Fondo de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea

MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA 2.0

Coordinación de Investigación, Políticas y Evaluación
Programa Agenda de Conectividad
Estrategia de Gobierno en línea

Bogotá, D.C., Diciembre de 2011

FORMATO PRELIMINAR AL DOCUMENTO

Título:	Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea 2.0				
Fecha elaboración aaaa-mm-dd:	2011-12-07				
Sumario:	El documento presenta una estrategia de preparación por parte del Gobierno para soportar al Sistema de Administración de Seguridad de la Información de Gobierno en Línea (SASIGEL) como modelo sostenible, y cubre desde la preparación de la entidad para comenzar la implementación del Modelo, la definición de las brechas, la alineación y la implementación del SGSI como modelo sostenible.				
Palabras Claves:	Modelo Seguridad PHVA SASIGEL SGSI (Sistema de Gestión de la Seguridad de la Información)				
Formato:	DOC		Lenguaje:		Español
Dependencia:	Ministerio de Tecnologías de la información y las Comunicaciones: Programa Agenda de Conectividad – Estrategia Gobierno en línea – Coordinación de Investigación, Políticas y Evaluación.				
Código:	N/A	Versión:	2.0.2	Estado:	Aprobado
Categoría:	Documento técnico				
Autor (es):	Centro de Investigación de Telecomunicaciones - CINTEL		Firmas:		
Revisó:	Julio César Mancipe Caicedo Líder de seguridad Estrategia de Gobierno en línea				
Aprobó:	Ana Carolina Rodríguez Rivero Coordinadora Coordinación de Investigación, Políticas y Evaluación Estrategia de Gobierno en línea				
Información Adicional:					
Ubicación:					

CONTROL DE CAMBIOS

VERSIÓN	FECHA	No. SOLICITUD	RESPONSABLE	DESCRIPCIÓN
1.0.0	08/08/2010		Equipo del proyecto	Versión inicial del documento
2.0.0	30/09/2011		Equipo del proyecto	Restructuración del modelo
2.0.1	30/11/2011		Equipo del proyecto	Restructuración del modelo
2.0.2	07/12/2011		Equipo del proyecto	Versión aprobada

TABLA DE CONTENIDO

TABLA DE ANEXOS

DERECHOS DE AUTOR

1. AUDIENCIA

Entidades públicas del orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno en línea y terceros que deseen adoptar el Modelo de Seguridad de la Información en el marco de la Estrategia Gobierno en línea.

2. INTRODUCCIÓN

Teniendo en cuenta lo establecido en el Plan Vive Digital, liderado por el Ministerio de las Tecnologías de la Información y las Comunicaciones, en cuanto a la infraestructura, los servicios, las aplicaciones y los usuarios en el marco de un ecosistema digital; las recomendaciones brindadas en el Plan Nacional de Desarrollo 2010-2014 en cuanto a la necesidad de reconocer la seguridad informática como un factor primordial para la apropiación de las TIC; la constante evolución de los mercados; y la dinámica de las entidades, se plantea un marco de seguridad de la información para la prestación de servicios a los ciudadanos a través de las tecnologías de la información, el cual deberá ser respaldado por una gestión, unas políticas y unos procedimientos adecuados, que resalten el papel de las personas como el primer eslabón de una compleja cadena de responsabilidades y que esté orientado a preservar los pilares fundamentales de la seguridad de la información:

- **CONFIDENCIALIDAD:** la información debe ser accesible sólo a aquellas personas autorizadas.
- **INTEGRIDAD:** la información y sus métodos de procesamiento deben ser completos y exactos.
- **DISPONIBILIDAD:** la información y los servicios debe estar disponible cuando se le requiera.

Para lograr estos objetivos, es fundamental contar con el acuerdo y compromiso de todos los involucrados, un respaldo de los niveles directivos dentro de la entidad y ser conscientes de los beneficios que se pueden obtener con una cultura enfocada a la seguridad, pero también del impacto que se puede afrontar por la materialización de riesgos que no se controlan y que se asocian al tema de seguridad de la información.

El Modelo de Seguridad de la Información reúne el conjunto de Lineamientos, Políticas, Normas, Procesos e Instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación de la Estrategia de Gobierno en Línea definida en manual GEL 3.0. El modelo está gestionado por el Sistema de Administración de Seguridad de la Información de Gobierno en línea (SASIGEL), y el modelo es implementado en un sistema de gestión de seguridad de la información en cada entidad.

El presente documento y modelo se estructura de la siguiente manera:

En el capítulo tres (3), se presenta la alineación del Modelo de seguridad de la Información con la arquitectura empresarial de la Estrategia de Gobierno en línea. En el capítulo cuatro (4), se presenta una estrategia de preparación por parte del gobierno central para soportar al Sistema de Administración de Seguridad de la Información de Gobierno en línea (SASIGEL) como modelo sostenible. Posteriormente, en el capítulo cinco (5), se cubre la preparación de la entidad para comenzar la implementación del Modelo, la definición de las brechas, la alineación y la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) como modelo sostenible.

3. VISIÓN ESTRATÉGICA

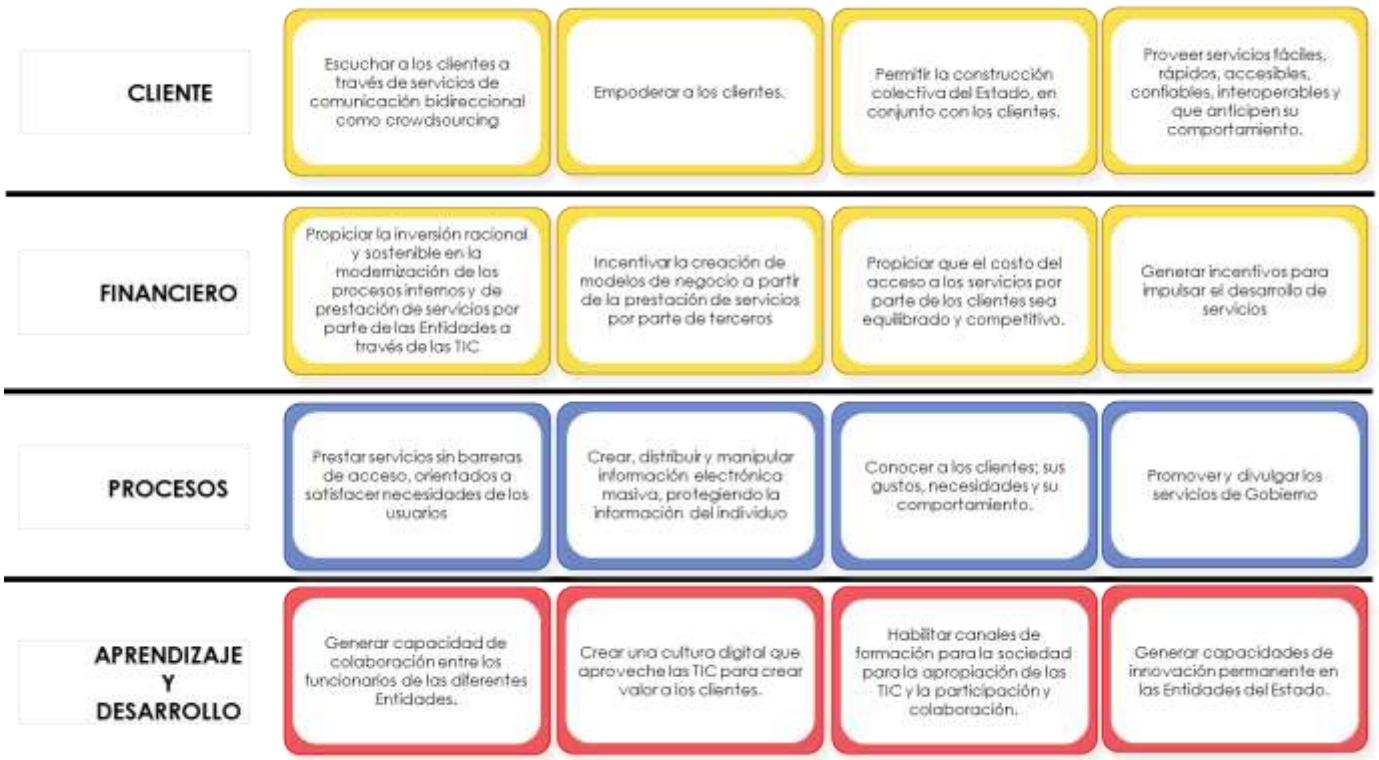
La estrategia de Gobierno en línea contribuye con la construcción de un Estado más eficiente, más transparente y participativo y que presta mejores servicios con la colaboración de toda la sociedad, mediante el aprovechamiento de las TIC. Lo anterior, con el fin de impulsar la competitividad y el mejoramiento de la calidad de vida para la prosperidad de todos los colombianos.

Para lograr esta visión, se han adoptado los siguientes objetivos:

- Facilitar la eficiencia y colaboración en y entre las entidades del Estado, así como con la sociedad en su conjunto
- Fortalecer las condiciones para el incremento de la competitividad y el mejoramiento de la calidad de vida
- Contribuir al incremento de la transparencia en la gestión pública
- Promover la participación ciudadana haciendo uso de los medios electrónicos

En el marco de las investigaciones que adelanta CINTEL, y con el fin de satisfacer los objetivos planteados por la Estrategia de Gobierno en línea, se han establecido los siguientes elementos estratégicos, que se han organizado desde las dimensiones Cliente, Financiera, Procesos y de Aprendizaje y Desarrollo:

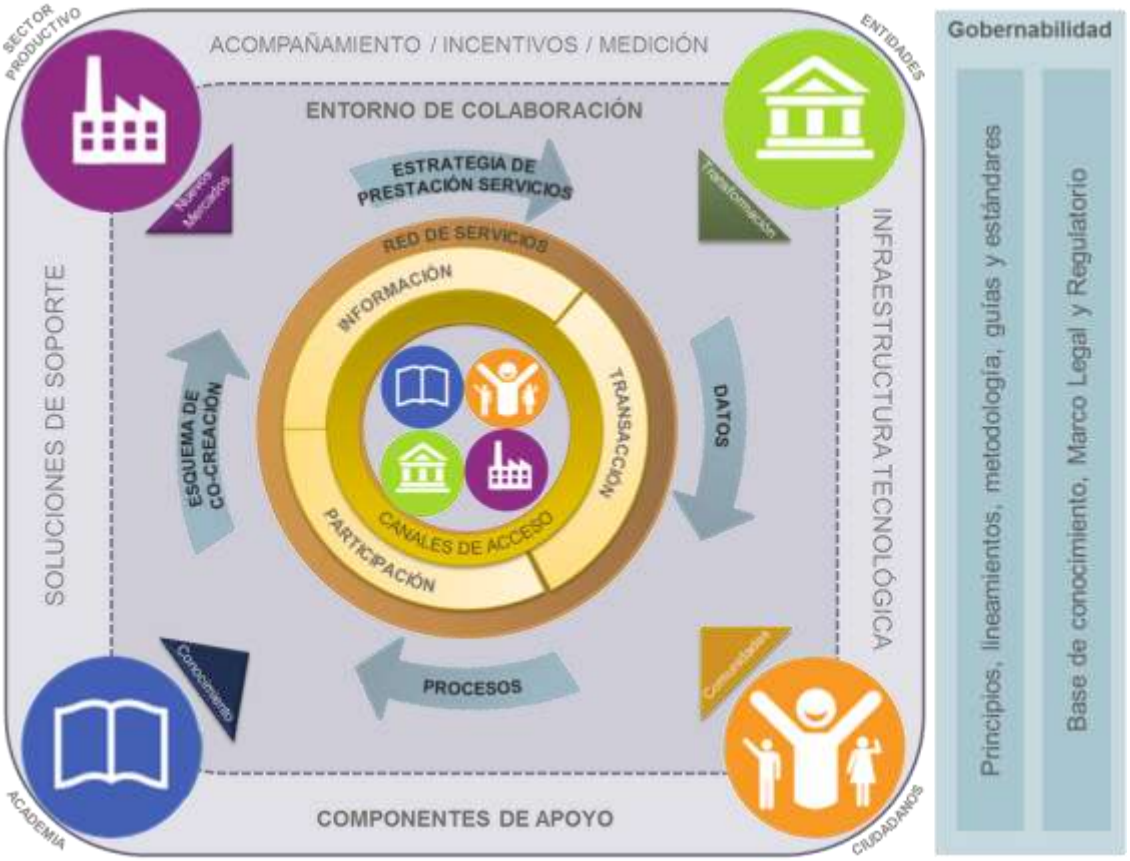
Figura 1 - Mapa estratégico para las investigaciones de Gobierno en línea



