Metodología para la Medición de la Efectividad de los Indicadores de Gestión del Modelo de Seguridad y Privacidad de la Información

Cristina Useche Samudio

Escuela Colombiana de Ingeniería Julio Garavito

Nota del autor

Cristina Useche Samudio, Facultad de Ingeniería de Sistemas, Escuela Colombiana de Ingeniería Julio Garavito

La información concerniente a este documento deberá ser enviada a Facultad de Ingeniería de Sistemas, Escuela Colombiana de Ingeniería Julio Garavito, Avenida carrera 45 205-59 Autopista Norte. E-mail: kristina_useche@yahoo.com

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Dedicatoria

Dedico este trabajo a Jehová por haberme dado la oportunidad de participar en este hermoso proceso de crecimiento personal y profesional, así como a mi mamá por ser una fuente constante de apoyo incondicional, siendo el mejor ejemplo para mi vida.

Agradecimientos

Al proyecto de Talento Digital, gracias a sus programa pude cursar la MAESTRIA EN GESTIÓN DE LA INFORMACIÓN de la Escuela de Ingenieros Julio Garavito, con la cual he podido mejorar mi experiencia académica, también ha enriquecido mis conocimientos y los puesto en práctica, logrando un mejoramiento de mi perfil y experiencia profesional.

Al Ingeniero Jorge Fernando Bejarano Lobo, Director de Estándares y Arquitectura del MINTIC, por permitirme desarrollar este proyecto en el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia y a todo el personal que me proporcionó información y guía para hacer de este proyecto una realidad aplicable a las necesidades de nuestro país.

A la Ingeniera Yubelly Astrid Monroy Álvarez, Subdirectora de Seguridad y Privacidad de TI, por su gran colaboración y asesoría en el desarrollo de este proyecto.

A la Ingeniera Victoria Eugenia Ospina Becerra por su apoyo y guía para la culminación con éxito de la Maestría de Gestión de Información.

A mi amiga Luz Andrea Peña Castro, con quien compartí este proceso de principio a fin, gracias por tu ayuda, apoyo y amistad

A mi madre Luz Marina Samudio Vargas y a mi tía Carmen Samudio Vargas, por su apoyo incondicional en todos los procesos de formación que he emprendido y llevado a feliz culminación, siendo participes incondicionales.

_____

Cristina Useche Samudio

Bogotá, Septiembre de 2016

Nota De Confidencialidad

La información presentada en este documento es propiedad intelectual del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, ha sido recolectada y procesada para dar respuesta a los requerimientos para optar al título de Magíster en Gestión de Información manifestados por La Escuela Colombiana de Ingeniería Julio Garavito como requisito indispensable para soportar el marco de referencia, metodológico y conceptual del proyecto de grado titulado "Metodología para la Medición de la Efectividad en la Implementación del MSPI en Entidades del Estado (Modelo de Seguridad y Privacidad de la Información)"

Los documentos, formatos y esquemas contenidos en esta investigación contienen información de carácter sensible y son clasificados como confidenciales y restringidos de uso privado del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, su divulgación, reproducción, distribución y uso para fines diferentes al establecido en el proyecto

de grado en mención no están permitidos, de igual forma los anexos complementarios e imágenes contenidas en este documento son de carácter confidencial y van dirigidos en forma exclusiva a su destinatario, La Escuela Colombiana de Ingeniería Julio Garavito.

De lo anterior, se manifiesta que el uso o discusión de este documento fuera del ámbito académico asociado al proyecto de grado relacionado y de su aprobación, así como la reproducción, distribución o comunicación de información, mapas y del contenido del mismo por cualquier medio, queda expresamente prohibido sin el consentimiento escrito del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

Contenido

ABSTRACT

Methodology for Measuring the Effectiveness of Management Indicators Model Security and Privacy Information designed for entities to identify whether the indicators implemented in each of the entities are being effective. The methodology that can be implemented seeks an indicator of overall effectiveness for entities with which the process owners and senior management to make decisions to improve the processes of the organization.

INTRODUCCIÓN

El Estado Colombiano tienen su máximo interés en mejorar los servicios que cada una de las entidades públicas brindan a los ciudadanos en los diferentes áreas de servicio al cliente, adicionalmente y no menos importante lograr que la información ya sea de clientes, proveedores, o propia de la entidad o de cualquier otro tipo sea salvaguardada de la manera más eficaz (Comunicaciones M. -M., Estrategia de Gobierno en Línea)

Por medio de la implementación del Plan Vive Digital 2, el Estado Colombiano busca lograr la masificación del internet y el desarrollo del ecosistema digital definido para el periodo 2014 – 2018 el cual se encuentra divido en 4 grandes áreas:

Ilustración 1. Ejes del ecosistema digital 1

1. **APLICACIONES**: Herramientas que permiten a los usuarios comunicarse, realizar trámites, entenderse, orientarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores, tabletas o celulares. Las aplicaciones se han dividido en sociales, de gobierno y de contenido (Gobierno Colombiano, 2015).

2. **USUARIOS**: Son quienes hacen uso de las aplicaciones e indirectamente de los servicios e infraestructura para consumir y producir información digital. Los usuarios en este ecosistema somos todos los que usamos Internet, telefonía celular o cualquier otro medio de comunicación digital (Gobierno Colombiano, 2015).

3. **INFRAESTRUCTURA**: Son los elementos físicos que proveen conectividad digital. Algunos ejemplos son las redes de fibra óptica, las torres de telefonía celular con sus equipos y antenas, y las redes de pares de cobre, coaxiales o de fibra óptica tendidas a los hogares y negocios (Gobierno Colombiano, 2015).

4. **SERVICIOS**: ofrecidos por los operadores hacen uso de la infraestructura y permiten desarrollar la conectividad digital. Algunos ejemplos de servicios son el servicio de Internet, el servicio de telefonía móvil o el servicio de mensajes de texto (SMS) (Gobierno Colombiano, 2015).

Con el fin de lograr la integración del Plan Vive Digital 2, el Ministerio de Tecnologías de la Información y las Comunicaciones desarrollo como estrategia el Modelo de Seguridad y Privacidad de la Información versión 3.0.2, en el cual se estructura la prestación a los ciudadanos quienes son el principal actor y quien dispara el proceso para la protección de los datos personales, los activos de información con cumplir con los pilares fundamentarles de seguridad de la información: Integridad, Confidencialidad y Disponibilidad.

Para el cumplimiento de los objetivos del Modelo de Seguridad y Privacidad de la Información se reunión un conjunto de lineamientos, políticas, normas, procesos que involucran a todas las entidades del estado colombiano que tengan que implementar el modelo.

Este proyecto, "Metodología para la Medición de la Efectividad de los Indicadores de Gestión del Modelo de Seguridad y Privacidad de la Información", se encuentra enmarcado principalmente en la fase de Mejora Continua, ya que los nueve (9) indicadores servirán de base para generar el indicador de efectividad por cada una de las entidades, así como generar recomendaciones y hacer seguimiento.

Durante el proceso de desarrollo del proyecto se identificó se definió que se pueden implementar planes de mejoramiento hasta que la entidad alcance la completa implementación

del Modelo de Seguridad y Privacidad de la Información. Para lograr que la herramienta desarrollada sea atractiva a los usuarios, su desarrollo pensando en que sea amigable al usuario final y fácil de interpretar.

Con el fin de lograr que los usuarios sientan seguridad en el uso de la información, y así también lograr que se presente un equilibrio real entre la privacidad y la seguridad, para los clientes, proveedores y para las mismas entidades del estado, con el fin de lograr que el estado se fortalezca y logre la estabilidad económica de los ciudadanos.

1. PLANTEAMIENTO DEL PROBLEMA

En el año 2010 se realizó la primera versión del Modelo de Seguridad y Privacidad de la Información diseñado por el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, el cual busca la construcción de un Estado eficiente, más transparente y participativo, proteger tanto la información como los sistemas mediante la definición del Marco de Seguridad y Privacidad de la Información, la implementación del Modelo en las Entidades de orden Nacional y Territorial, el monitoreo y la mejora continua (Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC, 2015).

En la actualidad el Modelo de Seguridad y Privacidad de la Información se encuentra en su versión número 3.0.2, la cual se publicó en Julio del año 2016, la cual fue distribuida para su implementación a las entidades del estado; sin embargo, el MINTIC a hoy no tiene información que permita determinar cuál es el nivel de implementación del modelo y si ha sido efectivo o no a nivel entidad y a nivel del sector público. Esto principalmente porque no se cuenta con una metodología que le permita al MINTIC, conocer a través de un tablero de mando cual es el estado de implementación del modelo por empresa y a nivel global todo el sector.

El modelo actualmente cuenta con indicadores de cumplimiento y de gestión, los cuales deben ser calculados por cada entidad; así mismo el Marco de Arquitectura Empresarial publicado el 6 de noviembre de 2014, también creada por el MINTIC, cuenta con otra serie de indicadores relacionados con la implementación de controles de seguridad en las entidades. El MINTIC en el modelo y en el marco de arquitectura, definió claramente cómo medir los procesos, pero no, cómo centralizar esta información, la cual es de vital importancia para la mejora continua del modelo.

Es por esto que este proyecto plantea una solución a esta problemática, mediante la creación de una metodología para la medición de efectividad, centralizando el cálculo de indicadores críticos por entidad y definiendo un indicador de efectividad global. Esta información le permitirá al MINTIC conocer la acogida del modelo, hacer seguimiento a la implementación en las entidades, establecer mejoras y planes de acción con las entidades que han tenido inconvenientes con el modelo.

2. **JUSTIFICACIÓN**

El Modelo de Seguridad y Privacidad de la Información reúne el conjunto de lineamientos, políticas, normas, procesos e instituciones que son las encargadas de promover la puesta en marcha, supervisión, mejora y control de la implementación, no solo del Modelo de Seguridad y Privacidad de la Información, sino también de la implementación de la Estrategia de Gobierno en Línea, que busca prestar mejores servicios al ciudadano y lograr la excelencia de la gestión.

Para poder medir el avance en la implementación del modelo, se hace necesario manejar un indicador que calcule la efectividad del mismo, que permita evaluar el impacto en el logro de los resultados y el grado de cumplimiento de los objetivos. En el caso del Modelo de Seguridad y Privacidad de la Información el indicador le permitirá a el MINTIC conocer con datos y estadísticas qué tan efectivo ha sido la implementación, como ha sido la acogida del Modelo por parte de los usuarios y de las entidades de orden Nacional y Territorial, así como la identificación de los problemas que enfrentan en el momento de hacer la implementación.

La medición de la efectividad del Modelo de Seguridad y Privacidad de la Información cobra mayor importancia para el MINTIC, ya que se conocerá si el logro de los resultados

programados en el modelo es eficaces y eficientes en términos de tiempo, costos y beneficio, es decir, si han logrado cumplir con los objetivos trazados, en los tiempos y con los recursos programados.

Las Entidades que implementen el Modelo de Seguridad y Privacidad de la Información pueden alcanzar muchos beneficios, ya que el modelo impulsa el desarrollo de un sistema de seguridad efectivo, con el cual se logra la protección de la información y sus activos más importantes, minimizar los costos que se puedan presentar por demandas o quejas de ciudadanos por inconformidad en los servicios que reciben, igualmente se reduce la pérdida de clientes y ayuda a la mejora en las relaciones con los proveedores.

Al definir el indicador de efectividad para realizar la medición del Modelo, las Entidades podrán identificar las fallas o falencias, así como las fortalezas, para la implementación y la puesta en marcha del Modelo, así mismo es importante que se establezca un canal de comunicación entre las Entidades que implementaran el Modelo de Seguridad de la Información y el MINTIC, que será entidad recolectora de la información para calcular el indicador general de efectividad de todo el Modelo.

Una vez se realice la implementación del indicador de efectividad para la medición del Modelo, el MINTIC podrá reducir la incertidumbre presentada de no tener la información centralizada y como consecuencia no poder identificar las falencias que se presentan en cada una de las entidades, teniendo en cuenta que cada una de ellas es diferente y su grado de capacidad para la implementación es diferente.

Dentro de los beneficios que se alcanzaran al identificar la efectividad de la implementación, se podrá motivar a los equipos encargados de la implementación y no solo a las directivas; y otros beneficiarios son los usuarios o ciudadanos ya que disfrutaran de la eficiencia y eficacia en los servicios que cada una de las entidades prestará generando satisfacción en la utilización de los servicios, también el personal encargado de prestar los servicios aprovechando los recursos que se asignan generando calidad en los servicios.

Otro de los beneficios al implementar un control para medir la efectividad en la implementación del Modelo de Seguridad y Privacidad de la Información es la de realizar seguimiento a la efectividad de la implementación de 24 guías diseñadas por el MINTIC, con el fin de evaluar y visualizar periódicamente su evolución, llegando a ser actividades claves en la implementación del Modelo.

Igualmente cuando se logre tener centralizada la medición de la efectividad de todas las entidades se podrá realizar un Benchmarking, el cual es un proceso continuo y sistemático de evaluar los productos, servicios o procesos de las entidades que son reconocidas por ser representativas de las mejores prácticas para efectos de mejora organizacional (Gerencia y Negocios en Hispanoamérica, 2015). Una forma de comparación del desempeño de una entidad con otras del mismo sector, con el fin de validar si están teniendo los mejores resultados. Las empresas pueden realizar comparaciones con sus propios resultados, sin embargo los resultados puede que no sean los mejores comparados con las demás.

Como estrategia corporativa la medición de la efectividad del Modelo de Seguridad y Privacidad de la información, presentará beneficios para la gerencia del cambio, abriendo la oportunidad para que se replanteen nuevos esquemas en la toma de decisiones para cada entidad, considerando las diferencias entre ellas.

Este proyecto busca que a las entidades tengan una visión general de la efectividad que tienen cada una de las entidades en la implementación de los indicadores y los controles cuya finalidad es la implementación del Modelo de Seguridad y Privacidad de la información, con el tiempo

lograr una consolidación de la información de los indicadores de todas las entidades, con el fin de tener un control general en la implementación.

3. **OBJETIVOS**

3.1. **Objetivo General**

Diseñar y desarrollar una metodología para la medición de la efectividad de los indicadores de gestión del Modelo de Seguridad y Privacidad de la Información versión número 3.0.2 en las entidades del Estado Colombiano.

3.2. **Objetivos específicos**

- Creación y cálculo del indicador de efectividad de los Indicadores de Gestión del Modelo de Seguridad y Privacidad de la Información versión número 3.0.2.

- Diseño y desarrollo de un Tablero de Mando para la consolidación de los indicadores por parte de cada una de las entidades.

- Definición de indicadores adicionales que requiera la metodología para el cálculo del indicador de efectividad.

- Generación de la plantilla de informe de los resultados del indicador de efectividad.

- Generación de observaciones de mejora para cada indicador, de acuerdo al nivel de cumplimiento en el que se encuentre.

4. **ALCANCE**

El Modelo de Seguridad y Privacidad de la Información (versión 3.0.2, publicada el 29 de Julio de 2016) para la Estrategia de Gobierno en Línea 2.0., hace parte del Plan Vive Digital, el cual busca que el país de un salto tecnológico mediante la masificación del Internet y el desarrollo del ecosistema digital nacional (Comunicaciones, MINTIC - Ministerio de Tecnologías de la Información y las, s.f.), es por ello que centra sus esfuerzos en preservar los pilares fundamentales de la seguridad de la información a saber confidencialidad, integridad y disponibilidad.

El Modelo de Seguridad y Privacidad de la Información, cobija a las Entidades Nacionales y Territoriales, las cuales lo implementarán basándose en las 24 guías en las cuales se centra el Modelo.

De acuerdo con lo anterior el alcance de éste proyecto tiene aplicación a todas las entidades de orden Nacional y Territorial, que implementen el Modelo de Seguridad y Privacidad de la Información a las cuales el MINTIC ya que se hace necesario que cuenten con una herramienta para realizar la medición de la efectividad de los indicadores que están implementando, y así identificar si el modelo para la entidad está teniendo los resultados esperados.

