madurez, indicados en los lineamientos para la implementación del modelo de seguridad de la información 2.0.

En este caso se estudiará la **Fase Planear – Nivel inicial de Madurez**, donde se incluye el desarrollo e implementación de una política de seguridad, la categorización y clasificación de activos de información. Actividades que se definen así:

- Política de seguridad: la definición de esta política a ser implementada se orienta hacia la protección de los activos de información en los procesos y servicios que provee la entidad, considerados activos públicos que deben protegerse adecuadamente, garantizando que reciban el nivel de protección apropiado de acuerdo con su clasificación según la necesidad, las prioridades y el grado de protección

que se espera en la manipulación, administración, procesamiento y almacenamiento de los mismos. Teniendo como base el conocimiento en temas relacionados con protección de la información, datos personales y activos de información, entendido como "todo activo que contiene información que posee un valor y es necesario para los servicios de Gobierno en Línea [38]".

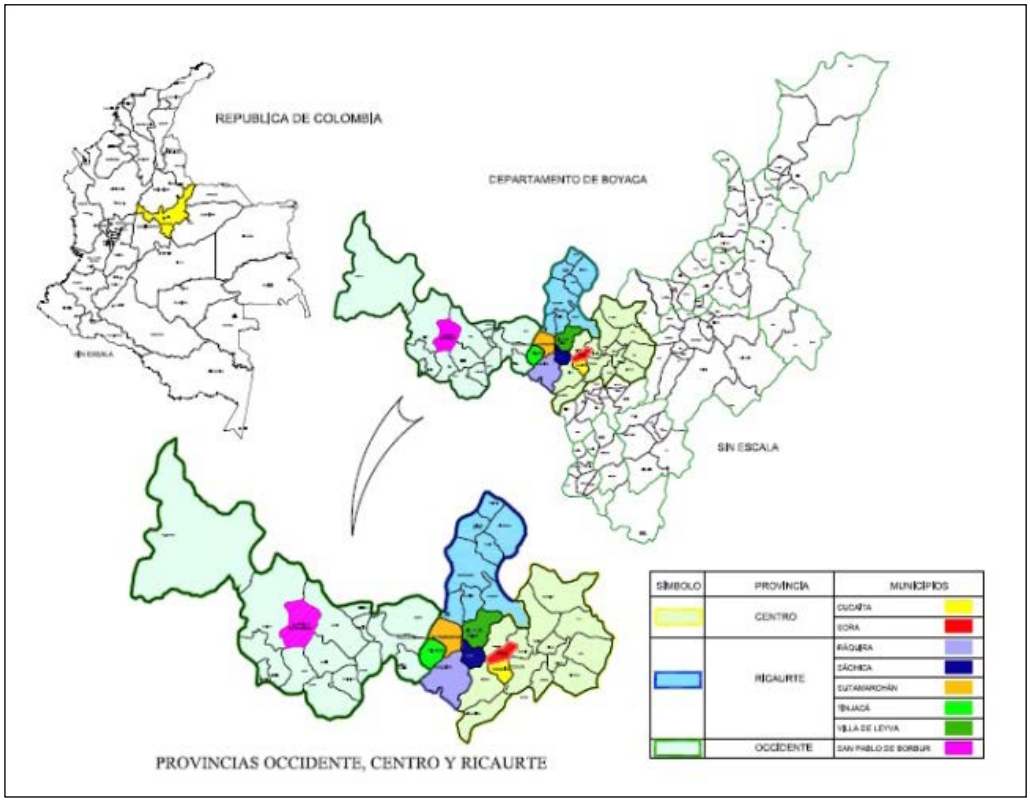
- Categorizar y clasificar los activos de información de acuerdo con sus contenidos, la información que fluye a través de los diferentes servicios de GEL como son: transacciones en línea, democracia en línea, transformación en línea, servicios de interacción con la comunidad, plataformas tecnológicas que soportan los diferentes servicios y sistemas de información, plataformas tecnológicas de seguridad, procesos operacionales, de soporte y aseguramiento de los servicios, material impreso y activos intangibles entre los cuales se clasifican las ideas, el conocimiento, competencias y experiencia [39].

