

La importancia de la seguridad de la información en el sector público en Colombia

Erney Alberto Ramírez Camargo¹ Miguel Alberto Rincon Pinzon¹

erneyramirez@unicesar.edu.co; Miguelrincon@unicesar.edu.co

¹ Universidad Popular del Cesar.

DOI: 10.17013/risti.46.87-99

Resumen: El presente artículo nace como respuesta a la importancia que ha tomado en el sector público la protección de la información que se comparte con los usuarios en la búsqueda de una gestión basada en la transparencia que garantice procesos eficientes y oportunos que beneficien a todas las partes interesadas. En el documento se exploran el origen y fundamentos del Gobierno en Línea, así como su marco legislativo. De igual manera, realiza una descripción del significado de sector público y los alcances que han tenido las entidades que lo conforman en relación a la implementación de la estrategia digital, permitiendo además comparar el país con otros de la región de América Latina. Asimismo, el estudio hace énfasis en el nivel de cumplimiento del Gobierno Digital y Seguridad Digital de los municipios de sexta categoría que pertenecen al sur del Departamento del Cesar, evidenciando una baja capacidad de respuesta a los factores evaluados. Finalmente, se planean los aspectos que deben tenerse en cuenta para la puesta en marcha de la estrategia del Gobierno en línea, soportado en el Decreto 2693 de 2012 y que debe contener los componentes de: a) elementos transversales, b) información en línea, c) interacción en línea, d) transacción en línea, y d) democracia en línea.

Palavras-chave: Gobierno en línea, ISO 27001, sector público, TIC's.

The importance of information security in the public sector in Colombia

Abstract: This article is born as a response to the importance that the protection of information shared with users has taken in the public sector in the search for a management based on transparency that guarantees efficient and timely processes that benefit all interested parties. The document explores the origin and foundations of Online Government, as well as its legislative framework. In the same way, it makes a description of the meaning of the public sector and the scope that the entities that comprise it have had in relation to the implementation of the digital strategy, also allowing the country to be compared with others in the Latin American region. Likewise, the study emphasizes the level of compliance with the Digital Government and Digital Security of the sixth category municipalities that belong to the south of the Department of Cesar, evidencing a low response capacity to the evaluated factors. Finally, the aspects that must be taken into account for the implementation of the online Government strategy that must contain the

components of: a) transversal elements, b) online information, c) online interaction, d) online transaction, and d) online democracy.

Keywords: Online government, ISO 27001, public sector, TIC's

1. Introducción

La tecnología llegó para revolucionar la manera de hacer las cosas tanto en la cotidianidad como a nivel empresarial, haciendo que los procesos se reinventen y se vuelvan más eficientes. Es innegable que uno de los procesos que más se ha impactado es el proceso de comunicación, donde la información dejó de llevarse de manera física para ser digitalizada y almacenada en dispositivos y en el web, haciendo que se generen riesgos frente a su seguridad y los datos puedan ser vulnerados. En el presente artículo, se pretende realizar un análisis sobre la manera en que las empresas del estado, en especial las alcaldías municipales han incorporado herramientas que permiten garantizar la seguridad de la información que circula en un intercambio de entradas y salidas que son necesarias para dar cumplimiento a los diferentes procesos que se llevan a cabo en dichas entidades.

Dado lo anterior, conviene iniciar haciendo mención al sector público, siendo este el conjunto de instituciones que son administrados bien sea de manera directa o indirecta por el Estado colombiano y que se diferencian del sector privado porque prima la propiedad colectiva. En tal sentido, el Gobierno tiene la obligación de establecer procesos eficientes que garanticen además la transparencia en la ejecución de los mismos, con el fin de generar credibilidad entre la comunidad. Asimismo, en la búsqueda de una mejor prestación del servicio, tratando de disminuir la tramitología y fortalecer la oportunidad en su capacidad de respuesta, le ha apostado a la digitalización de los procesos a través de la prestación de servicios electrónicos que facilitan el registro, procesamiento y producción de información pública. Por tanto, se presenta el riesgo de que dicha información sea vulnerada y amenazada, llegando a comprometer su confidencialidad e integridad, y es por tal razón que el Gobierno viene implementando estrategias para la mitigación de dichos riesgos, como es la Resolución 500 de 2021 que establece los lineamientos y estándares para la estrategia de seguridad digital. Asimismo, existen normas como la ISO 27001 que brinda una serie de lineamientos y pautas para la puesta en marcha del Sistema General de Seguridad Informática y la ISO 27005 que establece las directrices para la gestión de riesgos de la seguridad la información.