La evaluación se realiza con el fin de identificar que entidades han logrado la implementación a satisfacción la cual se puede medir por el grado de eficacia, los problemas o fallas que se han presentado en el camino y el grado de participación de los stakeholders, los miembros de cada Entidad, los usuarios que se benefician de los servicios y el MINTIC quien es el encargado de realizar la medición final de nivel de implementación del modelo.

El Modelo De Seguridad Y Privacidad De La Información, definió 24 guías para su implementación y cada una de las Entidades debe realizar dependiendo de factores como el tamaño y el sector, así después de implementadas las guías se podrá evaluar el nivel de eficacia para cada una de las entidades, las guías definidas son las siguientes:

- Guía No. 1 - Encuesta de Seguridad
- Guía No. 2 - Estratificación para las entidades modelo de seguridad y privacidad de la información.
- Guía No. 3 - Auto-Evaluación de Seguridad.
- Guía No. 4 - Metodología de pruebas de efectividad
- Guía No. 5 - Política general MSPI v1.
- Guía No. 6 - Procedimientos de seguridad y privacidad de la información.
- Guía No. 7 - Roles y responsabilidades de seguridad y privacidad de la información.
- Guía No. 8 - Gestión de activos.

- Guía No. 9 - Gestión documental.
- Guía No. 10 - Gestión de riesgos.
- Guía No. 11 - Controles de seguridad.
- Guía No. 12 - Indicadores de gestión SI.
- Guía No. 13 - Continuidad de TI.
- Guía No. 14 - Impacto de negocio
- Guía No. 15 - Seguridad en la nube.
- Guía No. 16 - Guía de evidencia digital.
- Guía No. 17 - Plan de comunicación, sensibilización y capacitación.
- Guía No. 18 - Auditoría.
- Guía No. 19 - Mi pymes.
- Guía No. 20 - Mejora continua.
- Guía No. 21 - Lineamientos terminales de áreas financieras entidades pública.
- Guía No. 22 - Aseguramiento del protocolo IPv6.
- Guía No. 23 - Transición IPv4 a IPv6.
- Guía No. 24 - Gestión de incidentes.

La definición del indicador de efectividad busca acercar la realidad de la Entidad al cumplimiento del Modelo, identificando que acciones correctivas de deben implementar en caso de ser necesario para alcanzar el 100% de la efectividad para cada una de ellas.

5. MARCO TEORICO

Para el desarrollo de una herramienta que pudiera consolidar, analizar y sirviera para hacer seguimiento a los indicadores y así generar el indicador de efectividad se hace necesario tener claros los siguientes conceptos que están estrechamente relacionados con su desarrollo.

5.1. Seguridad de la Información

Para las entidades nacionales y territoriales, la implementación del Modelo de Seguridad y Privacidad de la Información es un aspecto fundamental para alcanzar el mejoramiento en los servicios brindados por cada una de las entidades, igualmente busca generar conciencia colectiva orientada a la importancia de clasificar, valorar y asegurar los activos de cada entidad[1].

[1] (Ministerio de Tecnologías de la Información y las Comunicaciones , 2016)

La seguridad de la información tiene como objetivos la protección de datos y la protección de la información. Las entidades deben entender la necesidad de proteger los datos, su pérdida o modificación no autorizada y se basa en tres pilares fundamentales:

Ilustración 2- Pilares de la seguridad de la Información

- **CONFIDENCIALIDAD:** Consiste en la característica que protege la información a nivel de usuario, pues se podrá acceder a la información dependiendo de su nivel de necesidad de saber, solo la utilizan quienes están autorizadas para hacerlo. La confidencialidad se puede perder haciendo caso omiso a las recomendaciones de seguridad.

- **INTEGRIDAD:** Hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina, y una gran garantía para mantenerla intacta es, como hemos mencionado en anteriores ocasiones, la firma digital.

- **DISPONIBILIDAD**: Consiste en que la información siempre este accesible cuando se necesite los usuarios, teniendo en cuenta los niveles de seguridad y los usuarios. la disponibilidad, puede en ocasiones chocar frontalmente con la confidencialidad, ya que un cifrado complejo o un sistema de archivado más estricto puede convertir la información en algo poco accesible, por lo que no se trata en absoluto de un punto menor y marca en gran medida el buen hacer del responsable de la seguridad de la información de la empresa u organización.

5.2. **Evolución de la Seguridad de la Información**

Ilustración 3-Hitos de la seguridad de la información.

La seguridad de la información se enfoca en la seguridad del negocio y sus inicios fueron a finales de los años 80 y principios de los años 90 y tenía su objetivo principal en la seguridad de los ordenadores que existían y eran utilizados por los usuarios, igualmente se centraba en la seguridad de los sistemas operativos, buscaban la protección ante virus informáticos ya que con el uso los mismos usuarios podían contaminar los equipos.

Con la aparición del internet en el año 1995 cuando se liberó su uso globalizado, tanto en las entidades educativas y las empresas se hizo posible que los equipos se contaminaran más fácilmente con nuevos virus, es por este motivo que se las empresas se interesaron ya no solo en la protección de los equipos de escritorio u ordenadores, también se interesaron en sus servidores y las redes en general, se inicia con el uso de los Firewalls para controlar los accesos a las redes.

La facilidad de tener más conexiones implica la aparición de nuevas vulnerabilidades o punto de falla que pueden ser explotados para extraer información o inhabilitar sistemas, es por esto que las empresas y por ende las entidades deben proteger la información para evitar pérdidas importantes.

Para el año 1997 Charles Plefeer generó una clasificación de las propiedades de la seguridad de la información, en la que indicó que éstas son: confidencialidad, integridad y disponibilidad (CID).

Entre los años 2001 y 2005 con la ayuda de varios investigadores y autores se trabaja en el desarrollo de las características definiendo la seguridad de la información de manera detallada considerando aspectos legales y las mejores prácticas que fueron registradas en los estándares ISO/IEC 27000 que fueron creadas en el año 2005 para los sistemas de gestión de seguridad de la información.

En 2008 la Unión Internacional de Telecomunicaciones de la ONU generó el estándar ITU-T X.1205, como “Redes de datos para la comunicación de sistemas abiertos y la seguridad de las telecomunicaciones”, en el que se da un panorama general sobre la seguridad cibernética

definida como “un conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, guías, la administración del riesgo, las acciones, mejores prácticas y tecnologías que se puedan usar para proteger los bienes de una organización y el uso del ciber espacio”.

En 2010 el estándar ISO/IEC 27032 incluye una guía general para la seguridad cibernética, tanto para los proveedores de servicios de comunicaciones como para los usuarios de internet con tal de que se reduzca spam, ataques de virus y malas prácticas. La norma define seguridad cibernética como “la preservación de la confidencialidad, integridad y la disponibilidad (CID) de la información en el espacio cibernético, razón por la cual también define espacio cibernético como el ambiente complejo resultante de la interacción de la gente, el software y los servicios de internet, soportado por equipos tecnológicos y redes interconectadas, las cuales no existen en forma física”.

Desde el año 2010 la seguridad cibernética y el espacio cibernético han ido refinando sus definiciones, incluso el gobierno de los EEUU cuenta con sus propias definiciones y en 2012 se ha discutido si es pertinente ejercer un control mucho más severo sobre internet. [2]

(Velázquez, 2014)

5.3. **Modelo de Seguridad y Privacidad de la Información versión 3.0.2. publicado 29 de julio de 2016**

El MINTIC por medio de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, busca dar cumplimiento a sus funciones, a través de las cuales contribuye a la construcción de un Estado más eficiente, más transparente y participativo, publica El Modelo de Seguridad y Privacidad de la Información. Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información en las entidades, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación Colombiana. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

El modelo implementado en las entidades del estado está compuesto por un modelo operacional compuesto por cinco (5) fases, cada una comprende objetivos, metas y herramientas guías, para que el modelo sea sostenible en el tiempo.

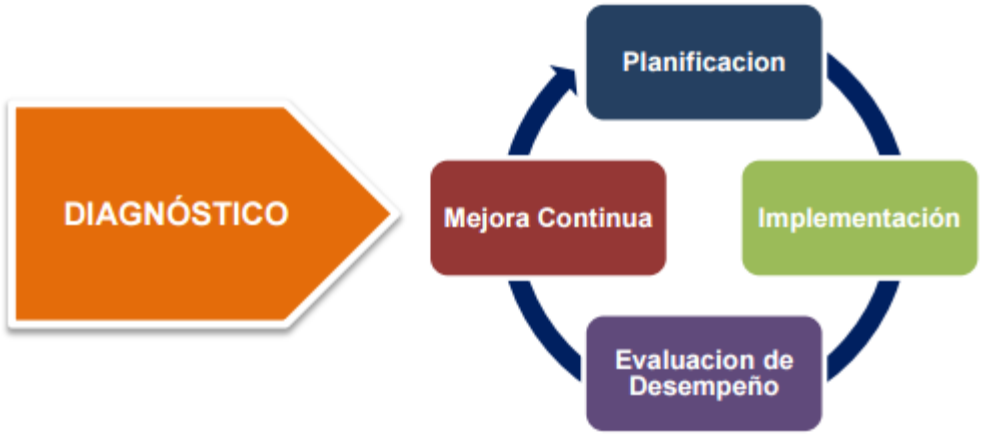

Ilustración 4-Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

- **Fase de Diagnóstico:** Identifica el estado inicial de la entidad antes de iniciar la implementación, valida el nivel de madurez e identificar los hallazgos encontrados en las pruebas de vulnerabilidad**.**

Ilustración 5- Etapas previas a la implementación

- **Fase de Planificación:** la entrada para este ciclo es el resultado del anterior, con el fin de diseñar el plan de seguridad orientado a los objetivos misionales de cada una de las entidades, utilizando la gestión de riesgos; se debe tener en cuenta los procesos que impactan el negocio, los servicios, objetivos misionales, entre otros.

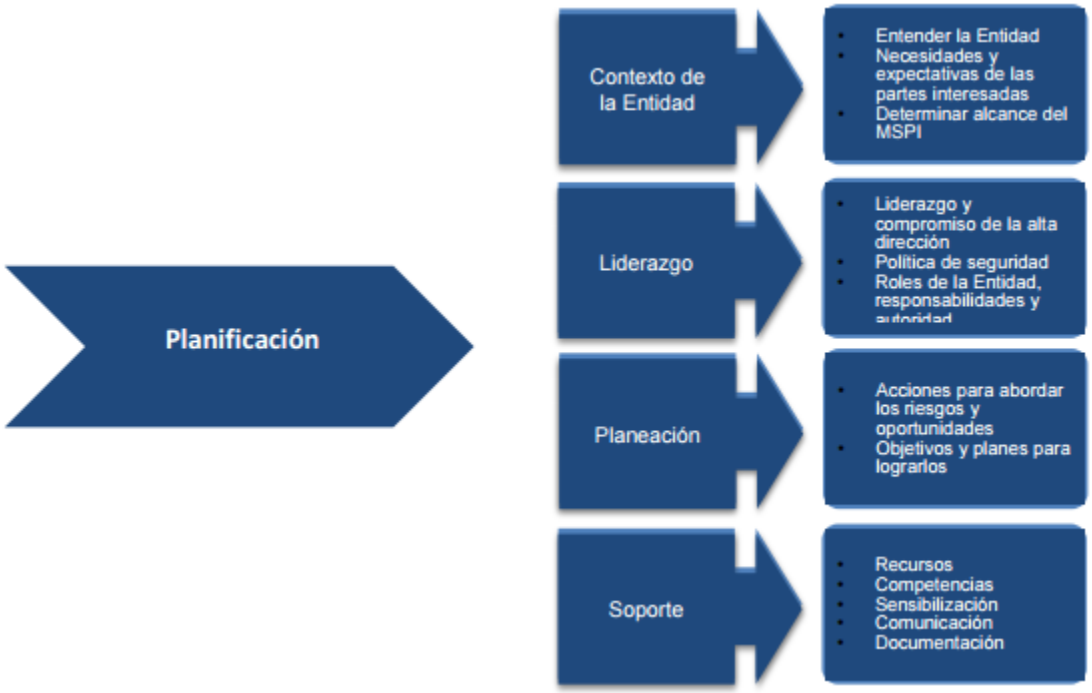

Ilustración 6- Fase de planificación

La base documental está compuesta por la Política de seguridad y privacidad de la información, los procedimientos, tabla de roles y responsabilidades (RACI),

inventarios de activos de información, identificación, valoración y tratamiento de riesgos, el plan de comunicaciones y el plan de transición de IPv4 a IPv6.

- **Fase de Implementación:** En esta fase se lleva a cabo la implementación según la planificación establecida para cada una de las entidades., se deben ejecutar la planificación y control operacional, la implementación del plan de tratamiento de riesgos, los indicadores de gestión y el plan de transición de IPv4 a IPv6.

Ilustración 7- Fase de implementación

- **Fase de Evaluación de Desempeño:** Para realizar seguimiento y monitoreo a la implementación y buen desempeño del modelo, se hace por medio de los resultados de los indicadores, las auditorías internas y la revisión por parte de la dirección.

Ilustración 8- Fase de evaluación de desempeño

- **Fase de Mejora Continua:** Todas las entidades con los resultados generados deben desarrollar un plan de mejora continua, con el fin de identificar oportunidades de mejora y mitigar riesgos futuros.

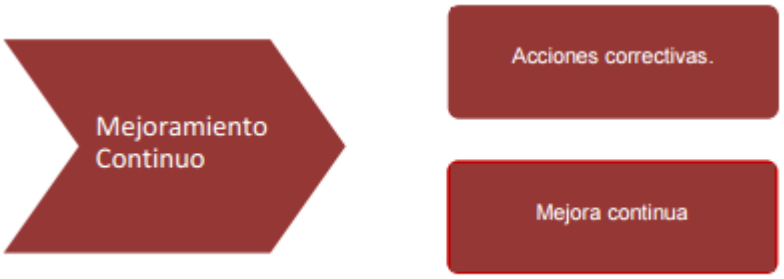

Ilustración 9- Fase de mejoramiento continuo

El modelo permite identificar el modelo de madurez de cada una de las entidades, el cual está dividido en 6 niveles (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016):

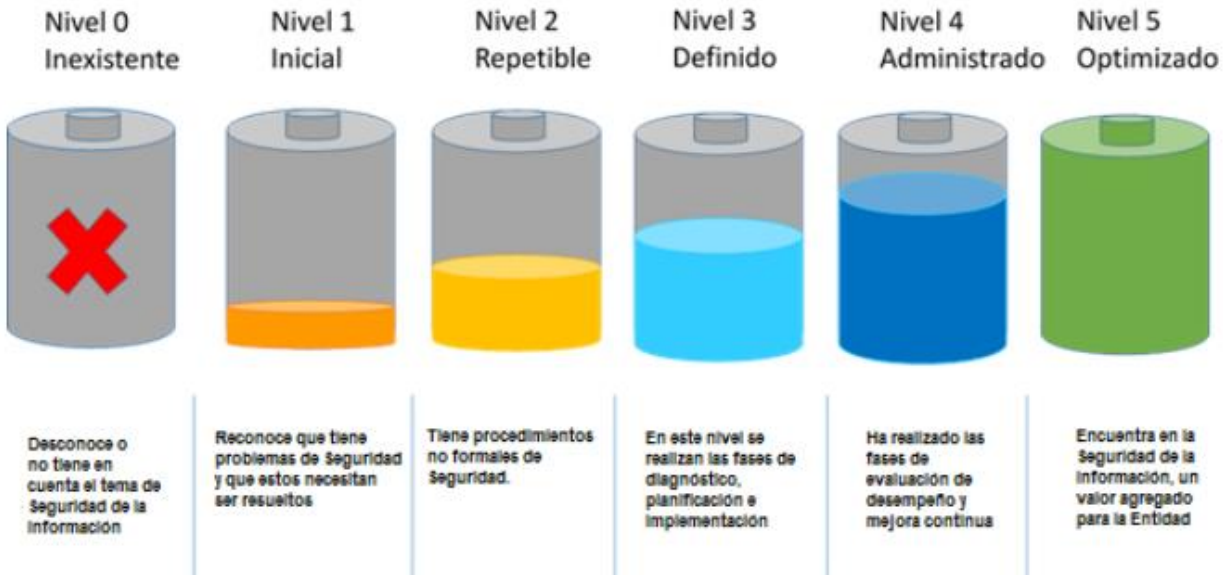

Ilustración 10- Niveles de madurez

Nivel 0 Inexistente

- Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo no están alineados a un Modelo de Seguridad.
- No se reconoce la información como un activo importante para su misión y objetivos estratégicos.
- No se tiene conciencia de la importancia de la seguridad de la información en la entidad.

