Gobierno en línea
·Colombia·

LINEAMIENTOS PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN 2.0

Gobierno en línea
Colombia

LINEAMIENTOS PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN 2.0.

Ministerio de Tecnologías de la Información y las Comunicaciones

Programa de Gobierno en línea
Francisco Camargo Salas – Gerente de Programa
Ana Carolina Rodríguez Rivero – Coordinadora Investigación, Políticas y Evaluación
Julio Cesar Mancipe Caicedo – Líder de Seguridad

Derechos de Autor
Ministerio de Tecnologías de la Información y las Comunicaciones
Programa de Gobierno en línea

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia

Bogotá, D.C., Diciembre de 2011

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Este documento busca proveer a las Entidades del Estado un conjunto de lineamientos de seguridad de la información para que la alta dirección de las entidades conozca los requisitos y etapas para la implementación del Modelo de Seguridad para la Estrategia de Gobierno en línea 2.0, abordando aspectos que cubren la preparación de la entidad, la definición de las brechas, la alineación y la implementación del SGSI como modelo sostenible.

1.1 Definiciones básicas

Para establecer un lenguaje común cuando se habla de seguridad de la información se recomienda adoptar los siguientes conceptos a los que hace referencia el presente documento.

Información: se refiere a toda comunicación o representación de conocimiento, como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea digital, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la información: se refiere al hardware y software operado por la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Seguridad de la información: se entiende como la preservación de las siguientes características:

- Confidencialidad: garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- Integridad: salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- Disponibilidad: garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una

transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones. disposiciones a las que está sujeto la entidad.
- **SGSI:** Sistema de gestión de Seguridad de la Información.
- **SASIGEL**: Sistema de Administración de Seguridad de la Información de Gobierno en Línea.

2. NOTA IMPORTANTE PARA LA DIRECCIÓN

Es importante tener en cuenta que para la implementación exitosa del Modelo de Seguridad de la Información es necesario contar con algunos pre-requisitos y requisitos que van a garantizar la permanencia y sostenibilidad del mismo.

2.1 Pre-requisitos

Antes de iniciar el proceso de implementación y adopción del modelo se hace necesario que la Entidad cuente con los siguientes requisitos:

- Contar con la estructura organizacional de Gobierno en línea. Para más detalle consultar el Anexo 1 del Modelo de Seguridad de la Información.
- Solicitar y recibir la capacitación para la implementación y reporte a SASIGEL descrita en el modelo en los numerales 4.5.1, 4.5.2, 4.5.3
- 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). Para que la Dirección tenga una alta participación se debe garantizar que los controles relacionados a los compromisos y responsabilidades de ella queden como obligatorios en la declaración de aplicabilidad de la entidad. Ver anexo 8.
- Cuando haya cambios en la dirección, comunicar la importancia de dar continuidad al SGSI y la aproximación de "arriba-a-abajo".
- Para las entidades que cuentan con otros sistemas de gestión implementados, reforzar sobre los elementos que son comunes a otros sistemas de gestión y su posibilidad de integración y apalancamiento.
- No se debe asignar la responsabilidad de manera exclusiva al equipo de tecnologías de información y comunicación. En el numeral 4.2.1.2 del modelo se identifican los responsables que la entidad debe tener en el tema de seguridad de la información.

2.2 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:

- 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).

- La entidad debe contar con la política de seguridad, la cual debe estar alineadas con su misión y sus objetivos, se debe ajustar a la cultura corporativa, se debe articular con todas las áreas de la entidad para concertar sobre la definición del alcance, la creación y aplicación de políticas, procedimientos y aseguramiento de los procesos y servicios ofrecidos. Ver anexo 5 "Formato Política SGSI".
- Requerimientos de seguridad claramente articulados con las necesidades de la entidad. Los cuales deben surgir después de la identificación y clasificación de sus activos de información. Ver anexo 7 "Metodología de clasificación de activos".
- Realizar un análisis de riesgo que enlace los activos, su criticidad en términos de confidencialidad, integridad y disponibilidad, las amenazas, los riesgos, los requisitos normativos, legislativos y regulatorios, los controles implementados, los controles propuestos y el riesgo residual. Ver anexo 6 "Metodología de gestión de riesgo".
- 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). En el numeral 4.2.1.2.1 del modelo se definen los perfiles de los responsables de la entidad para este comité.
- Realizar concientización, entrenamiento y educación.
- Establecimiento de métricas para la evaluación del desempeño del SGSI que además sirvan para reportar a SASIGEL.

