2025

METODOLOGÍA PARA EL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. INTRODUCCIÓN 2
2. OBJETIVOS 3
3. MARCO NORMATIVO 4
4. ENTENDIMIENTO ESTRATÉGICO 5
5. DIAGNÓSTICO 6
5.1. Análisis de situación actual 6
5.2. Arquitectura de seguridad SABSA 6
5.3. Oportunidades de mejora 8
6. ANÁLISIS ESTRATÉGICO DE LA POSTURA EN SEGURIDAD 9
6.1. Análisis estratégico 9
6.2. Análisis financiero 9
6.3. Análisis DOFA interno y externo 9
6.4. Definición de las estrategias del PESI 10
7. DEFINICIÓN DE LOS PROYECTOS PARA EL PESI 12
7.1. Priorización de proyectos definidos 12
7.2. Presupuestos requeridos 13
7.3. Definición de la hoja de ruta para los proyectos 13
7.4. Inversiones requeridas 14
7.5. Sistema de Gestión de la Seguridad de la información 14
8. TRANSFERENCIA DE CONOCIMIENTO Y COMUNICACIONES 16
8.1. Caracterización, concepto y diseño de estrategia 16
8.2. Definición de metodología 17
8.3. Material didáctico y presentaciones 17
8.4. Invitaciones a grupos de interes 17
8.5. Evaluación del conocimiento 17
9. SEGUIMIENTO Y CONTROL 18
9.1. Tablero de Indicadores de seguimiento 18
9.2. Caracterización y hoja de vida indicadores 18
10. CONCLUSIONES 19
11. GLOSARIO DE TÉRMINOS 20
12. BIBLIOGRAFÍA 21
13. ANEXOS 22

1. INTRODUCCIÓN

Este capítulo explica la metodología utilizada para desarrollar el documento Plan estratégico de Seguridad de la información PESI, como el documento que expone el diagnóstico realizado y los proyectos dentro de un marco temporal.

A continuación, se presenta el esquema metodológico recorrido para lograr desarrollar el PESI:

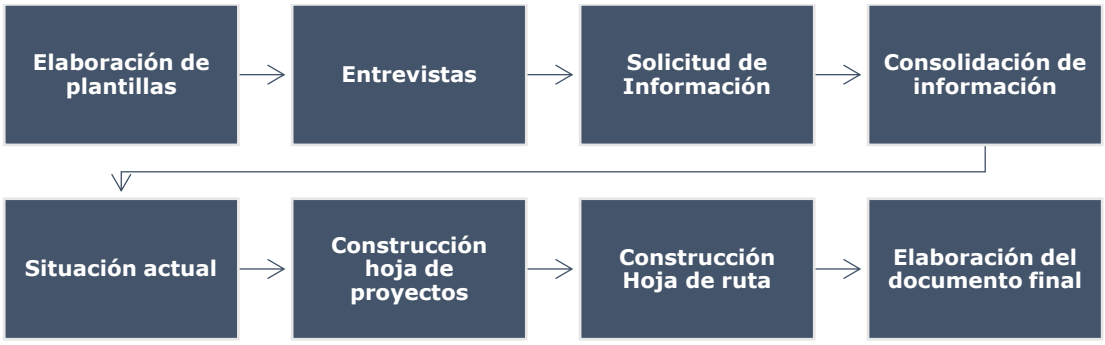

Figura No. 0. Metodología para elaboración de un PESI.

Elaboración de plantillas: en esta fase inicial de la construcción del documento PESI se define la estructura documental de los entregables del proyecto y también se consideran las metodologías que se utilizarán.

Entrevistas: se solicita la información que servirá de insumo para construir el PESI, con base en la identificación de las necesidades de información relacionadas con cada una de las fases para de construcción, con lo cual se constituye la línea base del entendimiento y comprensión del funcionamiento de la organización.

Solicitud de Información: se solicita la información que servirá de insumo para construir el PESI, con base en la identificación de las necesidades de información con lo cual se establece la línea base del entendimiento y comprensión del cumplimiento en seguridad de la información.

Consolidación de la información: en esta fase del documento PESI se agrupan todas las vulnerabilidades o debilidades encontradas para que más adelante se puedan establecer los proyectos.

Situación actual: conforme a lo establecido en el anexo de especificaciones técnicas de este contrato se realiza el análisis de situación actual o diagnostico el cual será utilizado en etapas posteriores para la construcción de la hoja de ruta.

Construcción hoja de proyectos: en esta etapa con base en la información suministrada por medio de las entrevistas y los insumos solicitados se procede a la construcción del catálogo de proyectos con su respectiva priorización.

Construcción hoja de ruta: en este paso, con base en los proyectos definidos estos se estructuran considerando su costo y el tiempo requerido de implementación.

Elaboración documento final: una vez realizadas todas las labores expuestas anteriormente se procede a ensamblar el documento PESI con base en los dos hitos principales de diagnóstico y de proyección de iniciativas. Este documento tendrá un control de versiones y su respectiva codificación. En lo que sigue de este documento se expondrán con más detalles estas fases aquí presentadas.

2. OBJETIVOS

Determinar las cuestiones internas y externas en el ámbito de la seguridad y privacidad de la información que son pertinentes para determinada compañía y esto corresponde al objetivo general del proyecto PESI. Se propone una tabla de contenido y en paralelo una metodología que apoye el proceso de construcción de un PESI.

3. MARCO NORMATIVO

Este apartado de la metodología corresponde a lo que normalmente llamamos normograma el cual es una herramienta de las organizaciones públicas y privadas que permite delimitar las normas que regulan sus actuaciones en desarrollo con su objeto misional. Contiene normas externas como leyes, decretos, acuerdos, circulares y resoluciones que afectan la gestión de una organización. Este capitulo es parte fundamental del PESI ya que nos muestra el entorno legal en que los proyectos serán propuestos, obviamente teniendo como lineamientos esta normatividad.