Nivel 1 Inicial

- Se han identificado las debilidades en la seguridad de la información.
- Los incidentes de seguridad de la información se tratan de forma reactiva.
- Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.

Nivel 2 Repetible

- Se identifican en forma general los activos de información.
- Se clasifican los activos de información.
- Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información.
- Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión.
- La entidad cuenta con un plan de diagnóstico para IPv6.

Nivel 3 Definido

- La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.
- La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información.
- La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas.
- La Entidad tiene procedimientos formales de seguridad de la Información
- La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.
- La Entidad ha realizado un inventario de activos de información aplicando una metodología.
- La Entidad trata riesgos de seguridad de la información a través de una metodología.
- Se implementa el plan de tratamiento de riesgos.
- La entidad cuenta con un plan de transición de IPv4 a IPv6.

Nivel 4 Administrado

- Se revisa y monitorea periódicamente los activos de información de la Entidad.
- Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información.
- Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.
- La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.

Nivel 5 Optimizado

- En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización.
- Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.
- La entidad genera tráfico en IPv6.

5.4. **Medición definida por el Marco de Arquitectura Empresarial**

El MINTIC diseño un Marco de Referencia de Arquitectura Empresarial, como soporte para todas las instituciones y el cual será adaptado a las necesidades y características propias de cada sector y entidad (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

El Marco de Referencia de AE está compuesto por Principios, Dominios y Base de Conocimiento.

Ilustración 11- Estructura del Marco de Referencia de AE para la Gestión de TI en el Estado colombiano.

- **Principios:** Son reglas de alto nivel que se deben tener en cuenta para el desarrollo de las arquitecturas empresariales sectoriales, institucionales y territoriales, se desarrolla con fundamento en los principios consagrados en los Artículos 209 de la Constitución Política, 3° de la Ley 489 de 1998 y 3° de la Ley 1437 de 2011

- **Dominios:** Son seis dominios

- **Estrategia TI:** Tiene el fin de apoyar el proceso de diseño, implementación y evolución de la Arquitectura TI en las instituciones, para lograr que esté alineada con las estrategias organizacionales y sectoriales.

- **Gobierno TI:** Brinda directrices para implementar esquemas de gobernabilidad de TI y para adoptar las políticas que permitan alinear los procesos y planes de la institución con los del sector.

- **Información:** Permite definir el diseño de los servicios de información, la gestión del ciclo de vida del dato, el análisis de información y el desarrollo de capacidades para el uso estratégico de la misma.

- **Sistemas de Información: P**ermite planear, diseñar la arquitectura, el ciclo de vida, las aplicaciones, los soportes y la gestión de los sistemas que facilitan y habilitan las dinámicas en una institución.

- **Servicios Tecnológicos: P**ermite gestionar con mayor eficacia y transparencia la infraestructura tecnológica que soporta los sistemas y servicios de información en las instituciones.

- **Uso y Apropiación: P**ermite definir la estrategia y prácticas concretas que apoyan la adopción del Marco y la gestión TI que requiere la institución para implementar la Arquitectura TI.

- **Base de Conocimiento** provee un portafolio de instrumentos y herramientas que guían y ayudan a la implementación del Marco de Referencia de AE e incluye entre otros: estándares, lineamientos, guías, modelo de gestión de TI, mejores prácticas, soluciones y casos de éxito.

Los dominios del Marco de Referencia de AE, para el Estado colombiano están alineados con las definiciones hechas en el Diseño Contextual del Marco de Referencia de AE (Unión temporal Everis / Tecnocom, 2014) y son similares a los niveles que se presentan en los conceptos tradicionales de Arquitectura Empresarial, como se puede ver a continuación:

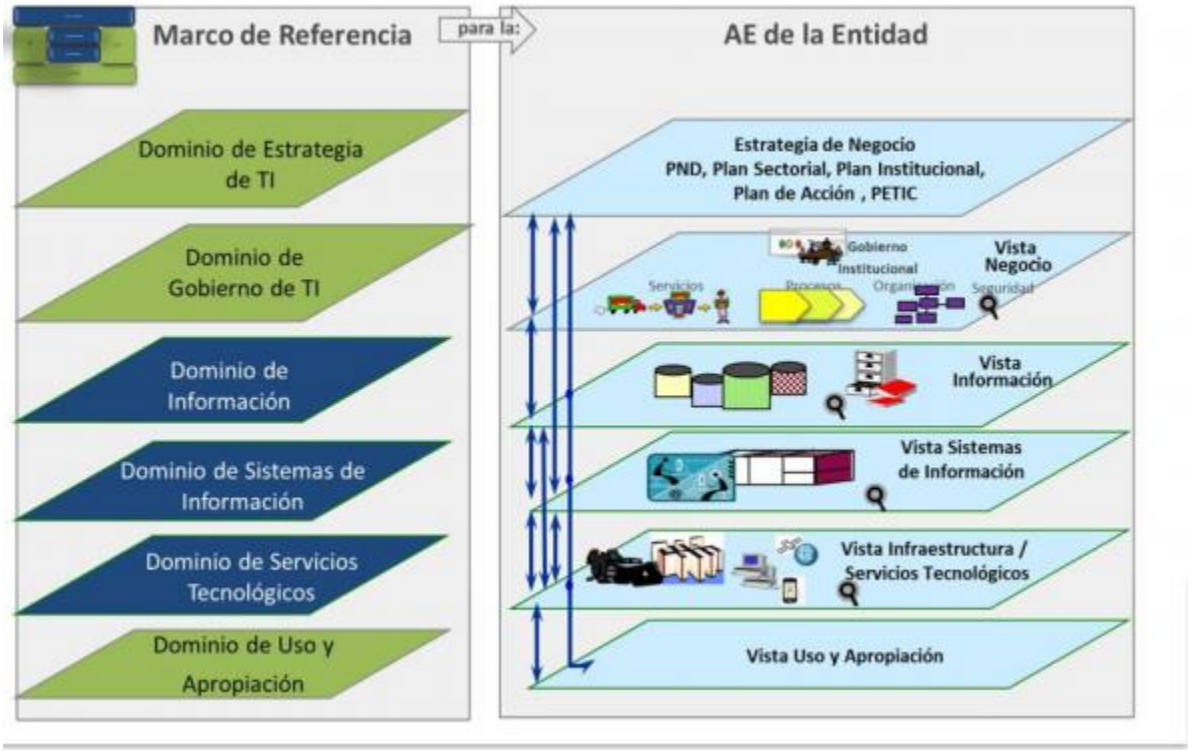

Ilustración 12- Modelo de contexto de los dominios

5.5. **Indicadores de Medición del Modelo de Seguridad de la Información**

Los indicadores de gestión está orientada principalmente en la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora (Ministerio de Tecnologías de la Información , 2015).

El Modelo de Seguridad y Privacidad de la Información definió 16 indicadores, de los cuales 5 son de gestión y 11 son de cumplimiento:

1. **ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN. (Indicador de gestión):** permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad.

2. **CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN (**Indicador de Gestión): permite determinar y hacer seguimiento al cubrimiento que se realiza a nivel de activos **críticos** de información de una entidad y los controles aplicados.

3. **TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (**Indicador de Gestión): El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.

4. **PLAN DE SENSIBILIZACIÓN (**Indicador de Gestión) permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.

5. **CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD (**Indicador de Cumplimiento) Cumplimiento de políticas de seguridad de la información en la entidad

6. **IDENTIFICACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD (**Indicador de Cumplimiento) Grado de la seguridad de la información y los equipos de cómputo.

7. **VERIFICACIÓN DEL CONTROL DE ACCESO (**Indicador de Cumplimiento) Grado control de acceso en la entidad

8. **ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE (**Indicador de Cumplimiento) Busca identificar la existencia de lineamientos, normas o estándares en cuanto a la adquisición o desarrollo de aplicaciones.

9. **IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA (**Indicador de Cumplimiento**)** Grado de existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.

10. **DETECCIÓN DE ANOMALÍAS EN LA PRESTACIÓN DE LOS SERVICIOS DE LA ENTIDAD (**Indicador de Cumplimiento**)** Grado de implementación de los mecanismos encaminados a la detección de anomalías e irregularidades

11. **POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD (**Indicador de Cumplimiento**)** Grado de implementación de políticas privacidad y confidencialidad de la entidad.

12. **VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN (**Indicador de Cumplimiento**)** Grado de implementación de mecanismos para la integridad de la información de la entidad.

13. **POLÍTICAS DE DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN (**Indicador de Cumplimiento**)** Grado de cumplimiento de las políticas de disponibilidad del servicio y la información.

14. **ATAQUES INFORMÁTICOS A LA ENTIDAD (**Indicador de Cumplimiento) Porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios.

15. **PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIO DE GOBIERNO EN LÍNEA QUE PRESTA LA ENTIDAD (**Indicador de Cumplimiento) Porcentaje de disponibilidad de los servicios que presta la entidad.

16. **PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES (**Indicador de Gestión) grado de avance en la implementación de controles de seguridad

5.6. **Medición**

5.6.1. Indicadores de Gestión

Un Indicador es una expresión cualitativa o cuantitativa observable que permite describir características, comportamientos o fenómenos de la realidad a través de la evolución de una variable o el establecimiento de una relación entre variables, la que comparada con periodos anteriores o bien frente a una meta o compromiso, permite evaluar el desempeño y su evolución en el tiempo (Departamento Administrativo Nacional de Estadística (DANE), 2014).

En todos los proyectos cobra importancia el poder realizar mediciones, con el fin de identificar si el sistema implementado está cumpliendo con los objetivos planteados, por esta razón se implementan indicadores de gestión.

Para poder controlar la gestión se debe tener en cuenta que "*todo se puede medir y por lo tanto se puede controlar*", porque "*lo que no se mide, no se puede administrar*" (Bank, 2003)

Los indicadores de gestión deben cumplir ciertos requisitos y elementos para poder apoyar la gestión y alcanzar el objetivo, las cuales pueden ser (Matiz, 2014):

- Simplicidad: capacidad para definir el evento que se pretende medir de manera poco costosa en tiempo y recurso.
- Validez en el tiempo: propiedad de ser permanente en un periodo deseado
- Adecuación: facilidad de la medida para describir por completo el fenómeno o efecto. Debe reflejar la magnitud del hecho analizado y mostrar la desviación real del nivel deseado.
- Utilidad: estar siempre orientado a buscar las causas que han llevado a que alcance un valor particular y mejorarlas.
- Participación de los usuarios: habilidad para estar involucrados desde el diseño, y debe proporciónaselas los recursos y formación necesarios para su ejecución.
- Oportunidad: capacidad para que los datos sean recolectados a tiempo, igualmente se requiere que le información sea analizada oportunamente para poder actuar.

5.6.2. Tipología de indicadores

Para la clasificación de los indicadores existen diferentes metodologías, por lo tanto existen diferentes clasificación.

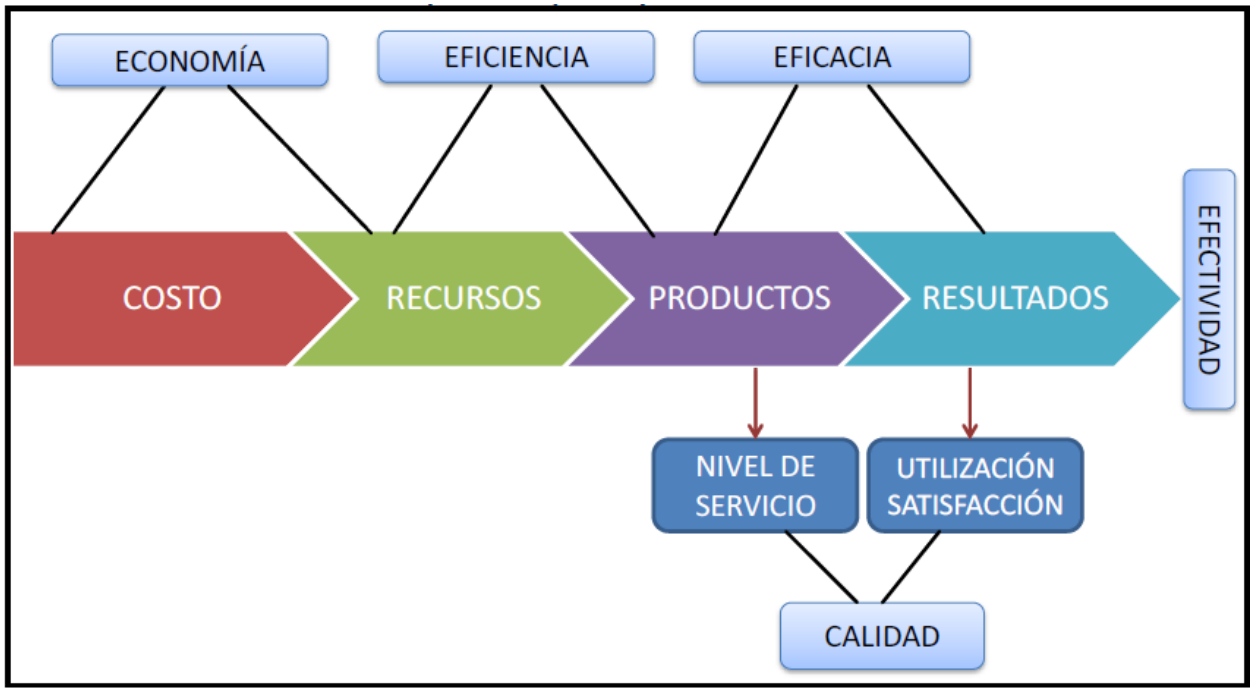

Ilustración 13- Interrelación entre los procesos y los tipos de indicadores. Adaptado de Indicadores de desempeño en el Sector Público. Comisión Económica para América Latina y el Caribe – CEPAL. Santiago de Chile. Noviembre de 2015

Adicionalmente existen cuatro tipos de clasificaciones comunes en la teoría sobre indicadores (según medición, nivel de intervención, jerarquía y calidad). Sin embargo, se debe tener en cuenta que estas clasificaciones no son excluyentes y que en muchos casos se pueden agrupar de formas diferentes dependiendo de las necesidades del proceso estadístico. Como lo explica Vos (1995), "en muchos casos es difícil hacer una distinción muy exacta y rígida entre los diferentes

tipos de indicadores, y es preferible interpretarlos como una cadena de indicadores que permitan relacionar ‘insumos’ con ‘resultados’ en términos de los objetivos inmediatos de los programas y proyectos y con los ‘efectos últimos’ en términos del impacto sobre un conjunto más amplio de objetivos en el desarrollo” (DANE).

5.6.3. Indicador de Eficacia

Mide el desempeño de las entidades para alcanzar los planes propuestos para el desarrollo de la entidad. A mayor grado de cumplimiento en las metas trazadas mayor será el grado de eficacia. Se hace referencia únicamente a la obtención de resultados y productos, sin tener en cuenta los insumos y los recursos que se requieren.