5. ACTUALIDAD DE LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LAS ALCALDÍAS MUNICIPALES CATEGORÍA 6.

El decreto 2693 de 21 de diciembre de 2012, siendo un acto administrativo de carácter Nacional, pide la implementación de la estrategia GEL en todas las entidades del orden Nacional como Territorial, para dar cumplimiento a esta orden, se "adjudica la licitación pública No. 005 de 2011 [40] al operador Corporación Centro de Ciencia y Tecnología de Antioquia que promoverá, por medio de actividades de capacitación, la identificación e implementación de trámites y servicios en línea en la región oriental que faciliten la relación de los ciudadanos con el Estado local". Entidad que se ciñe a lo plasmado en el manual GEL 3.1 y, a su vez, busca motivar a la alta dirección, funcionarios y terceros para que den cumplimiento de los criterios establecidos en los componentes presentes en este documento.

Siendo el sistema de seguridad de la información una de las actividades que se deben establecer en el elemento de componentes trasversales del manual 3.1 de GEL; el CTA, mediante el Anexo 4 [41] denominado autoevaluación definición de brecha del modelo de seguridad de la información de la estrategia GEL 2.0, realiza un diagnóstico de la situación actual en los departamentos y municipios de Boyacá, Santander, Guainía, Vichada, Meta y Arauca, frente al cumplimiento en la implementación del SGSI. En nuestro caso de estudio nos basaremos en la información suministrada por el CTA, en los siguientes municipios del departamento de Boyacá, indicando sus respectivas provincias: Provincia centro (Sora y Cucaita), Provincia Alto Ricaurte (Tinjacá, Sutamarchán, Ráquira, Sáchica y Villa de Leyva) y Provincia de Occidente (San Pablo de Borbur), como se muestra en la figura 2. Así mismo, la figura 2 nos permite conocer el nombre y ubicación de los 8 municipios, cuya información fue suministrada por el CTA, con el fin de estudiar el nivel actual de madurez en seguridad, en estas alcaldías.

Figura 2. Localización geográfica de los municipios a analizar.