2.3 Requisitos

Los requisitos de seguridad con los cuales la entidad debe cumplir de acuerdo con el Manual de Gobierno en línea 3.0 y dónde puede consultar la implementación de dichos requisitos, se encuentran a continuación:

Tabla 1- Requisitos de Seguridad según el Manual de Gobierno en línea 3.0.

Nivel	Requisito	Consultar
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:	Anexo 5 del modelo. "Formato de política de seguridad"
	Identificar el nivel de conocimiento al interior, en temas de seguridad de la información y seguridad informática	Numeral 5.2.2 del modelo
	Definir la política de seguridad a ser implementada.	Anexo 5 del modelo. "Formato de política de seguridad"

Nivel	Requisito	Consultar
Plan de Seguridad Nivel Inicial	Divulgar la política de seguridad al interior de la misma	Numerales 4.5.1, 4.5.2 y 4.5.3 del modelo
	Conformar un comité de seguridad o asignar las funciones de seguridad al comité GEL.	Numeral 5.2.1.2 del modelo
	Identificar los activos de información en los procesos, incluyendo los activos documentales (records), de acuerdo con el análisis de procesos realizado.	Anexo 7 del modelo. "Metodología de clasificación de activos"
	Identificar los riesgos y su evaluación, en dichos procesos	Anexo 6 del modelo. "Metodología de gestión de riesgos"
	Definir el plan de acción con los controles y políticas que se implementarán para mitigar los riesgos identificados.	Numerales 5.3.1.8 y 5.3.1.9 del modelo
Plan de Seguridad Nivel básico	Con base en el análisis de procesos realizados 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.	Numeral 5.3.2 del modelo
	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.	Numeral 5.3.2.4 del modelo
	La entidad inicia la documentación de políticas y procedimientos de seguridad, de acuerdo con el plan definido.	Revisar el modelo de seguridad donde indica que actividades la entidad debe documentar.
Plan de Seguridad Nivel avanzado	La entidad culmina la implementación de controles definidos en el nivel inicial	Numeral 5.3.2 del modelo
	La entidad documenta la totalidad de políticas y procedimientos de seguridad	Revisar el modelo de seguridad donde indica que actividades la entidad debe documentar.
	La entidad ejecuta las actividades de capacitación en temas de seguridad, con todos los servidores públicos	Numerales 4.5.1, 4.5.2 y 4.5.3 del modelo
	La entidad define el plan de verificación periódica de los controles, procedimientos y políticas de seguridad	Numeral 5.3.4 del modelo
	La entidad reporta los avances del cumplimiento del plan	Numeral 5.3.4.5 y 5.3.4.6 del modelo