Permite evaluar si los planes fueron bien planteados, desarrollados, la eficiencia en la aplicación, si los productos resultados del proyecto son los planteados al inicio. Es una medida de la fase de evaluación, que su éxito depende de la buena planificación en los procesos.

El indicador de eficacia busca que se alcancen los planes y programas de la entidad, los cuales son determinados con anterioridad, que evalúa la oportunidad (Cumplimiento de la meta en los

plazos estipulados), al igual que la cantidad (volumen de bienes y servicios generados en el tiempo). La eficacia está asociada a aspectos como:

- **Cobertura:** que hace referencia al grado en que las actividades que se realizan y los productos que las entidades ofrecen cubren la demanda y alcanzan las expectativas de los usuarios.

- **Focalización:** se relaciona con el nivel de precisión con que los servicios que entrega la entidad a los usuarios que se benefician de ellos. Se puede determinar mediante una evaluación para validar si los usuarios objetivos del programa se están beneficiando o si quienes están sacando beneficio son otras personas.

- **Capacidad de cubrir la demanda**: Se evalúa si la entidad cuenta con lo necesario para absorber de manera adecuada los niveles de la demanda de cada uno de los servicios que ofrecen, con las condiciones de calidad y en el tiempo adecuado.

- **Resultado Final**: Comprar los resultados obtenidos, no solamente hace referencia a alcanzar los objetivos planteados al inicio del proyecto, se debe enfocar en la posibilidad

de superarlo o realizar retroalimentaciones satisfactorias para el mejoramiento de los servicios a los usuarios.

5.6.4. Indicador de Eficiencia

La eficacia mide la relación entre los servicios prestados y los recursos o insumos que se utilizan para lograr que el producto final cumpla con las expectativas de los usuarios, aprovechando al máximo los insumos, sin desperdicios, aprovechamiento al máximo.

Los indicadores de eficiencia, se enfocan en el control de los recursos, evaluando la relación entre los recursos y se grado de aprovechamiento. Se basa en un examen de costos en el que incurren las entidades, para alcanzar sus objetivos y resultados.

El análisis de eficiencia se refiere a la adquisición y el aprovechamiento de los insumos, que deben ser adquiridos en tiempo oportuno, al mejor costo posible, en la cantidad adecuada y con calidad óptima, por lo que se incluyen recursos humanos, materiales y financieros.

Cuando las entidades generan productos o servicios incompletos o que no alcanzan a satisfacer las necesidades de los usuarios, se deben enfocar los recursos en la mejora de los esfuerzos de las instituciones para lograr el cumplimiento de las metas y los objetivos trazados.

5.6.5. Indicador de Efectividad

Se mide involucrando la eficiencia y la efectividad, mide el impacto en "el logro de los resultados programados en el tiempo con los costos más razonables posibles" (DANE)

Para el cálculo de la efectividad se debe relacionar con el nivel de satisfacción del usuario, cuáles son sus requerimientos y lo que espera del producto o del servicio en las mejores condiciones costos razonables y la mejor cobertura, es decir no solo importa alcanzar los objetivos, también cobra relevancia en la forma como se logra el impacto que se esperaba.

Indicadores como rendimiento, crecimiento, competitividad, productividad, participación, adaptación y cobertura son considerados como indicadores que miden la efectividad (Metropolitano, 2010).

5.6.6. Indicadores según medición

Indicadores cuantitativos: este tipo de indicadores son una representación numérica de la realidad; su característica más importante es que, al encontrarse valores diferentes, estos pueden ordenarse de forma ascendente o descendente.

Indicadores cualitativos: es otro instrumento que permite tener en cuenta la heterogeneidad, amenazas y oportunidades del entorno organizacional y/o territorial. Además, permiten evaluar, con un enfoque de planeación estratégica, la capacidad de gestión de la dirección y demás niveles de la organización. Su característica principal es que su resultado se refiere a una escala de cualidades. Los indicadores cualitativos pueden expresarse así: - Categóricos: por ejemplo, bueno, aceptable, regular, malo. - Binarios: por ejemplo, sí, no.

- Indicadores según nivel de intervención. Hacen referencia a la cadena lógica de intervención, es decir, a la relación entre los insumos, los resultados y los impactos; tratan de medir en cuánto se acerca a las metas esperadas con los insumos disponibles. Para esto se dispone de cinco tipos de indicadores:

- Indicadores de impacto: se refieren a los efectos, a mediano y largo plazo, que pueden tener uno o más programas en el universo de atención y que repercuten en la sociedad en su conjunto.

- Indicadores de resultado (outcome): se refieren a los efectos de la acción institucional y/o de un programa sobre la sociedad.

- Indicadores de producto (outputs): se refieren a la cantidad y calidad de los bienes y servicios que se generan mediante las actividades de una institución o de un programa.

- Indicadores de proceso: se refieren al seguimiento de la realización de las actividades programadas, respecto a los recursos materiales, personal y/o presupuesto. Este tipo de indicadores describe el esfuerzo administrativo aplicado a los insumos para obtener los bienes y servicios programados.

- Indicadores de insumo: se refiere al seguimiento de todos los recursos disponibles y utilizados en una intervención.

5.6.7. Indicadores según jerarquía

- Indicadores de gestión: este tipo de indicadores también son denominados indicadores internos y su función principal es medir el primer eslabón de la cadena lógica de

intervención, es decir, la relación entre los insumos y los procesos. Aunque este tipo de indicadores se usan cuando se da comienzo al cronograma, se conciben en la etapa de planeación, cuando para cada situación plateada se programan tareas, actividades y recursos físicos, financieros, así como talento humano. Dentro de esta categoría, se tienen en cuenta los indicadores administrativos y operativos, esto es, aquellos que miden el nivel o cantidad de elementos requeridos para la obtención del producto, servicio o resultado.

- Indicadores estratégicos: permiten hacer una evaluación de productos, efectos e impactos, es decir, la forma, método, técnica, propuesta, solución y alternativa son elementos que pertenecen, bajo el criterio de estrategia, a todo el sistema de seguimiento y evaluación. En este sentido, 5. 18 Herramientas estadísticas para una gestión territorial más efectiva Guía para Diseño, Construcción e Interpretación de Indicadores los indicadores estratégicos permiten medir los temas de mayor incidencia e impacto.

5.6.8. Importancia de la medición de procesos

Para el buen funcionamiento de las entidades se han definido procesos específicos, que buscan el mejoramiento continuo. En culturas como la japonesa implementaron métodos de trabajo en equipo y tener la participación de todo el personal para las mejoras a implementar en las empresas, así definieron modelos para realizar retroalimentaciones continuas a sus procesos.

Kaoru Ishikawa propagó por todo el mundo su modelo de Método sistemático o científico de mejora de procesos, basado en el recorrido de una serie de pasos o etapas, desde la detección de un problema o de una posibilidad de mejora (dependiendo de que el motor sea una serie de defectos detectados, o una nueva posibilidad tecnológica u organizativa), pasando por su estudio en busca de sus causas, de posibles perfeccionamientos o soluciones, la elección de la solución o conjunto de soluciones que parecen idó- neas, hasta llegar a su implantación y a la medida de las mejoras conseguidas.

Es necesario tener en cuenta que existe un vínculo entre esta y la planeación estratégica o planeación institucional, toda vez que la medición permite "comparar una magnitud con un patrón preestablecido, lo que permite observar el grado en que se alcanzan las actividades propuestas dentro de un proceso específico" (Departamento Administrativo Nacional de Estadística (DANE), 2014)

Los resultados obtenidos a través de la medición permiten mejorar la planificación, dado que es posible observar hechos en tiempo real, logrando tomar decisiones con mayor certeza y confiabilidad.

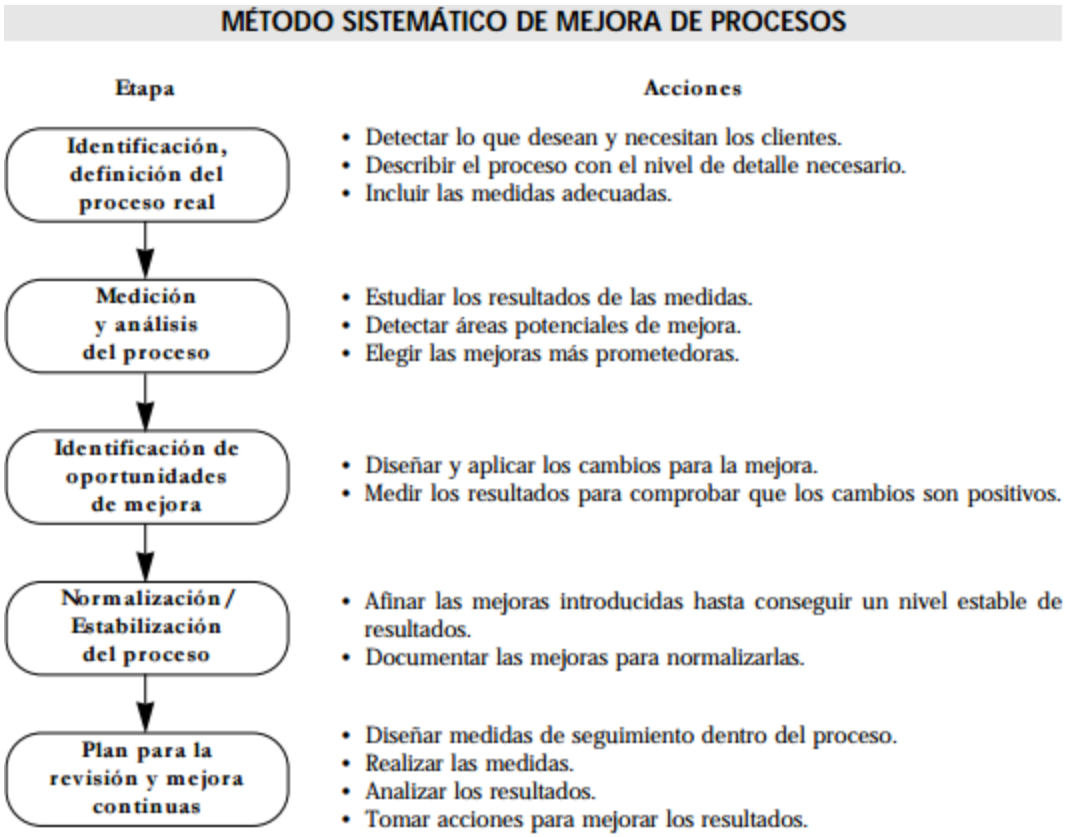

Ilustración 14- Método sistemático de mejora de procesos

Uno de los rasgos característico del Método sistemático de mejora de procesos es su continuo recurso a las medidas, a los datos objetivos, para la detección de los puntos a mejorar, para confirmar el hallazgo de la causa real de los defectos detectados, para corroborar que la solución adoptada es la apropiada y para cuantificar el nivel de mejora alcanzado (ZARATIEGUI, 1999).

Se cuenta con cinco etapas, de la necesidad de verificar muchas de las decisiones tomadas mediante la toma de mediciones y su análisis, de encargar su desarrollo a equipos más o menos estables y de otros detalles secundarios, este método pretende conseguir mejoras apreciables, pero no espectaculares, de forma sostenida a lo largo del tiempo.

La medición con indicadores es un elemento esencial de acuerdo a los parámetros establecidos en las normas internacionales, para identificar los procesos, es una herramienta importante que define objetivos y metas anuales, con las cuales todos los involucrados deben estar familiarizados.

El uso frecuente de indicadores puede ayudar a las entidades a mejorar su rendimiento, aplicar buenas prácticas, asegurar que las entidades identifiquen sus prioridades, las áreas de desempeño más relevantes, y cumplir con los procesos de mejora continua de acuerdo a las necesidad manteniendo alineados las metas de la entidad con la misión y visión de la entidad.

Lo más importante en la medición es que es el lenguaje de los directivos, porque son estas las herramientas gerenciales que buscan medir el desempeño de los productos, el cumplimiento a las metas, las estrategias de mercado, el nivel de ventas y a la investigación y desarrollo de nuevos

productos y/o servicios. No sin antes mencionar que la medición es un arma eficaz contra los reprocesos al igual que cargar con los sobrecostos del servicio postventa, siempre enfocado al control y mejoramiento (BUITRAGO, 2011).

5.7. Ciclo básico de construcción de indicadores (Comisión Económica para América Latina y el Caribe (CEPAL), 2005)

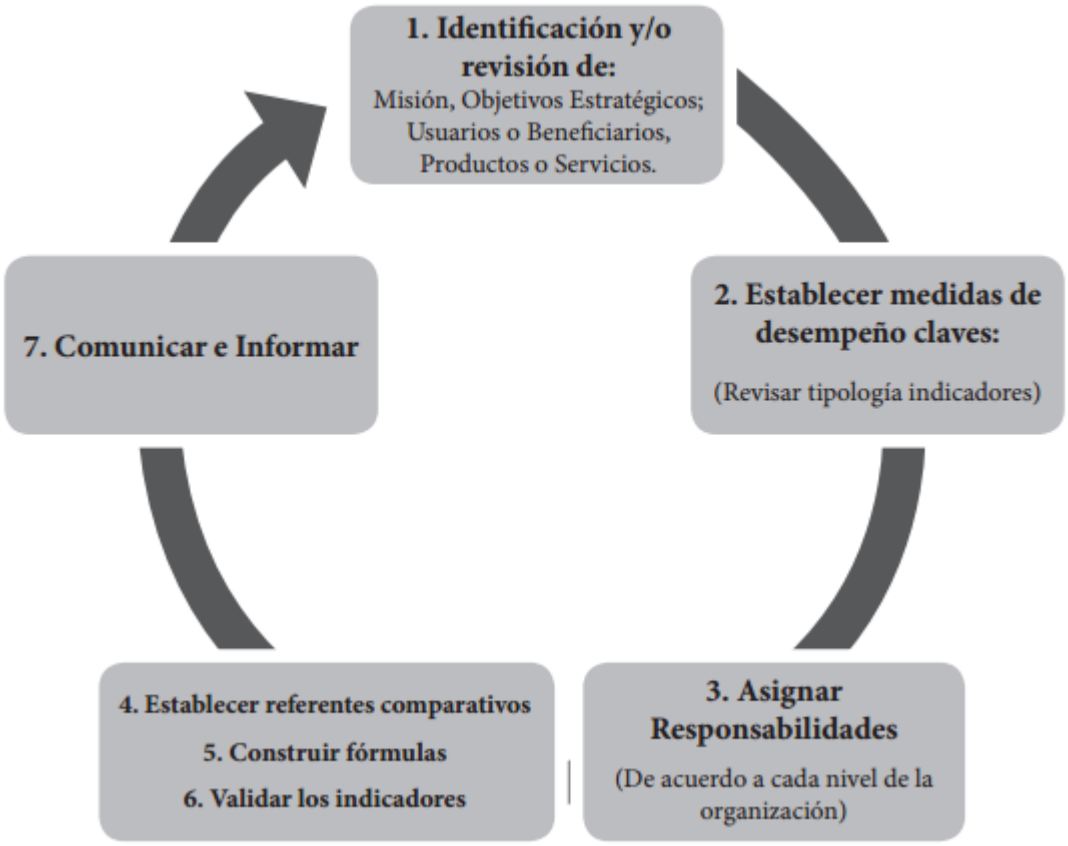

Ilustración 15- Ciclo básico de construcción de indicadores. Fuente: Comisión Económica para América Latina y el Caribe (Cepal)

Para la construcción de indicadores efectivos se deben iniciar por la formulación y claridad en la respuesta de las siguientes preguntas:

- **¿Qué se hace en la entidad?:** Identificar las actividades principales que permiten cumplir con la razón de ser de la entidad.
- **¿Qué se quiere medir?:** Selección de aquellas actividades que se consideren prioritarias. Se puede establecer una valoración y después priorizar las actividades por orden de importancia.
- **¿Quién utilizará la información generada?:** Seleccionar los destinatarios de la información, ya que los indicadores deben definir sustancialmente en función de quién los va a utilizar.
- **¿Frecuencia de medición?** Periodicidad con la que se desea obtener la información. Para definir la periodicidad se debe tener en cuenta la entidad y las personas que van a utilizar la información generada.
- **¿Con que se comparará los resultados obtenidos?:** Establecerse referentes respecto a su estructura, proceso o resultado, que pueden ser tanto internos a la organización, como externos a la misma y que servirán para efectuar comparaciones.