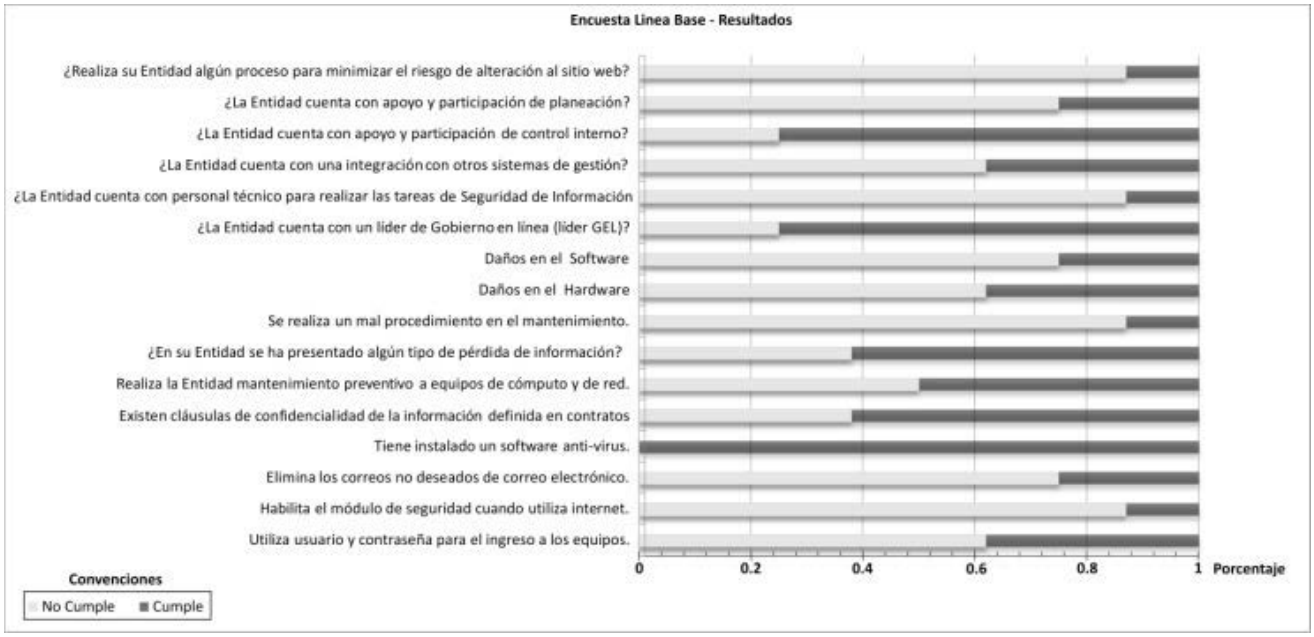
Fuente: los autores, 2013

6. DIAGNÓSTICO DE LA AUTOEVALUACIÓN HECHA A LAS ALCALDÍAS MUNICIPALES CATEGORÍA 6.

Esta herramienta de evaluación, llamada Línea base, por el equipo de trabajo del CTA, se aplica con el objetivo de implementar un SGSI, que mejore los procesos misionales, como los procesos de apoyo, para lo cual se contempla el diseño, implantación, mantenimiento de un conjunto de procesos que gestionen eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando los riesgos [42].

Los valores que se describen en esta sección, se obtienen del trabajo que realiza el delegado del CTA mediante la licitación No. 005; aplicando la Encuesta de Seguridad, propuesta por el programa GEL, documento llamado Línea base, en cada uno de los ocho municipios, mediante la investigación hecha por el Operador CTA. En la Figura 3, se puede evidenciar el nivel de cumplimiento de cada uno de los aspectos encuestados.

Figura 3. Resultados Encuesta.



Fuente: Centro de Ciencia y Tecnología de Antioquia (CTA).

En la Figura 3, las preguntas que aparecen numeradas del 1 al 16 fueron aplicadas en cada uno de los municipios que se indicaron con anterioridad.

El análisis al uso de políticas de seguridad de la información, se ve reflejada en cada una de las preguntas plasmadas en la encuesta realizada, y cuyos resultados serán analizados en este capítulo, dando como primer resultado que el 100% de las entidades no tienen implementado un sistema de gestión de seguridad de la información. Así mismo, carecen de políticas y manuales relacionados con el mismo.

Se consulta al líder Gobierno en Línea de cada municipio, sobre las medidas de protección de la información que usan en la entidad, de lo cual se puede apreciar que: el 62% de las alcaldías utiliza usuario y contraseña para el ingreso a los equipos; el 87% de las alcaldías, habilita el módulo de seguridad cuando utiliza internet; el 75% de las alcaldías, elimina los correos no deseados de correo electrónico; el 100% de las alcaldías, tienen un software antivirus instalado y el 100% de las mismas no lo tienen licenciado; el 62% de las alcaldías, incluyen cláusulas de confidencialidad de la información definida en contratos de los empleados, contratistas y terceros; el 50% de las alcaldías, realizan mantenimiento preventivo a equipos de cómputo y de red; el 62% de las alcaldías, advierte que ha perdido información bajo estas circunstancias: el 17% lo ocasionó un mal procedimiento durante el mantenimiento, el 38% ocurrió por daño en el Hardware y el 29% por daños de Software. El 72% de las alcaldías, tienen nombrado un líder para el programa Gobierno en Línea (líder GEL); el 87% de las alcaldías, tienen en su recurso humano, un profesional que atiende las tareas de la seguridad de la información; el 62% de las alcaldías, está integrando a otros Sistemas de Gestión. Ej.: Modelo Estándar de Control Interno (MECI); el 72% de las alcaldías, tienen el respaldo y participación de la Oficina de Control Interno; el 38% de las alcaldías, tienen el respaldo de la oficina de Planeación, quien se encarga del manejo de proyectos en la mayoría de las Entidades Territoriales encuestadas; el 87% de las alcaldías, implementa algún proceso para mitigar el riesgo de alteración al sitio web.

