Modelo de Seguridad y Privacidad de la Información

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Modelo

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	15/12/2010	Versión inicial del documento
2.0.0	30/09/2011	Restructuración de forma
2.0.1	30/11/2011	Actualización del documento
3.0.0	03/03/2015	Revisión documento
3.0.1	11/03/2016	Actualización del documento
3.0.2	29/07/2016	Actualización del documento

Contenido

1. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en el compendio de las normas técnicas colombianas NTC ISO/IEC 27000 vigentes, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

2. AUDIENCIA

Entidades públicas de orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea.

3. INTRODUCCIÓN

Este documento se elaboró con la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL.

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos,, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

Para el desarrollo del componente de Seguridad y Privacidad de la Información, se ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información, los cuales a lo largo de los últimos años, han sido utilizados por las diferentes entidades tanto del orden nacional como territorial, para mejorar sus estándares de seguridad de la información. El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad

será actualizado periódicamente; así mismo recoge además de los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información; de otro lado el MSPI especifica los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

El Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

El presente modelo pretende facilitar la comprensión del proceso de construcción de una política de privacidad por parte de la entidad, que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información.

Finalmente, a nivel metodológico es importante tener presente que se han incluido una serie de guías en cada una de las fases del modelo, para que los destinatarios del mismo tengan claridad de cuáles son los resultados a obtener y como desarrollarlos.

4. JUSTIFICACIÓN

El Ministerio TIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones, a través de las cuales contribuye a la construcción de un Estado más eficiente, más transparente y participativo, publica El Modelo de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea.

Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información en las entidades, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación Colombiana.

5. 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 entidad 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 determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Autorización:**
  Consentimiento previo, expreso 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 entidades 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, art 6)

- **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 oficiales 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, art 6)

- **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 entidades 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 entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades 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. (Ley 1581 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 entidad. (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.

6. OBJETIVOS

6.1 OBJETIVO GENERAL

Generar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado.

6.2 OBJETIVOS ESPECÍFICOS

- Mediante la utilización del Modelo de Seguridad y Privacidad para las Entidades del Estado, se busca contribuir al incremento de la transparencia en la gestión pública.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Orientar a las entidades en las mejores prácticas en seguridad y privacidad.
- Optimizar la gestión de la seguridad de la información al interior de las entidades.
- Orientar a las entidades en la transición de lPv4 a IPv6 con la utilización de las guías disponibles para tal fin.
- Orientar a las entidades en la adopción de la legislación relacionada con la protección de datos personales.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.

- Contribuir en el desarrollo del ejercicio de arquitectura empresarial apoyando en el cumpliendo de los lineamientos del marco de referencia de arquitectura empresarial para la gestión de TI del estado colombiano.

- Orientar a las entidades destinatarias en las mejores prácticas para la construcción de una política de tratamiento de datos personales respetuosa de los derechos de los titulares.

- Optimizar la labor de acceso a la información pública al interior de las entidades destinatarias.

- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

7. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

En el presente Modelo de Seguridad y Privacidad de la Información se contemplan 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

8. DESCRIPCIÓN DEL CICLO DE OPERACIÓN

En el presente capítulo se explica el ciclo de funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden. Estas, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades.