Por lo dicho hasta aquí, las instituciones públicas tienen la obligación constitucional de proteger la información que se maneja de los ciudadanos, ya sean funcionarios públicos que contribuyen con el desarrollo del objetivo de la entidad pública o el usuario que llega a depositar sus datos personales en busca de acceso a la justicia o al gobierno en general, dado que existe peligro de difusión o mala utilización de los datos. La información es un activo vital dentro de cualquier institución, la seguridad de la información y la ciberseguridad está definidas por un compuesto de instrucciones y elementos, que tienen como misión brindar las tres características fundamentales de la misma las cuales son: disponibilidad, confidencialidad, integridad; implementar políticas de y controles de seguridad de los datos se ha convertido en un proceso de vital importancia para que las organizaciones mantengan salvaguardada sus sistemas ataques, daños o pérdidas.

Las entidades del orden público en la república de Colombia deben tener altos niveles de protección en el tratamiento de datos, desde la exigibilidad de la normatividad, toda vez que la posibilidad de vulneración de derechos fundamentales y en general de toda la gama de derechos que emergen de la constitución y del bloque de constitucionalidad.

2. Materiales y métodos

El propósito del artículo es identificar los aspectos relevantes de la seguridad de la información y el gobierno de TI en el sector público, en especial en las alcaldías municipales, siendo entonces necesario definir de manera concreta el planteamiento del problema, así como los objetivos a desarrollar con el estudio. El trabajo inicia con la exploración del tema central, es decir, el rol de la seguridad de la información en el sector público, a través de los autores más representativos que han expuesto sus teorías y los cambios a través del tiempo. Por tanto, se recurrió a la investigación documental mediante libros y artículos científicos que son referentes en lo concerniente al tema de estudio. El estudio obedece al tipo de investigación descriptiva, el cual permite que puedan analizarse de manera independiente las diferentes variables que intervienen en la seguridad informática (Hernández Sampieri, 2010). Como población objeto de estudio se estableció el conjunto de alcaldías de sexta categoría del Departamento del César, siendo en total 8. Como técnica para recopilación de la información que permitiera establecer el estado actual de estas entidades en relación a la seguridad de la información, se definió una lista de chequeo ISO inspirada en la ISO 27001:2013.

3. Resultados

3.1. Sector público colombiano

El sector público reúne todas aquellas instituciones o entidades que fueron creadas para cumplir con funciones administrativas orientadas a la satisfacción de las necesidades de los habitantes del país, cumpliendo así a cabalidad con la legislación que se rige a través de la Constitución Política de Colombia. De igual manera, se divide entre sector financiero y no financiero que se dedica a producir o suministrar bienes y servicios según sus funciones y se divide en gobierno general de la administración pública y empresas no financieras del Estado. El gobierno general de la administración pública está conformado por aquellas instituciones prestan servicios educativos, de justicia, defensa, etc., y sus recursos son provenientes del cobro de impuestos y otras contribuciones de carácter obligatorias aplicadas a la comunidad. En tanto que las empresas no financieras de estado son aquellas que producen y venden bienes y servicios y cuyos recursos se obtienen de los ingresos que generan.

3.2. La información del sector público

La información que se produce a nivel nacional en los estamentos públicos, es de vital importancia para el desarrollo de los diferentes procesos que se llevan a cabo para dar solución a las diferentes necesidades de la comunidad, es de recordar que dicha información se considera de carácter público y que de acuerdo a lo definido por la Constitución Política de Colombia todas las personas tienen derecho a su acceso cuando

así lo crean conveniente. Asimismo, en el afán de cumplir con uno de los principios del Estado que es la transparencia, se deben hacer públicos los procesos de contratación de bienes y servicios, a través de licitaciones abiertas, al igual que los informes de gestión y demás información concerniente a la gestión nacional (Campos Ramírez, 2017).