Una vez se tiene respuesta a estas preguntas se procede con los pasos establecidos anteriormente.

1. Identificación y/o Revisión de Productos y Objetivos que serán medidos: Es el paso inicial en el cual se establece la coherencia a de los indicadores que se pretende construir,, su análisis definirá el tipo de medición y los esfuerzos necesarios para obtener la información, pero cómo determinar lo que se considera estratégico para la organización,

2. Establecer medidas de desempeño claves: El número y tipo de indicadores dependerá de los objetivos determinados para la evaluación de las características de la entidad y del nivel de la organización que se pretendan desarrollar.

3. Asignar las responsabilidades: Identificación de lo que se medirá es establecer las responsabilidades institucionales para el cumplimiento en el manejo de la información, tanto para alimentar el indicador como para su análisis y presentación de resultados.

4. Establecer referentes comparativos: El referente comparativo se encuentra asociado al punto 1, en él se establecieron las metas asociadas a los objetivos que se pretenden medir, por lo que un primer referente lo constituye lo planeado por la entidad; sin embargo, también es posible establecer un referente respecto de otras entidades similares o comparables o respecto de datos históricos, todo dependerá de las necesidades planteadas desde los objetivos iniciales.

5. Construir fórmulas: La construcción de la fórmula debe asegurar que su cálculo obtenga información de las variables que se están tratando de medir, es decir el resultado del indicador.

6. Validar Indicadores: permitir asegurar su transparencia y confiabilidad del indicador para que se constituya en una herramienta para la toma de decisiones y la rendición de cuentas. Para poder realizarla a continuación se determina un conjunto de criterios, sobre los cuales se deben examinar los indicadores para analizar su coherencia y la capacidad de cumplir los fines para los cuales fueron construidos.

CRITERIO	DESCRIPCIÓN
Pertinencia	Debe referirse a los procesos y productos esenciales que desarrolla cada institución para reflejar el grado de cumplimiento de sus objetivos institucionales. La medición de todos los productos o actividades que realiza la institución genera una saturación de información, tanto en la organización como fuera de esta.
Relevancia	Asegurarse de que estoy midiendo los objetivos vinculados a lo estratégico. Cuando se trata de organizaciones que tienen más de un producto o servicio, es conveniente desarrollar un conjunto de indicadores globales que represente su accionar estratégico vinculado a su misión.
Homogeneidad	Este criterio implica preguntarse cuál es la unidad de producto (atenciones médicas, asesorías legales, visitas inspectoras, etc.) y, más importante, procurar que dichas unidades de producto sean equivalentes entre sí en términos de los recursos institucionales que consumen (horas hombre, cantidad de insumos materiales, etc.). Si no se da la equivalencia para alcanzar las metas se tenderá a ejecutar solo las acciones que demandan relativamente menos recursos, postergando o anulando las más costosas o complejas, que a menudo son las que tienen un mayor impacto sobre la gestión institucional.

CRITERIO	DESCRIPCIÓN
Independencia	Los indicadores deben responder en lo fundamental a las acciones que desarrolla y controla la institución o a las variables del entorno que se vean afectadas directamente por esas acciones. No puede estar condicionado a factores externos, tales como la situación general del país, la labor legislativa del parlamento o la actividad conexa de terceros (públicos o privados).
Costo	La obtención de la información para la elaboración del indicador debe ser a costos que tengan correlación con los recursos que se invierten en la actividad.
Confiabilidad	Digno de confianza, independiente de quien realice la medición. En principio la base estadística de los indicadores debe estar en condiciones de ser auditada por las autoridades de la institución y examinada por observadores externos.
Simplicidad y Comprehensividad	Existe una tensión entre ambos criterios: se deben cubrir los aspectos más significativos del desempeño, pero la cantidad de indicadores no puede exceder la capacidad de análisis de los usuarios, tanto internos como externos. Los indicadores deben ser de fácil comprensión, libre de complejidades.
Oportunidad	Debe ser generado en el momento oportuno dependiendo del tipo de indicador y de la necesidad de su medición y difusión.
No redundancia	Debe ser único y no repetitivo.

CRITERIO	DESCRIPCIÓN
Focalizado en áreas controlables	Focalizado en áreas susceptibles de corregir en el desempeño de los organismos públicos, generando a la vez responsabilidades directas en los funcionarios y el personal.
Participación	Su elaboración debe involucrar en el proceso a todos los actores relevantes, con el fin de asegurar la legitimidad y reforzar el compromiso con los objetivos e indicadores resultantes. Esto implica además que el indicador y el objetivo que pretende evaluar sea lo más consensual posible dentro de la organización.

Tabla 1- Características de los Indicadores - Fuente: Indicadores de Desempeño en el Sector Público. Comisión Económica para América Latina y el Caribe (CEPAL).

7. Comunicar e Informar: Es importante precisar que los indicadores pueden ser utilizados para diferentes propósitos, dependiendo del objetivo de la evaluación, el ámbito en que se realiza y los usuarios a los que se dirige, por lo que para la comunicación de los resultados es necesario tener en cuenta que los indicadores “no siempre podrán dar cuenta en forma integral del desempeño institucional, requiriéndose de otros antecedentes complementarios para esto, lo que refuerza un uso prudente de esta información” (Comisión Económica para América Latina y el Caribe (CEPAL), 2005), razón por la cual se hace necesario trabajar baterías de indicadores, que permitan desde diferentes puntos de vista realizar el análisis de la situación y las medidas correctivas de ser necesario.

Así mismo es necesario enfocar la comunicación de acuerdo a los interesados, si los resultados están orientados a la rendición de cuentas a la ciudadanía, su presentación exige en lo posible un componente educativo, un lenguaje sencillo y entendible, para que puedan cumplirse con las expectativas de dichos usuarios frente a la información suministrada.

Por su parte, los informes para la Alta Dirección o Gerencia, requiere una periodicidad frente a la presentación de informes, de modo tal que pueda dar una línea base para el análisis o una continuidad de los procesos para efectos de una acertada toma de decisiones.

5.8. **Como interpretar un indicador**

Una vez se lleve a cabo la evaluación del indicador es fundamental relacionar dicho resultado con la tendencia histórica que se presenta, como parámetro para la toma de decisiones y generación de acciones de tipo preventivo o correctivo según sea el caso. El análisis de la tendencia se puede clasificar en dos categorías, de la siguiente manera: (Beltran, 2003)

- Tendencia a la maximización: Cuando el indicador tiene un comportamiento creciente, es decir va aumentando a medida que pasa el tiempo. Ejemplo: Indicadores relacionados con productividad, bienestar, percepción del cliente respecto de productos y servicios que se le ofrecen, imagen de la entidad.

- Tendencia a la Minimización: Cuando el valor del indicador muestra un comportamiento que va disminuyendo con el tiempo. Ejemplo: Disminución de quejas y reclamos, disminución en accidentes de trabajo, disminución en pérdidas y desperdicios de insumos o papelería, disminución en consumos de energía, agua u otros servicios.

Estas tendencias deben llevar a preguntarse las razones y circunstancias de por qué se obtuvo ese nivel de resultado y si se encuentra fuera de los límites planteados al inicio de la construcción del indicador. La evaluación que se realiza a partir de los resultados obtenidos, entrega insumos para los siguientes tipos de análisis:

- Revisar las metas que fueron definidas, estableciendo si estas fueron o no realistas.

- Priorizar la asignación de los recursos hacia determinados programas o productos, justificar la asignación de mayores recursos; disminuir o abandonar los programas o la

provisión de determinados bienes y servicios por otras alternativas más eficientes y con el mismo grado de eficacia, son un ejemplo.

No hay una medida única que demuestre por sí sola el desempeño de la institución. En general se requiere una combinación de ellas que permita demostrar la eficacia, eficiencia, calidad, economía con que se llegue a los productos o resultados.

- Las desviaciones entre los productos que se obtienen y los esperados (medidas de cobertura, focalización, capacidad de cubrir la demanda, etc.). A partir de la interpretación de la evaluación del desempeño a nivel de eficacia es importante dar explicaciones por qué se producen las diferencias. Algunas posibles causas pueden ser:

- Se sobre o subestimó la capacidad de proveer los bienes y servicios.
- Hubo una mayor demanda por factores exógenos (capacidad de cubrir la demanda, no en focalización, ni cobertura, dado que previamente se definen los parámetros).

5.9. **Estándares y normas aplicables**

5.9.1. ISO 9001:2008

La norma ISO 9001:2008 es la base del sistema de calidad, es una norma internacional y que se centra en todos los elementos de administración de calidad con los que una empresa debe contar para tener un sistema efectivo que le permita administrar y mejorar la calidad de sus productos o servicios.

Está basada en el entorno de la organización, los cambios y los riesgos asociados, sus necesidades cambiantes, los objetivos, productos, procesos y el tamaño y estructura de la organización.

Maneja el ciclo PHVA (Organización Internacional para la Normalización (ISO), 2008)

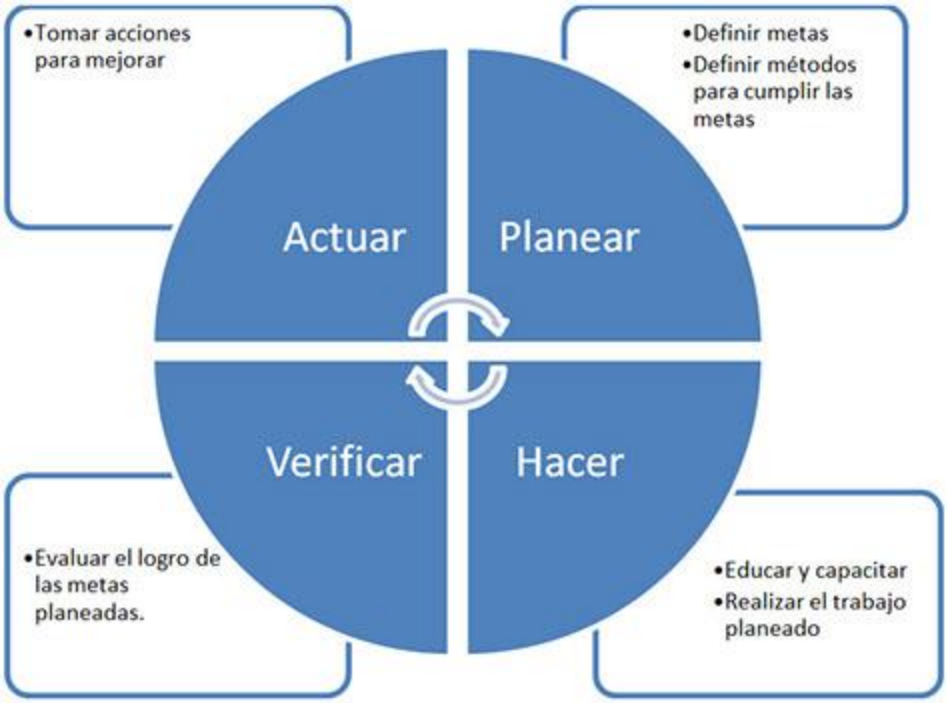

Ilustración 16- Ciclo PHVA

- **Planificar:** Establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos del diente y las políticas de la organización.

- **Hacer:** Implementar los procesos.

- **Verificar**: realzar el seguimiento y la medición de los procesos y los productos respecto a las políticas, los objetivos y los requisitos para el producto, e informar sobra los resultados.

- **Actuar:** tornar acciones para mejorar continuamente el desempeño de 1% procesos.

5.9.2. Sistema de Gestión de la Calidad NTCGP 1000:2004

La norma NTCGP 1000:2004 esta dirigida a todas las entidades y tiene como propósito mejorar su desempeño y su capacidad de proporcionar productos y/o servicios que respondan a las necesidades y expectativas de sus clientes.

La orientación de esta norma promueve la adopción de un enfoque basado en los procesos, el cual consiste en identificar y gestionar, de manera eficaz, numerosas actividades relacionadas entre sí. Una ventaja de este enfoque es el control continuo que proporciona sobre los vínculos entre los procesos individuales que hacen parte de un sistema conformado por procesos, así como sobre su combinación e interacción (Republica Colombiana, 2004).

Esta norma es de aplicación genérica y no es su propósito establecer uniformidad en la estructura y documentación del sistema de gestión de la calidad de las entidades, puesto que reconoce que éstas están influenciadas por diferentes marcos legales, objetivos, estructuras, tamaños, necesidades, procesos y productos y/o servicios que suministran.

Como base para la elaboración de este documento se han empleado las normas internacionales de la serie ISO 9000:2000 sobre gestión de la calidad. En esta medida, la implementación de la presente norma permite el cumplimiento de la norma internacional ISO 9001:2000, puesto que ajusta la terminología y los requisitos de ésta a la aplicación específica en las entidades. Sin embargo, la presente norma integra requisitos y conceptos adicionales a los del estándar ISO. En el Anexo A se presenta una correlación entre los requisitos de esta norma y los de la ISO 9001:2000.

5.9.3. ITIL V3 Mejora Continua

El proceso de Mejora Continua del Servicio está orientado a alinear los servicios de TI de acuerdo las necesidades de las entidades por medio de la identificación e implementación de las mejoras en los servicios. Está orientada a hacer recomendaciones para implementar mejoras, revisar y analizar los resultados de los acuerdos de servicio, identificar e implementar las actividades para perfeccionar los servicios y procesos de TI y por ende mejorar la rentabilidad sin sacrificar a los usuarios (Information Technology Infraestructure Libary, 2011).

La mejora continua se alcanza mediante la monitorización y medición de todas las actividades y procesos en la prestación de los servicios.

- Conformidad: Los procesos se adecuan a los nuevos modelos y protocolos
- Calidad: se cumplen los objetivos preestablecidos en plazo y forma.
- Rendimiento: los procesos son eficientes y rentables para la organización TI.
- Valor: los servicios ofrecen el valor esperado y se diferencian de la competencia.

Los principales objetivos de esta fase son:

- Recomendar mejoras para todos los procesos y actividades involucrados en la gestión y prestación de los servicios de TI.
- Monitorizar y analizar los parámetros de seguimiento de Niveles de Servicio y contrastarlos con los SLAs (Acuerdos de Servicios).
- Proponer mejoras que aumenten el ROI (Retorno de la inversión) y VOI (Valor de la Inversión) asociados a los servicios TI
- Dar soporte a la fase de estrategia y diseño para la definición de nuevos servicios y procesos (actividades asociados a los mismos.

Los resultados de esta fase se ven reflejados en Planes de Mejora del Servicio que incorporen toda la información necesaria.

- Mejorar la calidad de los servicios prestados.
- Incorporar nuevos servicios que se adapten mejor a los requisitos de los clientes y el mercado.
- Mejorar y hacer más eficientes los procesos internos de la organización TI

5.10. **Marco Legal**

Decisión 351 de 1993: está orientada a reconocer una adecuada protección para los autores y sus derechos, la cual aplica a obras en el campo literario, artístico o científico. La duración de la protección no es inferior a la vida del autor y cincuenta años después de su muerte, si el titular de la obra es una persona jurídica, el plazo no será inferior a los 50 años contados a partir de la publicación de la obra. (Comunidad Andina, 1993). Es de aplicación directa y preferente a las leyes internas de cada país miembro (Bolivia, Ecuador, Colombia, Perú).

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

Decreto 1360 de 1989: Reglamenta la inscripción de soporte lógico (software) en "Derecho de Autor & Expresiones Culturales Tradicionales, Ley (N° 23), 1982", mediante la adición de disposiciones y medidas especiales para el Registro Nacional del Derecho de Autor, las sociedades de gestión colectiva de derechos de autor y derechos conexos, sanciones y otros derechos.