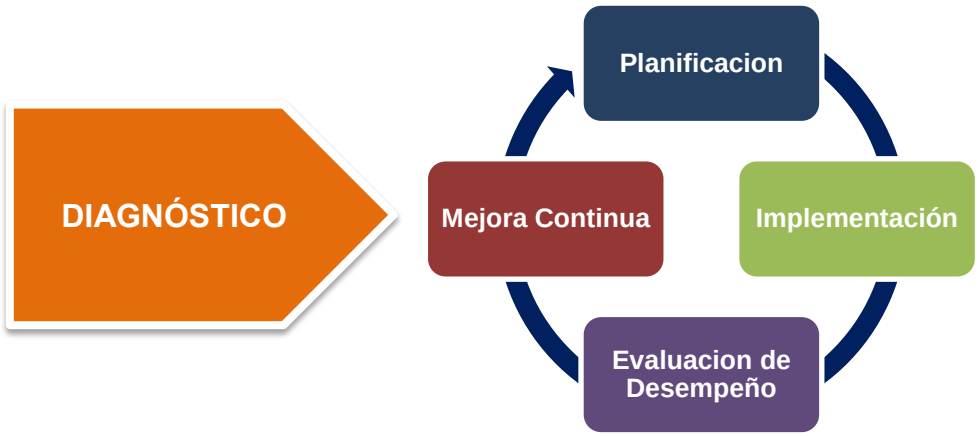


Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

8.1 FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información,

Figura 2 – Etapas previas a la implementación

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

Diagnostico			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación MRAE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14
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.	Herramienta de diagnóstico	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico	

En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.

- 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 entidad.
- 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

Para realizar dicha fase las entidades 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 entidad 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.

8.2 FASE DE PLANIFICACIÓN

Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, 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 permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad.

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.

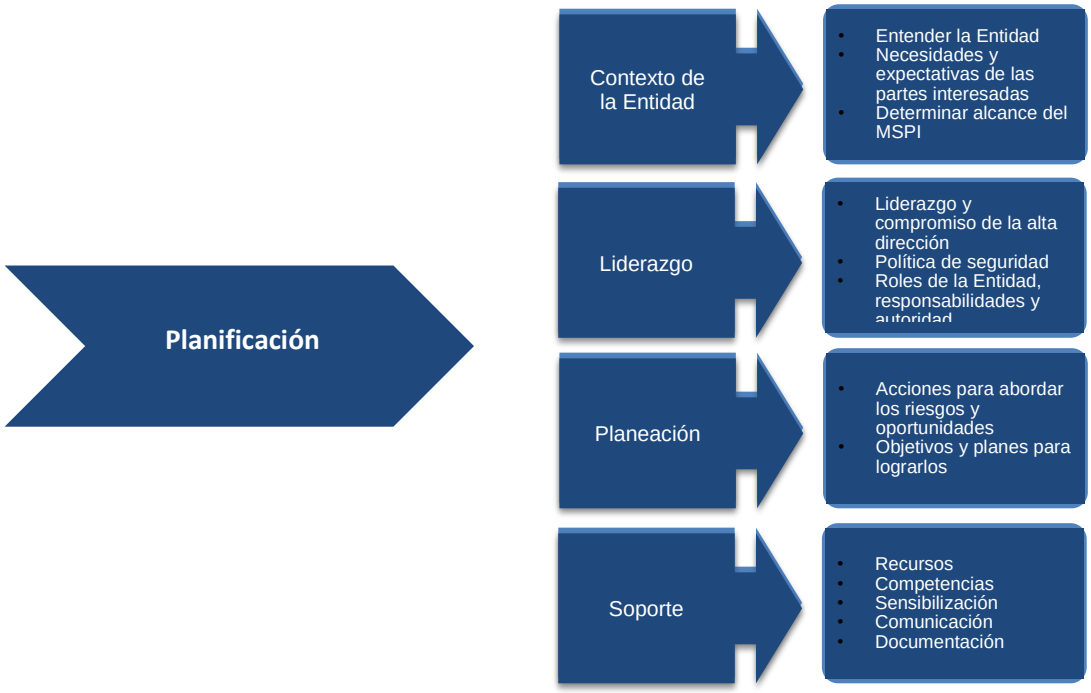


Figura 3 - Fase de planificación[1]

Tabla 2 - Metas, Resultados e Instrumentos de la Fase de Planificación

Planificación			
Metas	**Resultados**	**INSTRUMENTOS MSPI**	**MRAE**
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 Entidad.	Guía No 2 – Política General MSPI	LI.ES.02 LI.ES.06 LI.ES.07 LI.ES.08

[1] El contenido de la figura 3 fue tomada de la Norma ISO IEC 27001 Capítulos 4, 5, 6, 7, que permite orientar como se desarrolla la planificación del MSPI.