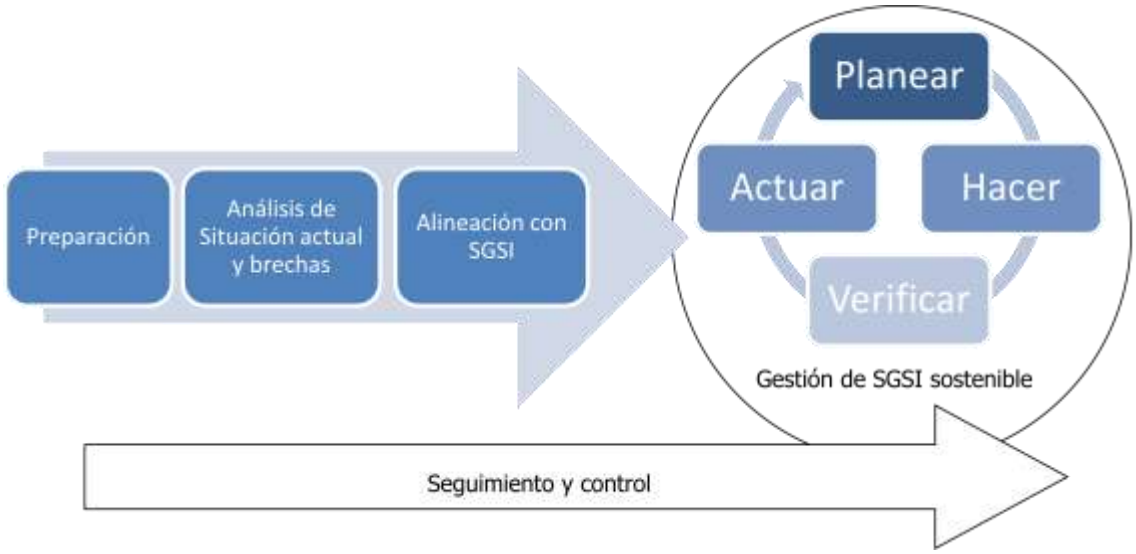
Nivel	Requisito	Consultar
Plan de Seguridad Nivel de mejoramiento permanente	La entidad refuerza la divulgación de las políticas de seguridad	Numerales 4.5.1, 4.5.2 y 4.5.3 del modelo
	La entidad ejecuta los procedimientos y políticas de seguridad, de manera repetitiva	Numeral 5.3.5 del modelo
	La entidad realiza la revisión periódica interna de los riesgos inicialmente detectados, políticas, procedimientos y controles	Numeral 5.3.5 del modelo
	La entidad evalúa sus políticas de seguridad e implementa acciones para mejorarlas	Numeral 5.3.5.1 del modelo

3. LINEAMIENTOS DE IMPLEMENTACIÓN

Para garantizar una adecuada implementación del Modelo de Seguridad de la Información en las entidades del Estado se plantea una estrategia de trabajo que está estructurada en cinco (5) lineamientos básicos de la implementación del modelo, los cuales están alineados con los niveles de madurez del Manual GEL 3.0.

El plan de implementación se enfoca en que las entidades deben identificar el nivel actual de madurez que han desarrollado en cuanto a seguridad de la información y a partir de esta identificación, iniciar un ciclo PHVA sostenible, tal como muestra la figura 1.

Figura 1 - Plan de Implementación del Sistema de Gestión de Seguridad de la Información en las entidades



3.1 Lineamiento: Identificar el Nivel de Madurez en Seguridad de la Entidad.

Antes de iniciar la implementación del Modelo de seguridad propuesto por Gobierno en línea se hace necesario que las entidades identifiquen el nivel de madurez en el cual se encuentran, para ello se definen objetivos, actividades y duración, tal como se desarrolla a continuación.

3.1.1 Objetivos lineamiento para identificar nivel de madurez en las entidades

Los objetivos para que la entidad identifique el nivel de madurez de seguridad en que se encuentra son los siguientes:

- Sensibilizar a la entidad en cuanto a la importancia de la seguridad de la información.
- Conocer los perfiles y responsabilidades de la seguridad de cada personaje al grupo de trabajo.
- Identificar las personas idóneas para desempeñar los roles de seguridad.
- Definir la situación actual de la entidad en cuanto a seguridad de la información.
- Alinear la entidad al Sistema de Gestión de Seguridad de la Información propuesto por el modelo.

3.1.2 Actividades lineamiento para identificar nivel de madurez en las entidades.

Las actividades tenidas en cuenta para que la entidad identifique su nivel actual de madurez en seguridad son las siguientes: preparación, análisis de la situación actual y brechas y 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. Consultar capítulo 3 del modelo.