Decreto 460 de 1995: Reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito legal.

Decreto 162 de 1996: Por el cual se reglamenta la Decisión Andina 351 de 1993 y la Ley 44 de 1993, en relación con las Sociedades de Gestión Colectiva de Derechos de Autor o de Derechos Conexos

Ley 545 de 1999: Aprueba el tratado de la OMPI – Organización Mundial de Propiedad Intelectual- sobre interpretación o ejecución y fonogramas (WPPT) adoptado en Ginebra el 20 de diciembre de 1996.

Ley 565 de 2000: Aprueba el tratado de la OMPI – Organización Mundial de Propiedad Intelectual- sobre derechos de autor (WCT) adoptado en Ginebra el 20 de diciembre de 1996.

Ley 603 de 2000: Mediante esta Ley se obliga a las empresas a presentar un detallado informe de gestión, en donde se resalte el tipo de software que usa la compañía, con el fin de proteger la propiedad intelectual y evitar el incremento de la piratería.

Decisión 486 de la C.A.N.: Regula el otorgamiento de marcas y patentes y protege los secretos industriales y las denominaciones de origen.

Decreto 2591 de 2000: Reglamenta parcialmente la Decisión 486 de la Comunidad Andina, Diseños Industriales, indicaciones geográficas, información no divulgada como secretos comerciales, marcas y modelos nombres comerciales.

Ley 463 de 1998: Por medio de la cual se aprueba el "Tratado de cooperación en materia de patentes (PCT)".

Ley 178 de 1994: Por medio del cual se aprueba el "Convenio de París para la protección de la propiedad industrial", la cual hace referencia a las patentes de invenciones, los modelos de utilidad, los dibujos o modelos industriales, las marcas de fábrica o de comercio, las marcas de servicio, el nombre comercial, las indicaciones de procedencia, así como la represión de la

competencia desleal.

En el país desde el 21 de abril de 1998 el Ministerio de Transporte, Ministerio de Comercio Exterior, Ministerio de Desarrollo Económico y el Ministerio de Justicia presentaron el proyecto de ley 227 de 1998, el cual fue aprobado, con el cual se buscaba definir y reglamentar el uso del comercio digital, las firmas digitales y el decreto se basó en las siguientes normas:

Decreto 663 De 1993, Artículo 139: Estaba orientado a las corporaciones de ahorro y vivienda, en el cual se autorizó el cobro por uso de transacciones electrónicas.

Decreto 2150 De 1995, Artículo 26: Se habilitó el sistema de trasmisión electrónica de datos, para establecer la comunicación entre los usuarios y la entidad.

Ley 527 Del 18 De Agosto De 1999: En la cual se "define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y el alcance probatorio de los mensajes de datos", con esta ley se comienza a establecer un orden y reglamentaciones para los documentos electrónicos debido a que éstos se convierten en material probatorio por su confiabilidad y rapidez de acceso.

Ley 527 De 1999: Se define y reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y firmas digitales y se establecen las entidades de certificación.

Decreto 1747 De 2000: Reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación y las firmas digitales.

Resolución 26930 De 2000: Fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.

Ley 1341 De 2009: "por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones –TIC- se crea la agencia nacional de espectro y se dictan otras disposiciones"

CONPES 3701 Del 14 De Julio De 2011: busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema. La problemática central se fundamenta en que la capacidad actual del Estado para enfrentar las

amenazas cibernéticas presenta debilidades y no existe una estrategia nacional al respecto. A partir de ello se establecen las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. Para la aplicabilidad de la estrategia se definen recomendaciones específicas a desarrollar por entidades involucradas directa e indirectamente en esta materia. Así lo ha entendido el Gobierno Nacional al incluir este tema en el Plan Nacional de Desarrollo 2010-2014 "Prosperidad para Todos", como parte del Plan Vive Digital. (Social, 2011)

Decreto 2618 Del 2012: Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones.

Decreto 2573 De 2014: conocido como el nuevo Decreto de Gobierno en línea, con el que se busca garantizar al ciudadano la calidad, disponibilidad y seguridad de los trámites con el Estado. Su objeto consiste en definir los lineamientos, instrumentos y plazos de la estrategia Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con fin de contribuir con la construcción de un Estado abierto, más eficiente, y más transparente y más participativo y que preste mejores servicios con la colaboración toda la sociedad.

Ley 1341 De 2009: Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

6. METODOLOGIA

Este proyecto se enfoca en la medición de efectividad del Modelo de Seguridad y Privacidad de la Información, el cual está conformada por 24 guías que suministra el MINTIC para que las entidades de orden nacional y territorial implementen, con el fin de construir un Sistema de Gestión de Seguridad de la Información y generar conciencia colectiva sobre la importancia de clasificar, valorar y asegurar los activos de las diferentes entidades.

La definición del indicador de efectividad en la implementación del Modelo de Seguridad y Privacidad de la Información, se basó en la metodología y buenas prácticas de ITIL versión 3.0 en su proceso de mejora continua, el cual se centra en identificar claramente que vamos a medir; que podemos medir, en términos de datos y origen de los mismos; estrategia de recolección de datos; precisar quién, cómo, cuándo, recopila e integra datos; procesar los datos, definir reportes, frecuencia y exactitud; analizar relaciones, tendencias, avance del plan y acciones correctivas; evaluar y presentar el resumen de la situación, proponer plan de acción e implementar el plan de mejora.

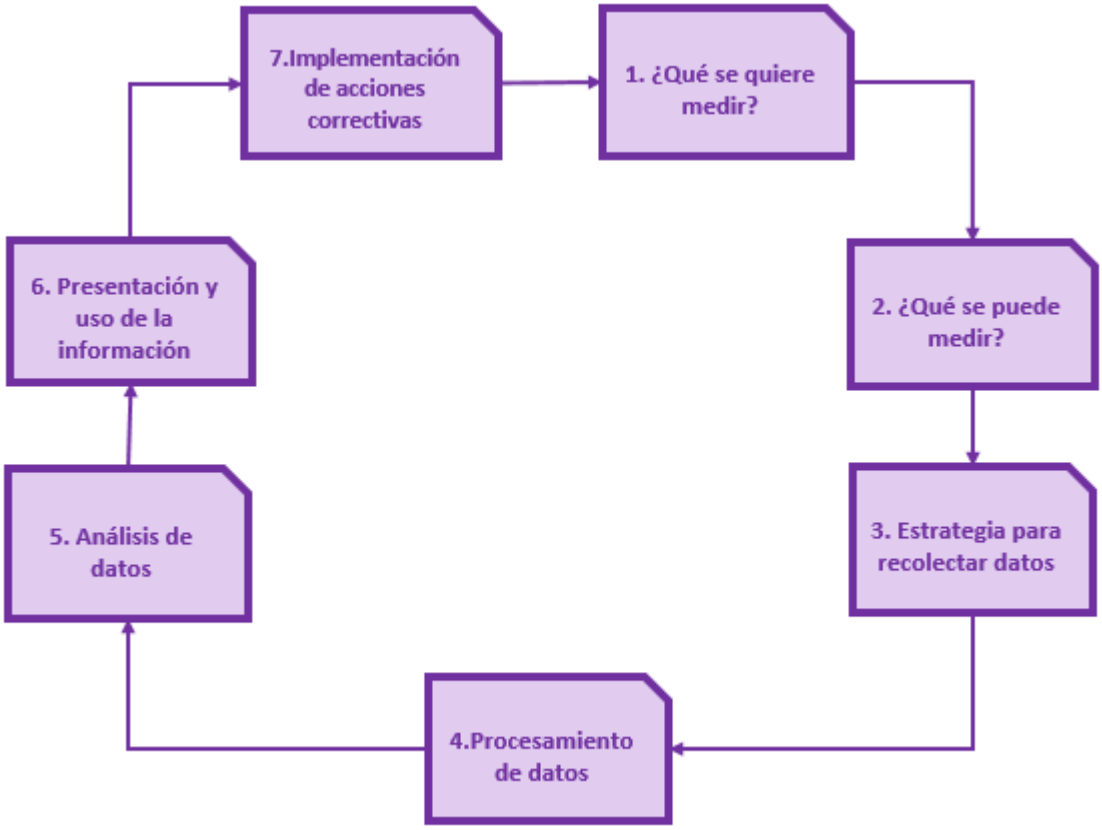

Ilustración 17- Ciclo de metodología para medición de la efectividad

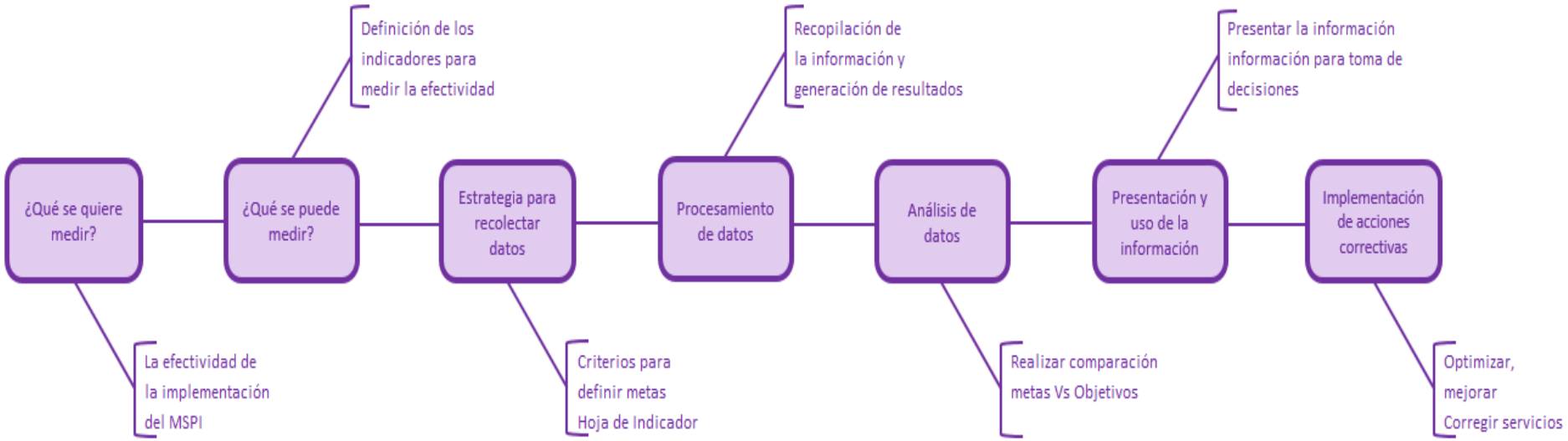

Ilustración 18- Metodología para la medición de la efectividad del MSPI

6.1. **¿QUÉ SE QUIERE MEDIR?**

El Modelo de Seguridad y Privacidad de la Información está compuesto de 24 guías, que son la base para que las Entidades realicen la implementación, es necesario definir cómo se va a medir el grado de efectividad de la implementación del modelo, para lograrlo se debe tener claro lo que se desea medir.

Para alcanzar la una implementación eficiente del Modelo de Seguridad y Privacidad de la Información, se debe cumplir con las metas trazadas para cada una de las entidades, diseñando e implementando los indicadores necesarios, así como realizar las mediciones durante los periodos programados y esta información servirá de base para el cálculo general del indicador de efectividad y evidenciar si se cumplió a cabalidad con la implementación del modelo o cual fue el porcentaje de su implantación o las fallas en el mismo.

La información necesaria en la generación del indicador, se debe saber de dónde o cual es el origen de la información a trabajar, es decir cuál será la entrada en el proceso. Para la medición de la efectividad la fuente de datos principal será la información que se proporcione de los indicadores de cada Entidad.

El presente proyecto realiza un análisis de los factores de efectividad que se pueden medir en las entidades y establece una base para su desarrollo.

6.2. **¿QUÉ PODEMOS MEDIR?**

Para definir el indicador claramente, se debe tener presente que en ocasiones no todo se puede medir, sin embargo se debe tener claro porque es importante la medición que se quiere realizar, se debe realizar un listado de los procesos o herramientas que se pueden medir.

Dentro del Modelo de Seguridad y Privacidad de la Información se tienen definidos diferentes tipos de indicadores que proporcionan la información del estado de la Entidad, si están en cumplimiento del modelo, para la generación del indicador de efectividad, se deberá evaluar si los indicadores ya están definidos y en caso contrario se deben definir nuevos indicadores para la medición correcta.

Para realizar la medición de la efectividad hay unos indicadores de entrada, que sirven como insumo, como son la eficiencia, eficacia, la economía y la calidad.

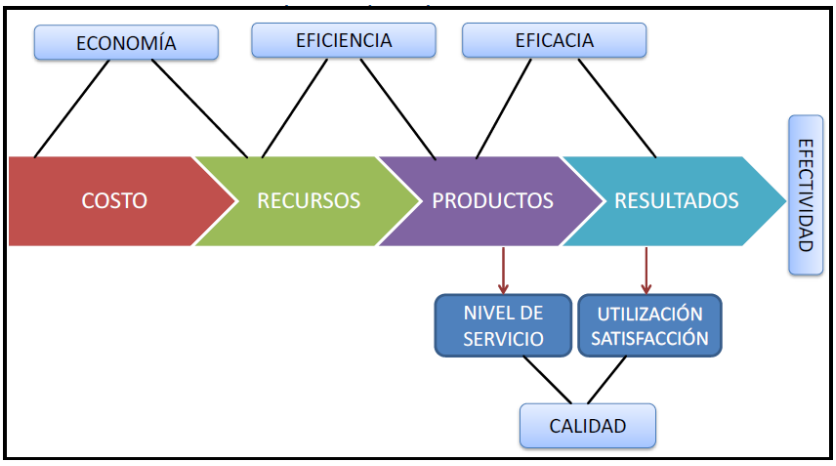

Ilustración 19- Interrelación entre los procesos y los tipos de indicadores. Adaptado de Indicadores de desempeño en el Sector Público. Comisión Económica para América Latina y el Caribe – CEPAL. Santiago de Chile. Noviembre de 2015

6.2.1. Eficacia

Mide el desempeño de las entidades para alcanzar los planes propuestos para el desarrollo de la entidad. A mayor grado de cumplimiento en las metas trazadas mayor será el grado de eficacia. Se hace referencia únicamente a la obtención de resultados y productos, sin tener en cuenta los insumos y los recursos que se requieren.

Permite evaluar si los planes fueron bien planteados, desarrollados, la eficiencia en la aplicación, si los productos resultados del proyecto son los planteados al inicio. Es una medida de la fase de evaluación, que su éxito depende de la buena planificación en los procesos.

El indicador de eficacia busca que se alcancen los planes y programas de la entidad, los cuales son determinados con anterioridad, que evalúa la oportunidad (Cumplimiento de la meta en los plazos estipulados), al igual que la cantidad (volumen de bienes y servicios generados en el tiempo).

La eficacia está asociada a aspectos como:

- **Cobertura:** que hace referencia al grado en que las actividades que se realizan y los productos que las entidades ofrecen cubren la demanda y alcanzan las expectativas de los usuarios.

- **Focalización:** se relaciona con el nivel de precisión con que los servicios que entrega la entidad a los usuarios que se benefician de ellos. Se puede determinar mediante una evaluación para validar si los usuarios objetivos del programa se están beneficiando o si quienes están sacando beneficio son otras personas.

- **Capacidad de cubrir la demanda:** Se evalúa si la entidad cuenta con lo necesario para absorber de manera adecuada los niveles de la demanda de cada uno de los servicios que ofrecen, con las condiciones de calidad y en el tiempo adecuado.

- **Resultado Final:** Comprar los resultados obtenidos, no solamente hace referencia a alcanzar los objetivos planteados al inicio del proyecto, se debe enfocar en la posibilidad de superarlo o realizar retroalimentaciones satisfactorias para el mejoramiento de los servicios a los usuarios.