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 Entidad.	Guía no 2 - Política General MSPI	LI.ES.09 LI.ES.10 LI.GO.01 LI.GO.04 LI.GO.07 LI.GO.08 LI.GO.09 LI.GO.10 LI.INF.01 LI.INF.02 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.SIS.22 LI.SIS.23 LI.SIS.01 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12 LI.ST.13 LI.ST.14 LI.UA.01 LI.UA.02 LI.UA.03 LI.UA.04 LI.UA.05 LI.UA.06
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.	
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 entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.	
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	Guía No 5 - Gestión De Activos Guía No 20 - Transición Ipv4 a Ipv6	
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Guía No 6 - Gestion Documental	
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.	Guía No 7 - Gestion de Riesgos Guía No 8 - Controles de Seguridad	
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan de comunicación, sensibilización y capacitación	
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Guía No 20 - Transición IPv4 a IPv6	

A continuación se explica de manera general la fase de planificación del Modelo de Seguridad y Privacidad de la Información.

Política de seguridad y privacidad de la información.

La Política de Seguridad y Privacidad de la información está contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.

La política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento.

La política debe ser aprobada y divulgada al interior de la entidad.

Políticas de Seguridad y Privacidad de la Información.

Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información

En el manual de políticas de la entidad, se debe explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente.

La entidad debe evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

Procedimientos de Seguridad de la Información.

En este Ítem se debe desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad.

Para desarrollar esta actividad, la Guía No 3 - describe los procedimientos mínimos que se deberían tener en cuenta para la gestión de la seguridad al interior de la entidad.

Roles y Responsabilidades de Seguridad y Privacidad de la Información.

La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que

permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad.

Para desarrollar estas actividades, la Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información, brinda información relacionada para tal fin.

Inventario de activos de información.

La entidad debe desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.

La Guía No 5 - Gestión De Activos, brinda información relacionada para poder llevar a cabo la realización de las actividades mencionadas previamente.

Integración del MSPI con el Sistema de Gestión documental.

La entidad deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación.

La Guía No 6 - Gestión Documental, brinda información relacionada para poder llevar a cabo la realización de las actividades mencionadas previamente.

Identificación, Valoración Y Tratamiento de Riesgos.

La entidad debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, asi como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se recomienda emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad.

Para definir la metodología, la entidad puede hacer uso de buenas prácticas vigentes tales como: ISO 27005, Margerit, Octave, ISO 31000 o la Guía No 7 - Gestión de Riesgos emitida por el MinTIC.

Para la elaboración del plan de tratamiento de riesgos y la declaración de aplicabilidad, puede emplearse la Guía No 8 - Controles de Seguridad.

Plan de Comunicaciones.

La Entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad.

Este plan será ejecutado, con el aval de la Alta Dirección, a todas las áreas de la Entidad.

Para estructurar dicho plan puede utilizar la Guía No 14 – plan de comunicación, sensibilización y capacitación.

Plan de transición de IPv4 a IPv6.

Para llevar a cabo el proceso de transición de IPv4 a IPv6 en las entidades, se debe cumplir con la fase de planeación establecida en la Guía No 20 - Transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

8.3 FASE DE IMPLEMENTACIÓN

Esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.