Los funcionarios y demás personal vinculado con las entidades territoriales, no están aplicando los

siguientes controles, que hacen parte de la autoevaluación: cambio frecuente de las contraseñas, al alejarse del puesto de trabajo bloquea el equipo para impedir el ingreso a terceros, apagar el módem cuando no se ocupa, impedir el uso de dispositivos externos en sus equipos (USB, CD), definir un procedimiento para modificación o destrucción de la información, usar un software para limitar el acceso a la información por los diferentes actores de la Entidad, control de acceso de usuarios a la red, realizar copias de seguridad de la información.

La segunda parte de esta autoevaluación, pretende conocer el involucramiento de las entidades territoriales, con el sistema de seguridad, determinando el nivel de apoyo vertical y transversal en el modelo, cuyos resultados fueron: el 72% de las alcaldías, tienen un líder GEL; el 87% de las alcaldías, cuenta con personal técnico para realizar las tareas de la seguridad de la información; el 62% de las alcaldías, se integran con otros sistemas de gestión; el 72% de las alcaldías, cuenta con apoyo y participación de control interno; el 72% de las alcaldías, cuenta con apoyo y participación de la Secretaría de Planeación; el 87% de las alcaldías, realiza procesos para minimizar el riesgo de alteración al sitio web.

Estos son los controles, que no se han tenido en cuenta por las Entidades Territoriales o alcaldías: crear el Comité de Seguridad de la información [43], nombrar oficial de seguridad (o director de seguridad de la información), responsabilidades de funcionarios respecto a la iniciativa de seguridad de la información de la Entidad, responsabilidades de proveedores respecto a la iniciativa de seguridad de la información de la Entidad, responsabilidades de ciudadanos respecto a la iniciativa de seguridad de la información de la Entidad, establecer controles de seguridad de la información según las necesidades de cada dependencia.

El resultado de la aplicación de esta herramienta de evaluación, ubica a estas entidades en el nivel inicial de madurez en seguridad, evidenciándose una respuesta negativa a los criterios consultados; razón por la cual se inicia un plan de trabajo que busca implementar, mediante el anexo 5. Formato política SGSI – Modelo de seguridad de la información para la estrategia de Gobierno 2.0 [44], el uso de una política concisa, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. Se trata de un declaración corta, que enmarca los principios que guiarán las actividades dentro de la entidad. Para garantizar los principios de seguridad de la información y darle sostenibilidad al Modelo de Gestión de Seguridad de la información.

7. PASOS PARA LA IMPLEMENTACIÓN DE LA FASE INICIAL

Para la implementación del SGSI, establecido por el programa GEL; las alcaldías, que para este caso son categoría 6, deben empezar por la Fase inicial, haciendo uso de los documentos suministrados por el programa GEL, procurando tener en cuenta los pasos indicados en la siguiente tabla:

Tabla 2. Pasos implementación del nivel inicial.

ACTIVIDAD	DESCRIPCIÓN	CÓMO HACERLO
Política de seguridad [45]	Definir una política de seguridad, que proteja su activo de información y que además asegure el cumplimiento de los principios de integridad, disponibilidad y confidencialidad.	Guiarse por el documento ANEXO 5 del Modelo "Formato de Política de Seguridad", propuesto por el Programa Gobierno en Línea.