6.2.2. Eficiencia

La eficiencia mide la relación entre los servicios prestados y los recursos o insumos que se utilizan para lograr que el producto final cumpla con las expectativas de los usuarios, aprovechando al máximo los insumos, sin desperdicios, aprovechamiento al máximo.

Los indicadores de eficiencia, se enfocan en el control de los recursos, evaluando la relación entre los recursos y se grado de aprovechamiento. Se basa en un examen de costos en el que incurren las entidades, para alcanzar sus objetivos y resultados.

El análisis de eficiencia se refiere a la adquisición y el aprovechamiento de los insumos, que deben ser adquiridos en tiempo oportuno, al mejor costo posible, en la cantidad adecuada y con calidad óptima, por lo que se incluyen recursos humanos, materiales y financieros.

Cuando las entidades generan productos o servicios incompletos o que no alcanzan a satisfacer las necesidades de los usuarios, se deben enfocar los recursos en la mejora de los esfuerzos de las instituciones para lograr el cumplimiento de las metas y los objetivos trazados.

6.2.3. Efectividad

Se mide involucrando la eficiencia y la efectividad, mide el impacto en "el logro de los resultados programados en el tiempo con los costos más razonables posibles" (DANE)

Para el cálculo de la efectividad se debe relacionar con el nivel de satisfacción del usuario, cuáles son sus requerimientos y lo que espera del producto o del servicio en las mejores condiciones costos razonables y la mejor cobertura, es decir no solo importa alcanzar los objetivos, también cobra relevancia en la forma como se logra el impacto que se esperaba.

Indicadores como rendimiento, crecimiento, competitividad, productividad, participación, adaptación y cobertura son considerados como indicadores que miden la efectividad (Metropolitano, 2010)

Para realizar la medición de la efectividad se debe tener en cuenta que los indicadores que se seleccionen deben tener fuentes de información que nutran o proporcionen información fácilmente.

6.2.4. Definición de Indicadores

Para el desarrollo del presente proyecto se han elegido 9 indicadores de efectividad, los cuales relacionamos a continuación:

INDICADOR	FORMULA	DESCRIPCIÓN DE LAS VARIABLES	FRECUENCIA
Organización de Seguridad de la Información	(VSI01/VSI02)*100	**VSI01**: Número de personas con su respectivo rol definido según el modelo de operación Capitulo 2 **VSI02:** Número de personas con su respectivo rol definido después de un año.	Trimestral
Cubrimiento del SGSI en Activos de Información	(VSI03/VSI04)*100	**VSI03:** Número de activos críticos de información incluidos en el alcance de implementación del modelo, incluidos en la zona de riesgo inaceptable y la implementación del control no requiere adquisición de elementos de hardware o software. **VSI04:** Número de activos críticos de información incluidos en el alcance de implementación del modelo; activos incluidos en la zona de riesgo inaceptable.	Trimestral

INDICADOR	FORMULA	DESCRIPCIÓN DE LAS VARIABLES	FRECUENCIA
Tratamientos de Eventos Relacionados en el Marco de Seguridad y Privacidad de la Información	(VSI05/VSI06)*100	**VSI05:** Número de anomalías cerradas. **VSI06:** Número total de anomalías encontradas.	Trimestral
Plan de Sensibilización	(VSI07/VSI08)*100	**VSI07:** Número de fallas o no cumplimientos encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema. **VSI08:** Total de personal a capacitar.	Trimestral
Recurrencia de incidentes de seguridad	R= # IR / # IP (((meta-resultado)*(1/meta))+1)	**R:** % de incidentes recurrenes **#IR** : Número incidentes recurrentes **#IP** : Número Incidentes presentados	Mensual
Porcentaje de Implementación de Controles	(VSI32/VSI33)*100	**VSI32:** Número de Controles Implementados. **VSI33:** Número de Controles que se planearon implementar	Trimestral
Efectividad de controles de seguridad implementados	E= Y/X * 100	**E** : Efectividad del control implementado **X** : Número de incidentes previos a la implementación del control **Y**: Númerode incidentes posteriores a la implementación del control	Trimestral
Nivel de satisfacción de usuarios	S=(#US/#UE)*100	**S:** Satisfacción del usuario **#US** : Número de usuarios satisfechos **#UE** : Número de usuarios evaluados	Semestral
Oportunidades de mejora	IC=(#OMI/#TAI)*100	**IC:** Controles implementados **#OMI:** Número de oportunidades de mejora y/o acciones preventivas implementadas **#TAI**: Número total de acciones a implementar	Semestral

Tabla 2 Indicadores definidos

- **Organización de Seguridad de la Información:** Dentro de las funciones de cada una de las entidades es muy importante tener la posibilidad de medir el compromiso de las entidades y la alta dirección se definió un indicador para realizar el seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información.

- **Cubrimiento del SGSI en Activos de Información:** Cada una de las entidades cuenta en su estructura con activos que son críticos para el almacenamiento y el manejo de la información y de los cuales se debe ejercer control para el cumplimiento del marco de seguridad y privacidad de la información.

- **Tratamientos de Eventos Relacionados en el Marco de Seguridad y Privacidad de la Información:** dentro del Modelo de seguridad y privacidad de la información es necesario reflejar la gestión y evolución de los eventos de seguridad y la evolución de los mismos.

- **Porcentaje de Implementación de Controles:** La medición de la implementación del Modelo de seguridad y privacidad de la información hace parte importante del proceso para poner en marcha el modelo en cada una de las entidades.

- **Plan de Sensibilización:** Debido a que el éxito de la implementación del Modelo de Seguridad y Privacidad de la Información radica en la participación de todos los implicados en su desarrollo, se hace necesario que todos sus colaboradores estén ampliamente capacitados en las funciones que cada uno de ellos debe realizar y como su participación es importante; para ello, se debe establecer la efectividad del plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.

- **Recurrencia de incidentes de seguridad:** Una de las funciones del Modelo es la identificación de los incidentes de seguridad que se presentan en las entidades, a las cuales se les da un tratamiento de acuerdo con los procedimientos establecidos, con el fin de que no se vuelvan a presentar; sin embargo, en ocasiones hay incidentes de seguridad, a los cuales los tratamientos no son efectivos y por esta razón se vuelven a presentar. Este indicador nos permitirá identificar el porcentaje de incidentes de seguridad que son reincidentes.

- **Efectividad de controles de seguridad implementados:** El Modelo de Seguridad y Privacidad de la Información, define una serie de controles que las entidades deben implementar para garantizar la correcta implementación. De acuerdo con lo anterior se debe identificar si los controles que se implementan son efectivos para la función que

fueron diseñados; con este indicador se permite medir el grado de efectividad de los controles de seguridad implementados.

- **Nivel de satisfacción de usuarios**: La Estrategia de Gobierno en Línea (GEL) del cual hace parte el Modelo de Seguridad y Privacidad de la Información "busca construir un Estado más eficiente, más transparente y más participativo…Prestará los mejores servicios en línea al ciudadano". De acuerdo con lo anterior es de especial importancia la satisfacción de los usuarios o ciudadanos, por lo tanto este indicador tiene como objetivo medir el porcentaje de satisfacción de los usuarios con el servicio prestado en la entidad.

- **Oportunidades de mejora**: Al realizar la implementación del Modelo, los participantes podrán identificar oportunidades de mejora en los procesos o también identificar acciones correctivas con el fin de evitar la materialización de riegos que no fueron identificados al inicio. El indicador permite que la entidad establezca la presencia de oportunidades de mejora y las acciones correctivas a implementar o que ya fueron implementadas.

6.3. **ESTRATEGIA DE RECOPILACIÓN DE DATOS**

Se debe garantizar que la información que se recopile sea la correcta y la que se necesita para la medición del indicador, sea que esta recopilación de información sea manual o automatizada, con el objeto identificar posibles mejoras y enfocarse en las excepciones.

La recopilación de la información de cada una de las Entidades, se debe realizar mediante el registro de los indicadores en la plantilla diseñada para tal fin, esta plantilla genera un cuadro de mando y dentro de los indicadores de gestión se encuentran los indicadores de efectividad previamente definidos.

6.3.1. Criterios para definir metas

El Modelo de Seguridad y Privacidad de la Información debe ser aplicado a todas las entidades de orden nacional y territorial. Para cumplir con la implementación en todas las

entidades, las metas se deben ajustar a cada una de ellas, debido a que la medición no será igual para una entidad territorial que por ejemplo cuente con 5 empleados, atienda las peticiones de 1000 ciudadanos, a una entidad nacional con 5.000 empleados y que atienda 300.000 ciudadanos.

Se debe realizar una clasificación de las entidades, para definir la meta del cumplimiento de los indicadores. Para realizar la calificación de la entidad se deberá realizar la evaluación de acuerdo a los siguientes criterios:

CRITERIOS DE EVALUACIÓN	CALIFICACION	PUNTOS
Presupuesto en Millones de pesos	0 - 2.999	1
	3.000 - 50.000	2
Existencia y función del área de sistemas	No hay área de sistemas	1
	Soporte básico día a día y de usuario final. Reactiva	2
	Área con funciones definidas, administración de presupuesto y desarrollo de proyectos a futuro. Proactiva	3
Número de PC's	0 - 99	1
	100 - 500	2
	> 500	3
Número de servidores	0 - 3	1
	4 - 20	2
	> 20	3
Existencia y Objeto de la WAN	Internet. Solo correo (externo) y navegación	1
	Internet con servicios públicos ofrecidos	2
	Todo lo anterior más WAN privada	3
Transaccionalidad en la WEB	Solo consulta	1
	Transaccionalidad local (solo datos propios)	2
	Transaccionalidad e interoperabilidad (utiliza datos propios y provee o consulta datos de otras entidades o terceros	3

CRITERIOS DE EVALUACIÓN	CALIFICACION	PUNTOS
Desarrollo de software	No incluye hosting básico de WEB y correo	1
	Aplicativos internos	2
	Aplicativos externos (servicios a terceros) Puede o no incluir desarrollos internos	3
Número de empleados de sistemas	0 - 5	1
	6 - 50	2
	> 50	3

Tabla 3 Criterios de evaluación. Tomado de Anexo 3. Estratificación de entidades

Los resultados de la evaluación se deben interpretar de la siguiente manera:

EVALUACIÓN	SOBRESALIENTE	SATISFACTORIA	MÍNIMA
Las entidades que en su evaluación obtengan un puntaje entre 8 a 12 puntos	≥90% de la meta del período	≥89% y < 80% de la meta del período	<79% de la meta del período
Las entidades que en su evaluación obtengan un puntaje entre 13 a 19 puntos	≥80% de la meta del período	≥79% y < 70% de la meta del período	<69% de la meta del período
Las entidades que en su evaluación obtengan un puntaje entre 20 a 24 puntos	≥70% de la meta del período	≥69% y < 60% de la meta del período	<59% de la meta del período

Tabla 4 Evaluación de resultados

6.3.2. Hoja de Vida del Indicador

Todos los indicadores cuentan con su hoja de vida la cual contiene los siguientes ítems:

- Identificación del indicador que son el código del Indicador, fecha de la última actualización, la versión, página y nombre del indicador.

CÓDIGO		NOMBRE DEL INDICADOR	MinTIC Ministerio de Tecnologías de la Información y las Comunicaciones
FECHA			
VERSIÓN			
PÁGINA			

Ilustración 20- Identificación del indicador

- Los datos del indicador como son el Objetivo, responsable de su diligenciamiento, descripción de las variables a utiliza, la fórmula para su cálculo, origen y la frecuencia.

OBJETIVO		RESPONSABLE	
DESCRIPCIÓN DE VARIABLES		FORMULA	
ORIGEN		FRECUENCIA	

Ilustración 21- Datos del indicador

- Los rangos de gestión o las metas a cumplir. Estas metas se fijan de acuerdo a la definición de metas realizada y es la misma para todos los indicadores de la misma entidad. La medición de las metas se dan en Sobresaliente (cumplimiento total de la meta), Satisfactoria (es un rango cerca a la meta, pero no se ha alcanzado) y Mínima (No ha alcanzado la meta)

Rango de gestión		
SOBRESALIENTE	SATISFACTORIA	MÍNIMA
≥90% de la meta del período	≥80% y <90% de la meta del período	<80% de la meta del período

Ilustración 22- Rangos o metas

- Seguimiento del indicador, es un cuadro en el cual se registrará el comportamiento del indicador de acuerdo a la frecuencia establecida.

MES / AÑO	VSI01	VSI02	INDICADOR	META
ene-16	0	100	0%	80%
feb-16	10	100	10%	80%
mar-16	20	100	20%	80%
abr-16	30	100	30%	80%
may-16	40	100	40%	80%
jun-16	50	100	50%	80%
jul-16	60	100	60%	80%
ago-16	70	100	70%	80%
sep-16	80	100	80%	80%
oct-16	90	100	90%	80%
nov-16	100	100	100%	80%
dic-16	110	100	110%	80%

Ilustración 23- Registro de indicador

- Grafica del comportamiento del indicador, y la tendencia del mismo de acuerdo a la meta.

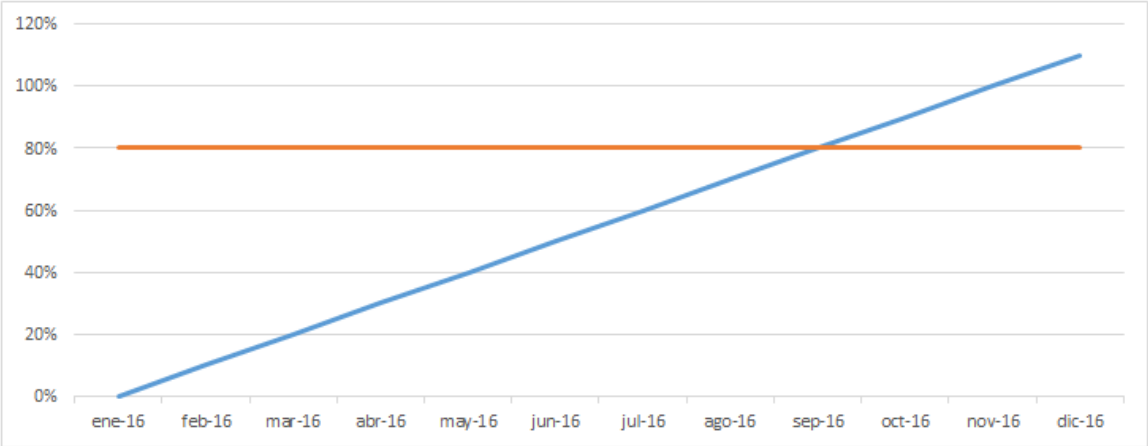

Ilustración 24- Gráfica de comportamiento con tendencia

- Análisis de resultados del periodo, en donde el encargado de diligenciar los indicadores deberá registrar los motivos por los cuales se no se alcanzó la meta, factores críticos a tener en cuenta.

MES / AÑO	ANÁLISIS DE RESULTADOS DEL PERIODO
ene-16	
feb-16	
mar-16	
abr-16	
may-16	
jun-16	
jul-16	
ago-16	
sep-16	
oct-16	
nov-16	
dic-16	

Ilustración 25- Análisis de resultados

- De acuerdo a los resultados del indicador para cada periodo se deberán tomar acciones correctivas, se les debe asignar un responsable, una fecha de ejecución, si el no cumplimiento de la meta es repetitivo se puede generar una acción correctiva o una acción preventiva y finalmente tiene un campo para los seguimiento.

MES / AÑO	ACCIONES A TOMAR	RESPONSABLE	FECHA	AC / AP	SEGUIMIENTO
ene-16					
feb-16					
mar-16					
abr-16					
may-16					
jun-16					
jul-16					
ago-16					
sep-16					
oct-16					
nov-16					
dic-16					

Ilustración 26- Acciones a tomar

6.4. **PROCESAMIENTO DE LOS DATOS**

Para realizar el procesamiento de los datos, se hace entrega de una herramienta en Excel, la cual realizara las siguientes funciones:

- Centralizador de datos de los indicadores, ya que en esta herramienta se registrarán los resultados de los indicadores de efectividad previamente definidos, con la frecuencia establecida para cada uno de ellos.