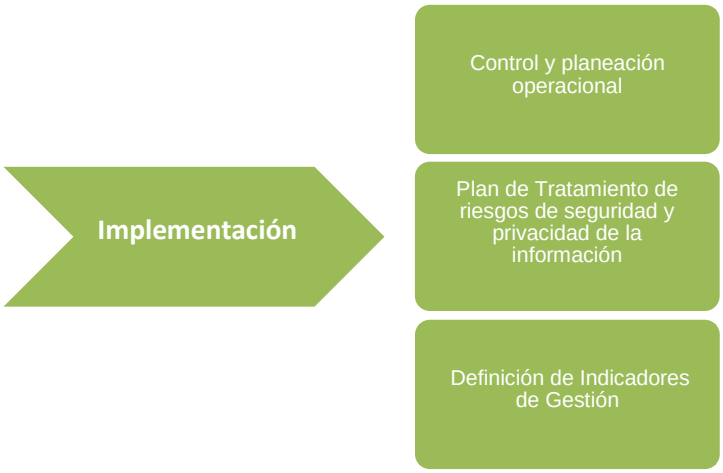


Figura 4 - Fase de implementación[2]

Tabla 3 - Metas, Resultados e Instrumentos de la Fase de Implementación

Implementación			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad.	LI.ES.09 LI.ES.10 LI.GO.04 LI.GO.09 LI.GO.10 LI.GO.14 LI.GO.15 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.INF.15 LI.SIS.22 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos.	
Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Guía No 9 - Indicadores de Gestión SI.	

[2] El contenido de la figura 4 fue tomada de la Norma ISO IEC 27001 Capítulo 8, que permite orientar como se desarrolla la implementación del MSPI.

Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. Guía No 20 - Transición de IPv4 a IPv6 para Colombia. Guía No 19 – Aseguramiento del Protocolo IPv6.	LI.ST.13 LI.UA.01

Con base a los resultados de la fase de planeación, en la fase de implementación deberá ejecutarse las siguientes actividades:

Planificación y Control Operacional.

La entidad debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos.

La entidad debe tener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado, adicionalmente, deberá llevarse un control de cambios que le permitan tomar acciones para mitigar efectos adversos cuando sea necesario.

Implementación del plan de tratamiento de riesgos.

Se debe implementar el plan de tratamiento de riesgos de seguridad de la información, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la entidad, en donde la base para ejecutar esta actividad es la Guía No 8 - de controles de seguridad y privacidad del MSPI.

Es preciso tener en cuenta que la aplicación del control sobre los riesgos detectados deben estar aprobados por el dueño de cada proceso.

Indicadores De Gestión.

La entidad deberá definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

Los indicadores buscan medir:

- ✓ Efectividad en los controles.
- ✓ Eficiencia del MSPI al interior de la entidad.
- ✓ Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora continua.
- ✓ Comunicar valores de seguridad al interior de la entidad.
- ✓ Servir como insumo al plan de control operacional.

La Guía No 9 - Indicadores de Gestión, brinda información relacionada para poder llevar a cabo la realización de esta actividad.

Plan de Transición de IPv4 a IPv6.

Se deberá generar el documento detallado con el plan de transición e implementación del protocolo IPv6 en la entidad.

Las guías de apoyo para esta labor son “Guía de Transición de IPv4 a IPv6 para Colombia” y “Guía de Aseguramiento del Protocolo IPv6”.

8.4 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.

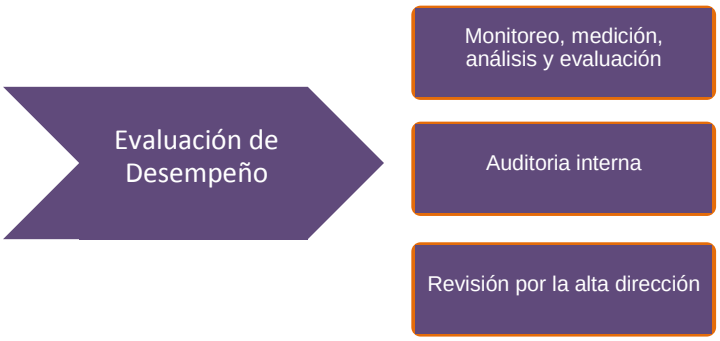


Figura 5 - Fase de Evaluación de desempeño[3]

Tabla 4 - Metas, Resultados e Instrumentos de la Fase de Evaluación de Desempeño

Evaluación del Desempeño			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
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.	Guía No 16 – Evaluación del desempeño.	LI.ES.12 LI.ES.13 LI.GO.03 LI.GO.11 LI.GO.12 LI.INF.09 LI.INF.11 LI.INF.13 LI.INF.14 LI.INF.15 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.08 LI.ST.15 LI.UA.07 LI.UA.08
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.	Guía No 15 – Guía de Auditoría.	