ACTIVIDAD	DESCRIPCIÓN	CÓMO HACERLO
Autoevaluación [46]	Permite obtener un diagnóstico de la realidad de cada entidad, respecto al SGSI. Ésta debe aplicarse a la alta gerencia.	Aplicar el Anexo 4 Autoevaluación definición de brecha del modelo de seguridad de la información de la estrategia GEL 2.0.
Conformación Comité de Seguridad [43]	Se debe crear un Comité de Seguridad de la información, que se responsabilice y comprometa a la implantación del Modelo.	Para la conformación del Comité se deben tener en cuenta los siguientes aspectos: ✓ El Comité se debe crear por acto administrativo. ✓ El acto administrativo debe nombrar al líder SGSI. ✓ El Comité lo deben conformar un representante de cada dependencia, y de cada entidad que esté presente en la alcaldía y haga uso de los recursos tecnológicos de la entidad. ✓ El Jefe de control interno debe conformar este Comité.
Inventario de información[47]	Cada entidad debe identificar la información generada en medios digitales y físicos, mediante un inventario, para así asegurar debidamente este recurso.	El líder del Comité de Seguridad de la información, puede basarse en el Anexo 7 del modelo. "Metodología de clasificación de activos".

Fuente: los autores, 2013

La implementación de estos pasos, requiere del compromiso de la alta gerencia [48][49], además de realizar sensibilizaciones que permitan disolver la resistencia al cambio que se presentan en algunos funcionarios, al momento de implementar las políticas. Así mismo, estas actividades dan a la entidad elementos comparativos entre el desempeño actual, contra el propuesto, afianzando la protección de la información y la toma; fase programada para adelantarse en un tiempo aproximado de 4 meses [50].

8. CONCLUSIONES

En las entidades territoriales se evidencia una falta de compromiso por la correcta administración y aplicación de la estrategia GEL, y específicamente en el componente elementos trasversales, donde se encuentra la implementación de un modelo de seguridad; así mismo, se evidencia falta interés por parte de cada uno de los involucrados en la implementación del SGSI; es importante que la alta gerencia de las entidades asignen recursos para la implementación del modelo de seguridad establecido en la estrategia GEL, y para que su aplicación sea más acorde con los lineamientos, metodologías, guías y estándares establecidos en el manual; se debe solicitar el apoyo y acompañamiento por parte del estado haciendo uso de los componentes indicados en el manual GEL y el modelo de seguridad. La alta gerencia y los funcionarios de la entidad deben tomar conciencia de la necesidad de implementar un SGSI dinámico que asegure la protección de los activos en todos los niveles. Por lo tanto, es vital para la correcta

administración y protección de los activos de información, que el Estado colombiano promulgue una ley o un decreto en el cual se asigne un especialista en seguridad de la información o un funcionario para el área de Sistemas, en cada entidad del orden territorial, organizando un grupo técnico de apoyo; para de esta forma darle continuidad y respaldo al Modelo de Seguridad.

REFERENCIAS

[1] Ley 617 del 2000, (2000), capítulo 1, artículo 6, Categorización de los distritos y municipios. [On line] p.10. Disponible en http://www.minhacienda.gov.co/portal/page /portal/HomeMinhacienda/asistenciaentidadesterritoriales/Publicaciones/Manuales/Ley%20617%20de%20200%20version%202008.pdf.

[2] ISO, Sistema de Gestión de la Seguridad de la Información. [On line]. Disponible en http://www.iso27000.es/sgsi.html.

[3] O. A. Schmitz, (2008), Principios Básicos de Seguridad de la Información, CXO Community Latam. [On line]. Disponible en http://cxo-community.com.ar/articulos/blogs/blogs-seguridad-informatica/45-principios-bcos-de-seguridad-de-la-informaci.html

[4] INDECOPI, Principios de la Seguridad de la Información, Perú. [On line]. Disponible en http://www.indecopi.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=0&JER=1529

[5] Ó. Blanco, D. Rojas, Principios de seguridad de la información en entornos de salud, CEPAL. [On line]. Disponible en http://www.seis.es/documentos/informes/secciones/adjunto1/16_Principios_de_seguridad_de_la_informacion_en_entornos_de_salud.pdf

[6] MinTIC, (2012), Manual de Gobierno en Línea 3.1. [On line]. Disponible en http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0d f10529195223c011ca6762 bfe39e/manual-3.1.pdf.