3.3. Legislación y estándares referentes a la Seguridad de la Información

Artículos de la constitución política de Colombia

Las entidades públicas, ministerios, gobernaciones, alcaldías, poseen bases de datos o sistemas de información de sus usuarios que puede ser vulnerada en caso que sus TI sean vulneradas, sin embargo, estas deben garantizar que esta información que sea de carácter reservada no vaya a ser publicada sin previa autorización o parte de su información pueda prestarse para exponerla a calumnias o difamaciones. En este sentido el artículo 15 de la CPC, determina como derecho de todos los colombianos a su intimidad personal y familiar y a su buen nombre, exigiendo además que el Estado los respete y haga respetar. Además de poder conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas (Secretaría Senado, 2021).

En igual sentido se observa que el art. 12 de la Declaración Universal de los derechos humanos y el art. 11 de la Convención Americana de DDHH de 1969 protege la honra y la reputación de todos los seres humanos, estipulando el derecho de la protección de la ley contra injerencia o ataques.

- El artículo 20 de la Constitución política ampara los derechos de libre expresión y difusión de pensamiento y opiniones, además del derecho a la rectificación en condiciones de equidad. La TI se han convertido en un medio de difusión rápido, oportuno y universal para abrir la oportunidad a muchas personas que puedan participar y enterarse de la información que procesa el sector público (Secretaría Senado, 2021).
- La constitución política de Colombia ha definido en su artículo 75 el espectro electromagnético como un bien público inajenable imprescriptible, además garantiza el pluralismo informativo y la competencia, por tanto, las TI no son exclusivas del sector público, esto exige un mejor desempeño por parte de las entidades para que la información que producen sea de interés y atractiva para la comunidad.

Leyes relacionadas con el manejo de la información en Colombia

En el país se han definido una serie de normas que han procurado proteger la información y los datos de los ciudadanos, donde se pueden destacar las siguientes:

Ley 23 de 1982: hace referencia a la protección de los derechos de autor.

Ley 1273 de 2009: es una Ley que tiene como objetivo incluir penalizaciones para los delitos informáticos y, además, de igual manera, busca garantizar un adecuado proceso en relación al uso de las tecnologías de la información y la comunicación.

Ley 1581 de 2012: Habeas Data: trata de la protección de datos personales, brindándole al usuario el poder de decidir sobre la exposición de información sensible, la cual debe

ser autorizada para que las empresas y entidades puedan disponer de ella y actualizarla en sus bases de datos.

Estrategia de Gobierno en línea

Recientemente el Ministerio de Tecnología y la Información estableció los criterios generales para la ejecución del MSPI (Modelo de Seguridad y Privacidad de la Información), la guía metodológica de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de incidentes de seguridad lógica, y, establecer los estándares a aplicar para la estrategia de seguridad digital, a través de la Resolución 500 de 2021. Esta reglamentación trae a los municipios a través de sus Alcaldías a mejorar los procesos que involucran la TI puesto que deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital (Mintic, 2020).

Norma ISO 27001: Sistemas de Gestión de Seguridad de la Información (SGSI)

Esta norma creada en el año 2005 tiene como finalidad establecer un modelo para la implementación y administración de un sistema de gestión para la seguridad de la información, con énfasis en procesos, análisis de riesgos y formulación de controles que contribuyan a la protección de los datos y mitiguen los riesgos existentes. Es de resaltar que dicha norma fue tomada en cuenta por el Estado para formular su estrategia de Gobierno en Línea, en su última versión que es del año 2013 y que pone su foco en el diagnóstico tomando en consideración el contexto para establecer tanto los factores externos e internos que pueden impactar en la gestión de la información. Es de resaltar que la implementación de la ISO 27001 permite controlar riesgos tales como la violación de datos personales, el vandalismo, el crimen cibernético, ataques de virus, entre otros; asimismo, resulta ser compatible con otros sistemas de gestión como bien puede ser la ISO 9001, y es independiente de la plataforma de tecnología de la información (Magazcitur, 2013).



Figura 1 – Elementos de la ISO 27001
Fuente: Magazcitur (2013)

Norma ISO 31000:2009. Gestión de Riesgos

Señala una familia de normas sobre Gestión del riesgo en normas codificadas por la organización International Organization for Standardization. El propósito de la norma ISO 31000:2009 es proporcionar principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo. El propósito de la norma ISO 31000:2009 es aplicar y adaptar al público, cualquier empresa pública o privada, comunidad, asociación, grupo o individuo.