3.1.2.1 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 cuenten con las siguientes actividades completadas, para iniciar con esta etapa. Las actividades son:

- "Formación de Capacitadores" descrita en la sección 4.5.3 del modelo,
- "Campaña de Sensibilización a las entidades públicas y privadas" descrita en la sección 4.5.2.1 del modelo y

- "Plan de capacitación para las entidades públicas" descrita en la sección 4.5.2.2 del modelo, 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:

3.1.2.1.1 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 (ver tabla 1) los cuales la entidad debe cumplir de acuerdo con el Manual GEL 3.0, una vez el SGSI está implementado y en operación.

3.1.2.1.2 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.

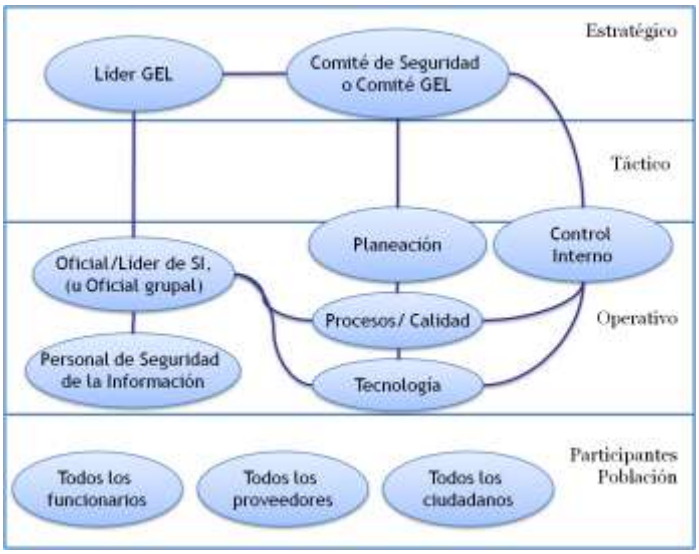
3.1.2.1.2.1 Perfiles y responsabilidades

Se deben dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol. Consultar el Anexo No. 1 - Organigrama modelo y SASIGEL.", el numeral "3.7 Equipo de gestión al interior de cada una de las entidades" del modelo de seguridad de la Información de Gobierno en línea donde se encuentran definidas las responsabilidades.

El sistema cuenta con la interacción los siguientes perfiles y su interrelación es mostrada en la figura 1:

- Comité de seguridad. Las funciones de este comité pueden ser tomadas por comité de GEL, de acuerdo al Manual GEL 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.

Figura 2 – Actores SGSI.



3.1.2.2 Análisis de la situación actual y definición de brechas

Esta actividad se enfoca en tener un conocimiento inicial de la situación que presenta la entidad frente al modelo de seguridad y los lineamientos del manual GEL 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). 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.

3.1.2.2.1 Aplicar la encuesta

La encuesta se plantea para realizar el diagnóstico actual de la entidad. Para esta actividad, consultar y aplicar el documento de encuesta del Anexo No. 2 - Encuesta de seguridad. Los resultados serán utilizados para la definición de brecha.

3.1.2.2.2 Definir nivel de madurez

De acuerdo a los lineamientos del Manual GEL 3.0, cada entidad tiene un nivel de madurez inicial y una ruta a seguir, con unos requerimientos para cada nivel. La tabla 1 contiene los requerimientos transversales de seguridad presentes en el Manual.

Se debe realizar la autoevaluación con respecto a los niveles de seguridad transversales definidos en el Manual GEL 3.0, utilizando los formatos del

Anexo No. 4 - Autoevaluación – definición de brecha, del modelo.

3.1.2.2.3 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 GEL 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 la actividad 3.1.2.1.2.1 de este documento.
- Revisión por niveles de madurez de acuerdo a los requisitos definidos en la tabla 1.
- 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.

3.1.2.3 Alineación con el SGSI

Esta actividad debe estar alineada con 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.

Una vez la entidad ha sido alineada con los requisitos del Manual GEL 3.0, entra en el ciclo PHVA del SGSI. Dependiendo de su madurez, es posible que la entidad se encuentre en las siguientes fases:

- 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.

3.1.2.3.1 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 la actividad definición de brechas 3.1.2.2.3.