4. ENTENDIMIENTO ESTRATÉGICO

Se pretende en esta etapa de la metodología entender las estrategias existentes que guían la organización. Se debe conocer la estrategia general de las organizaciones, cuáles son sus partes interesadas y que linemientos gubernamentales o de otro tipo rigen su operación. En la siguiente figura se muestran los aspectos mínimos que deben ser considerados:

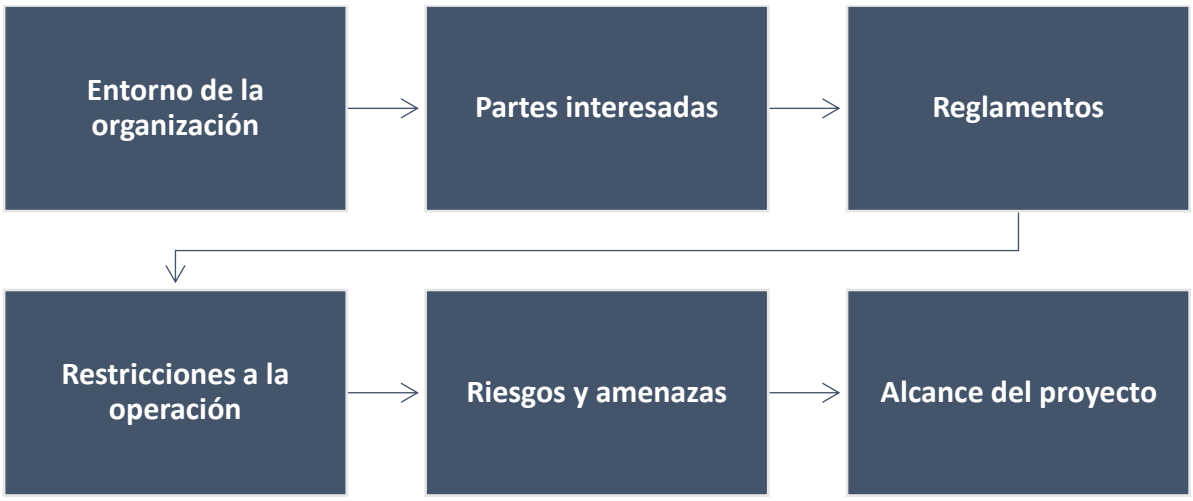

Figura No. 1. Entorno estratégico de la organización.

Entorno de la organización: en esta fase inicial de la construcción del documento PESI se analiza el entorno económico y social de la organización

Partes interesadas: en esta fase se determinan los mayores interesados en los resultados de la implementación del PESI.

Reglamentos: en esta fase se analiza el normograma para entender su impacto para la organización.

Restricción operaciones: se solicita la información que servirá de insumo para construir el PESI, con base en la identificación de las restricciones operativas que puedan existir.

Riesgos y amenazas: en esta fase se determina el entorno de riesgos y amenazas existentes que puede impactar a la organización.

Alcance del proyecto: finalmente se determina el alcance del proyecto con base en lo anteriormente expuesto.

5. DIAGNÓSTICO

5.1. Análisis de situación actual

En este capítulo se abordará lo referente a la situación actual y el estado de madurez con respecto a la seguridad de la información y la protección de datos personales. Se considerarán los siguientes aspectos:

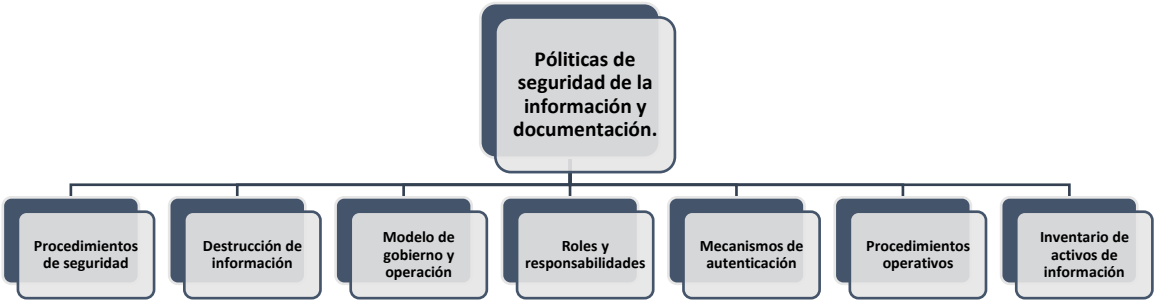

Figura No. 2. Políticas de seguridad de la información y documentos asociados.

A continuación, se presentan las diferentes categorías existentes para una adecuada gestión de la seguridad de la información. Estas categorías serán revisadas durante el proceso de elaboración de este PESI:

Figura No. 3. Evaluación de la gestión en seguridad de la información.

A continuación, se presentan las diferentes categorías existentes para las metodologías utilizadas y la arquitectura de seguridad digital.

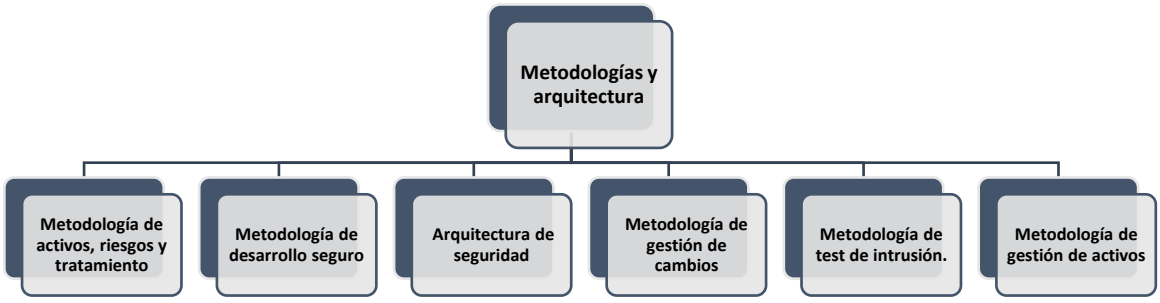

Figura No. 4. Metodologías y arquitectura de seguridad.