[7] ISO, ISO 27000: Seguridad de la información. [On line]. Disponible en http://www.iso27000.es/download/doc_iso27000_all.pdf.

[8] MinTIC , Entregables 3, 4, 5 y 6: informe final – modelo de seguridad de la información, sistema SANSI-SGSI, Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea, 2012, p. 136.

[9] ISO, ISO/IEC 27001: 2005: (2005), Estándar Internacional, Tecnología de la información, Técnicas de Seguridad, Sistemas de Gestión de Seguridad de la Información, Primera Edición. [On line] p. 12. Disponible en http://mmujica.files.word press.com/2007/07/iso-27001-2005-espanol.pdf

[10] MinTIC, (2012), Decreto 2693 de 2012, Lineamientos generales de la estrategia Gobierno en Línea. [On line]. p.1. Disponible en http://programa.gobiernoen linea.gov.co/apcaafiles/eb0df10529195223c011ca6762bfe39e/decreto-2693-de-2012. pdf

[11] Centro de Tecnología de Antioquia CTA, El CTA y la estrategia Gobierno en Línea, [On line]. Disponible en http://www.ctagel toriente.org/index.php?option=com_ content&view=article&id=48

[12] MinTIC, (2011), Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. [On line]. Disponible en http://programa.gobiernoenlinea.gov.co/ apc-aa-files/da4567033d075590cd3050598756222c/Modelo_Seguridad_Informacion_2_0.pdf

[13] MinTIC, (2001), Anexo 4 GEL Autoevaluación- Definición de brecha, 2001, [On line] pp. 8. Disponible en http://programa.gobiernoenlinea.gov.co/ lineamientos.shtml?scrl=116&apc=ahx;x;x;x5-&scr_116_Go=6 pp. 8

[14] MinTIC, Anexo 4 GEL Autoevaluación-Definición de brecha, 2011, [On line] pp. 9. Disponible en http://programa.gobiernoen linea.gov.co/lineamientos.shtml?scrl=116& apc=ahx;x;x;x5-&scr_116_Go=6 pag 9

[15] MinTIC, (2009) Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. [On line] pp. 10-11. Disponible en http://programa.gobiernoenlinea.gov.co/ apc-aa-files/5854534aee4eee4102f0bd5ca294791f/GEL_MetodologiaMonitoreoEvaluacionGEL.pdf

[16] MinTIC, (2008), Decreto 1151 de 2008, Lineamientos generales de la estrategia Gobierno en Línea, [On line] pp.2. Disponible en http://programa.gobiernoen linea.gov.co/apc-aa-files/e5203d1f18ecfc98d25cb0816b455615/decreto1151abril14de2008_1.pdf

[17] W. Edwards, (2011), Círculo de Deming: ciclo PDCA de mejora continua, [On line]. Disponible en http://gestionempresarial4.word press.com/174-2/

[18] MinTIC, (2012), Estrategia Gobierno en Línea, La estrategia Gobierno en Línea y su evolución. [On line] pp.3. Disponible en https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&ved=0CDwQFjAC&url=http%3A%2F%2Fprograma.gobiernoenlinea.gov.co%2Fapc-aa-files%2Fprograma%2Festrategia-gobierno-en-linea.docx&ei=3mhyUuzCJO vmsAT9zIGYDA&usg=AFQjCNEHk7c6AGHbe3jiangN4RJGT1uVgQ&bvm=bv.55819444,d.cWc

[19] MinTIC, (2011), Fondo de Tecnologías de la Información y las Comunicaciones, GEL, modelo de seguridad de la información para la estrategia de gobierno en línea 2.0, diciembre. [On line] pp. 13. Disponible en http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/Modelo_Seguridad_Informacion_2_0.pdf

[20] MinTIC, (2012), Manual 3.1 para la implementación de la estrategia de Gobierno en Línea de la República de Colombia, Bogotá, D.C. Colombia, Monitoreo y evaluación. [On line] pp. 10. Disponible en http://programa.gobierno enlinea.gov.co/apc-aa-files/e5203d1f18ecfc 98d25cb0816b455615/minticmanual 3.0.pdf