Como resultado, la entidad contará con la alineación de su sistema, con los requisitos del

Manual GEL 3.0 y entrará en el ciclo PHVA del SGSI.

3.1.3 Duración para la implementación del Lineamientos identificar nivel de madurez en las entidades

Las entidades deben identificar el nivel de madurez en seguridad en un periodo no mayor a 2 meses.

3.2 Lineamiento: Llevar a la Entidad a un Nivel de Madurez Inicial en Seguridad.

Dependiendo del nivel de madurez en seguridad identificado por la entidad, ésta entrará a la fase planear. Para este escenario, se define este lineamiento que consta de objetivos, actividades y duración que llevarán a la entidad a completar un nivel de madurez básico, tal como se desarrolla a continuación.

3.2.1 Objetivos Lineamiento Nivel Inicial

Los objetivos para llevar a la entidad a un nivel de madurez inicial en seguridad, según los requisitos del manual GEL 3.0 son los siguientes:

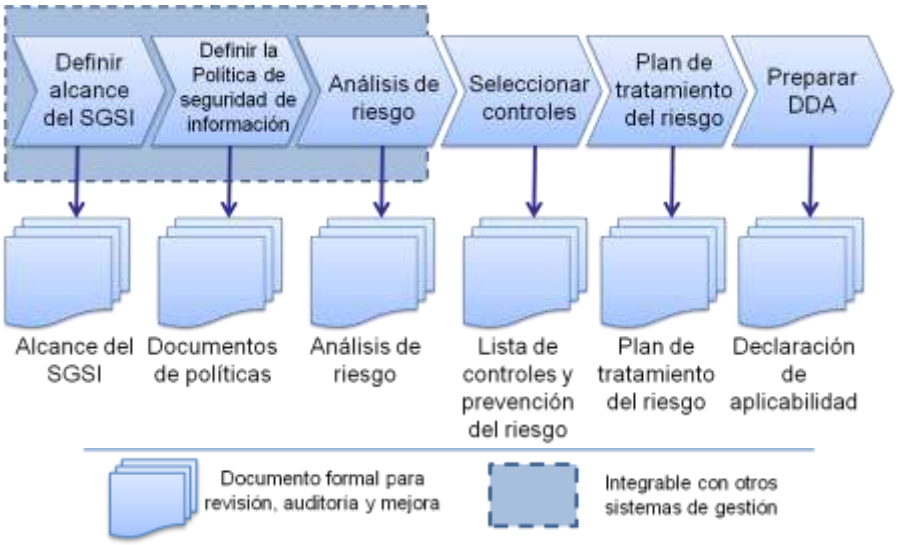
- Definir la política de seguridad a ser implementada.
- Divulgar la política de seguridad al interior de la misma.
- Conformar un comité de seguridad o asignar las funciones de seguridad al comité GEL.
- Identificar los activos de información en los procesos, incluyendo los activos documentales (records), 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.

3.2.2 Actividades Lineamientos Nivel Inicial

Este lineamiento detalla cómo llegar al nivel de madurez inicial propuesto por el Manual GEL 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 3. Los elementos cubiertos por las áreas sombreadas generalmente son comunes a otros sistemas de gestión y pueden ser integrados para apalancarse y unir esfuerzos, por lo tanto la entidad puede basarse de otros sistemas de gestión en dichas actividades.

Las actividades que tienen relacionadas documentos en la figura 3, la entidad debe documentarlos y realizarles actualizaciones periódicas, ya que son formales y son el insumo para las auditorías internas y externas, y para el mejoramiento continuo del SGSI.

Figura 3 – Actividades para la fase Planear – Nivel Inicial de Madurez.



3.2.2.1 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.

3.2.2.2 Definir la política del SGSI

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.

El Modelo de seguridad de la información en su anexo 5, propone un ejemplo de política de seguridad; de ser adoptada por la entidad, debe adaptarse a las condiciones específicas y particulares de ella según corresponda, para que sean aprobadas por la entidad (cuando se habla de aprobación por la entidad, se debe garantizar que la dirección y la alta gerencia firmen este documento y se comprometan con lo que esta política conlleva).