1. En la perspectiva Cliente, para satisfacer las necesidades de los clientes del Gobierno en línea es necesario considerar elementos como:
    a. Escuchar a los clientes a través de mecanismos de comunicación bidireccional, es decir entre las entidades y los clientes (*crowdsourcing*).
    b. Empoderar a los clientes en la toma de decisiones.
    c. Permitir la construcción colectiva del Estado, en conjunto con los clientes.
    d. Proveer servicios fáciles, rápidos, accesibles, confiables, interoperables y que anticipen el comportamiento de los clientes.
2. En la perspectiva Financiera, con el fin de involucrar a toda la sociedad en el desarrollo de la Estrategia de Gobierno en línea, se debe:
    a. Propiciar la inversión racional y sostenible en la modernización de los procesos internos y de prestación de servicios por parte de las Entidades a través de las TIC.
    b. Incentivar la creación de modelos de negocio a partir de la prestación de servicios por parte de terceros.
    c. Propiciar que el costo del acceso a los servicios por parte de los clientes sea equilibrado y competitivo.
    d. Generar incentivos para impulsar el desarrollo de servicios, tanto por las entidades como por terceros.
3. En la perspectiva de Procesos, es necesario orientar los procesos a:
    a. Prestar servicios sin barreras de acceso, orientados a satisfacer necesidades de los usuarios.
    b. Crear, distribuir y manipular información electrónica masiva, protegiendo la información del individuo.
    c. Conocer a los clientes; sus gustos, necesidades y su comportamiento.
    d. Promover y divulgar los servicios de Gobierno.
4. Finalmente, en la perspectiva de Aprendizaje y desarrollo, se deben contemplar los siguientes aspectos estratégicos:
    a. Generar capacidad de colaboración entre los funcionarios de las diferentes Entidades.
    b. Crear una cultura digital que aproveche las TIC para crear valor a los clientes.
    c. Habilitar canales de formación para la sociedad para la apropiación de las TIC y la participación y colaboración.
    d. Generar capacidades de innovación permanente en las Entidades del Estado.

Posteriormente, y con el fin de organizar todos los modelos en una arquitectura de referencia, se ha venido construyendo la siguiente visión de arquitectura de Gobierno en línea, la cual es una definición conceptual del modelo a desarrollar por la Estrategia de Gobierno en línea:

Figura 2 - Arquitectura de Gobierno en línea



La arquitectura está compuesta de tres componentes: Una red de servicios, un entorno de colaboración y un componente de Gobernabilidad.

1. La red de servicios, contiene una serie de servicios interrelacionados de información, transacción y participación; los cuales son accedidos a través de diferentes Canales de Acceso. Entre los canales de acceso que se puede encontrar están la Televisión, el Internet, el Celular, los Canales Presenciales, entre otros.

    - Los servicios de información corresponden a aquellos servicios que se generan exclusivamente para publicar información. Entre los servicios de información encontramos el Portal Único de Contratación, los Portales Territoriales, los Portales de las Entidades, entre otros.

    - Los servicios de transacción corresponden a aquellos servicios sobre los cuales los clientes pueden realizar operaciones con el Estado. Entre estos servicios encontramos la Ventanilla Única de Registro de Propiedad del Inmueble, el Certificado de Antecedentes Fiscales, la Solicitud de constancia juramentada por perdida, extravió de documentos o elementos, entre otros.

- Los servicios de Participación corresponden a aquellos que dispone el Gobierno para promover la participación ciudadana en la toma de decisiones. Entre estos servicios se encuentra la Urna de Cristal, el Micrositio de Vive Gobierno en línea, entre otros.

2. El entorno de colaboración es el lugar donde interactúan todos los actores de la sociedad en la construcción de los servicios que serán prestados en la Red de Servicios. En este entorno se pueden identificar Ciudadanos, Empresas del Sector Productivo, Entidades del Estado y la Academia. Este entorno de colaboración da origen a un proceso continuo de Publicación de datos, publicados por las Entidades; generación de procesos de negocio que hacen uso de estos datos, por parte de todos los actores; esquemas de co-creación, que permiten la interacción de múltiples actores de la sociedad para la prestación de los servicios, y finalmente estrategias de prestación de servicio, en donde cada actor define cómo prestar el servicio que va a colocar en la red de servicios. Adicionalmente, este proceso se retroalimenta a partir de la participación de los usuarios, desde la mejora a la calidad de los datos, hasta la estrategia de prestación de servicio. Lo que da origen a un proceso permanente que promueve la publicación de más datos, que a su vez conllevan a la prestación de más servicios.

En el Entono de Colaboración los diferentes actores interactúan de la siguiente manera:

- Entidades: Requieren transformarse para poder integrar a los diferentes actores de la sociedad en la prestación de servicios.

- Sector Productivo: Genera nuevos modelos de negocio, para facilitar la prestación y provisión de servicios a los ciudadanos.

- Academia: Participa entregando conocimiento a partir de sus investigaciones sobre los actores de la sociedad.

- Ciudadano: Participa a través de la creación de comunidades para la participación y construcción colectiva.

Este entorno de colaboración se soporta en unos componente de apoyo, que involucran tanto Soluciones de soporte como de Infraestructura Tecnológica.

- Las Soluciones de soporte corresponden a aquellas soluciones que se requieren por uno o varios servicios, y que facilitan la dinámica del entorno de colaboración al facilitar la concentración de esfuerzos en la construcción de funciones de valor para los clientes. Entre las soluciones de soporte encontramos la solución de Autenticación en línea, Notificación en línea, Botón de pago, Tramitador en línea. Estas soluciones pueden ser provistas tanto por las entidades del Estado, como por terceros, y dependerá de su uso estratégico quien las desarrolle.

- La Infraestructura Tecnológica corresponde a la base tecnológica sobre la cual operarán los servicios de la Red de Servicios. Entre los componentes de la Infraestructura Tecnológica encontramos Centros de Datos, Redes de Comunicación, Centros de Contacto. Cada uno de estos componentes puede ser prestado por varias Entidades o Empresas, y debe cumplir con un conjunto de estándares de calidad, prestación de servicio y seguridad, que hacen parte de la Gobernabilidad.

- Finalmente, se encuentran en este componente de apoyo, los esquemas de incentivos, acompañamiento y medición, los cuales facilitan la masificación de la Estrategia y la construcción del Entorno de Colaboración.

3. El componente de Gobernabilidad facilita que la construcción de la arquitectura se pueda realizar por parte de todos los actores de la sociedad, a partir de unos principios, lineamientos, metodologías, guías y estándares, así como con la administración de la base de conocimiento y la revisión permanente del Marco legal y regulatorio.

3.1. Relación Modelo de Seguridad.

Desde el punto de vista de seguridad, el modelo que se plantea en este documento busca ayudar a las entidades en la provisión de servicios confiables a los clientes, a partir de unos procesos con los que se pueda crear, distribuir y manipular información electrónica masiva, protegiendo la información del individuo. Para esto, se ha contemplado también que se desarrollen entre otras, competencias relacionadas con seguridad en la creación de una cultura digital que aproveche las TIC para crear valor a los clientes y se generen capacidades de colaboración entre los funcionarios de las diferentes Entidades, para poder implementar de manera más eficiente el modelo.

Por lo tanto, el modelo de seguridad se involucra dentro de la arquitectura como un principio, que debe regir todo lo que se construya, y a partir de allí se entregan una serie de lineamientos, metodologías, guías y estándares, que están al servicio de las entidades para la implementación de la Estrategia, e incluyen:

Lineamientos:
- Organigrama del modelo y Sistema de Atención de Seguridad de Información de Gobierno en línea
- Estratificación de Entidades
- Control de seguridad
- Indicadores de seguridad.
- Lineamientos para la implementación del modelo de seguridad de la información.

Metodologías:
- Metodología para gestión de riesgos
- Metodología de clasificación de activos

Guías:
- Encuesta de seguridad
- Autoevaluación de entidades, para el análisis de brecha
- Plantilla de política de seguridad del Sistema de Gestión de Seguridad de la Información – SGSI para las entidades
- Ejemplos de procedimientos estándares usados
- Guías de implementación de política

Finalmente, se incluyen una serie de recomendaciones en cada uno de los componentes de la arquitectura, relacionados en la Red de servicios y el Entorno de colaboración.

4. SISTEMA DE ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE GOBIERNO EN LÍNEA - SASIGEL

4.1. Sistema Administrativo de Seguridad de la Información para Gobierno en línea[1]

El Modelo de Seguridad de la Información para las entidades del Estado, se apoya en la creación del Sistema Administrativo de Seguridad de la Información para Gobierno en línea – SASIGEL y en la conformación de la Comisión de Seguridad de la Información para Gobierno en línea, para tomar acciones estratégicas y definir los lineamientos que permitan la implementación, seguimiento y mantenimiento del Modelo de Seguridad de la Información en cada una de las entidades públicas de orden nacional y territorial y en las entidades privadas que sean proveedoras de los servicios de Gobierno en línea.

La creación del Sistema Administrativo de Seguridad de la Información para Gobierno en línea, permite el cumplimiento de los principios definidos en la Ley 1341 de 2009 y en la Estrategia de Gobierno en línea, que corresponden a la protección de la información del individuo y la credibilidad y confianza en el Gobierno en línea.

En particular, para lograr el cumplimiento de estos principios, se requiere que tanto los servicios de Gobierno en línea, como la Intranet Gubernamental y las entidades que participen en la cadena de prestación de los servicios de Gobierno en línea, cumplan con los tres elementos fundamentales de la seguridad de la información: disponibilidad de la información y los servicios; integridad de la información; y, confidencialidad de la información. Para la correcta administración de la seguridad de la información, se deben establecer y mantener programas y mecanismos que busquen cumplir con los tres requerimientos mencionados.

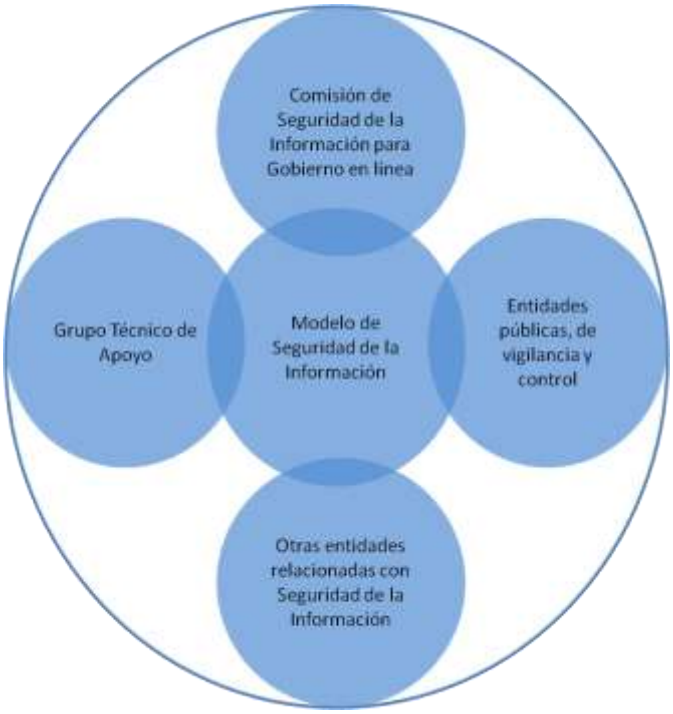
El SASIGEL surge, como la necesidad de dirigir las interacciones de los actores públicos, privados y de la sociedad civil que interactúan y afectan la seguridad de la información de las entidades públicas.

En este sentido, el SASIGEL coordinará las actividades relacionadas con la formulación, ejecución, seguimiento y mantenimiento de las políticas y lineamientos del modelo, necesarios para fortalecer la adecuada gestión de la seguridad de la información de las entidades públicas a nivel nacional. La figura 3 muestra la estructura de SASIGEL.

Ahí se encuentran la Comisión de Seguridad de la Información para Gobierno en línea, el Grupo Técnico de Apoyo, el Equipo de Gestión del Proyecto a Nivel Central (ver Anexo No. 1 - Organigrama modelo y SASIGEL.)

[1] Tomado y adaptado del documento "INFORME FINAL – MODELO DE SEGURIDAD DE LA INFORMACIÓN – SISTEMA SANSI – SGSI. MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA", Programa Gobierno en línea (2008).