Para una eficaz gestión del riesgo en las organizaciones, la ISO 31000 determina los siguientes principios básicos:

- Crea valor.
- Está integrada en los procesos de una organización.
- Forma parte de la toma de decisiones.
- Trata explícitamente la incertidumbre.
- Es sistemática, estructurada y adecuada.
- Está basada en la mejor información disponible.
- Está hecha a medida.
- Tiene en cuenta factores humanos y culturales.
- Es transparente e inclusiva.
- Es dinámica, iterativa y sensible al cambio.
- Facilita la mejora continua de la organización.

3.4. Situación actual de las alcaldías municipales de sexta categoría del Departamento del César

Los municipios de Colombia se categorizan de acuerdo a su demografía, sus ingresos corrientes de libre destinación y situación geográfica, tal como lo establece el decreto 2106 de 2019 (SUIN, 2019), específicamente en su artículo 153; definiendo además tres grupos, así: Grandes municipios, municipios intermedios y municipios básicos; en este último grupo se tienen los de quinta y sexta categoría. Siendo la sexta categoría la última en clasificación de los municipios, es importante aclarar cuáles son sus características, respecto a la población tienen diez mil (10.000) o menos habitantes y en proporción a sus ingresos corrientes de libre destinación en la vigencia fiscal, éstos no son superiores a quince mil (15.000) SMLMV, equivalentes para la vigencia 2021 a trece mil millones seiscientos veintisiete mil ochocientos noventa pesos corrientes (\$13.627.890.000 MCT) (Contaduría General Nación, 2021).

De los 25 municipios que el departamento del Cesar posee, son ocho los localizados en la zona Sur (Aguachica, Gamarra, González, La Gloria, Pelaya, Río de Oro, San Alberto, San Martín) y de estos seis se encuentran en sexta categoría. A pesar que estos municipios presentan menos ingresos para cubrir sus obligaciones legales y satisfacer las necesidades de sus comunidades, a sus alcaldías le son atribuibles iguales retos en su desempeño institucional; entre las cuales se encuentran las actividades y funciones de la TI. En los tiempos actuales, es decir, en toda la era de desarrollo de las ciencias computacionales el activo vital más importante de cualquier organización es la información, debido al gran auge que ha tenido las áreas relacionadas, las tecnologías de información en la actualidad cumple un rol cada vez más importante en cualquier organización tanto del sector público o privado alrededor del mundo (Marulanda, 2017),

es por ello que la automatización de la información para las organización, ha venido creciendo gradualmente en las últimas años, lo cual ha provocado que las mismas sean cada vez más efectivas y fructíferas (Baena., 2015).

Según el artículo de colaboración de la Universidad Nacional Mayor de San Marcos de Lima Perú, en el año 2019, se han identificado cinco factores que inhiben la implementación del Gobierno de las TI: la falta de comunicación, el inadecuado involucramiento de los interesados, la falta de principios y políticas claros de Gobierno de TI, la falta de procesos, e inadecuado soporte de recursos financieros.

En Colombia, la Función Pública evalúa el desempeño de las entidades, apoyado en un Modelo Integrado de Gestión y Desempeño, que se encuentra conformado por 7 dimensiones y 18 políticas, entre las cuales se encuentran las de Gobierno Digital y Seguridad Digital, teniendo como finalidad desarrollar acciones encaminadas al fortalecimiento de las TIC's (Correa Ortiz, Toro García, & Gutiérrez Vargas, 2020). Tomando en consideración una evaluación realizada en el año 2020 a los seis municipios que conforman la subregión sur del departamento del Cesar y que se encuentran catalogados como municipios de sexta categoría, se tienen los siguientes resultados en relación a las políticas de Gobierno y Seguridad Digital (Función Pública, 2020):

Municipio	Gobierno Digital	Seguridad Digital
Gamarra	40,8	60,7
González	61,4	49,1
La Gloria	72,6	66,6
Pelaya	66,7	71
Río de Oro	37,9	32,5
SAN ALBERTO	58,9	64,4

Fuente: Función Pública (2021)