Plan de revisión y seguimiento a la implementación del MSPI.

En esta actividad la entidad debe crear un plan que contemple las siguientes actividades:

[3] El contenido de la figura 5 fue tomada de la Norma ISO IEC 27001 Capítulo 9, que permite orientar como se desarrolla la evaluación de desempeño del MSPI.

- ✓ Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- ✓ Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- ✓ Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.
- ✓ Seguimiento al alcance y a la implementación del MSPI.
- ✓ Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- ✓ Medición de los indicadores de gestión del MSPI
- ✓ Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI)

Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

La Guía No 16 - Evaluación del Desempeño, brinda información relacionada para poder llevar a cabo la realización de esta actividad.

Plan de Ejecución de Auditorias

La entidad debe generar un documento donde se especifique el plan de auditorías para el MSPI, donde especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Se debe llevar a cabo auditorías y revisiones independientes a intervalos planificados que permitan identificar si el MSPI es conforme con los requisitos de la organización, está implementado adecuadamente y se mantiene de forma eficaz; así mismo es necesario difundir a las partes interesadas, los resultados de la ejecución de las auditorías.

Es importante conservar la información documentada como evidencia de los resultados de las auditorías.

La Guía No 15 - Guía de Auditoría, brinda información relacionada para poder llevar a cabo la realización de esta actividad.

8.5 FASE DE MEJORA CONTINUA

En esta fase la Entidad 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.

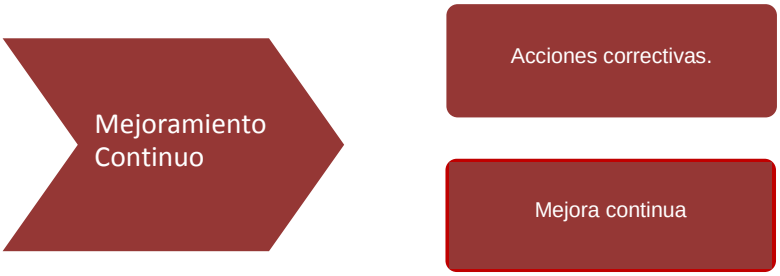


Figura 6 - Fase de mejoramiento continúo[4]

Tabla 5 - Metas, Resultados e Instrumentos de la Fase de Mejora Continua

Mejora Continua			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
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	LI.GO.03 LI.GO.12 LI.GO.13 LI.INF.14 LI.INF.15 LI.ST.15 LI.UA.9 LI.UA.10

[4] El contenido de la figura 6 fue tomada de la Norma ISO IEC 27001 Capítulo 10, que permite orientar como se desarrolla la fase de Mejoramiento Continuo del MSPI.

En esta fase es importante que la entidad 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 entidad puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI. 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 entidad. La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.

La guía No 17 - Mejora Continua, brinda información relacionada para poder llevar a cabo la realización de esta actividad.

9. MODELO DE MADUREZ

Este esquema permite identificar el nivel de madurez del MSPI en el que se encuentran las entidades, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado.

A continuación la figura 7, muestra los diferentes niveles que hacen parte del modelo de madurez.