Figura 3 - Sistema Administrativo de Seguridad de la Información para Gobierno en línea - SASIGEL

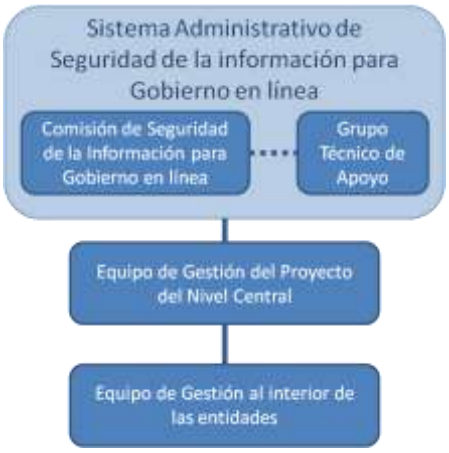


Fuente: tomado y adaptado del documento "INFORME FINAL – MODELO DE SEGURIDAD DE LA INFORMACIÓN – SISTEMA SANSI – SGSI. MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA" Programa Gobierno en línea (2008).

4.2. Estructura institucional

La estructura institucional, de la figura 4, toma las funciones de rector del Modelo, tanto a nivel general, como al interior de cada entidad que lo implemente, se encuentran en el capítulo tres (3) del Anexo No. 1 - Organigrama modelo y SASIGEL. Esta estructura garantiza el mantenimiento y sostenibilidad del Modelo de Seguridad de la Información en el tiempo, así como su correcta implementación.

Figura 4 - Organigrama para el Modelo de Seguridad de la Información



La estructura institucional de SASIGEL, junto a sus funciones se encuentra en el Anexo No. 1 - Organigrama modelo y SASIGEL., la participación de sus actores, se muestra en la figura 4. Ahí se encuentran la Comisión de Seguridad de la Información para Gobierno en línea, el Grupo Técnico de Apoyo, el Equipo de Gestión del Proyecto a Nivel Central y el Equipo de Gestión a nivel de las entidades.

El sistema, es apoyado y divulgado a alto nivel por la **Comisión de Seguridad de la Información para Gobierno en línea**, órgano que:

- Se apoyará técnicamente en el Grupo Técnico de Apoyo para definir y establecer el Modelo de Seguridad (Proceso **PLANEAR** ciclo PHVA) a implementar por las entidades objetivo.

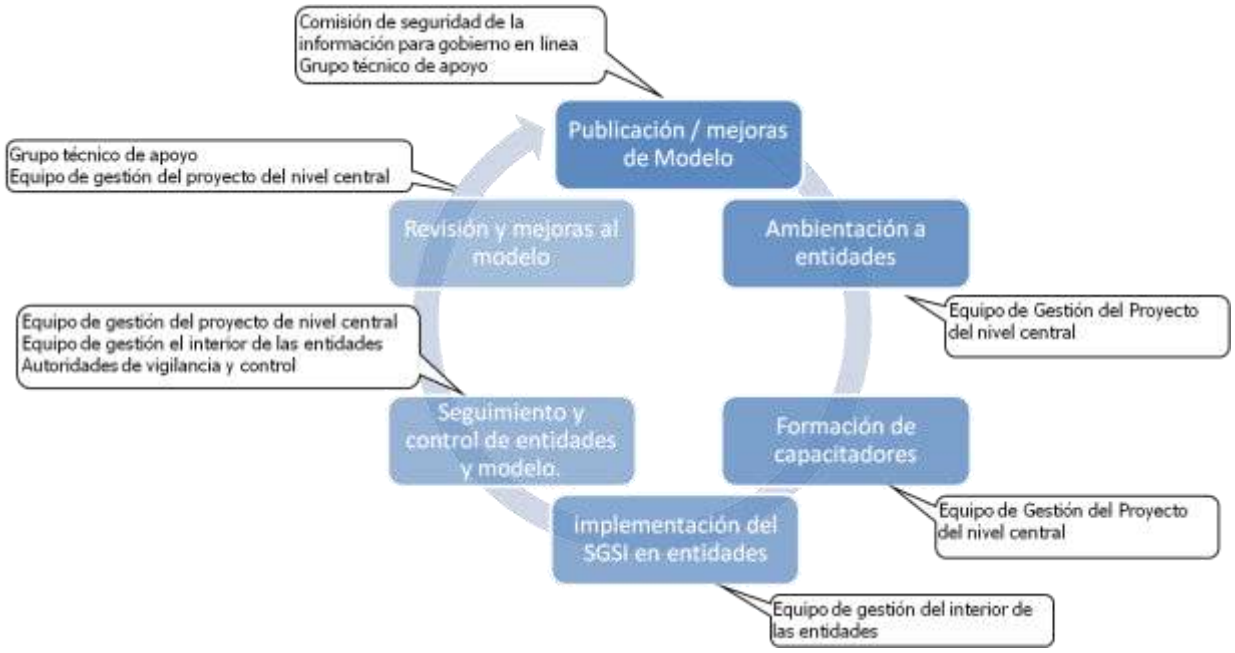
- Aprobará los cambios y mejoras planteadas para el modelo de seguridad de la información.

Para que el Modelo de Seguridad de la Información pueda ser implementando a nivel general se describe una estrategia de trabajo que está estructurada a partir de etapas, las cuales se muestran en la figura 5 y se explican en el siguiente numeral.

4.3. Aproximación por procesos para SASIGEL

El Sistema Administrativo de Seguridad de la Información para Gobierno en línea, adopta un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea, orientado hacia todas las entidades y los actores involucrados.

Figura 5 - Ciclo de vida para el SASIGEL y sus actores



La aproximación se hace a través del modelo PHVA de la figura 5, donde se identifica las diferentes etapas como son la **planeación** y publicación del modelo. El **hacer**, con la ambientación de las entidades, formación de capacitadores e implementación del SGSI en las entidades, este último desarrollado en detalle en el capítulo 5. El **verificar** mediante el seguimiento y control. Y el **actuar** mediante la revisión y mejoras al modelo.

En este modelo las salidas de cada etapa, se convierten en las entradas de la siguiente, y mediante una disposición cíclica permite que el Sistema Administrativo de Seguridad de la Información para Gobierno en línea sea un modelo auto-sostenible, que funciona eficazmente.

4.4. Fase Planear de SASIGEL

Durante esta fase se ha definido el modelo que aplica para las entidades públicas. El modelo en detalle se encuentra en el capítulo cuatro (4) de este documento.

SASIGEL define la estructura del SGSI teniendo en cuenta las siguientes premisas para el sistema:

- Los instrumentos normativos para apoyar la implementación del Modelo de Seguridad.
- Los lineamientos, requerimientos y la política del Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea, definidas por el manual GEL 3.0 para cada nivel de madurez.

4.5. Fase Hacer de SASIGEL

Las entidades públicas que provean servicios de Gobierno en línea, deberán **implementar y operar** (Proceso **HACER** del ciclo PHVA) la política, recomendaciones y controles definidos en el modelo en el capítulo 5, para dar cumplimiento a la normatividad, a los requerimientos, y que a su vez, les permita ser más competitivas y ofrecer mejores y más seguros servicios para proveer mayor confianza a los ciudadanos que hagan uso de sus servicios y productos.

El modelo de seguridad de la información lleva a la entidad a alinearse con un ciclo PHVA para realizar la implementación de un sistema de gestión de seguridad de la información alineado con los niveles de madurez definidos en el manual de Gobierno en línea 3.0. El modelo incluye las claves para el éxito de la implementación del mismo, y la descripción detallada de cada una de las actividades de las fases.

4.5.1. Ambientación a entidades

Se deberá realizar una sesión de preparación con las entidades y sus equipos de gestión del proyecto, con el propósito de hacer claridad sobre los objetivos que se persiguen con el Modelo, las directrices y premisas sobre las cuales se va a desarrollar el mismo y las reglas de juego que a nivel de logística aplicarán durante esta actividad. Serán parte del temario de estas capacitaciones:

1. Condiciones de implementación del modelo.
2. Tiempos estimados de implementación por características de entidad.

3. Sensibilización sobre el alcance y objetivo de la autoevaluación.
4. Definición de la brecha.
5. Implementación y ajustes al modelo de seguridad de la información.
6. La relación del Responsable de Seguridad de la Información y el Modelo de Seguridad de la Información.
7. Auto sostenibilidad del modelo.

Con el fin de llevar a cabo la implementación del modelo en las entidades se define un Plan de Sensibilización que se detalla a continuación.

4.5.2. Plan de sensibilización[2]

El objetivo de este plan es sensibilizar a las entidades, tanto públicas y privadas, en la utilización y provecho del Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea, también busca capacitar al funcionario público encargado de gestionar la seguridad de la información al interior de su entidad y alinearla con los objetivos de seguridad para la Estrategia de Gobierno en línea.

Para la realización del plan de sensibilización, se sugiere la ejecución de las siguientes etapas.

4.5.2.1. Campaña de sensibilización a las entidades públicas y privadas

En esta etapa, se realizará la divulgación y sensibilización masiva a las entidades objetivo, públicas y privadas que tienen que acogerse al Modelo de Seguridad de la Información, de forma que estas entidades conozcan sus nuevas responsabilidades, cómo alinearse y cómo armonizar sus avances con los sistemas de gestión de calidad (como NTC-GP1000 o ISO9001), control interno (MECI) y Sistema de gestión de seguridad de la información (como ISO27001).

El plan de divulgación y sensibilización hará uso de los siguientes medios:

- Medios impresos: Afiches, plegables y elementos de recordación que contendrán información resumida pero importante acerca del nuevo Modelo, en qué consiste, cuáles son sus objetivos principales y cuál es la responsabilidad de las entidades, funcionarios y empleados dentro del modelo de seguridad. También mostrará información sobre cómo se puede ayudar a la entidad tanto en la implementación como en la mejora del Modelo.

- Medios interactivos: Fondos de escritorio para los computadores de las entidades, protectores de pantallas y videos con información relacionada tanto a las principales políticas en seguridad de la información como con el nuevo Modelo de seguridad.

[2] Tomado y adaptado del documento "ENTREGABLE 14: ESTRATEGIAS DE IMPLEMENTACIÓN - MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA", desarrollado en el 2008 por el Programa Gobierno en línea.

- A través de Internet: Presentación de información completa y detallada en la Intranet Gubernamental de Gobierno en Línea, documentos de trabajo, diagramación de procesos y servicios relacionados con el Modelo de seguridad.

4.5.2.2. Plan de capacitación para las entidades públicas

El equipo central de SASIGEL está a cargo de realizar las capacitaciones en seguridad de la información, en el Modelo de seguridad y en estrategias para la implementación exitosa orientada a los funcionarios públicos responsables por la implementación y gestión del Modelo de seguridad de la información al interior de sus entidades. Los contenidos de los cursos podrán descargarse de la Intranet Gubernamental y estarán disponibles para su consulta en línea. Las capacitaciones son dictadas periódicamente a través del año.

4.5.2.3. Campaña de sensibilización masiva

Campaña en la que se involucra al ciudadano, el objetivo principal es lograr que el ciudadano tenga mayor confianza y credibilidad en el Estado Colombiano al momento de realizar sus trámites y transacciones por medios electrónicos y cuando haga uso de los servicios de Gobierno en línea. Los medios de divulgación principalmente serán: televisión, radio, medios impresos y publicación en el sitio www.gobiernoenlinea.gov.co.

4.5.3. Formación de Capacitadores

El equipo central de SASIGEL está a cargo de realizar la ejecución de los procesos de capacitación a los líderes seleccionados por las entidades para que repliquen al interior de cada entidad comprometida en la implementación del modelo con el *know how* que garantice la implementación exitosa del mismo al interior de cada una de estas entidades.

Si la entidad considera certificarse respecto al estándar ISO27001, es un requisito demostrar que el personal ha recibido la capacitación necesaria (cursos, especializaciones, diplomados, etc.) para realizar sus funciones, y en el caso de los auditores internos, que se cuente además con el entrenamiento formal de auditores internos en SGSI NTC: ISO/IEC 27001:2005.

4.5.4. Implementación del modelo a través del SGSI en entidades

Una vez las entidades se encuentren sensibilizadas y preparadas deben iniciar con la implementación del modelo de seguridad de la información al interior de la misma.

El modelo y su implementación se encuentran definidos en el capítulo cuatro (5). Allí se define como se establece, implementa, opera, monitorea y revisa, mantiene y mejora el SGSI.

Notas:

- Como parte de la implementación, es necesario que se mantenga la ejecución del plan de sensibilización al interior de todas las entidades.

- Se debe capacitar al funcionario público encargado de gestionar la seguridad de la información al interior de su entidad con el fin de que se alinee con los objetivos de seguridad para la Estrategia de Gobierno en Línea.