3.2.2.3 Análisis de riesgo

El modelo de seguridad de la información lo que busca es abordar la seguridad de la información mediante una aproximación del riesgo, reconociendo y reduciendo el riesgo existente a los activos de la entidad de una forma objetiva y alineada. A través de las siguientes etapas, se logra dicho objetivo.

3.2.2.3.1 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 la entidad no cuenta con una metodología para la gestión del riesgo, puede consultar y utilizar la metodología existente en el Este documento presenta una plantilla de política de seguridad de la información que las entidades pueden adaptar según sus objetivos estratégicos. **Anexo No. 6 – Metodología de gestión del riesgo**.

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

3.2.2.3.2 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.

Si la entidad no cuenta con una metodología para clasificación de activos, puede consultar el Anexo No. 7 – Metodología de clasificación de activos.

3.2.2.3.3 Identificar los riesgos

La metodología adoptada por la entidad, sugeridas en el numeral 3.2.2.3.1, la guiará identificación de amenazas potenciales y vulnerabilidades para cada

activo, y los niveles de confidencialidad, integridad y disponibilidad de los activos.

3.2.2.3.4 Analizar el riesgo, en contexto de los objetivos de la entidad y de las partes interesadas.

La entidad debe asignar 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 Este documento presenta una plantilla de política de seguridad de la información que las entidades pueden adaptar según sus objetivos estratégicos. **Anexo No. 6** o las sugeridas en el numeral 3.2.2.3.1.

3.2.2.4 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, como el conjunto de controles disponibles para realizar esta actividad.

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

3.2.2.5 Plan de tratamiento del riesgo.

En esta actividad la entidad 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.

3.2.2.6 Preparar declaración de aplicabilidad

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.

3.2.3 Duración para la implementación del Lineamientos Nivel Inicial

Las entidades deben implementar el lineamiento nivel inicial de madurez en seguridad en un periodo no mayor a 4 meses.

3.3 Lineamiento: Llevar a la Entidad a un Nivel de Madurez Básico en Seguridad.

Dependiendo del nivel de madurez en seguridad identificado por la entidad, ésta entrará a la fase hacer. Para este escenario, se define este lineamiento que consta de objetivos, actividades y duración que llevarán a la entidad a completar un nivel de madurez básico, tal como se desarrolla a continuación.

3.3.1 Objetivos Lineamiento Nivel Básico

Los objetivos para llevar a la entidad a un nivel de madurez básico en seguridad, según los requisitos del manual GEL 3.0 son los siguientes:

- Iniciar la ejecución del plan de seguridad definido por la entidad en el nivel inicial, para implementar los controles que mitigarán los riesgos identificados, lo cual implica que la entidad presenta avances en la implementación de tales controles.
- Ejecutar el plan de capacitación definido por la entidad en el nivel inicial. La entidad debe ejecutar las acciones de capacitación en seguridad, con los responsables de los controles y procesos con los cuales se inicia la ejecución del plan.
- Iniciar la documentación de políticas y procedimientos de seguridad, de acuerdo con el plan definido en el nivel inicial.

3.3.2 Actividades Lineamientos Nivel Básico

Este lineamiento detalla cómo llegar al nivel de madurez básico propuesto por el Manual GEL 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 4.

Los elementos cubiertos por las áreas sombreadas generalmente son comunes a otros sistemas de gestión y pueden ser integrados para apalancarse y unir esfuerzos, por lo tanto la entidad puede basarse de otros sistemas de gestión en dichas actividades.

Las actividades que tienen relacionadas documentos en la figura 4, la entidad debe documentarlos y realizarles actualizaciones periódicas, ya que son formales y son el insumo para las auditorías internas y externas, y para el mejoramiento continuo del SGSI.

Figura 4 – Actividades para la fase Hacer – Nivel Básico de Madurez.

3.3.2.1 Ejecutar el plan de tratamiento de 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.

.

3.3.2.2 Documentar controles

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, piense sobre 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 fácilmente 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?

