PROPUESTA PARA IMPLEMENTACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
MSPI

OFICINA ASESORA DE DIRECCIONAMIENTO ESTRATEGICO TIC
SEGURIDAD DE LA INFORMACIÓN

Ibagué – Colombia

GLOSARIO

Acceso a la Información Pública:
Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo
En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información:
En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo:
Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Corporación pública o Privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenazas
Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo
Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría
Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determiner el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autorización:
Consentimiento previo, xpreso e informado del Titular para llevar a cabo el
Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales:
Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley
1581 de 2012, art 3)

Ciberseguridad
Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio
Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control
Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos:
Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Corporaciónes públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art6)

Datos Personales:
Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos:
Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados:
Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos:
Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles:
Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad
Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad:
Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos:
Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información
Procesos para detectar, reportar, evaluar, responder,tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada:
Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada:
Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo

cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art6)

Ley de Habeas Data:
Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública:
Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales:
Lo constituyen las distintas alternativas con que cuentan las Corporaciónes destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio
Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos
Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad:
En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la Corporación en el marco de las funciones que a ella le compete realizar y que generan en las Corporaciónes destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Registro Nacional de Bases de Datos:
Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada:
Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos:
Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información:

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley1581 de 2012, art 3)

Tratamiento de Datos Personales:

Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Corporación. (ISO/IEC 27000).

Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Partes interesadas (Stakeholder)

Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Contenido

1. INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información (MSPI) es una guía que conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos mediante la aplicación de un proceso de gestión del riesgo, el cual deberá consolidarse en un Sistema de Gestión de la Seguridad de la Información (SGSI) y este a su vez articularse al Sistema Integrado de Gestión (S.I.G) de CORTOLIMA; esto a través de la implementación de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información que se puedan presentar.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización, así como los externos del entorno. En general el SGSI debe permitir obtener una visión global del estado de los sistemas de información y observar las medidas de seguridad aplicadas y los resultados obtenidos, para poder, con todos estos elementos, tomar mejores decisiones estratégica

2. JUSTIFICACIÓN

En CORTOLIMA, La seguridad de la información se entiende como el conjunto de medidas técnicas, operativas, organizativas y legales que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma para nuestros usuarios internos y externos dentro del context de nuestro Sistema de gestion de calidad. En este mismo sentido la Oficina Asesora de Direccionamiento Estratégico TIC conoce y tiene como unas de sus prioridades, implementar activamente la seguridad al interior de la Corporación.

A razón de ello se encuentra desarrollando el Modelo de Seguridad y Privacidad de la Información MSPI de acuerdo con los lineamientos del Ministerio de Tecnologías de la Información y las comunicaciones Min TIC V; así mismo mediante la implementación de este modelo, se busca contribuir en el desarrollo del modelo integrado de planeación y gestión MIPG.

MODELO DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LA INFORMACIÓN – MSPI.

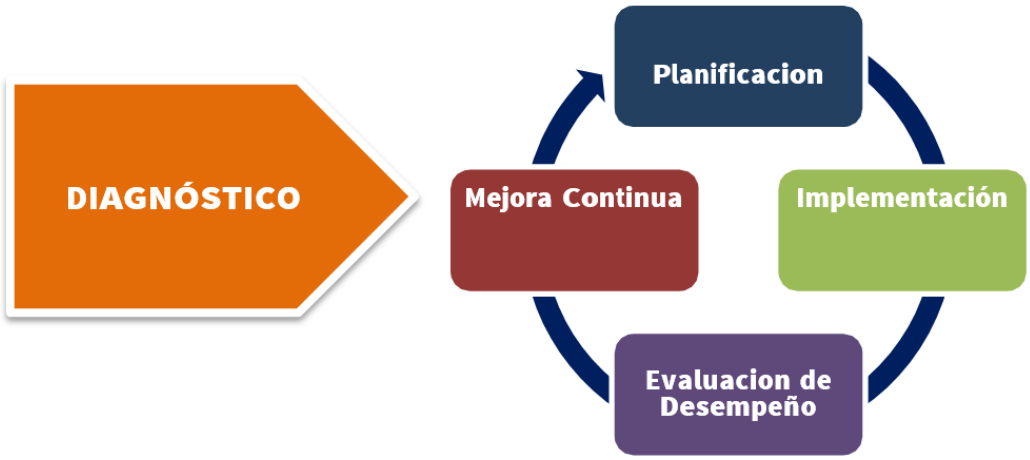

Figura 1. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

El ciclo de operación del Modelo de seguridad y privacidad de la información – **MSPI**, cuenta con 5 fases, cada una de ellas contienen objetivos, metas y herramientas (guías) que permiten que el modelo sea sostenible, estas fases son:

Fase 1: Diágnostico
Fase 2: Planificación
Fase 3: Implementación
Fase 4: Evaluación del Desempeño
Fase 5: Mejora Contínua

3. FASE DE DIAGNOSTICO

Figura 2. Etapas Fase de Diagnóstico del Modelo de Seguridad y Privacidad de la Información

En esta primera fase se describen las etapas previas a la implementación del MSPI, esta fase tiene tres etapas:

Etapa 1: Estado actual de la Infraestructura de TI de la Corporación
Etapa 2: Identificación del estado de madurez
Etapa 3: Levantamiento de Información

Mediante la elaboración de la fase de Diagnóstico se busca:

1. Determinar el estado actual de la gestión de seguridad y privacidad de la información en el interior de la Corporación.
2. Identificar el nivel de madurez de seguridad y privacidad de la información.
3. Identificar las vulnerabilidades técnicas y administrativas que sirvan de insumo para la fase de planificación.
4. Identificar el nivel de cumplimiento con la legislación vigente relacionada con protecciónde datos personales.
5. Identificación del uso de buenas prácticas en ciberseguridad.

Teniendo en cuenta que claramente en CORTOLIMA se cuenta con un manual de políticas de seguridad de la informacón, identificación clara de activos de información con la matriz de riesgos, politicas y controles de seguridad dentro de su infraestructura; en el proceso de mejoramiento contínuo se pretende en la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestion de seguridad y privacidad de la información al interior de la Corporación.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la Corporación.

- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

Para ello se recomienda utilizar los siguientes instrumentos:

- Herramienta de diagnostico
- Instructivo para el diligenciamiento de la herramienta
- Guía No 1 - Metodología de Pruebas de Efectividad

Tabla 1 - Metas, Resultados e Instrumentos de la fase etapas previas a la implementación:

Diagnostico	
Metas	**Resultados**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.

3. 1 Estado actual de la Infraestructura de TI de la Corporación

Para realizar dicha fase las Corporaciónes deben efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad.

Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la Corporación se procede al desarrollo de la fase de Planificación. Es importante aclarar que si bien de forma documentada actualmente no se tiene un

documento contega los lineamientos del MSPI indicado por MINTIC; se cuentan con elementos claros a nivel de seguridad:

- La Corporación se certificó en la Norma ISO 27001 en el 2018
- Manual de la política del sistema de gestión de seguridad de la información SGSI
- Plan de Seguridad de la información
- Matriz de Activos de Información
- Matriz de Riesgos de Seguridad
- Políticas de Seguridad implementadas en el UTM que gestiona la seguridad a nivel de la infraestructura de red e internet
- Políticas de Control de Acceso
- Cumplimiento con la Fase de Dagnostico y proceso de implementación del plan de transicción de Ipv4 a Ipv6 reportado en la plataforma dispuesta de **MINTIC**

Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.

3.2 Identificación del estado de madurez

La madurez de la seguridad y privacidad de la información se puede medir únicamente a través de la capacidad de la Corporación para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de muchas disciplinas. La madurez de la seguridad y privacidad de la información incluye los controles tanto administrativos como técnicos, la competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles, así como la eficiencia de los controles establecidos dentro de la organización.

Para el desarrollo de este diagnóstico, el nivel de madurez se identifica mediante el diligenciamiento del Instrumento de Evaluación MSPI, en la hoja llamada MADUREZ, la cual está divida en 5 niveles:

NIVEL	CUMPLE ?
OPTIMIZADO	FAL
GESTIONADO CUANTITATIVAMENTE	FAL
DEFINIDO	FAL
GESTIONADO	FAL
INICIAL	FAL

Figura 03. Descripción Niveles de Madurez y Cumplimiento

Tabla 02. Nivel de Madurez - Instrumento de Evaluación MSPI.