4.6. Fase Verificar de SASIGEL

4.6.1. Seguimiento y control de entidades y modelo

En el proceso **VERIFICAR** del ciclo PHVA, en el que se realizará **revisión y seguimiento** de la implementación y cumplimiento del Modelo de Seguridad, tomarán parte:

- Las entidades públicas que provean servicios de Gobierno en línea, quienes tomarán las medidas necesarias para evaluar el nivel de cumplimiento del modelo,

- Las autoridades de vigilancia y control, como la Contraloría y la Procuraduría, para auditar y revisar el cumplimiento del modelo de seguridad por parte de las entidades y,

- El Equipo de Gestión de Nivel Central, verificando la implementación del modelo.

Esta etapa comprende el control de todos los recursos (humanos, financieros y físicos) con el fin de asegurar que los resultados del Sistema, por una parte, se produzcan oportuna y eficazmente en función de los costos y por otra parte que el alcance definido se cumpla dentro de los tiempos estimados o planeados.

Esta labor debe realizarse al interior de las entidades bajo la supervisión y lineamientos del equipo de gestión del nivel central de manera continua. Mediante la realización de auditorías periódicas, y el monitoreo de los indicadores a nivel central que la entidad debe reportar regularmente a SASIGEL.

4.6.1.1. Indicadores del modelo SASIGEL

Se definirán un conjunto de indicadores a nivel central con el fin de realizar la medición tanto sobre el desempeño de SASIGEL, como de los SGSI de cada entidad. Con los indicadores, se tendrá una forma sistemática, confiable y repetible de obtener los indicadores de ambos sistemas. El Anexo No. 9 – Indicadores de seguridad presenta los indicadores de gestión de SASIGEL.

En la Tabla 1 se presentan las métricas definidas por parte del equipo del nivel central para el monitoreo de cada uno de los SGSI implementados por las entidades. Esta tabla se basa en las métricas publicadas por el "Center for Internet Security" (CIS).[3]

Tabla 1 – Métricas de gestión

Métricas de acuerdo a CIS.	
Seguridad de aplicaciones	Número de aplicaciones
	Porcentaje de aplicaciones críticas
	Cobertura de evaluación de Riesgo
	Cobertura de las pruebas de seguridad
Configuración de la Gestión del Cambio	Tiempo medio para completar los cambios
	Porcentaje de cambios con revisión de Seguridad
	Porcentaje de cambios con excepciones de seguridad
Financiero	Información del Presupuesto de Seguridad como % del presupuesto de TI
	Asignación del presupuesto de Seguridad de la Información
Manejo de Incidentes	Tiempo medio de detección de incidentes
	Tasa de Incidentes
	Porcentaje de incidentes detectados por los controles internos
	Tiempo medio entre incidentes de seguridad
	Tiempo medio de recuperación
Gestión de parches	Cumplimiento de la política de parches
	Cobertura de la Gestión de parches
	Tiempo medio para parchar
Gestión de vulnerabilidades	Cobertura de escaneo de vulnerabilidades
	Porcentaje de sistemas sin vulnerabilidades graves conocidas
	Tiempo medio para mitigar las vulnerabilidades
	Número de instancias de vulnerabilidades conocida

Funte: CIS

4.6.2. Auditoría a las entidades

La auditoría a las entidades puede ser realizada por entidades con experiencia certificada en auditoría y certificación en ISO 27001, o a través de SASIGEL. Estas auditorías pueden fundamentarse en la estructura definidas por el estándar ISO/IEC 27006 e ISO 19011.

[3] Center for Internet Security – CIS Url: http://www.cisecurity.org/

4.6.2.1. Preparación del equipo y plan de auditoría por SASIGEL

La preparación del equipo de auditoría y el plan de auditoría incluye los siguientes puntos:

- Contar con un auditor líder con conocimientos generales y un auditor con conocimiento técnico detallado de acuerdo a la entidad, de tal manera que el equipo demuestra el conocimiento sobre los siguientes temas:
    - Sistemas de gestión y procesos aplicables del SGSI
    - Identificación de amenazas e incidentes de seguridad
    - Conocimiento de los controles y su implementación
    - Conocimiento de la revisión de la eficacia y la medición de controles
    - Conocimiento de estándares, buenas prácticas, políticas y procedimientos
    - Conocimiento de respuesta a incidentes y continuidad del negocio
    - Conocimiento de activos tangibles e intangibles y análisis de impacto
    - Conocimiento sobre gestión del riesgo y de métodos para el análisis de riesgo
- Realizar una revisión del alcance en término de las características de negocio, ubicación, activos y tecnología, incluyendo todos los requisitos del sistema y del manual GEL 3.0.
- Revisar que el análisis de riesgo y su tratamiento refleja apropiadamente las actividades de la entidad.
- La auditoría tiene una duración entre 5 y 16 días que depende de:
    - El alcance del SGSI
    - Complejidad del SGSI
    - Tipo de negocio dentro del SGSI
    - Extensión y diversidad de tecnología de los diversos controles del SGSI
    - Número de sitios, en cuyo caso se puede utilizar técnicas de muestreo
    - Desempeño previo del SGSI
    - Extensión de acuerdos con terceros y servicios tercerizados dentro del alcance del SGSI
    - Estándares y regulación aplicables
- La metodología utilizada debe permitir mostrar que la entidad cuenta con planes de auditoría interna, y que los programas y procedimientos son operacionales y se puede mostrar su operación.
- El plan de auditoría debe incluir la selección de técnicas adecuadas de acuerdo a la situación.
- El equipo de auditoría debe realizar un informe y brindar la oportunidad de dar a conocer a la entidad su progreso y realizar preguntas sobre los hallazgos.
    - El informe cuenta con un resumen ejecutivo
    - Un reporte del análisis de riesgo de la entidad
    - Tiempo total utilizado
    - Preguntas, razones para su selección y metdología empleada

- Observaciones positivas y negativas
- No conformidades de los requerimientos y sus comentarios

- El auditor debe demostrar su conocimiento
  - Experiencia realizando auditorías de sistemas de gestión de seguridad de la información
  - Credenciales que lo acrediten como auditor de sistemas de gestión de seguridad de la información
  - Cursos aprobados de sistemas de gestión de seguridad de la información
  - Estar registrado como auditor
  - Demostración práctica de haber participado en auditorías de sistemas de gestión de seguridad de la información

4.6.2.2. Proceso de auditoría en la entidad

Durante la auditoría a la entidad, SASIGEL recolectará la información de la entidad y realizará la auditoría en dos etapas:

- Los requisitos iniciales para la auditoría incluyen:
  - Información general sobre el SGSI y las actividades que cubre
  - Copia de la documentación del SGSI requerido y según sea requerido, la documentación adicional.
- La primera etapa se enfoca en la revisión de los documentos y la planeación de la revisión en sitio, con el fin de conocer en mayor nivel de detalle el sistema y de la preparación actual de la entidad. Posteriormente se debe comunicar a la entidad la documentación adicional requerida.
- La segunda etapa incluye confirmar que la entidad se adhiere a sus propias políticas, objetivos y procedimientos. También que cumple con los requisitos del SGSI y manual GEL 3.0 y esta logrando los objetivos de la política de la entidad. Se debe enfocar en lo siguiente de la entidad.
  - Evaluación de los riesgos relacionados con la seguridad de la información y que la evaluación produce resultados reproducibles y comparables.
  - Revisiones de la eficacia del SGSI y medida de la eficacia del SGSI con respecto a los objetivos del SGSI.
  - Revisiones de la dirección y auditorías internas.
  - Responsabilidad de la dirección para la política de seguridad de la información.
  - Correspondencia entre los controles seleccionados e implementados, la declaración de aplicabilidad, y los resultados del proceso de la evaluación del riesgo y tratamiento del riesgo y la política del SGSI y sus objetivos.
  - Implementación de los controles teniendo en cuenta las mediciones de eficacia de los controles por la entidad, para determinar si los controles están implementados y son eficaces para lograr los objetivos planteados.
  - Trazabilidad de los programas, procesos, procedimientos, registros, auditorías internas y revisiones de la eficacia del SGSI, con las desiciones de la dirección, la política del SGSI y los objetivos.

- La existencia del normograma y un sistema de gestión que permite dar cumplimiento legal y regulatorio a la entidad de los requisitos relacionados con la seguridad de la información.
- Nota sobre integración de sistemas de gestión. La entidad puede combinar la documentación del SGSI con otros sistemas de gestión, siempre y cuando el SGSI pueda ser claramente identificado junto con las interfaces apropiadas a los otros sistemas.

4.7. Fase Actuar de SASIGEL

En el proceso **ACTUAR** del ciclo PHVA, se realizan las mejoras al modelo, tanto para el modelo aplicable a las entidades como para SASIGEL, así:

- Las entidades toman las acciones de mejora resultantes de la auto-evaluación realizada y/o las auditorías externas para implementar controles de seguridad que permitan mejorar su nivel de cumplimiento del modelo de seguridad y por ende, su postura en seguridad de la información.

- El Equipo de Gestión de Nivel Central genera opciones de mejora como la definición de nuevos controles, procesos, lineamientos y políticas que serán puestos a consideración del Grupo Técnico de Apoyo y aprobación por parte de la Comisión de Seguridad de la Información para Gobierno en línea para que sean parte de las actualizaciones del Modelo a ser implementado.

4.7.1. Mantenimiento y sostenibilidad del modelo

Cuando se complete cada ciclo PHVA, dentro de la fase planear, se realizarán los ajustes al modelo resultantes de su aplicación a las entidades y el análisis de posibles fallas y vacíos que se hayan identificado y reportado por las entidades.

En cuanto al mantenimiento del modelo de seguridad de la información para la estrategia de Gobierno en línea, una vez ha sido implementado, debe cubrir aspectos como:

- Planificación y control de seguridad.
- Control de la implantación de políticas preventivas adicionales a las existentes en el modelo.
- Control a la implantación y/o ajustes a los controles existentes.
- Control y gestión de los riesgos (basado en metodologías de gestión del riesgo).
- Garantizar la continuidad del servicio.
- Cumplimiento legislación vigente.
- Ayuda a las auditorías de seguridad (basadas en la NTC:ISO/IEC 27001:2005) .

4.7.1.1. Mejora continua del SASIGEL

Con los resultados de la medición y el control sobre la ejecución de la implementación del modelo en las entidades, se realizarán las siguientes actividades:

- Comunicación de resultados de medición y control por el equipo de nivel central.

- Ajustes al modelo por el grupo técnico de apoyo.
- Ajustes a la estrategia de difusión y capacitación.
- Ajustes a la estrategia de implementación por el grupo técnico de apoyo.
- Aprobación de los cambios, por la Comisión.
- Difusión y publicación de los cambios.

4.7.1.2. Mejora continua del SGSI para las entidades

La mejora del modelo SGSI como parte de SASIGEL contará con sus actualizaciones de acuerdo a los ciclo definidos por el equipo central.

La mejora continua de la implementación del modelo en cada entidad es una etapa que se cubre en el ítem "5.3.4.5 Proceso continuo y Gestión auto sostenible del modelo de las entidades", como parte del ciclo PHVA del SGSI que debe ser realizado por la entidad.

5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LAS ENTIDADES

5.1. Introducción

La implementación del Sistema de Gestión de Seguridad de la Información - SGSI en las entidades, es un componente de la fase **hacer** del ciclo PHVA de la figura 5, que se desarrolla en detalle durante este capítulo.

Para garantizar una adecuada implementación del Modelo de Seguridad de la Información en las entidades del Estado se describe una estrategia de trabajo que está estructurada a partir de etapas alineadas con los niveles de madurez de manual de Gobierno en línea 3.0, las cuales se detallan en este capítulo y son coherentes con los lineamientos del estándar NTC:ISO/IEC 27001:2005.

Para abordar el tema de la seguridad de la información se debe contar con aprobación y apoyo sostenido de la dirección de la entidad. Esto permitirá que la gestión del riesgo (lo cual incluye el análisis, la identificación de controles adecuados, su implementación, su medición y mejora continua), sea aprobada y apoyada con los recursos necesarios a través de todas las etapas e instancias del sistema.

Nota: se aclara que el estándar internacional se complementa de manera armónica con otras iniciativas y estándares nacionales e internacionales, tales como MECI (Modelo Estándar de Control Interno), COBIT, ITIL, entre otros[4].