[22] J. Amaya, Gerencia de procesos: Método de control de procesos, (PHVA). [On line]. Disponible en http://www.unalmed.edu.co /josemaya/Ing_prod/Control%20de%20 Proceso -%20Metodo.pdf

[23] Sistemas Integrados de Gestión, PHVA. [On line]. Disponible en http:// www.implementacionsig.com/index.php/ generalidades-sig/ 55- ciclo-de-deming

[24] ITILV3, Gestión de Servicios TI, PHVA. [On line]. Disponible en http://itilv3. osiatis.es/proceso_mejora_continua_ servicios_TI/ciclo_deming.php

[25] MinTIC, Lineamientos para la implementación de la seguridad de la información, Lineamientos de implementación, Figura No. 1, pp.11. [On line]. Disponible en http://programa. gobiernoenlinea.gov.co/apc-aa-files/da 4567033d075590cd3050598756222c/ GEL308_IPE_Lineamientos_Seguridad.pdf

[26] MinTIC, (2011), Lineamientos para la implementación de la seguridad de la información, Lineamientos de implementación, [On line] p.15. Disponible en http://programa.gobiernoen linea.gov.co/apc-aa-files/da4567033d0 75590cd3050598756222c/ GEL308_IPE_ Lineamientos_Seguridad.pdf

[27] MinTIC, (2011), Lineamientos para la implementación de la seguridad de la información, Lineamientos de implementación. [On

line] pp.15. Disponible en http://programa.gobiernoen linea.gov.co/apc-aa-files/da4567033d 075590cd3050598756222c/GEL308_IPE _Lineamientos_Seguridad.pdf

[28] MinTIC, (2011), Fondo de las Tecnologías de la Información y las Comunicaciones, Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. [On line] pp. 35. Disponible en http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/Modelo_Seguridad_Informacion_2_0.pdf

[29] M. Muñoz, Introducción a la Metodología OCTAVE, [On line]. Disponible en http://www.acis.org.co/memorias/JornadasSeguridad/IVJNSI/MauricioMunoz-IVJNSI.pdf

[30] R. Gómez, D. Pérez, Y. Donoso, A. Herrera, (2010, junio), Metodología y gobierno de la gestión de riesgos de tecnología de la información, Revista de Ingeniería Scielo, [On line]. Disponible en http://www.scielo.unal.edu.co/scielo.php?script=sci_arttext&pid=S0121-49932010000 100012&lng=es&nrm=

[31] MC. Crespo, (2013), El análisis de riesgos dentro de una auditoría informática: pasos y posibles metodologías, Universidad Carlos III de Madrid. [On line] pp. 151. Disponible en http://e-archivo.uc3m.es/bitstream/handle/10016/16802/PFC_Carmen_ Crespo_Rin. pdf?sequence=1

[32] CLUSIF, Metodología MEHARI, 2010. [On line]. Disponible en http://www.clusif.asso.fr /fr/production/ouvrages/pdf/ MEHARI-2010-Introduccion.pdf

[33] J. A. Peña, (2010), Metodologías y Normas para el análisis de riesgos, ¿Cuál debo aplicar? [On line]. Disponible en http:// www.isaca. org/chapters7/Monterrey/ Events/Documents/20100302%20 Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf

[34] Gobierno de España, (2012), Portal de Administración, Metodología MAGERIT versión 3. NIPO: 630-12-171-8. [On line]. Disponible en http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Up1hdsRg_pU

[35] A. Huerta, (2013, Marzo) Introducción al análisis de riesgos, Metodologías I, [On line]. Disponible en http://www.securityartwork.es/2012/03/30/introduccion-al-analisis -de-riesgos-metodologias-i/

[36] ISO, ISO/IEC 27005:2008, Tecnología de la Información - Técnicas de seguridad - Información de gestión de riesgos de seguridad. [On line]. Disponible en http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107