Tabla 1 – Medición de políticas de Gobierno de Seguridad Digital de la vigencia

Estos resultados evidencian la baja capacidad de dichos municipios en su estructura de TI y en los mecanismos de Seguridad Digital. Cabe además mencionar que dentro de los factores que más influyen en estos deficientes resultados, se encuentra el desconocimiento de políticas y normas de Seguridad de la Información y de los riesgos de TI (Arévalo Ascanio, 2016). En tal medida, puede establecerse que las alcaldías no han adoptado en su totalidad los lineamientos definidos por el Gobierno Nacional como es el El estándar de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra organizado con el Marco de Referencia de Arquitectura TI y soporta transversal los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión (Mintic, 2014). Asimismo, el Gobierno Nacional en el año 2014 definió el Modelo de Gestión IT4+, sin embargo, este no tuvo el impacto esperado en sus niveles de implementación, debido a la escasa capacitación y la falta de recursos para desarrollar las actividades requeridas.

3.5. Aspectos a tener en cuenta para la implementación del Gobierno en Línea

El Gobierno en Línea en el país tiene sus orígenes a comienzos del siglo XXI, como una respuesta a la llegada de la tecnología para el fortalecimiento de los procesos en las instituciones, logrando además la modernización de la infraestructura digital de las entidades públicas bajo los principios de eficacia, eficiencia, responsabilidad y transparencia, que garanticen el manejo de la información de manera flexible y segura, propiciando además la prestación de servicios de calidad, de manera oportuna y asequible para los ciudadanos a través de los servicios en línea y la disposición de la información para que sea consultada por la comunidad cuando lo consideren conveniente. Es importante resaltar que la puesta en marcha del Gobierno en Línea requiere la alineación con otras estrategias estatales tales como la Política de Rendición de Cuentas a la Ciudadanía, la Política Nacional Anticorrupción, la Política Nacional de Archivo y Gestión Documental, entre otras.

En cuanto a las experiencias de América Latina, el 73% de los países cuentan con una estrategia de Gobierno en Línea, sin embargo, menos del 30% de los trámites pueden hacerse enteramente en línea, y únicamente el 7% de los ciudadanos realizó en línea su último trámite con el gobierno.

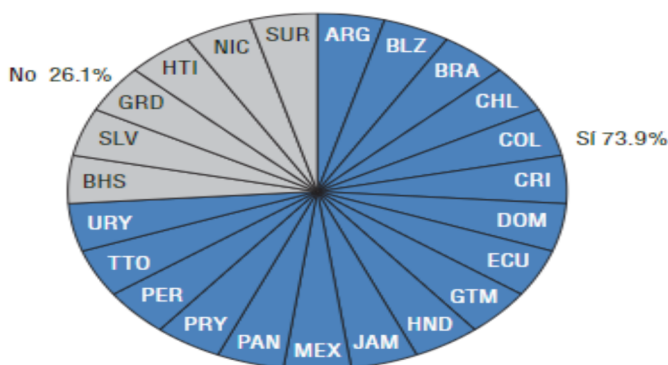


Figura 2 – Existencia de una estrategia nacional de gobierno digital o uso de TIC en el sector público

Fuente: OCDE 2015 Encuesta sobre desempeño de Gobierno Digital (2015)

No obstante, cabe destacar los beneficios que se obtienen con la implementación de dicha estrategia, encontrando que países como Brasil han ahorrado más de 200 millones de dólares al año sólo a través del recaudo electrónico del Impuesto de Propiedad de Vehículos Automotores (Banco Interamericano de Desarrollo, 2017). En general, las estrategias digitales implementadas en esta región, obedecen a servicios públicos generales como son el otorgamiento de licencias, permisos, certificados, etc., sin embargo, existen países como Chile, Uruguay y Colombia que han sido más ambiciosos en su estrategia digital y que han incluido servicios como educación y salud.

Pese a que como se mencionó anteriormente para Colombia, existen municipios como los del Departamento del Cesar, que no evidencian un alto desarrollo del Gobierno y Seguridad Digital, el país ha mostrado avances importantes, tanto así que ha tenido reconocimiento por parte de la Organización de las Naciones Unidas (ONU), quien evalúa los niveles de digitalización, los progresos en la prestación de servicios públicos online, la participación electrónica y la disponibilidad de datos abiertos, para finalmente asignar un puesto entre los países que son miembros, teniendo que el país para el año 2016 ocupó el lugar número 24 con una valoración de 52 puntos (Rivera Martínez, Sotelo Muñoz, & Quiñonez Zúñiga, 2021).