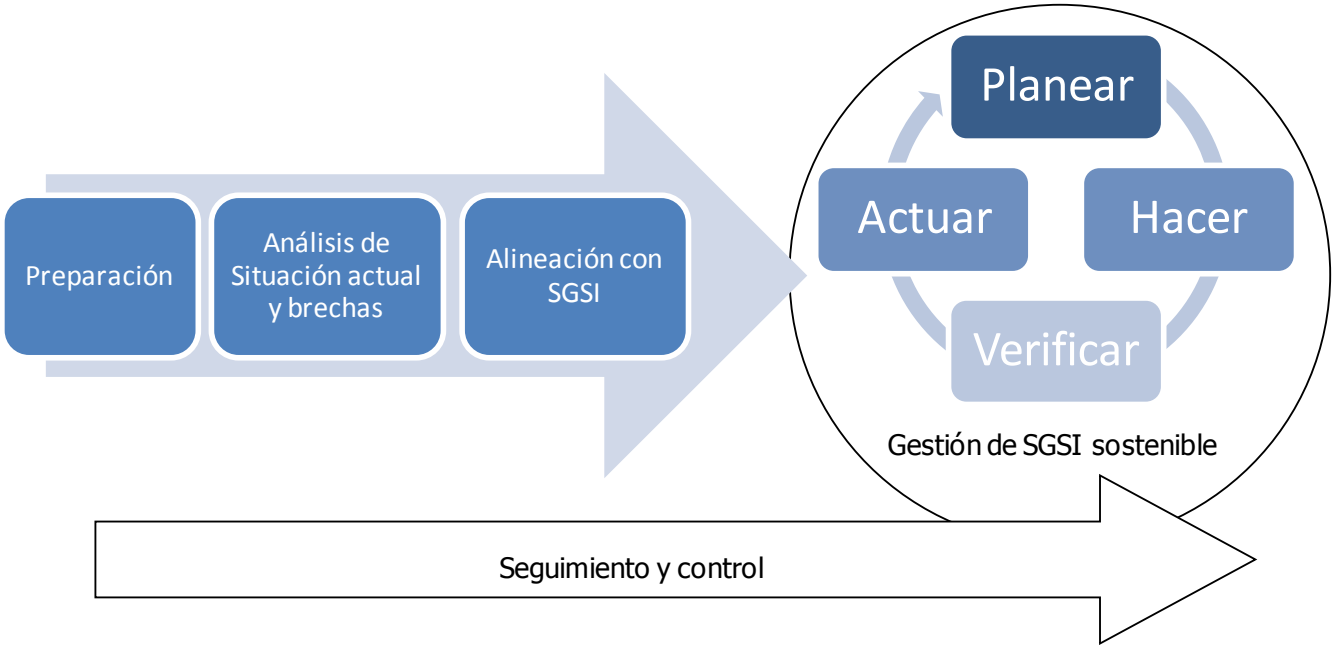
5.2. Etapas de implementación

Se ha definido como estrategia para la implementación del Modelo de seguridad de información en las entidades del Estado, la ejecución de cuatro (4) etapas como se muestra en la figura 6.

Las etapas son: preparación, análisis de la situación actual y brechas, alineación con el SGSI, las cuales conllevan a que la entidad entre en la etapa de gestión del SGSI sostenible basado en el ciclo PHVA, monitoreado por SASIGEL, a través del seguimiento y control de la sección 4.6.

[4] Se puede consultar un cuadro exhaustivo que muestra la correspondencia entre los estándares en el Anexo 12 – Correspondencia de Estándares. o directamente en Inglés http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf
Español http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf

Figura 6 - Plan de implementación



5.2.1. Preparación

Las etapas previas a la implementación del SGSI son fundamentales para lograr una adecuada sensibilización, motivación y compromiso por parte de la entidad y sus funcionarios. Como se describe en el capítulo 3, es responsabilidad de SASIGEL que las entidades tengan acceso a la capacitación, antes de iniciar con esta etapa. Las actividades son:

- "Formación de Capacitadores" descrita en la sección 4.5.3.
- "Campaña de sensibilización a las entidades públicas y privadas" descrita en la sección 4.5.2.1.
- "Plan de capacitación para las entidades públicas" descrita en la sección 4.5.2.2 definidas en el alcance del SASIGEL.

Para una correcta aproximación e implementación del SGSI, la entidad debe haber completado dicha sensibilización y capacitación para continuar con las siguientes actividades:

5.2.1.1. Involucrando y sensibilizando a la alta dirección

Revisar con la alta dirección y acordar el compromiso con el cumplimiento y preparación de los pre-requisitos para iniciar la implementación del SGSI, y así mismo de los requisitos los cuales la entidad debe cumplir de acuerdo con manual de Gobierno en línea 3.0, una vez el SGSI está implementado y en operación. El documento "Lineamientos para la Implementación del Modelo de Seguridad de la Información" cuenta con la nota importante para la dirección.

5.2.1.2. Identificación de los responsables

Uno de los factores críticos de éxito es el adecuado soporte por parte de representantes de alto nivel de la entidad para soportar y dar visibilidad a la iniciativa permanente para la implementación del modelo.

Los representantes de alto nivel de la entidad deben realizar los siguientes pasos en el orden planteado para contar con la lista de responsables al final del ejercicio: dar a conocer el perfil y responsabilidades de los responsables.

5.2.1.2.1. Perfiles y responsabilidades

Sin perjuicio de lo establecido en la Ley 489 de 1998, cada entidad en el menor tiempo posible (cada entidad establecerá los términos en los cuales se puede cumplir con esta obligación) deberá organizar el grupo de trabajo responsable para implementar el Modelo de seguridad de la información en las entidades del Estado, definiendo el perfil y rol de conformidad con lo establecido en este documento de política.

Es necesario que las responsabilidades asignadas en este documento de políticas cada perfil, sean incorporadas a los manuales de funciones de cada entidad de acuerdo al cargo de desempeñan.

Consultar el numeral "3.7 Equipo de gestión al interior de cada una de las entidades" del Anexo No. 1 - Organigrama modelo y SASIGEL." del modelo de seguridad de la Información de Gobierno en línea donde se encuentran definidas las responsabilidades.

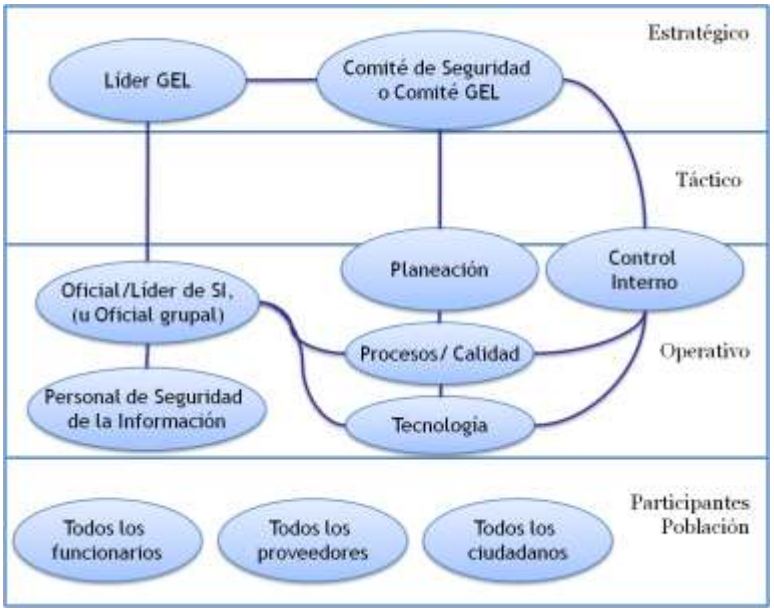
Actividad: Dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol.

El sistema cuenta con la interacción los siguientes perfiles:

- Comité de seguridad. Las funciones de este comité pueden ser tomadas por comité de GEL, de acuerdo al Manual de Gobierno en línea 3.0.
- Líder de proyecto: Líder de Gobierno en Línea.
- Oficial de Seguridad de la información o líder de seguridad. En aquellas entidades que así lo justifiquen, por ejemplo con insuficiencia de recursos técnicos o experticia, se recomienda la definición de un oficial de seguridad que responda simultáneamente para un conjunto de entidades que acuerden agruparse.
- Personal de seguridad de la información.
- Un representante del área de tecnología.
- Un representante del control interno.
- Un representante del área de planeación.
- Un representante de sistemas de gestión de calidad.
- Funcionarios, proveedores, y ciudadanos.

En la figura 7, se muestra la interrelación de todos estos actores y el nivel (estratégico, táctico, operativo y participativo) en donde se desempeñan cada uno de ellos.

Figura 7 - Actores del SGSI



5.2.1.3. Estratificación de entidades

La estratificación de las entidades permite identificar de manera general, el nivel de complejidad que puede significar para estas, la implementación del SGSI con el cual será revisado. Independientemente de la estratificación, las entidades deben utilizar la aproximación mediante la gestión del riesgo de la sección 5.3.1.5 para identificar el conjunto de controles mínimos sugeridos aplicables para cada una de ellas.

Actividad: consultar el modelo de estratificación relacionado en el Anexo 3 para la determinación del estrato en que queda clasificada la entidad frente al Modelo de Seguridad de la Información.

5.2.2. Análisis de la Situación actual y Definición de brechas

Esta etapa se enfoca en tener un conocimiento inicial de la situación que presenta la entidad frente al modelo de seguridad y los lineamientos del manual de Gobierno en línea 3.0, según el alcance definido por la clasificación en la que se encuentre. Con respecto a lo determinado en el punto anterior (responsables y estratificación). Los componentes de esta etapa y las tareas a realizar por el equipo definido son: aplicar la encuesta, definir el nivel de madurez, definición de brechas y definición de cronograma para reducir la brecha.

5.2.2.1. Aplicar la encuesta

La encuesta se plantea para realizar el diagnóstico actual de la entidad.

Actividad: Consultar y aplicar el documento de encuesta del Anexo No. 2 - Encuesta de seguridad. Los resultados serán utilizados en el capítulo 5.2.2.3 "Definición de brechas".

5.2.2.2. Definir nivel de madurez

De acuerdo a los lineamientos del Manual de Gobierno en línea 3.0, cada entidad tiene un nivel de madurez inicial y una ruta a seguir, con unos requerimientos para cada nivel. La tabla 2 contiene los requerimientos transversales de seguridad presentes en el Manual de Gobierno en línea 3.0.

Actividad: Realizar la autoevaluación con respecto a los niveles de seguridad transversales definidos en el Manual de Gobierno en línea 3.0, utilizando los formato del Anexo No. 4 - Autoevaluación – definición de brecha.

Tabla 2 - Niveles de seguridad, Manual de Gobierno en línea 3.0

Niveles de Seguridad según Manual de Gobierno en línea 3.0	
Plan de Seguridad Nivel Inicial	La entidad debe definir una política de seguridad que garantice la protección de la información, los datos personales y los activos de información con que cuenta. Para ello, deberá implementar las siguientes acciones: • Identificar el nivel de conocimiento al interior, en temas de seguridad de la información y seguridad informática • Definir la política de seguridad a ser implementada • Divulgar la política de seguridad al interior de la misma • Conformar un comité de seguridad o asignar las funciones de seguridad al comité GEL • Identificar los activos de información en los procesos ,incluyendo los activos documentales (records), de acuerdo con el análisis de procesos realizado • Identificar los riesgos y su evaluación, en dichos procesos • Definir el plan de acción con los controles y políticas que se implementarán para mitigar los riesgos identificados
Plan de Seguridad Nivel Básico	• Con base en el análisis de procesos realizado en el nivel inicial y la política o plan de seguridad definido, la entidad inicia la ejecución de dicho plan de seguridad para implementar los controles que mitigarán los riesgos identificados, lo cual implica que la entidad presenta avances en la implementación de tales controles. • De acuerdo con el plan de capacitación definido por la entidad en el nivel inicial, esta ejecuta las acciones de capacitación en seguridad, con los responsables de los controles y procesos con los cuales se inicia la ejecución del plan. • La entidad inicia la documentación de políticas y procedimientos de seguridad, de acuerdo con el plan definido.
Plan de Seguridad Nivel Avanzado	• La entidad culmina la implementación de controles definidos en el nivel inicial
	• La entidad documenta la totalidad de políticas y procedimientos de seguridad • La entidad ejecuta las actividades de capacitación en temas de seguridad, con todos los servidores públicos

Niveles de Seguridad según Manual de Gobierno en línea 3.0	
	• La entidad define el plan de verificación periódica de los controles, procedimientos y políticas de seguridad • La entidad reporta los avances del cumplimiento del plan
Plan de Seguridad Nivel de Mejoramiento Permanente	• La entidad refuerza la divulgación de las políticas de seguridad • La entidad ejecuta los procedimientos y políticas de seguridad, de manera repetitiva • La entidad realiza la revisión periódica interna de los riesgos inicialmente detectados, políticas, procedimientos y controles • La entidad evalúa sus políticas de seguridad e implementa acciones para mejorarlas

5.2.2.3. Definición de brechas

Una brecha es la ausencia total o parcial en la estructura, las políticas, los controles, directrices, procesos y/o procedimientos existentes al interior de la entidad, al ser comparadas con las requeridas por el Manual de Gobierno en línea 3.0, para cada etapa de madurez.