5.2. Arquitectura de seguridad SABSA

SABSA (Sherwood Applied Business Security Architecture) es una metodología probada para desarrollar arquitecturas de seguridad orientadas al negocio, centradas en el riesgo y las oportunidades, tanto a nivel empresarial como de soluciones, que respalden de forma trazable los objetivos comerciales. Este documento presenta una metodología para realizar al interior de la organización una arquitectura de seguridad siguiendo este modelo. Los aspectos principales de esta metodología son: La vista del negocio, la de arquitectura, la perspectiva de diseño, la fase de construcción y finalmente la vista de componentes que corresponden estos últimos a dispositivos y tecnologías:

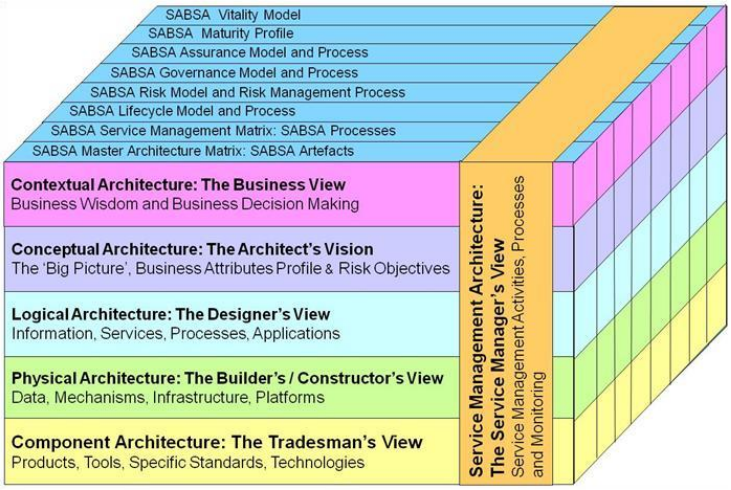

Figura No. 5. Modelo de arquitectura SABSA.

Conforme al Modelo de Arquitectura Empresarial dominio de Seguridad de la información, está alineado con en el marco de referencia SABSA, que establece los servicios de seguridad necesarios para proteger la información. Este enfoque permite alinear la seguridad con los objetivos estratégicos de la Entidad y mitigar los riesgos que se hayan identificados.

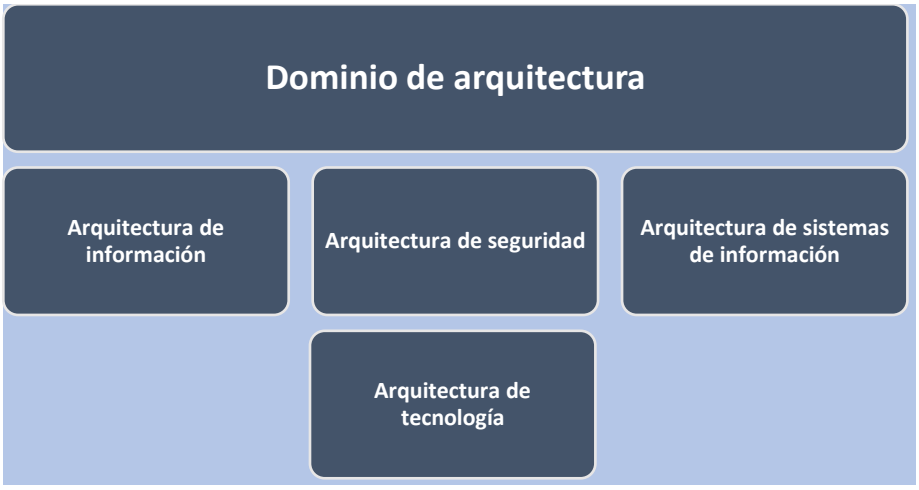

Figura No. 6. Modelo de arquitectura SABSA y sus relaciones.

Una arquitectura de seguridad no debe existir aislada de otros componentes al interior de la entidad. La seguridad de la información debe integrarse de modo estratégico. Se basa en la información de las entidades,

que ya está disponible en los ejercicios que se hayan realizado de arquitectura empresarial y esta arquitectura de seguridad genera artefactos e información que deberían ser integrado por los artefactos hasta ahora realizados de arquitectura empresarial. Ésta es la razón por la cual se recomienda que exista una estrecha integración y colaboración de la arquitectura de seguridad y la arquitectura empresarial.

Por otra parte, SABSA es un marco de referencia y una metodología integral diseñada para desarrollar arquitecturas de seguridad de la información basadas en riesgos. Su enfoque se centra en alinear la seguridad de la información con los objetivos estratégicos del negocio, ofreciendo así un proceso estructurado y sistemático para la gestión de los riesgos de seguridad. Es también un marco más amplio para la gestión de toda la arquitectura empresarial, incluyendo la tecnológica, los procesos, los datos y de aplicaciones, además incluye un dominio la Arquitectura de Seguridad.

5.3. Oportunidades de mejora

Las oportunidades de mejora son aspectos que se analizan y se estudian para optimizar procesos, habilidades, herramientas, componentes o actividades, con el fin de incrementar la eficacia, eficiencia, y la confianza digital. Estas oportunidades normalmente están ligadas a los instrumentos con los que se realizan los diagnósticos en lo referente a la seguridad de la información y los datos personales. La seguridad de la información entendido como un proceso estratégico y continuo debe ser siempre susceptible de mejoras que incrementen su nivel de madurez.

6. ANÁLISIS ESTRATÉGICO DE LA POSTURA EN SEGURIDAD

Este capítulo tiene como objetivo principal definir las estrategias de seguridad de la información y protección de datos personales que es la salida principal de la metodología propuesta del PESI. Para ello se requiere entender las fortalezas, debilidades, oportunidad y amenazas (DOFA) del área de seguridad de la información dentro de la OTIC y las entidades adscritas.