Dado lo anterior y con el ánimo de fortalecer los resultados obtenidos en relación a la implementación de la estrategia Gobierno en Línea, el Ministerio TIC desde la expedición del Decreto 1151 de 2008 ha establecido los Manuales para la Implementación de la Estrategia de Gobierno en Línea, los cuales son concebidos como herramientas de autoayuda, que buscan proporcionar a las entidades públicas, y a los privados que ejercen funciones administrativas, el enfoque, lineamientos y herramientas de apoyo que faciliten sus avances y mejoras, ya sea a través de las directrices incluidas en el mismo o mediante documentos complementarios a los que se hace referencia en el Manual. De igual manera, en el año 2021 se implementó como nueva estrategia para promover la implementación del Gobierno en Línea, soportado en el Decreto 2693 de 2012 y que contempla los siguientes elementos:

Elementos Transversales:

Hace referencia a todas las actividades que deben implementarse para identificar los grupos de interés y cuáles son sus necesidades con el fin de satisfacer sus requerimientos, teniendo en cuenta que debe realizarse un análisis periódico ya que sus intereses pueden variar en el tiempo. Asimismo, se busca que las entidades cuenten con una caracterización actualizada de la infraestructura tecnológica y establezcan un plan de ajuste permanente. Se reconoce también dentro de este componente, la importancia de que las entidades definan una política de seguridad que sea objeto de mejora continua y que tenga como objetivo principal la incorporación del Gobierno en Línea como parte esencial de los procesos de la organización, logrando que haga parte de su cultura y de una visión compartida con los funcionarios. Se determinan como actividades esenciales en este componente las siguientes:

- Institucionalizar la Estrategia de Gobierno en línea
- Centrar la atención en el usuario
- Implementar un sistema de gestión de Tecnologías de Información
- Implementar un sistema de gestión de seguridad de la información (SGSI)

Información en línea:

Este componente tiene como finalidad garantizar que las entidades ponen a disposición de la comunidad información relacionada con su planeación estratégica (misión, visión, valores, políticas, etc.) así como los diferentes servicios que ofrece, y todo lo relacionado con su quehacer, garantizando que dicha información cumpla con los estándares de seguridad y de fácil accesibilidad por parte de los usuarios. Las actividades de este componente están concentradas principalmente en dos aspectos:

- Publicación de información
- Publicación de datos abiertos

Interacción en línea:

Propicia la generación de procesos que faciliten la comunicación e interacción entre los funcionarios, comunidad y empresas, al igual que se presentan mecanismos de consulta en línea que fortalezcan las relaciones entre las entidades del estado y los usuarios, brindando mecanismos que ayuden a un mayor contacto y resolución de requerimientos. Las actividades están concentradas en dos aspectos: 1. Habilitar espacios electrónicos para interponer peticiones y 2. Habilitar espacios de interacción.

Transacción en línea:

Hace referencia al conjunto de actividades necesarias para que las instituciones puedan poner a disposición de la comunidad la prestación de servicios en línea, que empieza desde la solicitud del requerimiento hasta obtener el producto esperado, eliminando la tramitología y documentación que se exigían con anterioridad y que hacía que los procesos fueran más demorados. La actividad a adelantar por parte de las entidades para dar cumplimiento al Componente de Transacción en línea está relacionada principalmente con la posibilidad del ciudadano de realizar trámites y servicios en línea, lo cual implica:

- Formularios para descarga y/o diligenciamiento en línea
- Expedición en línea de certificaciones y constancias,
- Automatización de trámites y servicios
- Ventanillas Únicas Virtuales
- Pagos en línea
- Uso de firmas electrónicas y digitales