Mediante esta actividad, la entidad podrá comparar su desempeño actual, contra su desempeño propuesto y optimizado, la eficacia de su gestión de la seguridad de la información y planear su ruta para cerrar la brecha. Son actividades que pertenecen a esta etapa:

- Revisión de estructura organizacional. Comparar la estructura, visibilidad y funciones existentes con la estructura propuesta en el capítulo "5.2.1.2.1 Perfil".

- Revisión por niveles de madurez de acuerdo a los requisitos definidos en "5.2.2.2 Definir nivel de madurez".

- Revisión de controles de seguridad de la información, tanto los existentes como los ausentes. Del listado de controles existentes, revisar su presencia y nivel de eficacia de la implementación y operación actual de cada uno de los controles.

    - Revisión de políticas.
    - Revisión de existencia de controles
    - Revisión de existencia de métricas
    - Revisión de mejoramiento continuo

- Definición del plan o cronograma a seguir para disminuir la brecha, el cual debe darse a conocer al líder del nivel central.

Actividades:

- Utilizando el resultado de la encuesta, junto con el resultado de la determinación de la posición actual de madurez, y los requisitos del Manual de Gobierno en línea 3.0 para seguridad de la

información, se procede a definir el estado actual de seguridad de la información de la entidad, al comparar punto a punto, con lo mínimo esperado para el nivel actual de la entidad definido en el Manual de Gobierno en línea 3.0.

- La entidad puede utilizar el formato disponible Anexo 4 del modelo para diligenciar sus hallazgos. Este documento será evidencia del análisis donde se registre el cumplimiento o ausencia de cada elemento analizado. Y un insumo para definir el plan de alineación con el SGSI.
- Definir y acordar con el líder del SGSI, el plan o cronograma para disminuir la brecha y alinearse con el nivel de madurez más adecuado. Posteriormente comuníquelo con el líder de nivel central.

5.2.3. Alineación con el SGSI

El sistema de gestión de seguridad de la información para Gobierno en Línea, está alineado con la familia de estándares ISO/IEC 27000. Los requerimientos a ser evaluados en un sistema de gestión de seguridad de la información se encuentran en el estándar NTC:ISO/IEC 27001:2005. En caso de que la entidad requiera demostrar cumplimiento y eventualmente decida certificarse, la entidad debe cumplir con los requisitos allí definidos.

En esta sección se alinea la estrategia de seguridad de la entidad para la implementación de un SGSI, que dependiendo del nivel de madurez identificado estarán cubiertos y serán validados y homologados, o deberán ser trabajados para cubrir la brecha y alinearse con el estándar.

5.2.3.1. Factores críticos de éxito

Los siguientes factores son fundamentales para que la entidad cuente con un sistema de gestión de seguridad de la información sostenible. Estos factores son componentes incluidos en el SGSI, que requieren ser considerados y abarcados para reflejar su impacto en la entidad:

- Se debe realizar una aproximación de "arriba-a-abajo", es decir contar con el compromiso por parte de directores y alta gerencia de la entidad para promover y soportar la implementación, la operación y los recursos del SGSI. (la motivación, energía, apoyo y liderazgo debe partir de la dirección y luego extenderse hacia toda la entidad a todos sus niveles hasta convertirse en operaciones)
- Soporte visible por parte de gerentes y coordinadores (amplia comunicación sobre su apoyo activo al SGSI dirigido a todos los miembros mostrando su importancia para la entidad).
- Contar con la política de gobierno de seguridad.
- Requerimientos de seguridad claramente articulados con las necesidades de la entidad.
- Políticas de seguridad alineadas con la misión y objetivos de la entidad, que se ajusten a la cultura corporativa, y donde se articulen todas las áreas de las entidades para concertar sobre la definición del alcance, la creación y aplicación de políticas, procedimientos y aseguramiento de los procesos y servicios ofrecidos.
- Aprobación de la alta gerencia del proceso de implementación.
- Definición de responsabilidades para cada rol del SGSI.
- Definición del grupo de trabajo transversal para la seguridad (Comité de seguridad).
- Realizar concientización, entrenamiento y educación.

- Realizar un análisis de riesgo que enlace los activos, su criticidad en téminos de confidencialidad, integridad y disponiblidad, las amenazas, los riesgos, los requisitos normativos, legislativos y regulatorios, los controles implementados, los controles propuestos y el riesgo residual.
- Establecimiento de métricas para la evaluación del desempeño del SGSI que además sirvan para reportar a SASIGEL.

5.2.3.2. Ejecución del programa para la reducción de la brecha.

El equipo de seguridad de la información llevará a cabo la implementación del plan para la reducir la brecha con respecto al nivel de madurez identificado, tal como la entidad lo define en el numeral 5.2.2.3 Definición de brechas.

Como resultado, la entidad contará con la alineación de su sistema, con los requisitos del manual gobierno en línea 3.0 y entrará en el ciclo PHVA del SGSI.

5.3. Ciclo PHVA para el sistema de la seguridad de la información

Una vez la entidad ha sido alineada con los requisitos del manual de Gobierno en línea 3.0, como se muestra en la figura 6, la entidad entra en el ciclo PHVA del SGSI. Dependiendo de su madurez, es posible que la entidad se enganche a su fase correspondiente.

- Si el nivel de madurez es inicial, la entidad entrará directamente a la fase planear.
- Si el nivel de madurez es básico y la brecha se ha cerrado, la entidad entrará directamente a la fase hacer.
- Si el nivel de madurez es avanzado la entidad entrará directamente a la fase verificar.
- Si el nivel de madurez es de mejora continua la entidad entrará directamente a la fase actuar.

Las siguientes actividades están organizadas de acuerdo a su uso en el ciclo PHVA, que permiten la alineación de la etapa Planear, correspondiente a un nivel de madurez inicial y posteriormente se implementa, que corresponde al nivel básico de madurez.

5.3.1. Planear (Nivel inicial de madurez)

Este capítulo detalla cómo llegar al nivel de madurez inicial propuesto por el Manual de Gobierno en línea 3.0, para ello es necesario que las entidades recorran un camino en donde comiencen por definir el alcance del SGSI y terminen con la preparación del plan de acción en cuanto a seguridad de la información de la entidad, tal como lo muestra la figura 8.

Los elementos cubiertos por las áreas sombreadas generalmente son comunes a otros sistemas de gestión y pueden ser integrados para apalancarse y unir esfuerzos.

5.3.1.1. Obtener soporte de la dirección de la entidad.

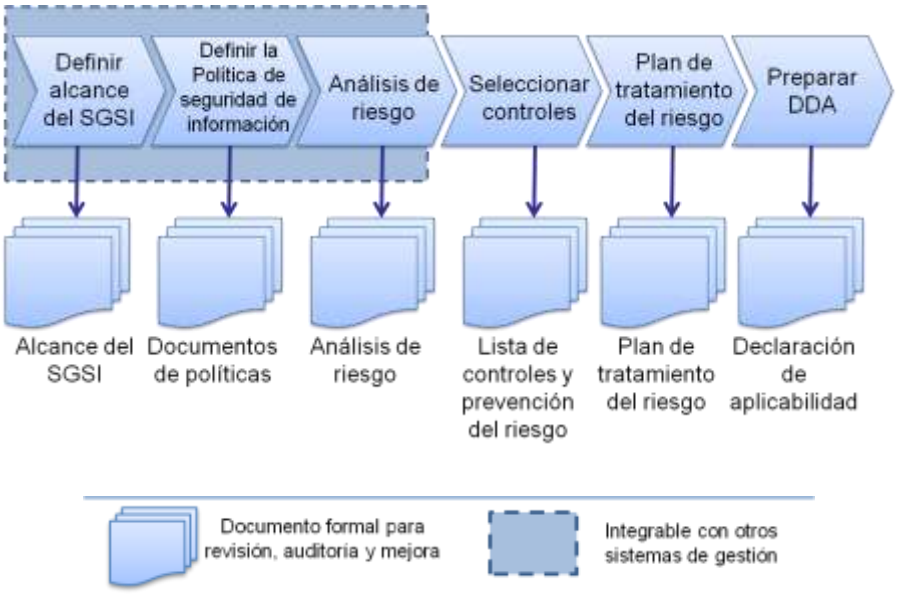
La gerencia debe aceptar el compromiso de establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI. El compromiso incluye actividades tales como garantizar que los recursos

requeridos estarán disponibles y que todos los funcionarios que se ven afectados por el alcance del SGSI, tienen una adecuada concientización, entrenamiento y competencia.

El soporte se ve cuando se crea y respalda: la política de seguridad de la información, los planes y objetivos de la seguridad de la información, la definición de roles y responsabilidades, anuncio o comunicación a la entidad sobre la importancia de adherirse a la política de seguridad de la información.

Otros ejemplos de cómo la dirección también lo demuestra cuando se determina y acepta el nivel de riesgo aceptable, cuando se revisa el SGSI en intervalos planeados, cuando el personal se le provee el entrenamiento de acuerdo a roles y responsabilidades.

Figura 8 - Documentación fase de planeación – Nivel inicial



5.3.1.2. Identificar legislación y normatividad aplicable

La legislación y marco regulatorio y otros requisitos que requieran de cumplimiento influye el alcance del SGSI y es necesario contar con estos documentos aplicables a la entidad actualizados, para lo cual se deberá tener en cuenta y dar aplicación en cada materia respectiva, el cuadro de normas.

5.3.1.3. Definir el alcance del SGSI

El alcance es una manera de acotar los límites del SGSI en términos de las características organizacionales tales como las sedes, las funciones claves de negocio, los activos clave y las tecnologías que estarán cubiertas por el SGSI. En organizaciones grandes y diversas, es posible definir múltiples SGSI agrupados por funciones o ubicaciones para mantenerlos manejables.

Como se ilustra en la figura 8, se trata de un documento formal que será parte de la auditoría, revisión y mejora.

5.3.1.4. Definir la política de la seguridad de la información

La política del SGSI es un documento de alto nivel que aborda la necesidad de un sistema de gestión para la seguridad de la información. Esta intenta transmitir el quién, qué, por qué, cuándo y cómo, alrededor de la intención de la política del SGSI.

Una buena política en concisa, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. Son cortas, y enmarca los principios que guían las actividades dentro de la entidad.

La política viene como una plantilla definida desde SASIGEL, y será adaptada a las condiciones específicas y particulares de cada entidad según corresponda para que sean aprobadas por la entidad, según lo detalla el Anexo 5 del modelo.

5.3.1.5. Análisis del riesgo.

Abordar la seguridad de la información mediante una aproximación del riesgo, permite contar con una forma objetiva y alineada con las entidades para reconocer y reducir el riesgo existente a los activos de información. A través de las siguientes etapas, se logra dicho objetivo.

Como se ilustra en la figura 8, se trata de un documento formal que será parte de la auditoría, revisión y mejora.

5.3.1.5.1. Definir la aproximación para la gestión del riesgo.

La gestión del riesgo requiere de la selección y aplicación de una metodología clara, sistemática, objetiva, repetible que se ajuste a la entidad. Independientemente del método seleccionado, este le permitirá:

- Evaluar el riesgo basado en los niveles de confidencialidad, integridad y disponibilidad.
- Definir los objetivos para reducir el riesgo a un nivel aceptable.
- Evaluar las opciones de tratamiento del riesgo.

Si no cuenta con una metodología para la gestión del riesgo, puede consultar y utilizar la metodología existente en el Anexo No. 6 – Metodología de gestión del riesgo.

Algunos ejemplos de metodologías son: ISO/IEC 13335, NIST SP 800-30, ISO/IEC 27005.

5.3.1.5.2. Identificación de activos

Los activos incluyen las funciones de negocio clave, el personal clave, la infraestructura clave que soporta al personal clave (TI, edificios, propiedades, programas, equipos), información de valor para la entidad, reputación de la entidad.

Actividad: Consultar la metodología de clasificación de activos existente, en el Anexo No. 7 – Metodología de clasificación de activos.

5.3.1.5.3. Identificar los riesgos

La metodología guiará hacia la identificación de amenazas potenciales y vulnerabilidades para cada activo, y los niveles de confidencialidad, integridad y disponibilidad de los activos.

Si no cuenta con una metodología para la gestión del riesgo, puede consultar la metodología de gestión de riesgos existente, en el Anexo No. 6 – Metodología de gestión del riesgo.

5.3.1.5.4. Analizar el riesgo, en contexto de los objetivos de la entidad y de las partes interesadas[5]

En esta etapa, se asignarán valores a los riegos para poder saber cuáles son los más relevantes, los más críticos, los más prioritarios y cuales se pueden tolerar de acuerdo a su impacto y otras métricas dependiendo de la metodología.