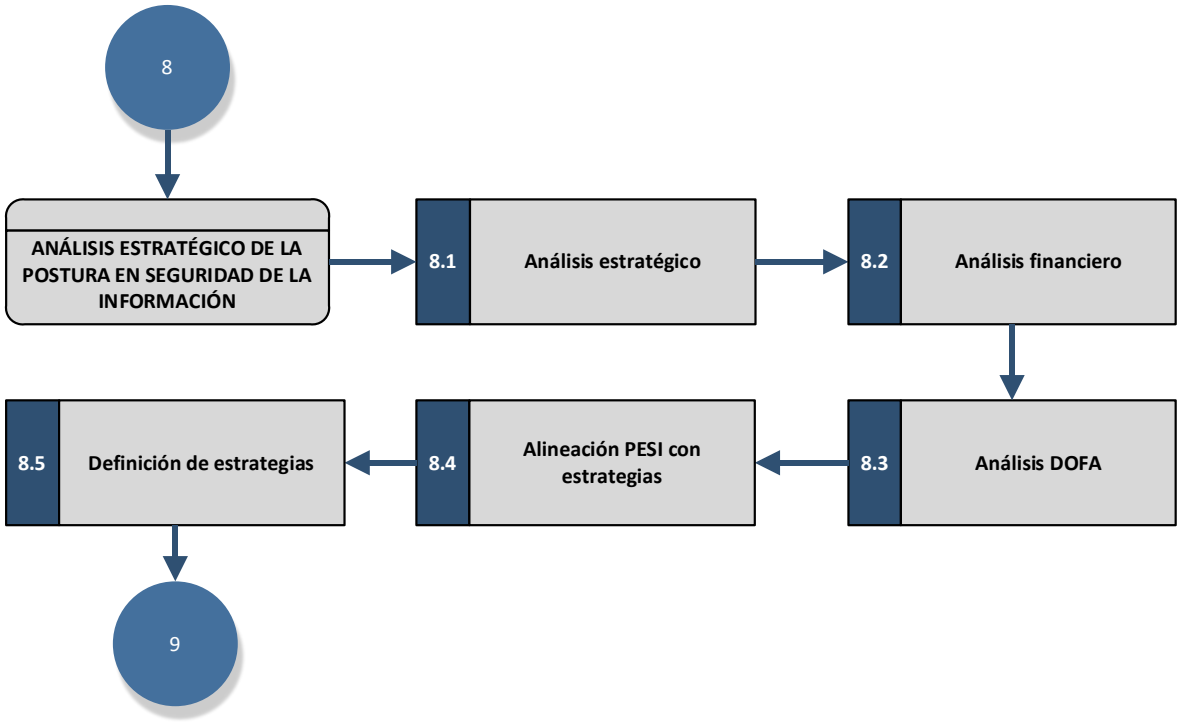

Figura No. 7. Análisis de la situación actual en seguridad.

6.1. Análisis estratégico

Con base en el capítulo de entendimiento estratégico, el análisis estratégico pretende establecer un PESI que este perfectamente alineado y que comprenda todas estas directrices de tal manera que la protección de los activos de información genere confianza al uso interno de la información.

6.2. Análisis financiero

El análisis financiero permite evaluar la situación financiera de una determinada organización y planear acciones futuras. Se basa en el estudio de la información contable para conocer su uso de recursos financieros, y obtener una visión objetiva de su rentabilidad, solvencia y liquidez. Con estas premisas el análisis financiero del PESI pretende estimar los gastos operativos del sistema de protección de la información y datos personales con el fin de que los proyectos aquí planteados y los existentes contribuyan a mejorar la eficiencia y la efectividad del Sistema de Gestión de la Seguridad de la Información (SGSI).

6.3. Análisis DOFA interno y externo

En la construcción del PESI se requiere analizar las debilidades, fortalezas, oportunidad y amenazas del área de seguridad de la información con el fin de elaborar estrategias que maximicen las fortalezas y disminuyan las amenazas, comprendiendo claramente las debilidades que hoy en día se tienen en la protección de la

información y las oportunidades concernientes al uso de las tecnologías emergentes y disruptivas que posibilites el logro de los objetivos estratégicos de la Entidad.

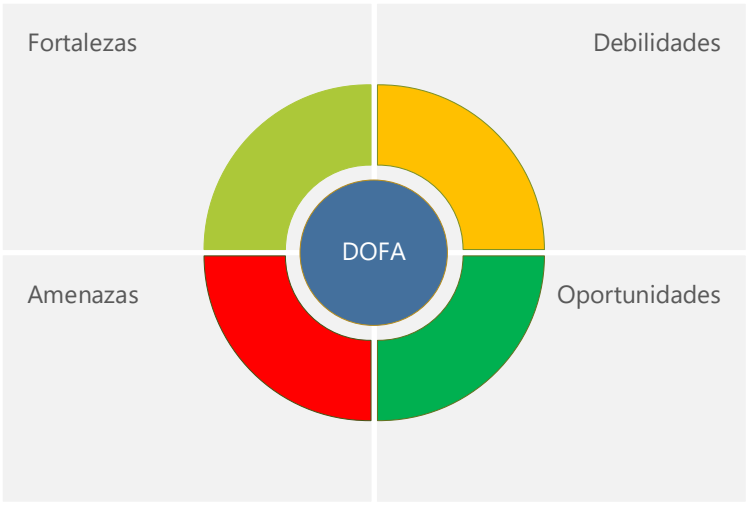

Figura No. 8. DOFA.

6.4. Definición de las estrategias del PESI

Una vez realizado el análisis de alineación estratégico del PESI y se tenga la certeza que los objetivos estratégicos propuesto apoyan la misión y la visión, estas estrategias pasarán a considerarse como iniciativos o proyectos que deben ser implementados durante la vigencia de este PESI. Las estrategias podrían considerar al menos cuatro dimensiones, en la primera de seguridad de la información consiste en:

1. Confidencialidad
2. Integridad
3. Disponibilidad

En la segunda dimensión deben considerar los procesos, los colaboradores y la tecnología:

1. Procesos
2. Factores humanos
3. Tecnología

En la tercera dimensión se deben tener en cuenta los estados de la información que son:

1. Durante la trasmisión
2. En el almacenamiento
3. En el procesamiento

Y finalmente, se deben considerar los requisitos en lo relacionado con el control de acceso en cada una de las estrategias utilizadas:

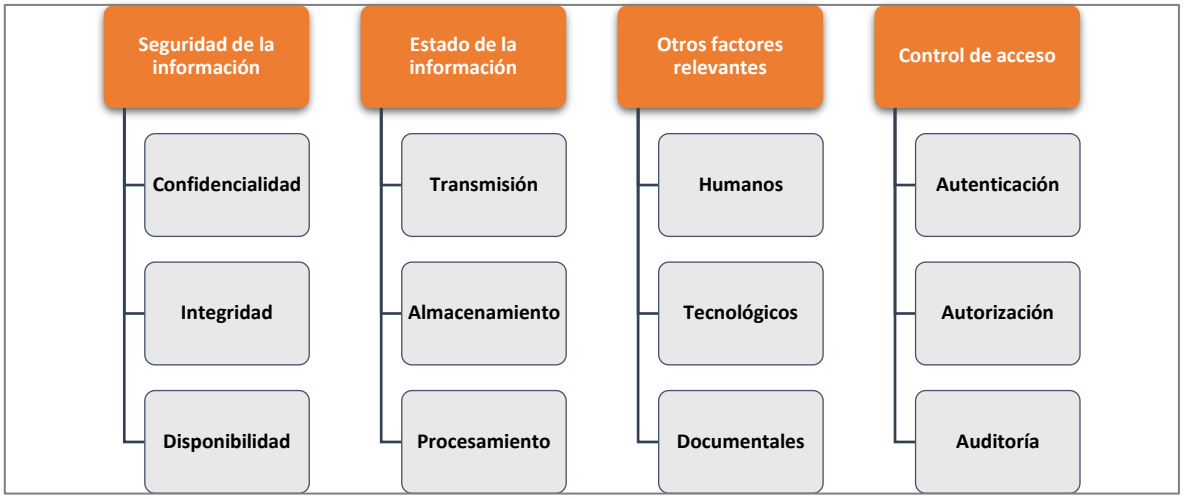

Figura No. 9. Las dimensiones consideradas por las estrategias del PESI.

Las estrategias definidas en el PESI deben poder analizarse desde estas tres dimensiones, por ejemplo, para un activo de información determinado debe cumplirse que, durante su transmisión, la tecnología que se usa debe preservar la confidencialidad. En otras palabras, al analizar un objetivo estratégico si se descubre que requiere la protección de los activos de información en algún sistema de información requerido esta metodología nos apoyará el proceso de alinear las estrategias del PESI con las de la organización.

En la siguiente tabla se muestra, a manera de ejemplo, el nivel de madurez en cada una de las entidades adscritas medida usando los valores 0, 0.5 y 1, (no implementado, parcial y cumplimiento total respectivamente) incrementándose el valor en proporción a la dependencia atribuida. Como parte de este análisis para cada uno de los controles auditados se debe predicar de cada uno su relación con los tres objetivos de la seguridad de la información y con esta información calcular cuál de los pilares de la seguridad de la información es más importante:

Controles auditados	Confidencialidad	Integridad	Disponibilidad	Nivel de madurez por con respecto a los controles.
Gestión de vulnerabilidades	1	1	1	2.5
Gestión de incidentes	1	1	1	2.5
Gestión de proveedores	1	1	1	2.5
Gestión cultura de seguridad	0.5	0.5	0.5	1.5
Gestión de alertas y logs	1	1	1	1.5
Gestión de la continuidad	0.5	0.5	0.5	1
Metodología de activos, riesgos y tratamiento	0.5	0.5	0.5	1.5
Metodología de desarrollo seguro	1	1	1	1.5
Metodologías caracterización ciudadanos	0.5	0.5	0.5	1
Arquitectura de seguridad y controles implementados	1	1	1	2
Metodología Protección datos personales	0.5	0.5	0.5	2
Capacidad y subcapacidades	0.5	0.5	0.5	1.5
Procedimientos de seguridad	0.5	0.5	0.5	1.5
Destrucción de información	0.5	0.5	0.5	1.5
Modelo de gobierno y operación	0.5	0.5	0.5	1.5
Roles y responsabilidades	0.5	0.5	0.5	1
Mecanismos de autenticación	1	1	1	2
Revisión y auditoría del MSPI	0.5	0.5	0.5	2
Caracterización de servicios de seguridad	0.5	0.5	0.5	1.5
Nivel de madurez	7	7	7	

Figura No. 10. Diagnóstico de seguridad de la información.

7. DEFINICIÓN DE LOS PROYECTOS PARA EL PESI

Los proyectos corresponden a las salidas obtenidas una vez realizado el proceso de alinear el PESI con el PETI. Una vez estos proyectos hayan sido definidos con base en las expectativas planteadas se procese a priorizarlos, realizar la proyección presupuestal, definir la hoja de ruta y finalmente, proponer el plan de proyectos de inversión, tal como se muestra en la siguiente figura:

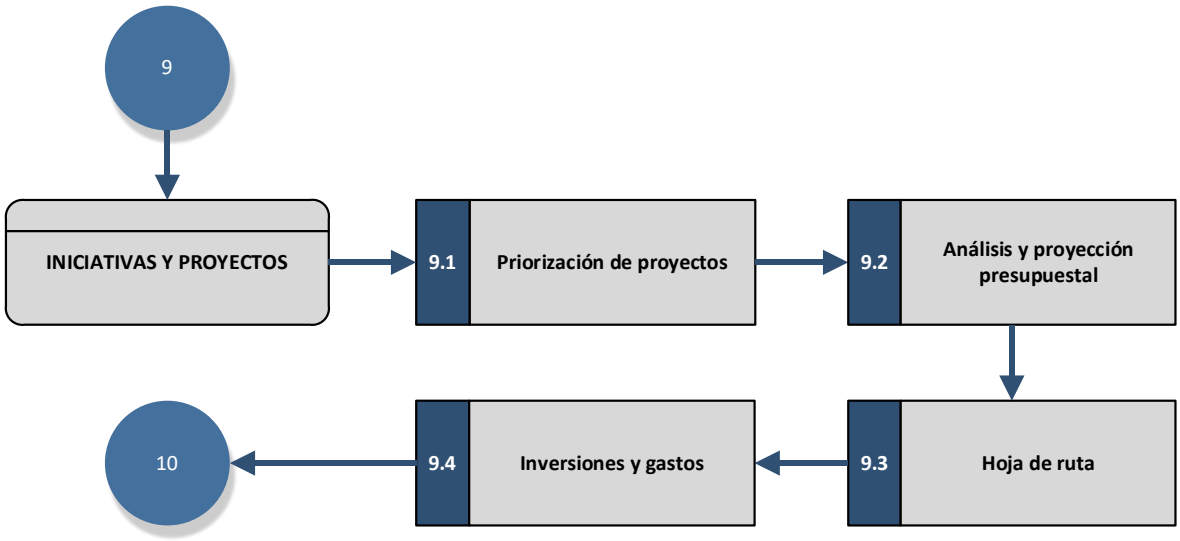

Figura No. 11. Definición de proyectos.