3.6. Metodología para implementar el Gobierno en Línea

La Estrategia de Gobierno en Digital debe ser incorporada por parte de las entidades de forma transversal dentro de sus planes de desarrollo y estratégicos sectoriales e institucionales, y anualmente dentro de los planes de acción, en donde se deben definir las actividades, responsables, metas y recursos presupuestales que les permitan dar cumplimiento a los lineamientos que se establecen en el Decreto de Gobierno en línea y en los Manuales para la implementación de la Estrategia. En tal sentido, el Gobierno en Línea se encuentra incluido en el Modelo Integrado de Planeación y Gestión como una herramienta dinamizadora para el cumplimiento de las metas de las Políticas de Desarrollo Administrativo, las cuales permiten enmarcar el quehacer misional y el de apoyo, tomando como referentes las metas de Gobierno establecidas en el Plan Nacional de Desarrollo y las competencias normativas asignadas a cada entidad. Para orientar la planeación de la Estrategia de Gobierno en Digital, el MINTIC ha definido pesos ponderados para cada una de las actividades contenidas en los Componentes de la Estrategia antes mencionados, según la importancia para su desarrollo. Igualmente ha establecido unos plazos para la implementación de la Estrategia y unos porcentajes mínimos de avance para los diferentes grupos de entidades que conforman la administración pública, desde el año 2018 hasta el año 2023 para entidades del orden nacional y desde el año 2018 hasta el año 2022 para entidades del

orden territorial. Estas actividades y respectivos pesos están plasmadas en la versión 3.1 del Manual para la Implementación de la Estrategia de Gobierno en línea. Los plazos para la implementación de la Estrategia establecidos en el Decreto 2693 de 2012 de Gobierno en Digital son los siguientes:

- A. Para alcaldías de categoría cuarta, quinta y sexta, la administración pública y demás sujetos obligados en el mismo orden, clasificación a la cual pertenecen las alcaldías de sexta categoría del sur del Departamento del Cesar son:

Año	Información en línea	Interacción en línea	Transacción en línea	Transformación	Democracia en línea	Transversales
2013	40%	25%	15%	15%	40%	35%
2014	55%	50%	35%	35%	65%	60%
2016	80%	75%	70%	60%	95%	85%
2017	100%	100%	100%	100%	100%	100%

Fuente: Decreto 2693 de 2012.

Tabla 2 – Plazos implementación Decreto 2693 de 2012

De igual manera, las entidades deben garantizar que realizan las acciones oportunas para realizar el monitoreo y evaluación del cumplimiento de la Estrategia de Gobierno en Digital, igualmente deberán adelantar las mediciones de impacto del uso y beneficio del Gobierno en Digital en sus usuarios, lo anterior de acuerdo con las metodologías y lineamientos respectivos definidos por el Ministerio TIC. Asimismo, y como complemento a la tarea de autoevaluación realizada por cada entidad, el Ministerio TIC debe adelantar acciones que permitan medir el avance en la implementación de la Estrategia de Gobierno en digital, así como el uso, calidad e impacto de la prestación de los más importantes trámites y servicios. Como consecuencia de este proceso de monitoreo, evaluación y seguimiento adelantado por cada ente territorial y por el Ministerio TIC, el Ministerio publica periódicamente el Índice de Gobierno en Digital, instrumento cuantitativo construido para la medición de avances de las entidades en la implementación de la Estrategia Gobierno en Digital. Asimismo, pueden establecerse los niveles de madurez que determinan el 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:

Nivel	Descripción
Inicial	Nivel en el cual se cuenta con las condiciones institucionales en términos tecnológicos, humanos, normativos, presupuestales y de planeación para habilitar cada uno de los componentes.
Básico	Nivel en el cual hay evidencia de la prestación de trámites y servicios en línea. Existe entendimiento dentro de la entidad pública sobre los objetivos y beneficios del uso de las tecnologías y las comunicaciones en la apertura de información en los procesos administrativos y en la interacción y prestación de servicios eficientes a los usuarios y ciudadanos que han sido caracterizados.

Nivel	Descripción
Avanzado	Nivel en el cual se masifica la prestación de trámites y servicios en línea de acuerdo con las necesidades identificadas de los ciudadanos y usuarios. El Gobierno en Línea está institucionalizado, es parte de la rutina diaria y la cultura del sujeto obligado y los procesos de rendición de cuentas y participación ciudadana en línea para la toma de decisiones que se realiza con frecuencia.
Mejoramiento permanente	Nivel en el cual hay interiorización, innovación y réplica de experiencias exitosas en cuanto al Gobierno en Línea. La entidad cuenta con datos abiertos a partir de los cuales se han generado servicios de valor agregado para los ciudadanos; implementa permanentemente acciones de mejora para garantizar la satisfacción de las necesidades de sus usuarios y de la ciudadanía en general, tanto en la prestación del servicio como en la discusión de políticas y promoción del control social