Si no cuenta con una metodología para la gestión del riesgo, puede consultar la metodología de gestión de riesgos existente, en el Anexo No. 6 – Metodología de gestión del riesgo.

Como se ilustra en la figura 8, se trata de un documento formal que será parte de la auditoría, revisión y mejora.

5.3.1.6. Enumerar las opciones para el tratamiento/reducción del riesgo (selección de controles)

Todas las metodologías para la gestión del riesgo, permiten orientar que los resultados permitan la selección de controles que ayuden a reducir el riesgo eficazmente.

Es posible utilizar el conjunto de controles existente en el Anexo No. 8 – Controles de seguridad", del modelo de seguridad actual, como el conjunto de controles disponibles para realizar esta actividad.

Otros conjunto de controles adicionales existentes son ISO 27002, NIST SP-800-53.

Como se ilustra en la figura 8, se trata de un documento formal que será parte de la auditoría, revisión y mejora.

[5] Cabe aclarar en este punto que las entidades del Estado pueden hacer uso de las directrices que sobre gestión de riesgo se han definido dentro del marco de operación del Sistema de Control Interno para las entidades del Estado Regidas por la Ley 87 de 1993 – MECI, del marco expresado por la Norma Técnica Colombiana para Gestión del Riesgo NTC 5254 o pueden referirse a la Metodología de Gestión de Riesgo.

5.3.1.7. Plan de tratamiento del riesgo

En esta etapa se debe aprobar los objetivos de control y controles a implementar con el fin de tratar los riesgos identificados. En el documento resultante se debe contar con:

- El método aplicable para cada riesgo: aceptar, reducir, transferir o eliminar.
- Listado de controles actualmente implementados.
- Controles adicionales propuestos
- Espacio de tiempo en el cual los controles propuestos serán implementados.

Los ajustes que considere necesarios, previos a la aprobación, se realizará por la dirección, quien será la responsable de la aceptación del riesgo residual y de suministrar los recursos para la implementación del plan de tratamiento del riesgo.

Como se ilustra en la figura 8, se trata de un documento formal que será parte de la auditoría, revisión y mejora.

5.3.1.8. Generar el DDA - Declaración de aplicabilidad

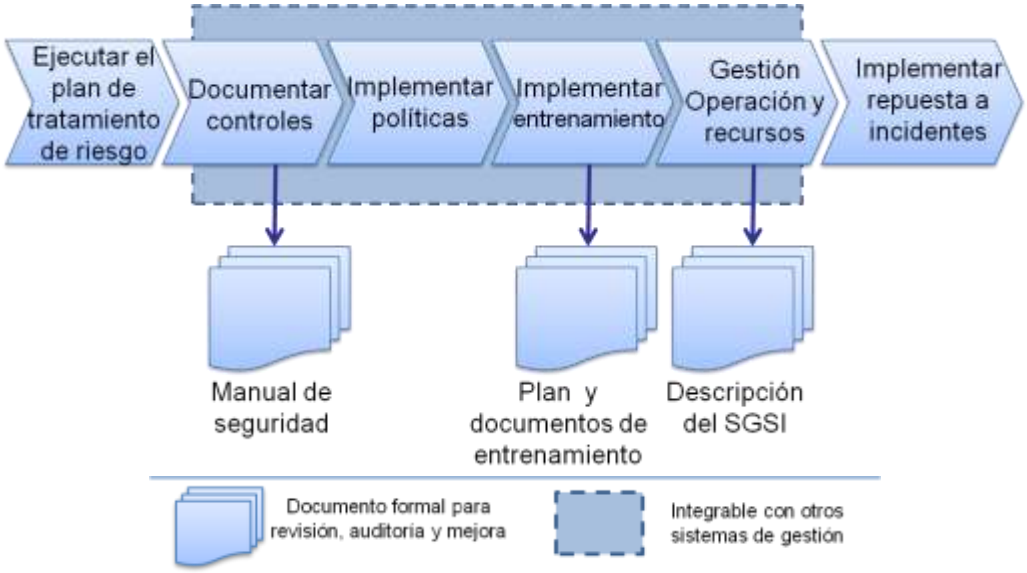
La declaración de aplicabilidad es un documento orientado a aquellas entidades que deseen dar cumplimiento al estándar NTC:ISO/IEC 27001:2005, y optar por una futura certificación. Este documento condensa el compromiso aceptado por la dirección con respecto a los controles que serán aplicados, respecto al total de controles existentes en el conjunto de controles utilizados y se justifica cada una de las excepciones. Este proceso ayuda a que la auditoría tenga un sólido punto de partida en la verificación de controles y de compromisos aceptados por la entidad y su dirección.

5.3.2. Hacer (Nivel básico de madurez)

Este capítulo se detalla cómo llegar al nivel de madurez básico propuesto por el Manual de Gobierno en línea 3.0, para ello es necesario que las entidades recorran un camino en donde comiencen por ejecutar el plan de tratamiento de riesgos y terminen con la implementación de los procedimientos, tal como lo muestra la figura 9.

Los elementos cubiertos por las áreas sombreadas generalmente son comunes a otros sistemas de gestión y pueden ser integrados para apalancarse y unir esfuerzos.

Figura 9 - Fase Hacer – Nivel básico



5.3.2.1. Implementar el plan de tratamiento del riesgo

El plan creado previamente enumera los riesgos e identifica las responsabilidades en la entidad para atender dicho riesgo y moverse de una posición estratégica a una operativa, es así como esta fase da inicio por parte de la entidad.

Para lograrlo en las siguientes sub secciones, se crean políticas detalladas de los controles seleccionados, estándares y procedimientos para estos mismos. Durante el proceso se prefiere mantener una trazabilidad al conjunto de controles, manteniendo la numeración y haciendo referencia al documento original.

5.3.2.2. Documentar los controles del SGSI.

La realización de políticas detalladas, procedimientos, estándares guías de implementación y de medición del desempeño de los controles seleccionados permite contar con la documentación de los controles. Durante la redacción de las políticas y procedimientos, se puede considerar las siguientes preguntas como ayudas para sustentar la elección y fin último del control:

- ¿Por qué el control fue seleccionado?
- ¿Quién es el responsable por la selección del control, su implementación y verificación de cumplimiento?
- ¿Cómo se implementa el control, como se verifica su cumplimiento?
- ¿Cuándo se implementa el control, cuando se verifica su cumplimiento?
- ¿Qué mediciones y métricas alimentan un reporte de actividad u otro reporte que muestre su uso, uso eficaz de la seguridad?

Una vez los documentos estén escritos, quien redacta debe considerar los siguientes puntos, estos ayudaran a que el documento sea claro, conciso y realizable para proteger la información de la entidad y sus activos de información:

- ¿Son las políticas y procedimientos claros y realistas? ¿Son facilmente interpretables?
- ¿Son demasiado largos?
- ¿Las políticas y procedimientos proveen suficiente guía? ¿Son accionables?
- ¿Están todas las partes del control incluidas en las políticas, estándares y procedimientos?
- ¿hay algún mecanismo para la medición de la eficacia de las políticas con ayuda de los procedimientos?
- ¿Cuál es la meta de desempeño? ¿Está claramente descrita dicha meta?
- ¿Qué se puede medir? ¿Cómo se puede medir? ¿Está presentado de una manera adecuada?
- ¿Hay una fecha de publicación en el documento?
- ¿Está presente la última fecha de revisión en el documento?
- ¿Es claro quién es el responsable del mantenimiento del documento?

5.3.2.2.1. Definir las métricas y medidas para medir el desempeño del SGSI orientadas a la implementación de la Estrategia de Gobierno en línea.

La razón para tener métricas en el sistema es poder tener una medición objetiva del desempeño de los controles, que ayuden a conocer su eficacia y a su vez, mediante una combinación de diferentes indicadores, generar una medición del sistema en su totalidad, que le permita a la entidad conocer el nivel de preparación y eficacia lograda en su gestión del riesgo, y a su paso reportar a cada funcionario interesado en términos de sus propios intereses (director, coordinador, líder, ingeniero, técnico).

Un conjunto de indicadores, Anexo No. 9 – Indicadores de seguridad, se ha puesto a disposición como punto de referencia inicial de algunas métricas de interés. Que pueden ayudar a aclarar la manera como Gobierno en línea evalúa la implementación del Modelo de Seguridad de la Información de manera global.

Las métricas son reportadas a SASIGEL, con el fin de contar con el monitoreo de todas las entidades, más fluido y dinámico que con auditorías anuales o semestrales.

5.3.2.3. Implementar políticas y controles de seguridad de la fase de planeación

La implementación de las políticas y los controles obedece a aquellos validados por la dirección. En esta etapa es importante recordar la cultura dentro de la entidad para las políticas, y las funcionalidades que son realmente requeridas de los controles y por las cuales se decidió implementar un control. La guía de los fabricantes, el entrenamiento y los posibles canales de ayuda y soporte, proveen una ruta hacia la implementación y despliegue de los controles de seguridad, y procedimientos asociados. Algunos procedimientos están disponibles en el anexo 11 "Ejemplo de procedimientos y estándares más usados".

Como se ilustra en la figura 9 se trata de un documento formal conocido como el manual de seguridad que será parte de la auditoría, revisión y mejora.

Nota: La protección de los documentos que conforman el SGSI, es muy importante. Estos documentos contienen detalles sensibles sobre la operación de seguridad y la postura de la entidad. Asegúrese de proteger la distribución a las personas adecuadas y el almacenamiento de estos documentos.

5.3.2.4. Implementar los planes de concientización y entrenamiento

Esta etapa se enfoca en dotar con las herramientas de conocimiento necesarias a los diferentes actores (ver figura 7) que interactúan con información de la entidad, para que respondan de una manera responsable a los retos diarios correspondientes a la protección de los activos de información que manejen.

- Concientización a los funcionarios, terceros y usuarios para que conozcan los riesgos y la manera como ellos pueden ayudar a la entidad a evitar pérdidas reportando las anomalías que identifiquen.
- Entrenamiento más detallado y educación, será brindado para los funcionarios que hacen parte del área de seguridad con el fin de tener bases más sólidas no solo para conocer sobre seguridad, sino para trabajar y aplicar sus conocimientos en el día a día.
- Este es un componente fundamental para contar con un sistema útil que madure con el apoyo de todos los participantes. Si se contempla dentro de las métricas, permite enriquecer el progreso de los programas en la entidad incluyendo:

    - Concientización: número de correos enviados para las campañas, resultados de las pruebas de conocimiento, resultados de participación en eventos.
    - Entrenamiento: número de seminarios atendidos, número de profesionales certificados en productos de seguridad.
    - Educación: número de profesionales con estudios en disciplinas relacionadas con seguridad, número de profesionales con credenciales en seguridad (nuevas y renovadas).

Como se ilustra en la figura 9 se trata de un documento formal conocido como el plan de entrenamiento que será parte de la auditoría, revisión y mejora.

5.3.2.5. Establecer y gestionar la operación del SGSI y sus recursos (documentación de procedimientos)

Posterior a la implementación inicial del SGSI, se continúa con la operación para mantener niveles aceptables de confidencialidad, integridad y disponibilidad de la información y sistemas de información. Esto requiere de la adecuada asignación de recursos, incluyendo, profesionales calificados y las herramientas necesarias para lograr el plan de acción propuesto.

La gestión de operaciones incluye contratación de personal, gestión de personal, adquisición de herramientas, y herramientas de gestión.

Aquí se debe documentar los procedimientos de las actividades de operación, incluyendo:

- Descripciones del perfil para cada función. (Experiencia requerida)
- Inventario de habilidades. (Experiencia existente)
- Procedimientos para la gestión del cambio

- Procedimientos para asignación de personal (segregación de responsabilidades)
- Procedimientos para la implementación de herramientas
- Procedimientos para la operación de herramientas.

También se incluye la definición e implementación de los procesos para la identificación de acciones preventivas y correctivas dentro de la operación del sistema durante su ejecución, las cuales son solucionadas durante la fase de actuar.

Como se ilustra en la figura 9, se trata de un conjunto de documentos utilizables durante la revisión y mejora, con el fin de demostrar que es repetible y produce resultados consistentes.

5.3.2.6. Implementar la infraestructura de repuesta a incidentes

La preparación incluye, la creación de una política, procedimientos, infraestructura, y herramientas que soporten lo siguiente con respecto a incidentes:

- Monitoreo
- Detección
- Notificación
- Escalación
- Respuesta
- Aislamiento
- Restauración
- Análisis de la causa raíz
- Retroalimentación a la entidad.

Las entidades pueden encontrar mayor detalle, capacitación y sensibilización sobre la implementación del equipo de respuesta a incidentes de seguridad informática - CSIRT de la entidad, a través de colCERT[6].