7.1. Priorización de proyectos definidos

En la construcción del PESI se requiere analizar la prioridad que las diferentes estrategias puedan tener con el fin de ordenarlas de la manera en que las mejoras se pueden notar al principio del ciclo de vida de la implementación de este documento. En una primera instancia se propone en esta metodología que las estrategias sean valoradas con respecto al costo, complejidad, duración y relevancia.

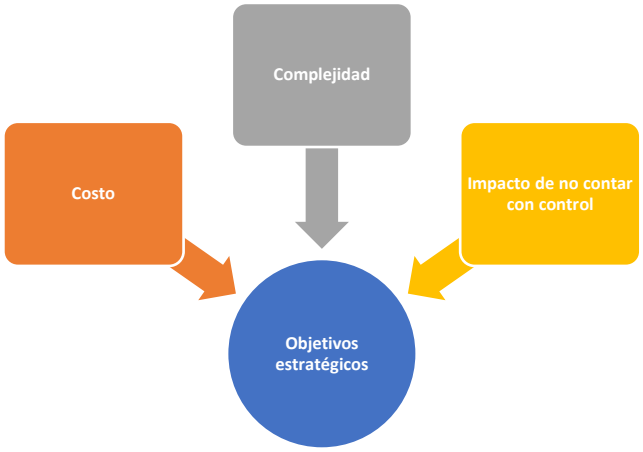

Figura No. 12. Priorización de las estrategias del PESI.

A continuación, se presenta la tabla que nos permitirá priorizar las diferentes estrategias consideradas teniendo en cuenta el costo, la complejidad y el impacto de no contar con un determinado control o requerimiento.

Control evaluado	Complejidad	Costo	Impacto de la ausencia del control o requerimiento.	Prioridad
Requerimiento 1	1	3	3	**7**
Requerimiento 2	3	2	3	**8**
Requerimiento 3	2	5	3	**10**
Requerimiento 4	2	2	5	**9**
Requerimiento 5	2	3	2	**7**
Requerimiento 6	1	5	2	**8**
Requerimiento 7	5	2	2	**9**
Requerimiento 8	1	2	5	**8**

Figura No. 13. Priorización de las estrategias.

7.2. Presupuestos requeridos

Una vez realizado el proceso de priorización se pasa a la siguiente etapa que es la proyección presupuestal teniendo en cuenta los costos asociados a cada proyecto con el fin de que la organización pueda realizar la asignación presupuestal para luego proceder a la adquisición o compra de los productos o servicios requeridos para implementar las estrategias del PESI.

7.3. Definición de la hoja de ruta para los proyectos

Una hoja de ruta es una guía visual que describe el camino para lograr objetivos específicos. Le ayuda a ver el panorama general mientras desglosa los pasos necesarios para alcanzar sus objetivos. Ya sea que esté trabajando en un proyecto, lanzando un producto o planificando estrategias a largo plazo, una hoja de ruta hace que sea más fácil mantenerse organizado y focalizado.

La salida principal del proceso de ejecución del PESI es la hoja de ruta que expone los proyectos que deben ser ejecutados una vez realizada la proyección presupuestal. En la siguiente figura se muestra un ejemplo de un formato utilizado para seguimiento de los proyectos estipulados por el PESI:

Actividad	Inicio	Duración anual	Responsable	Estado	Porcentages de ejecución	2025	2026	2027
Proyecto PESI 01	2025	1	2025	Pendiente	10%			
Proyecto PESI 02	2026	1	2026	Pendiente	10%			
Proyecto PESI 03	2027	1	2027	Pendiente	10%			
Proyecto PESI 04	2028	1	2028	Pendiente	10%			
Proyecto PESI 05	2025	1	2025	Pendiente	10%			
Proyecto PESI 06	2026	1	2026	Pendiente	10%			
Proyecto PESI 07	2027	1	2027	Pendiente	10%			
Proyecto PESI 08	2028	1	2028	Pendiente	10%			

Figura No. 14. Características minimalistas de una hoja de ruta.

7.4. Inversiones requeridas

Lo que se denomina comúnmente plan de proyecto de inversión es una propuesta formal que analiza la viabilidad de utilizar recursos en una oportunidad o proyecto específico con el objetivo de obtener beneficios en este caso relacionados con la mejora en la protección de la información. Lo anteriormente mencionado debe consolidarse en este instrumento que nos permitirá establecer una relación entre las inversiones ejecutadas y el beneficio obtenido de estas. Los proyectos deben considerar los siguientes puntos:

Actividad	Inicio	Presupuesto asignado	Ejecutado	Responsable	Valor del proyecto	2025	2026	2027
Proyecto PESI 01	2025	No	Parcial		1			
Proyecto PESI 02	2026	No	Parcial		1			
Proyecto PESI 03	2027	No	No		1			
Proyecto PESI 04	2028	No	No		1			
Proyecto PESI 05	2025	No	No		1			
Proyecto PESI 06	2026	No	No		1			
Proyecto PESI 07	2027	No	No		1			
Proyecto PESI 08	2028	No	No		1			
Total costo PESI					8			

Figura No. 15. Seguimiento de los proyectos.