Fuente: MinTic

Tabla 3 – Niveles de madurez de la estrategia de Gobierno en Línea

4. Conclusiones

Las empresas del Estado requieren fortalecer sus procesos con la incorporación de herramientas tecnológicas que además de proveer rapidez, flexibilidad y oportunidad a los usuarios, también garantice la protección de la información que se intercambia. Debe reconocerse el avance que el país ha tenido en la implementación de la estrategia de Gobierno en Línea, sin embargo, falta camino por recorrer para alcanzar altos estándares en la seguridad de la información y en la reducción del papeleo que ha sido característico del sector público. Asimismo, es importante que se apunte al desarrollo de competencias digitales para los servidores públicos, al igual que la creación de estrategias que permitan atraer y desarrollar talento humano creativo y con conocimientos específicos que aporten al desarrollo de los procesos de innovación tecnológica.

Es importante además, crear una cultura digital no solo entre los funcionarios, sino entre la comunidad, logrando que los procesos sean más amigables, reconociendo que la aplicación de la tecnología ya no es una opción sino un requisito en el camino hacia el logro de organizaciones competitivas que presten servicios de calidad a sus usuarios, reconociendo que estos también son actores principales en la relación que debe darse entre el estado y la comunidad para alcanzar mayores niveles de interacción y fomentar la confianza y transparencia como principios fundamentales del sector público.

Referencias

Arévalo Ascanio, J. G. (2016). *Documentación del sistema de seguridad de la información bajo los requisitos de la norma NTC/ISO/IEC 27001:2013*. <http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/13373/T658.562%20A321.pdf?sequence=1&isAllowed=y>

- Banco Interamericano de Desarrollo. (2017). *Panorama de las Administraciones Públicas América Latina y el Caribe 2017*. <https://publications.iadb.org/publications/spanish/document/Panorama-de-las-Administraciones-P%C3%BAblicas-Am%C3%A9rica-Latina-y-el-Caribe-2017.pdf>
- Campos Ramírez, J. F. (2017). *Seguridad de la información en el sector público colombiano*. Universidad Piloto de Colombia: <http://polux.unipiloto.edu.co:8080/00002657.pdf>
- Contaduría General Nación. (2021). *Categorización de los municipios*. <https://www.contaduria.gov.co/balance-general-y-otros-informes>
- Correa Ortiz, L. C., Toro García, A. F., & Gutiérrez Vargas, C. C. (2019). *Estrategia de gobierno digital para la construcción de Estados más transparentes y proactivos*. Instituto Tecnológico Metropolitano: <https://www.redalyc.org/journal/5343/534367793009/>
- Función Pública. (2020). *Medición del desempeño institucional*. <https://app.powerbi.com/view?r=eyJrIjoiZGE2MzQ1YTQtYWV3ZCooYTdiLWJkY2ItNzI2YmU3YzQ1ZTk5IiwidCI6IjU1MDNhYWMyLTdhMTUtNDZhZi1iNTIwLTJhNjc1YWQxZGYxNiIsImMiOiJ9&pageName=ReportSection396d1cd03a850a004c5>
- Magazcitur. (2013). *Estructura del nuevo estándar ISO/IEC 27001:2013*. http://www.magazcitur.com.mx/?p=2397#.VXdLP M9_NBc
- Mintic. (2020). *Modelo de gestión*. <https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8158.html#modelogestion>
- Mintic. (2020). *Resolución 500 de 2021*. https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_0500_2021.htm#:~:text=Por%20la%20cual%20se%20establecen,la%20pol%C3%ADtica%20de%20Gobierno%20Digital
- Mintic. (2020). *Gestión IT4+*. <https://mintic.gov.co/gestion-ti/Gestion-IT4>
- Rivera Martínez, W., Sotelo Muñoz, A. M., & Quiñonez Zúñiga, C. (2021). *Implementación de gobierno en línea: factores que inciden en el caso del municipio de Balboa*. REOALCEI. <https://dialnet.unirioja.es/servlet/articulo?codigo=8118942>
- Secretaría Senado. (2021). *Constitución Política de la República de Colombia*. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html
- SUIN. (2019). *Decreto 2106 DE 2019*. http://www.suin-juriscal.gov.co/viewDocument.asp?id=30038501#ver_30205980