3.3.2.2.1 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, 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", 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.

3.3.2.3 Implementar política

Corresponde la implementación de aquellos controles validados por la dirección. En esta etapa es importante recordar las funcionalidades que son realmente requeridas 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.

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 y almacenamiento de estos documentos.

3.3.2.4 Implementar entrenamiento

Esta actividad se enfoca en dotar con las herramientas de conocimiento necesarias a los diferentes actores (identificados en la figura 2) 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.
- El entrenamiento es una herramienta 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).

3.3.2.5 Gestionar operación y recursos

Luego de la implementación inicial del SGSI, viene la posterior 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.

En esta actividad la entidad 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.

3.3.2.6 Implementar respuesta a incidentes

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

- 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

.

3.3.3 Duración para la implementación del Lineamientos Nivel Básico

Las entidades deben implementar el lineamiento nivel básico de madurez en seguridad en un periodo no mayor de 18 meses.

3.4 Lineamiento: Llevar a la Entidad a un Nivel de Madurez Avanzado en Seguridad.

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. Este lineamiento propone objetivos, actividades y duración que llevarán a la entidad a completar un nivel de madurez avanzado.

3.4.1 Objetivos Lineamiento Nivel Avanzado

Los objetivos para llevar a la entidad a un nivel de madurez avanzado en seguridad, según los requisitos del manual GEL 3.0 son los siguientes:

- Culminar la implementación de controles definidos en el nivel inicial.
- Documentar la totalidad de políticas y procedimientos de seguridad.
- Ejecutar las actividades de capacitación en temas de seguridad, con todos los servidores públicos.
- Definir el plan de verificación periódica de los controles, procedimientos y políticas de seguridad.
- Reportar los avances del cumplimiento del plan a SASIGEL.

3.4.2 Actividades Lineamientos Nivel Avanzado

Las siguientes actividades están organizadas de acuerdo a su uso en el ciclo PHVA, que permiten la alineación de la etapa verificar, correspondiente a un nivel de madurez avanzado.

Este lineamiento detalla cómo llegar al nivel de madurez avanzado propuesto por el Manual GEL 3.0, para ello es necesario que las entidades recorran un camino en donde comiencen por ejecutar el plan operacional y terminen con el registro de impacto en el SGSI, tal como lo muestra la figura 5.

Los elementos cubiertos por las áreas sombreadas generalmente son comunes a otros sistemas de gestión y pueden ser integrados para apalancarse y unir esfuerzos, por lo tanto la entidad puede basarse de otros sistemas de gestión en dichas actividades.

Las actividades que tienen relacionadas documentos en la figura 5, la entidad debe documentarlos y realizarles actualizaciones periódicas, ya que son formales y son el insumo para las auditorías internas y externas, y para el mejoramiento continuo del SGSI.

Figura 5 – Actividades para la fase Verificar – Nivel Avanzado de Madurez.

3.4.2.1 Ejecutar plan operacional.

De manera periódica se contará con el monitoreo de la ejecución del plan operacional existente, definido en las fases anteriores (implementación de controles, procedimientos, capacitaciones, entre otros), 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.

3.4.2.2 Revisiones regulares de eficiencia

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.

3.4.2.3 Revisión del nivel de riesgo residual.

En esta actividad se procede a la revisión de ese nivel de riesgo que la dirección de la entidad ha aceptado en la fase inicial, es importante especialmente para evitar que el nivel de riesgo residual se eleve a un 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 5, 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.

3.4.2.4 Auditoría interna al SGSI

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
- ¿Por qué 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 procedimiento?
- ¿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?

3.4.2.4.1 Realizar auditorías externas

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

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 procedimiento. También que cumple con los requisitos del SGSI y manual GEL 3.0 y está logrando los objetivos de la política de la entidad. Se debe enfocar en 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 decisiones de la dirección, la política del SGSI y los objetivos.

- La existencia del cronograma 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.