5.3.3. Verificar (Nivel avanzado de madurez)

Este capítulo se detalla cómo llegar al nivel de madurez avanzado propuesto por el Manual de Gobierno en línea 3.0, para ello es necesario que las entidades recorran un camino en donde se inicia por empatar con la fase anterior, donde se ejecuta el plan operacional, y este queda documentado con lo realizado en la sección anterior, el cual es revisado de manera regular, y termina con el registro de impacto en el SGSI, tal como lo muestra la 10.

[6] Centro de Respuesta a Emergencias Cibernéticas de Colombia - colCERT

Los elementos cubiertos por las áreas sombreadas generalmente son comunes a otros sistemas de gestión y pueden ser integrados para apalancarse y unir esfuerzos.

Figura 10 - Fase Verificar – Nivel avanzado

5.3.3.1. Revisiones regulares de eficacia

La implementación del SGSI es revisada de manera regular realizando las siguientes tareas:

5.3.3.1.1. Monitorear y revisar políticas, estándares, procedimientos, y prácticas

De manera periódica se contará con el monitoreo de la ejecución del plan operacional existente, de acuerdo a las métricas definidas. En general se debe crear un cronograma en el que se tengan planeados o en cola para futuras reuniones, las revisiones a los diferentes componentes del SGSI.

5.3.3.1.2. Revisar la eficacia de las operaciones de seguridad usando métricas y mediciones (medida objetiva de la eficacia)

Las métricas que permiten medir la eficacia del SGSI, son revisadas con el fin de medir la eficacia de la operación del SGSI obtenida con respecto a las metas planteadas y tener los resultados de la revisión como un insumo para la identificación de futuras mejoras en el desempeño de los controles y por ende del SGSI.

5.3.3.2. Revisar el nivel del riesgo residual

La revisión de ese nivel de riesgo que la dirección de la entidad ha aceptado en la etapa inicial, es importante especialmente para evitar que el nivel de riesgo residual se eleve a nivel no aceptable durante el tiempo de operación del SGSI. La razón es que en un ambiente dinámico, nuevas vulnerabilidades aparecen, y el entorno del negocio cambia rápidamente. Esta revisión brinda la oportunidad de contemplar

estos nuevos retos, nuevas amenazas, nuevos controles y horizontes dentro de la gestión del riesgo que se realiza.

Como se ilustra en la figura 10, se trata de un documento que será parte de la auditoría, revisión y mejora, con el fin de demostrar que es repetible y produce resultados consistentes.

5.3.3.3. Realizar auditorías internas

Se debe tener en cuenta lo establecido por La Ley 87 de 1993 por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado, así como las previsiones de la ley 489 de 1998.

La auditoría interna determina si las políticas y procedimientos existen. También se revisa la eficacia de las políticas y procedimientos. Algunas guías generales para la auditoría incluyen:

- Identificar los controles
- ¿Porqué se seleccionó un determinado control?
- ¿Quién es el responsable de la política escrita para ese control?
- ¿Existe una política?
- ¿Existe un procedimiento?
- ¿Se utiliza el procedimiento?
- ¿Quién es el responsable por implementar el procedimiento?
- ¿Quién es responsable de hacerle seguimiento a la eficacia del proceedimiento?
- ¿Existen métricas para trazar la eficacia de un procedimiento?
- ¿Cómo mide la persona responsable las métricas?
- ¿Qué reportes existen para hacerle seguimiento a la eficacia?

Como se ilustra en la figura 10, se trata de un documento que será parte de la auditoría, revisión y mejora, con el fin de demostrar que es repetible y produce resultados consistentes.

5.3.3.3.1. Realizar auditorías externas

La auditoría externa es una herramienta que puede ser utilizada por aquellas entidades que optan por la certificación, o desean que una entidad independiente con experiencia en auditoría de SGSI, o SASIGEL realice la revisión del SGSI. Estas auditorías pueden fundamentarse en la estructura definidas por el estándar ISO/IEC 27006 e ISO 19011.

Los resultados de estas auditorías permiten identificar las debilidades del SGSI de la entidad y aporta valor a sus acciones de mejora y evaluación de la eficacia del SGSI por parte de la dirección.

La estructura de auditoría se encuentra disponible en la sección 4.6.2.

5.3.3.4. Revisión de la dirección del SGSI.

Esta revisión se enfoca en la eficacia lograda por el SGSI, en términos de soportar los objetivos de la entidad. De las diversas entradas que preceden esta etapa, es posible identificar mejoras y refinamientos para el SGSI. Se crea un plan de revisión del SGSI, que provee entrada a la siguiente fase del ciclo de PHVA, la fase de actuar.

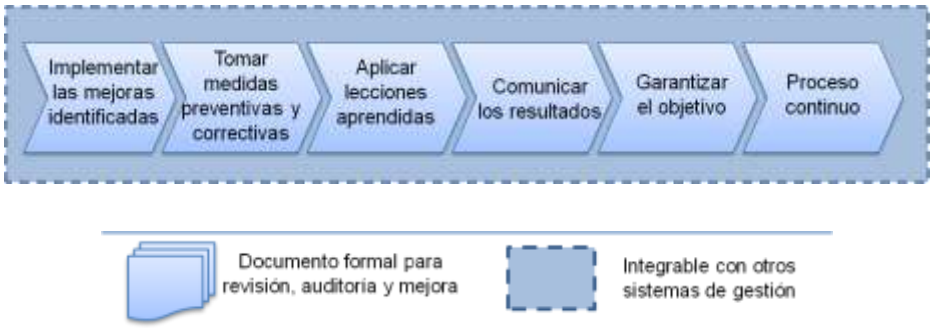
5.3.3.5. Registro del impacto en el SGSI.

El equipo de trabajo del comité de seguridad, utiliza el resultado de las revisiones de auditoría y de la dirección, para generar un plan de revisión del SGSI, donde se condensan los elementos a mejorar en el sistema de acuerdo a cambios en los objetivos de la entidad o el ambiente de operaciones. Este será utilizado para trabajar sobre la fase actuar.

5.3.4. Actuar (Nivel de madurez de mejora continua)

Este capítulo se detalla cómo llegar al nivel de madurez de mejora continua propuesto por el Manual de Gobierno en Línea 3.0, para ello es necesario que las entidades recorran un camino en donde comiencen por la implantación de mejoras identificadas en el nivel anterior y sigan en mejoramiento continuo, tal como lo muestra la figura 11.

Figura 11 - Fase Actuar – Nivel mejoramiento permanente



Los elementos cubiertos por las áreas sombreadas generalmente son comunes a otros sistemas de gestión y pueden ser integrados para apalancarse y unir esfuerzos.

5.3.4.1. Implementar las mejoras identificadas y aprobadas al SGSI en un nuevo ciclo

De la fase anterior se obtienen un conjunto de mejoras (las fuentes fueron el monitoreo, las auditorías internas, los ajustes de enfoque dados por la dirección y las auditorías externas), estas serán implementadas para fortalecer el SGSI.

5.3.4.2. Tomar medidas preventivas y correctivas

Durante la administración del SGSI, se han desarrollado procesos para la identificación de acciones preventivas y correctivas, en esta fase se toman estos elementos como entradas, para aplicarlas según correspondan para fortalecer el SGSI.

5.3.4.3. Aplicar las lecciones aprendidas

Como resultado de las revisiones periódicas del SGSI, la entidad empieza a generar lecciones aprendidas de las propias experiencias internas, su implementación refuerza al SGSI en la práctica.

5.3.4.4. Comunicar los resultados

De los cambios resultantes, es necesario reforzar el programa de concientización, entrenamiento y educación, para que los funcionarios y otros interesados, estén actualizados y preparados para seguir siendo parte fundamental del SGSI.

5.3.4.5. Proceso continuo y Gestión auto sostenible del modelo de las entidades

Una vez implementado el modelo, se da inicio a una fase en la que se realiza seguimiento y medición del funcionamiento del mismo, el cumplimiento de los objetivos que le dieron origen y los beneficios obtenidos durante el tiempo que lleve implementado y se toman una serie de acciones tendientes a mejorar el desempeño y la eficacia del modelo. Son actividades que pertenecen a esta etapa:

- Verificación del alcance del conjunto de políticas en la entidad
- Recopilación y análisis de los indicadores del modelo
- Análisis de estadísticas de incidentes de seguridad de la información en entidades del Estado
- Implementación de los ajustes

El mejoramiento continuo para las entidades, de acuerdo a los requisitos del Manual de Gobierno en línea 3.0, incluye:

- Reforzar la divulgación continua de políticas de seguridad.
- Gestión de controles (NTC:ISO/IEC 27001/27002)
    - Se ejecuta los procedimientos y políticas de seguridad, de manera repetitiva
    - Inventario de controles
    - Gestión de grado de implantación
    - Auditorías
- Realizar la revisión periódica interna de los riesgos inicialmente detectados, políticas, procedimientos y controles
    - Análisis de riesgos
        - Amenazas
        - Vulnerabilidades
        - Salvaguardas

- Gestión de documentación
  - Políticas
  - Lineamientos
  - Procedimientos
- Cuadro de mandos o control
  - Indicadores
  - Servicio de alertas y alarmas
  - Gestión de Informes

6. ANEXOS

Los siguientes documentos son recursos diseñados para que las entidades puedan implementar el Modelo de Seguridad de la Información.

Anexo No. 1 - Organigrama modelo y SASIGEL.

Este documento presenta la estructura orgánica del Modelo de Seguridad de la Información.

Anexo No. 2 - Encuesta de seguridad.

Este documento presenta un conjunto de preguntas que ayuda al levantamiento de la información de la infraestructura física, lógica y metodológica de seguridad de las entidades, como parte del estudio de la situación actual de cada una de ellas.

Anexo No. 3 - Estratificación de entidades.

Este documento presenta la estratificación de las entidades para la implementación del Modelo de seguridad.

Anexo No. 4 - Autoevaluación – definición de brecha

Este documento presenta un conjunto de herramientas de ayuda para medir de manera objetiva el nivel de implementación actual y da un listado de temas que componen la brecha con respecto a la Estrategia del Programa Gobierno en línea en cuanto a seguridad de la información.

Anexo No. 5 – Plantilla de política de seguridad para las entidades

Este documento contiene una plantilla de política de seguridad de la información del Sistema de Gestión de Seguridad de la Información, que las entidades pueden adaptar según sus objetivos estratégicos.

Anexo No. 6 – Metodología de gestión del riesgo

Este documento presenta una metodología para la gestión del riesgo al interior de las entidades del Estado en el marco del Programa de Gobierno en línea.

Anexo No. 7 – Metodología de clasificación de activos

Este documento presenta una metodología de clasificación de activos para las entidades del Estado en el marco del Programa Gobierno en línea.

Anexo No. 8 – Controles de seguridad

Este documento presenta el conjunto de políticas que deben ser cumplidas por las entidades y 133 controles recomendados para que la entidad genere el documento de aplicabilidad de controles para el Sistema de Gestión de Seguridad de la Información.

Anexo No. 9 – Indicadores de seguridad

Este documento presenta indicadores de seguridad, cuyo propósito es evaluar el estado de las entidades gubernamentales en materia de seguridad de la información, alineados con la Estrategia de Gobierno en línea.

Anexo No. 10 – Guía de implementación de políticas

Este documento presenta recomendaciones para la implementación de las políticas planteadas en el Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea.

Anexo No. 11 – Ejemplo de procedimientos y estándares más usados

Este documento presenta ejemplos de procedimientos y estándares más usados para la implementación de políticas y normas de seguridad de la información.

Anexo No. 12 – Correspondencia de estándares

Este documento presenta la correspondencia de estándares entre el Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea y otros de amplia utilización.

Anexo No. 13 – Tabla de contenido – Fase Plan

Este documento presenta la tabla de contenido para que las entidades sepan cómo estructurar el desarrollo de la fase "Plan" del ciclo PHVA planteado en el Modelo de Seguridad de la Información.

Anexo No. 14 – Tabla de contenido – Fase Hacer

Este documento presenta la tabla de contenido para que las entidades sepan cómo estructurar el desarrollo de la fase "Hacer" del ciclo PHVA planteado en el Modelo de Seguridad de la Información.

Anexo No. 15 – Tabla de contenido – Fase Verificar

Este documento presenta la tabla de contenido para que las entidades sepan cómo estructurar el desarrollo de la fase "Verificar" del ciclo PHVA planteado en el Modelo de Seguridad de la Información.

Anexo No. 16 – Tabla de contenido – Fase Actuar

Este documento presenta la tabla de contenido para que las entidades sepan cómo estructurar el desarrollo de la fase "Actuar" del ciclo PHVA planteado en el Modelo de Seguridad de la Información.