- Cuadro de Mando, con el cual los directivos de la entidad podrán monitorear de manera fácil los avances en la implementación del Modelo.

Una vez el personal encargado del diligenciamiento de los indicadores, dentro de los tiempos establecidos, el Director de TI de la entidad, realizará la revisión del cuadro de mando integral, el

cual reposara en la red de la entidad en la ruta seleccionada previamente definida. Se debe tener en cuenta que solo deberán tener acceso a la herramienta las personas previamente definidas y que en realidad necesiten el acceso, ya que la información es de carácter confidencial.

6.4.1. Cuadro de Mando Integral

Es un cuadro gerencial, en el cual se presenta resumen de cada uno de los indicadores que permite medir y evaluar los resultados, adicional a los datos de descripción de los indicadores, presenta el resultado equivalente a cada uno de los meses por cada indicador, el consolidado anual y el puntaje de cumplimiento.

CÓDIGO	TABMANDO	TABLERO DE MANDO	MinTIC Ministerio de Tecnologías de la Información y las Comunicaciones
FECHA	01/09/2016		
VERSIÓN	1		

INICIO — ANÁLISIS DE INDICADORES

No.	CÓDIGO DEL INDICADOR	INDICADOR	FÓRMULA	FRECUENCIA	META	MIN	mar-16	jun-16	sep-16	dic-16	PROMEDIO ANUAL	PUNTAJE DE EFECTIVIDAD
1	SGIN01	ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN	0S=(VSI01/VSI02)*100	TRIMESTRAL	80%	70%	90%	90%	90%	59%	82,25%	1
2	SGIN02	CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.	CA=(VSI03/VSI04)*100	TRIMESTRAL	80%	70%	70%	75%	85%	70%	75,00%	0,5
3	SGIN03	TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	TE=(VSI05/VSI06)*100	TRIMESTRAL	80%	70%	70%	69%	50%	59%	62,00%	0
PUNTAJE INDICADOR GENERAL DE EFECTIVIDAD												1,5
% DE CUMPLIMIENTO DEL INDICADOR GENERAL DE EFECTIVIDAD												17%

Ilustración 27- Cuadro de Mando

7. MODELO DE MEDICION DEL INDICADOR DE EFECTIVIDAD DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSION 3.0.2

El Puntaje de Cumplimiento para cada indicador, de acuerdo al porcentaje acumulado del año.

De acuerdo a los rangos de gestión que se definieron se utilizará el siguiente puntaje:

RANGO DE GESTIÓN	% DE CUMPLIMIENTO AÑO	PUNTAJE
SOBRESALIENTE	≥90% de la meta del período	1
SATISFACTORIA	≥80% y <90% de la meta del período	0,5
MINIMA	<80% de la meta del período	0

Tabla 5- Rangos de evaluación

Las metas de los indicadores son las mismas definidas para la entidad en Primer módulo Definición de metas.

El indicador de Efectividad se mide con los siguientes parámetros:

- Por cada uno de los indicadores se genera un puntaje que puede ser 0, 0,5 o 1.
- Se asigna 0 si el promedio anual del indicador está dentro de la meta mínima, es decir su color es Rojo
- Se asigna 0,5 si el promedio anual del indicador está dentro de la meta Satisfactoria, es decir es de color Amarillo.
- Se asigna 1 si el promedio anual del indicador está dentro de la meta Sobresaliente, es decir es de color Verde.
- Una vez todos los indicadores tienen calificación, la sumatoria de estos puntajes es la nota final de Puntaje del Indicador de Efectividad.
- El porcentaje de cumplimiento del Indicador General de Efectividad se calcula dividiendo el Puntaje del Indicador de Efectividad entre el puntaje objetivo.
- El puntaje objetivo corresponde a la sumatoria del mayor puntaje que podría tener cada uno de los indicadores, es decir si se tienen 9 indicadores el puntaje objetivo sería 9 puntos.

7.1. **ANÁLISIS**

Cuando el usuario ingresa por el botón de Análisis, encuentra:

El gráfico de los promedios anuales por cada uno de los indicadores.

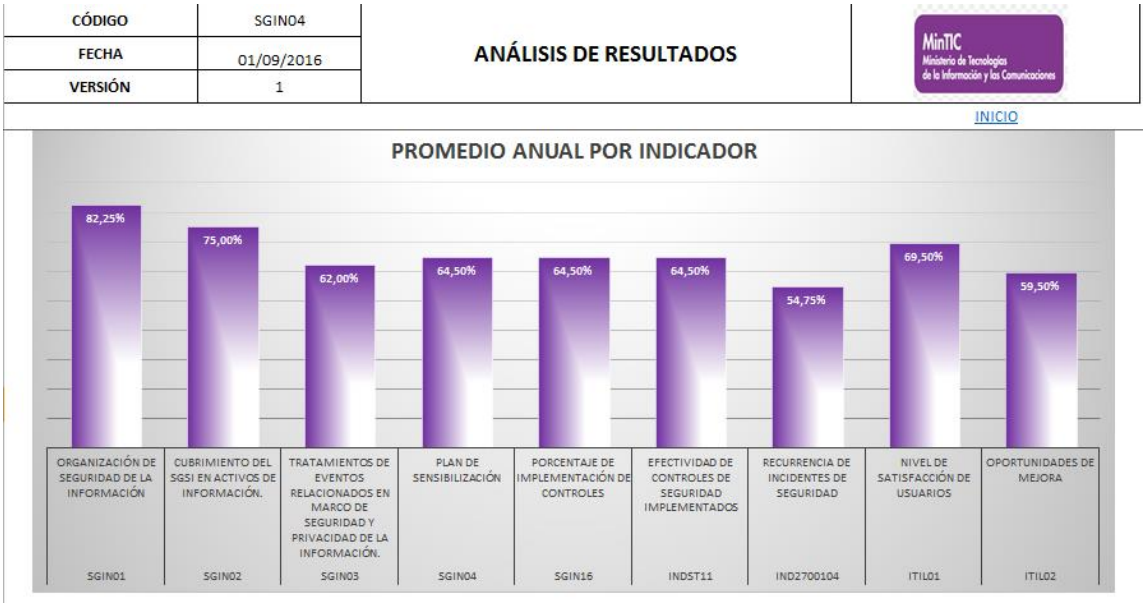

Ilustración 28- Promedio anual por indicador

El gráfico del porcentaje de cumplimiento del indicador General de Efectividad.

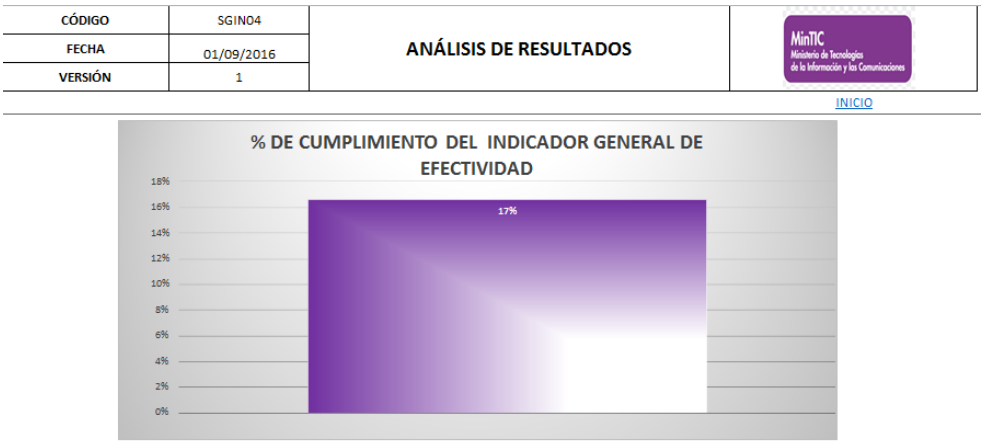

Ilustración 29- % de cumplimiento del indicador general de efectividad

Se encuentra Observaciones a tener en cuenta para la implementación o mejora del indicador. Para cada uno de los indicadores de acuerdo a la nota obtenida se da una observación para mejora para el indicador.

CÓDIGO	SGIN04	ANÁLISIS DE RESULTADOS	MinTIC Ministerio de Tecnologías de la Información y las Comunicaciones
FECHA	01/09/2016		
VERSIÓN	1		

INICIO

OBSERVACIONES A TENER EN CUENTA

INDICADOR SGIN01 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN NOTA 1
Descripción de políticas y estandares
INDICADOR SGIN02 CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN. NOTA 0,5
Definir listado de activos
INDICADOR SGIN03 TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. NOTA 0
No se cuenta con un modelo para el tratamiento de eventos
INDICADOR SGIN04 PLAN DE SENSIBILIZACIÓN NOTA 0
No cuentan con un plan de sensibilización, por lo tanto es importante que se genere diseñe un plan la para la implementación así
INDICADOR SGIN16 PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES NOTA 0
No se cuenta con controles de seguridad implementados
INDICADOR INDST11 EFECTIVIDAD DE CONTROLES DE SEGURIDAD IMPLEMENTADOS NOTA 0
No se cuenta con controles de seguridad

Ilustración 30- Observaciones por indicador

8. CONCLUSIONES

- El proyecto permitió profundizar en la implementación y manejo de indicadores para el uso fácil y continuo de metodologías y estándares internacionales que puedan ser aplicados en el Modelo de Seguridad y Privacidad de la Información que el gobierno está implementando.

- Entender y evidenciar la relación que existe entre la capacidad de los procesos y los indicadores de las entidades de acuerdo a las mediciones establecidas en el Modelo de Seguridad y Privacidad de la información.

- El desarrollo de la Herramienta para la Medición de la Efectividad de los Indicadores del Modelo de Seguridad y Privacidad de la Información proporciona una guía fácil de usar en cada una de las entidades al momento de realizar seguimiento a los indicadores definidos.

- Generar retroalimentación directa a las entidades sobre cada uno de los indicadores que se evalúan en la Herramienta para la Medición de la Efectividad de los Indicadores del

Modelo de Seguridad y Privacidad de la Información, teniendo en cuenta que la herramienta podrá ser usada con la periodicidad requerida por la entidad, con el fin de evaluar e identificar los avances que ha logrado la entidad.

- Abre la puerta para identificar nuevos indicadores para medir la efectividad en caso de ser requeridos.

- La implementación y el uso de la Herramienta para la Medición de la Efectividad de los Indicadores del Modelo de Seguridad y Privacidad de la Información permitirá a las entidades identificar fallas en la implementación y gestión de cada entidad que les impiden lograr sus objetivos de transparencia, eficiencia y participación.

- Generar participación de todas las áreas de la entidad involucrando a la alta dirección, con el objeto de lograr el cumplimiento de las metas conjuntas de la entidad y en la aplicación de los controles de forma general.

9. RECOMENDACIONES

- Motivar a la utilización de la Herramienta para la Medición de la Efectividad de los Indicadores del Modelo de Seguridad y Privacidad de la Información a las entidades del estado colombiano.

- Involucrar de manera activa a la alta gerencia en el uso de la de la Herramienta para la Medición de la Efectividad de los Indicadores del Modelo de Seguridad y Privacidad de la Información, buscando que la utilización sea participativa y constante, con el fin de generar retroalimentaciones de los indicadores con la periodicidad establecida.

- Realizar seguimiento continuo al uso e implementación de la de la Herramienta para la Medición de la Efectividad de los Indicadores del Modelo de Seguridad y Privacidad de la Información en las entidades, con el fin de lograr que se alcance la efectividad del modelo.

- En caso de que se requiera una actualización o adición de un nuevo indicador que sea incluido dentro de la Herramienta para la Medición de la Efectividad de los Indicadores del Modelo de Seguridad y Privacidad de la Información.

- Implementar la Herramienta para la Medición de la Efectividad de los Indicadores del Modelo de Seguridad y Privacidad de la Información en un formato web para que esté disponible y al alcance de todos los usuarios y se generen resultados inmediatos y sean centralizados para su análisis.

10. TABLA DE ILUSTRACIONES

11. TABLA DE ILUSTRACIONES

12. BIBLIOGRAFÍA

Comisión Económica para América Latina y el Caribe (CEPAL). (2005). *Indicadores de Desempeño en el Sector Público.* Santiago de Chile.

Comisión Económica para América Latina y el Caribe (CEPAL). (2005). *Adaptado de Indicadores de Desempeño en el Sector Público.* Santiago de Chile.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Diseño y Especificación del Marco de Referencia. - Diseño Detallado. Marco de Referencia de Arquitectura Empresarial. Bogotá, Cundinamarca, Colombia.

Bank, I.-A. D. (2003). *Gestion Efectiva De Emprendimientos Sociales.*

Beltran, J. M. (2003). *Indicadores de gestión. Herramientas para lograr la competitividad.* 3R Editores.

BUITRAGO, H. E. (2011). La Importancia De La Medición, El Análisis Y La Mejora En Un Sistema De Gestión De La Calidad En Una Empresa De Logística, De Acuerdo A Los Parámetros De La Norma Internacional ISO 90001:2008. Bogotá.

Comunicaciones, M. -M. (s.f.). *Estrategia de Gobierno en Línea.*

Comunidad Andina. (17 de Diciembre de 1993). *Comunidad Andina*. Recuperado el 10 de Julio de 2015, de http://www.comunidadandina.org/Seccion.aspx?id=83&tipo=TE&title=propiedad-intelectual

DANE, D. A. (s.f.). Guía para diseño, construcción e interpretación de indicadores.

Departamento Administrativo Nacional de Estadística (DANE). (2014). Guía para diseño, construcción e interpretación de indicadore.

DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADISTICAS - DANE. (s.f.). *Guía para Diseño, Contrucción e Interpretación de Indicadores.*

Gobierno Colombiano. (2015). *Mintic.* Recuperado el 05 de 11 de 2015, de http://micrositios.mintic.gov.co/vivedigital/2014-2018/

Information Technology Infraestructure Libary. (2011). *Service Improvement.*

Matiz, D. A. (2014). TEORÍA DE INDICADORES DE GESTIÓN Y SU APLICACIÓN.

Metropolitano, I. T. (2010). Manual de indicadores.

Ministerio de Tecnologías de la Información . (25 de 05 de 2015). Guía No. 12 Guía de Indicadores de Gestión para la Seguridad de la Información. Bogotá, Cundinamarca, Colombia.

Ministerio de Tecnologías de la Información y las Comunicaciones . (29 de 07 de 2016). *http://www.mintic.gov.co/.* Recuperado el 10 de 08 de 2016, de http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (29 de 07 de 2016). Modelo de Seguridad y Privacidad de la Información. Bogotá, Cundinamarca, Colombia.

Organización Internacional para la Normalización (ISO). (2008). Norma Internacional ISO 9001.

Republica Colombiana. (2004). NORMA TÉCNICA DE CALIDAD EN LA GESTIÓN PUBLICA NTCGP 1000:2004.

Social, C. N. (2011). Documento Conpes 3701. Bogota.

Unión temporal Everis / Tecnocom. (2014). Diseño y Especificación del Marco de Referencia de Arquitectura Empresarial para el País.

Velázquez, J. I. (03 de 02 de 2014). *Sabere & Ciencias.* Recuperado el 10 de 08 de 2016, de http://saberesyciencias.com.mx/2014/02/03/origen-evolucion-y-sistemas-para-el-monitoreo-de-la-seguridad-cibernetica/

ZARATIEGUI, J. R. (1999). La gestión por procesos: su papel e importancia en la empresa. *Economía Industrial*, 300.

13. ANEXOS

- Guía de medición de Efectividad
- Herramienta para la medición de la efectividad de los indicadores de gestión del Modelo de Seguridad y Privacidad de la Información.