3.4.2.5 Revisión por 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.

3.4.2.6 Registrar impacto en el SGSI.

Como resultado de la revisión por parte de la dirección, se generan recomendaciones (Listas de acciones y eventos) al plan de tratamiento del riesgo que apuntan a disminuir los cambios de los niveles de riesgos residuales identificados en las primeras fases, lo cual impacta el plan de operación del SGSI. Este registrado y aprobado por la dirección para darle sostenibilidad al modelo.

3.4.3 Duración para la implementación del Lineamientos Nivel Avanzado.

Las entidades deben implementar el lineamiento nivel avanzado de madurez en seguridad en un periodo no mayor a 3 meses.

3.5 Lineamiento: Llevar a la Entidad a un Nivel de Madurez de Mejoramiento Permanente en Seguridad.

Dependiendo del nivel de madurez en seguridad identificado por la entidad, ésta entrará a la fase actuar. Para este escenario, se define este lineamiento que consta de objetivos, actividades y duración que llevarán a la entidad a completar un nivel de madurez de mejoramiento permanente, consiguiendo un Sistema de Gestión para la Seguridad de la Información sostenible y eficaz, tal como se desarrolla a continuación.

3.5.1 Objetivos Lineamiento Nivel Mejoramiento Permanente

Los objetivos para llevar a la entidad a un nivel de madurez avanzado en seguridad, según los requisitos del manual GEL 3.0 son los siguientes:

- Reforzar la divulgación de las políticas de seguridad.
- Ejecutar los procedimientos y políticas de seguridad, de manera repetitiva
- Realizar la revisión periódica interna de los riesgos inicialmente detectados, políticas, procedimientos y controles
- Evaluar las políticas de seguridad e implementa acciones para mejorarlas.

3.5.2 Actividades Lineamientos Nivel Mejoramiento Permanente

Este lineamiento detalla cómo llegar al nivel de madurez de mejora continua propuesto por el Manual GEL 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 6.

Los elementos cubiertos por las áreas sombreadas generalmente son comunes a otros sistemas de gestión y pueden ser integrados para apalancarse y unir esfuerzos, por lo tanto la entidad puede basarse de otros sistemas de gestión en dichas actividades.

Figura 6 – Actividades para la fase Actuar – Nivel Mejoramiento Permanente.

3.5.2.1 Implementar las mejoras identificadas

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.

3.5.2.2 Tomar medidas preventivas y correctivas

Por medio de las actividades de auditoria externas e internas, y los incidentes de seguridad, se identifican riesgos que requieren un tratamiento, ya sea correctivo o preventivo. Esto genera una retroalimentación al SGSI que debe tratarse en el próximo ciclo PHVA de implementación.

3.5.2.3 Aplicar 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.

3.5.2.4 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.

3.5.2.5 Garantizar el objetivo

Siempre que propongan mejoras al SGSI de la entidad, se debe tener en cuenta que las acciones preventivas y/o correctivas seleccionadas para mitigar los riesgos detectados en la retroalimentación, estén alineados al alcance y a la política seguridad definidas por la entidad en la fase inicial de implementación del SGSI.

3.5.2.6 Proceso Continuo

Luego de pasar por todas las actividades anteriormente descritas, la entidad debe iniciar

el ciclo PHVA desde su fase planear iniciando con la revisión de los siguientes documentos, garantizando que estén alineados a los cambios de entorno y nuevos niveles de riesgos de esta nueva etapa de la entidad.

- Documento de política de seguridad.
- Alcance del SGSI
- Revisión de los activos de información de la entidad.
- Revisión del riesgo residual.

3.5.3 Duración para la implementación del Lineamientos Mejoramiento Permanente

Las entidades deben implementar el lineamiento nivel mejoramiento permanente de madurez en seguridad en un periodo no mayor a 2 meses.

4. DOCUMENTOS DE CONSULTA

La entidad puede consultar los siguientes documentos para profundizar en la implementación de los lineamientos descritos en este documento.

Modelo de Seguridad de la Información de Gobierno en línea.

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.

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 presenta una plantilla de política 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 una guía de 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.

Gobierno en línea
·Colombia·

Gobierno en línea
Colombia