[37] MinTIC, (2012), Manual de Gobierno en Línea, Elementos transversales. [On line]. pp. 42, Disponible en http://programa.gobiernoenlinea.gov.co/apc-aa-files/e5203d1f18ecfc98d25cb0816b455615 /minticmanual3.0.pdf

[38] MinTIC, Fondo de las Tecnologías de la Información y las Comunicaciones, Gobierno en Línea, anexo 1: metodología de clasificación de activos - modelo de seguridad de la información para la estrategia de Gobierno En Línea, Guías de clasificación. [On line]. Disponible en http://programa.gobiernoenlinea.gov.co/lineamientos.shtml?scrl=116&apc=ahx;x;x;x5-&scr_116_Go=6%20pag%208

[39] MinTIC, (2012). Manual de Gobierno en Línea, Elementos transversales [On line] pp. 43-44, Disponible en http://programa.gobiernoenlinea.gov.co/apc-aa-files/e5203d1f18ecfc98d25cb0816b455615/minticmanual3.0.pdf

[40] MinTIC, (2011), Adjudicación licitación para Gobierno en línea Territorial en el oriente colombiano. [On line]. Disponible

en http://www.mintic.gov.co/index.php/mn-news/662-20111205-ministerio-tic-adjudica -licitacion-gobierno-linea-territorial-oriente-colombiano

[41] MinTIC, Programa Gobierno en Línea, Lineamientos, Anexos 1-16, Anexo 4. [On line]. Disponible en http://programa. gobiernoenlinea.gov.co/lineamientos. shtml?scrl=116&apc=ahx;x;x;x5-&scr_116_Go=6%20 pag%208

[42] MinTIC, (2011), Lineamientos para la implementación del Modelo se seguridad de la Información. [On line]. pp.18. Disponible en: http://programa.gobiernoenlinea.gov.co/ apc-aa-files/da4567033d075590cd3050598756222c/GEL308_IPE_Lineamientos_Seguridad.pdf

[43] MinTIC, Conformación Comité de Seguridad, [On line]. Disponible en http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598 756222c/Modelo_Seguridad_Informacion_2_0.pdf

[44] MinTIC, (2012), Fondo las Tecnologías de la Información y las Comunicaciones, anexo 5: guía de implementación de políticas-modelo de seguridad de la información para la estrategia de gobierno en línea, [On line]. Disponible en http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee-4102f0bd5ca294 791f/ANEXO_5__Guia_de_Implementacion_de_Politicas.pdf

[45] MinTIC, (2012), Fondo las Tecnologías de la Información y las Comunicaciones, anexo 5: guía de implementación de políticas- modelo de seguridad de la información para la estrategia de gobierno en línea, [On line] pp. 10. Disponible en http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294 791f/ANEXO_5__Guia_de_Implementacion_de_Politicas.pdf

[46] MinTIC, Dirección de Gobierno en Línea, [On line]. Disponible en http://programa. gobiernoenlinea.gov.co/lineamientos.shtml?scrl=116&apc=ahx;x;x;x5-&scr_116_Go=6

[47] MinTIC, Inventario de información. [On line]. Disponible en http://viejoprograma. gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ANEXO_1_Metodologia_de_clasificacion_de_Activos.pdf

[48] MinTIC, (2012), Lineamientos para la implementación del Modelo de Seguridad de la Información, [On line] p.13. Disponible en http://programa.gobierno enlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/GEL308_IPE_Lineamientos_Seguridad.pdf

[49] MinTIC, (2012), Gobierno en Línea: Conceptos generales. [On line] p. 66. Disponible en http://programa.gobiernoen linea.gov.co/apc-aa-files/5854534aee4eee 4102f0 bd5ca294791f/Parte_2.pdf

[50] MinTIC, (2012), Lineamientos para la implementación del Modelo de Seguridad de la Información. [On line] p.20. Disponible en http://programa.gobiernoen linea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/GEL308_IPE_ Lineamientos_Seguridad.pdf