Nivel	D
Inicial	En este nivel se encuentran las Corporaciónes, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las Corporaciónes, en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las Corporaciónes que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados,
Administrado	En este nivel se encuentran las Corporaciónes, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las Corporaciónes, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo

De acuerdo con los elementos indicados con anterioridad y de acuerdo a los esfuerzo que la Corporación he realizado desde la Oficina Asesora de Direccionamiento Estratégico TIC en el area de seguridad de la información y el funcionamiento actual de la infraestructura de Seguridad y los controles implementados y teniendo en cuenta los niveles de madurez definidos por **MINTIC** Podemos se clasifica la **CORTOLIMA** en Nivel Repetible.

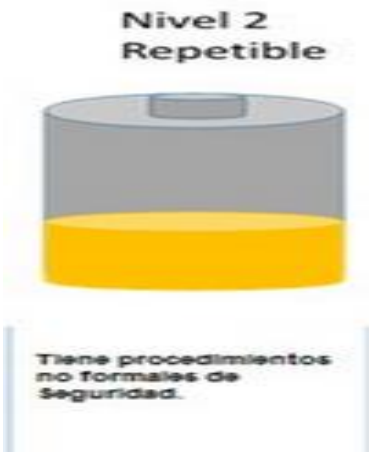

Figura 4. Nivel de Madurez CORTOLIMA

3.3 Levantamiento de Información

Para realizar dicha fase la Corporación deben efectuar la recolección de la información con la ayuda de la erramienta de diagnóstico y la metodología de pruebas de efectividad.

Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la Corporación se procede al desarrollo de la fase de Planificación.

Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.

4. FASE DE PLANIFICACION

Para el desarrollo de esta fase **CORTOLIMA** con base en los resultados de la etapa anterior procedera a actualizer el plan de seguridad y privacidad de la información alineado con el objetivo misional de la Corporación, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permitirá a la Corporación definir los límites sobre los cuales se implementará la seguridad y privacidad con a los lineamientos propuestos por MINTIC. Este enfoque es por procesos y debe extenderse a toda la Corporación.

Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones

Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

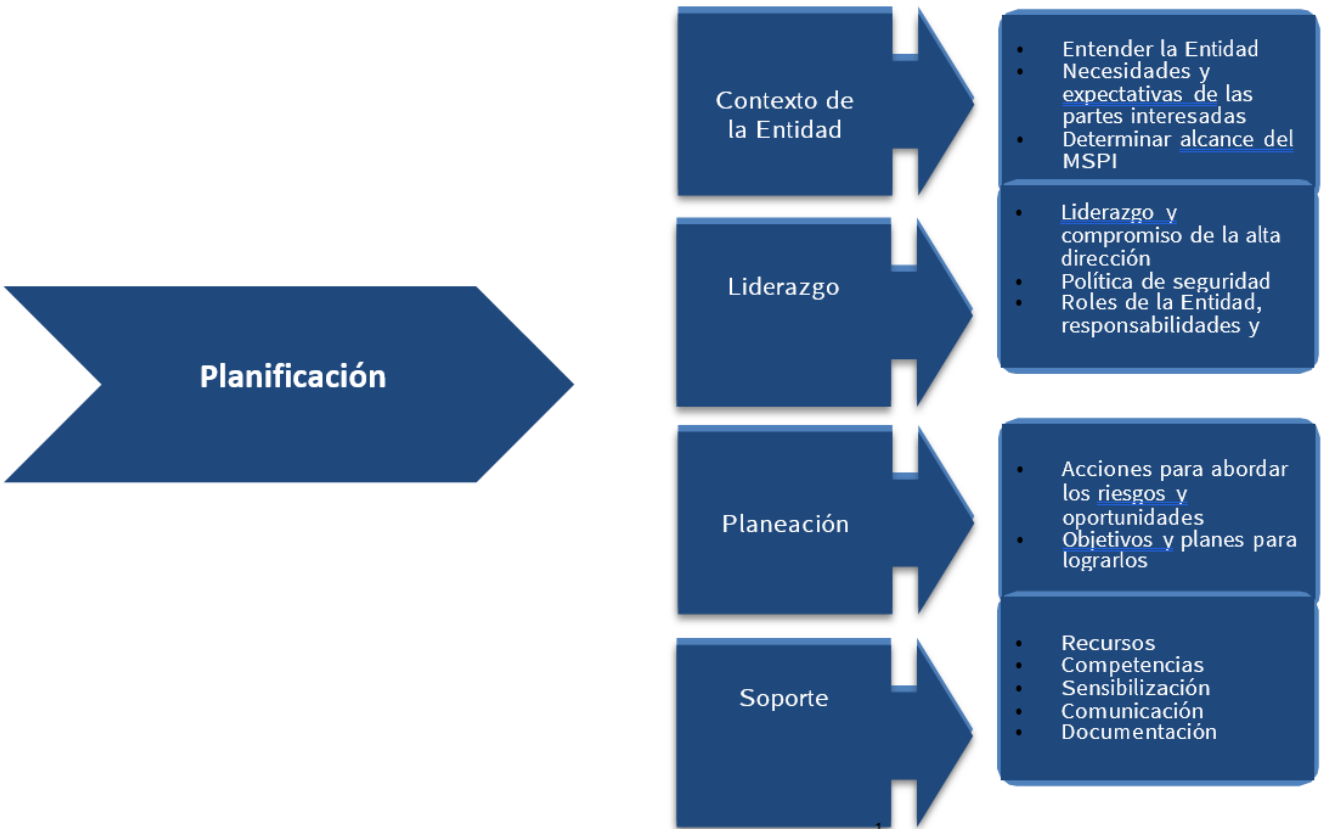

Figura 05. Elementos Fase de Planeación del MSPI

Tabla 03 - Metas, Resultados e Instrumentos de la Fase de Planificación

Planificación	
Metas	**Resultados**
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Corporación.
Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Corporación.
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la Corporación, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la Corporación.
Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la Corporación.
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la Corporación.
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.

5. FASE DE IMPLEMENTACIÓN

Esta fase le permitirá a CORTOLIMA, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI, teniendo en cuenta la actualización de los elementos indicados y la implementación de aquellos que aún no estan funcionales; pero sobretodo apropiar las herramientas de evaluación propuestas para determiner bien el nivel de madurez de manera continua hasta lograr una etructura que garantice que estemos con un Sistema de seguridad y privacidad de la información acorde a las necesidades del entorno interno y externo de la Corporación.

Figura 06. Elementos Fase de Implementación

Tabla 04 - Metas, Resultados e Instrumentos de la Fase de Implementación

Implementación	
Metas	**Resultados**
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.
Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la Corporación, aprobado por la Oficina de TI.
Plan de Transición de IPv4 a IPv6	Documento con las estrategias y pruebas del plan de implementación de IPv6 en la Corporación, aprobado por la Oficina Asesora de Direccionamiento Estraégico TIC.

6. FASE DE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Figura 07 - Fase de Evaluación de desempeño

Tabla 05 - Metas, Resultados e Instrumentos de la Fase de Evaluación de Desempeño

Evaluación del Desempeño	
Metas	**Resultados**
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.
Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.

7. FASE DE MEJORA CONTINUA

En esta fase la Corporación debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

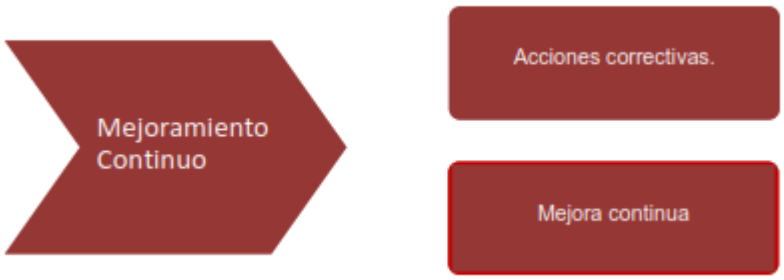

Figura 08 - Fase de mejoramiento continúo

Tabla 6 - Metas, Resultados e Instrumentos de la Fase de Mejora Continua

Mejora Continua		
Metas	**Resultados**	**Instrumentos**
		MSPI
Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Guía No 17 – Mejora Continua

En esta fase es importante que CORTOLIMA defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

- Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.
- Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

Utilizando los insumos anteriores, la Corporación puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI, actualizando de forma contínua todos los elemntos, políticas, manuals, formatos en general involucrados en cada uno de los procesos de seguridad de la información implementados. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección de la Corporación. La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.