7.5. Sistema de Gestión de la Seguridad de la información

El MinTIC ha elaborado el MSPI para la implementación de la estrategia de seguridad digital y un sistema de gestión de seguridad de la información (SGSI), teniendo como referencia el ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; por

otro lado, el modelo consta de cinco (5) fases: Diagnóstico, Planificación, Operación, Evaluación de desempeño, Mejoramiento continuo:

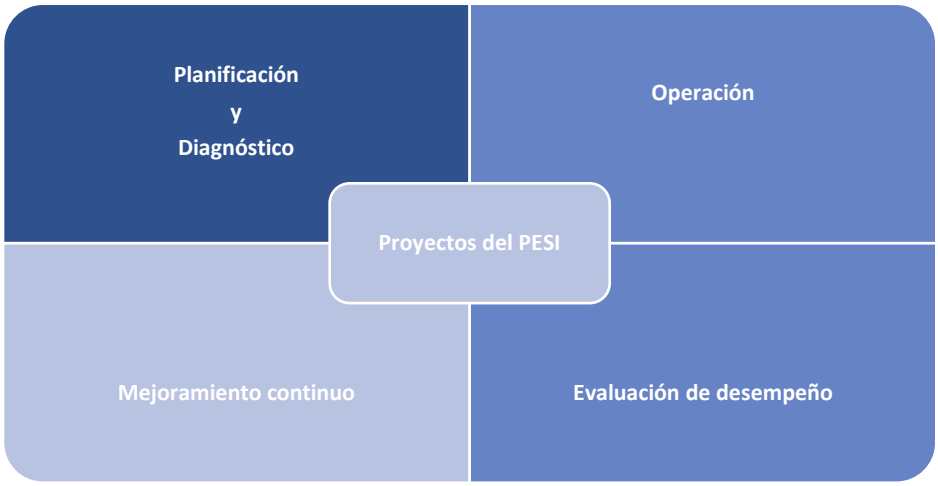

Figura No. 16. Modelo de gestión sugerido para el PESI

- **Diagnóstico:** en la fase inicial se requiere realizar un diagnóstico con respecto a la protección de la información.
- **Planificación:** se determinan las necesidades y objetivos de seguridad y privacidad de la información.
- **Operación:** se implementan los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos.
- **Evaluación de desempeño:** se determina la forma de evaluación para la adopción del modelo de seguridad.
- **Mejoramiento Continuo:** se establecen los procedimientos para optimizar el modelo.

8. TRANSFERENCIA DE CONOCIMIENTO Y COMUNICACIONES

La apropiación de una tecnología es un proceso que, simultáneamente, transforma al usuario y a la tecnología; es decir, no sólo da lugar a que el usuario cambie en sus conocimientos y sus habilidades, sino que también causa transformaciones en las propiedades de la tecnología. La transferencia de conocimiento es fundamental para que se realice la apropiación de lo concerniente con la seguridad de la información y la protección de los datos personales.

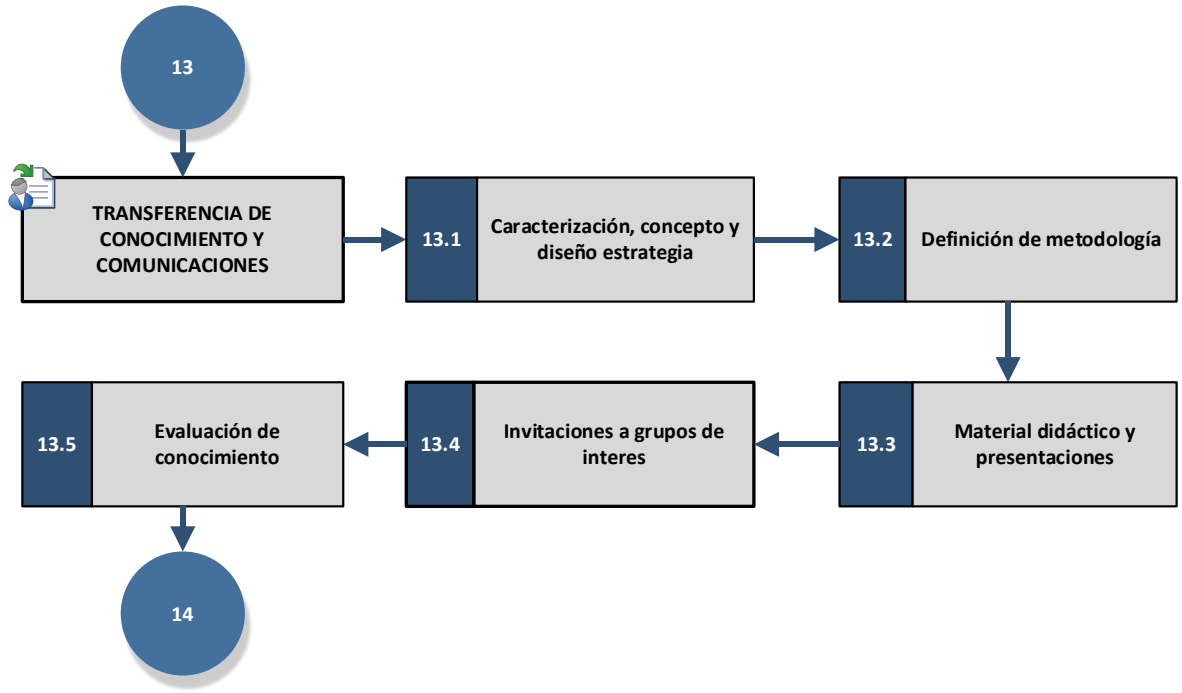

Figura No. 17. Transferencia de conocimiento

8.1. Caracterización, concepto y diseño de estrategia

En esta etapa de la transferencia de conocimiento y comunicaciones se debe realizar la caracterización de interesados sirve para orientar las acciones o estrategias que permitan llevar a los interesados de un punto inicial a un punto deseado, se requieren al menos cinco características, ya que la adaptación y la apropiación se da en la medida en que las personas progresan en cada una de estas cinco condiciones, que siguen un orden natural en que las personas experimentamos el cambio. Estas condiciones son:

- Conciencia de la necesidad del cambio.
- Deseo de participar y apoyar el cambio.
- Conocimiento para saber cómo apropiar el cambio.
- Habilidad de implementar las habilidades y conductas requeridas.
- Refuerzo para sostener el cambio.

Por otra parte, se debe definir el concepto estratégico junto con la definición del mensaje clave. Estos puntos son fundamentales para orientar la estrategia de transferencia de conocimiento y comunicaciones. Finalmente, con el concepto y los mensajes claves se procede al diseño de la estrategia de comunicaciones que requiere de la definición de una metodología como se expondrá en el siguiente numeral.

8.2. Definición de metodología

Las estrategias de comunicación para que sean efectivas deben comprender diferentes medios de comunicación para lograr que lo propuesto por el PESI sea interiorizado en las organizaciones con el fin de completar el proceso de implementación de controles de seguridad de la información. Se requiere de una metodología precisa para que se cumplan los objetivos de transferencia de conocimiento y la posterior apropiación de lo relacionado con la protección de la información.

8.3. Material didáctico y presentaciones

Una vez definida la metodología del proceso de transferencia de conocimiento se debe continuar con la elaboración del material didáctico, presentaciones y demás herramientas disponibles el cual debe cumplir con los siguientes requerimientos:

- Claridad
- Coherencia
- Consistencia
- Completitud

8.4. Invitaciones a grupos de interes

Una vez realizada las sesiones de capacitación y transferencia de conocimiento se debe dejar constancia de la asistencia de los colaboradores a las sesiones programadas. Finalmente, se debe entregar un certificado de asistencia como prueba y evidencia de la realización de la transferencia de conocimiento.

8.5. Evaluación del conocimiento

Las estrategias de comunicación para que sean efectivas deben comprender diferentes medios de comunicación para lograr que lo propuesto por el PESI sea interiorizado al interior de las entidades con el fin de completar el proceso de implementación de controles de seguridad de la información.

9. SEGUIMIENTO Y CONTROL

Los indicadores son una herramienta esencial para el seguimiento y control de las iniciativas estratégicas en las organizaciones. Permite comunicar eficazmente sus objetivos y metas, lo que facilita que todos se enfoquen en alcanzar los objetivos estratégicos.

Se deben definir indicadores específicos que deben ser monitoreados periódicamente. Estos indicadores permiten detectar desviaciones tempranas y tomar medidas correctivas de manera oportuna.

Los indicadores se clasifican en tres tipos:

- Indicadores para iniciativas de inversión: miden el progreso y cumplimiento de los proyectos definidos en el PESI para abordar las necesidades operativas.
- Indicadores de gastos de operación: evalúan el progreso y cumplimiento de los proyectos destinados a brindar soporte y mantenimiento de las operaciones.
- Indicadores de la estrategia de TI: Miden el progreso y cumplimiento de la estrategia lo relacionado con la gestión de la seguridad de la información.

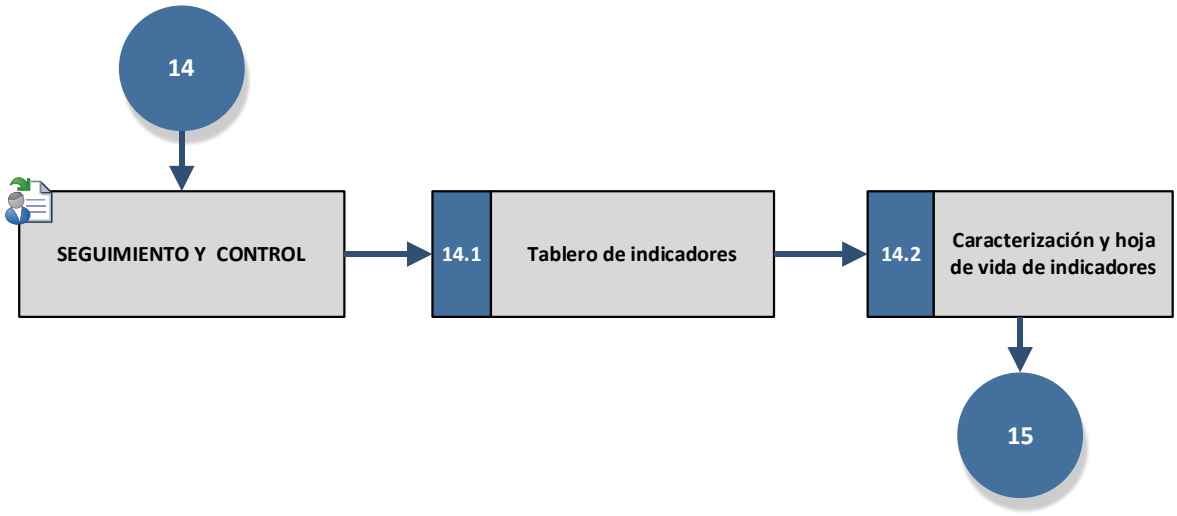

Figura No. 18. Seguimiento y evaluación.

9.1. Tablero de Indicadores de seguimiento

Para ello, se aplicarán indicadores de cumplimiento e indicadores de resultado, de acuerdo con los criterios de evaluación y seguimiento. Así mismo, se realizarán mediciones de calidad y finalmente, de manera específica se definirán indicadores de seguimiento para los proyectos considerados por el PESI.

9.2. Caracterización y hoja de vida indicadores

Aquí se establece los aspectos a ser desarrollados por los responsables de la gestión de seguridad de la información en todos los niveles de la organización, para así, evaluar y en donde sea aplicable, medir el desempeño del sistema contra la política, los objetivos y la experiencia práctica de la gestión de seguridad de la información, a la vez que se reportan los resultados a la dirección para su revisión y toma de decisiones.

Para el cumplimiento de esta fase la organización deberá desarrollar un conjunto de actividades de seguimiento donde se mantenga de manera continua la medición y verificación del cumplimiento de los aspectos planteados en la fase de Planificación del modelo y la forma como estas actividades se han ido desarrollando o ejecutando.

10. CONCLUSIONES

Las conclusiones del trabajo realizado hasta aquí deberían comprender:

- Proyectos menos costos y con más victorias tempranas
- Proyectos alineados con la visión estratégica de la organización
- Proyectos de apoyan la implementación del modelo de seguridad
- Proyectos que mitigan riesgos muy altos.

11. GLOSARIO DE TÉRMINOS

12. BIBLIOGRAFÍA

13. ANEXOS