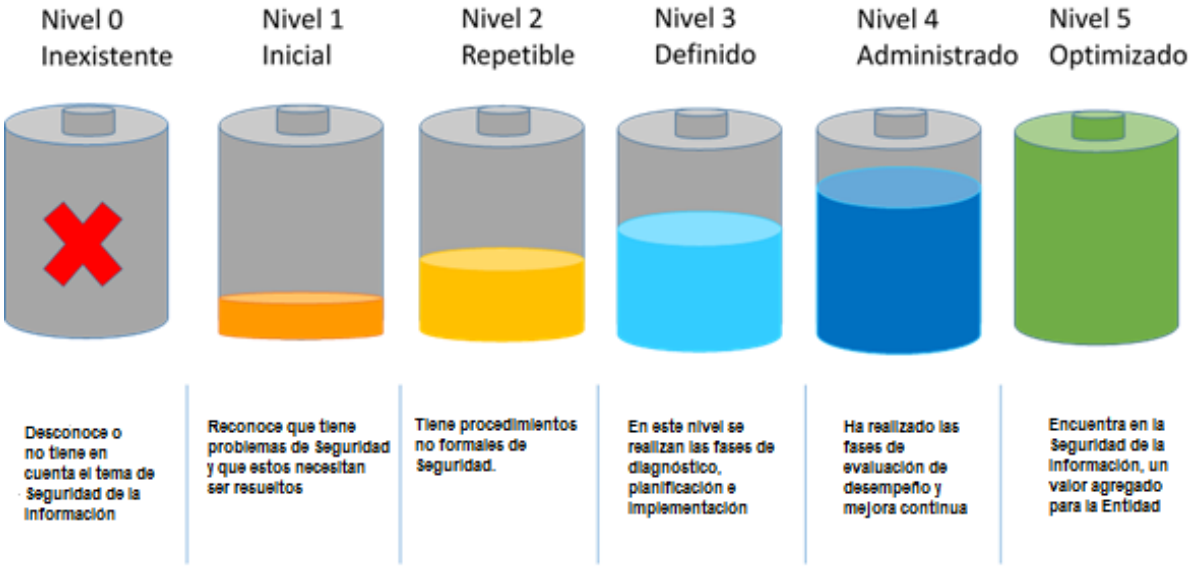


Figura 7- Niveles de madurez

El esquema que muestra los niveles de madurez del MSPI, busca establecer unos criterios de valoración a través de los cuales se determina el estado actual de la seguridad de la información en una entidad del Estado.

En la tabla No 6, se presentan las características de cada uno de los niveles de madurez con una descripción general.

Tabla 6 – Características de los Niveles de Madurez

Nivel	Descripción
Inexistente	• Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo no están alineados a un Modelo de Seguridad. • No se reconoce la información como un activo importante para su misión y objetivos estratégicos. • No se tiene conciencia de la importancia de la seguridad de la información en la entidad.
Inicial	• Se han identificado las debilidades en la seguridad de la información. • Los incidentes de seguridad de la información se tratan de forma reactiva. • Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.
Repetible	• Se identifican en forma general los activos de información. • Se clasifican los activos de información. • Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información. • Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión. • La entidad cuenta con un plan de diagnóstico para IPv6.
Definido	• La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. • La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. • La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. • La Entidad tiene procedimientos formales de seguridad de la Información • La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. • La Entidad ha realizado un inventario de activos de información aplicando una metodología. • La Entidad trata riesgos de seguridad de la información a través de una metodología. • Se implementa el plan de tratamiento de riesgos. • La entidad cuenta con un plan de transición de IPv4 a IPv6.
Administrado	• Se revisa y monitorea periódicamente los activos de información de la Entidad. • Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. • Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. • La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
Optimizado	• En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización. • Se utilizan indicadores de efectividad para establecer si la entidad

	encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales. • La entidad genera tráfico en IPv6.

10. PRIVACIDAD DE LA INFORMACIÓN

Uno de los objetivos del modelo de seguridad y privacidad de la Información es el de garantizar un adecuado manejo de la información pública en poder de las entidades destinatarias, la cual es uno de los activos más valiosos para la toma de decisiones, el modelo propende por un doble enfoque a saber: a nivel de seguridad marcando un derrotero para que las entidades destinatarias construyan unas políticas de seguridad sobre la información a fin de salvaguardar la misma a nivel físico y lógico, de manera que se pueda en todo momento garantizar su integridad, disponibilidad y autenticidad. En esa línea el aseguramiento de los procesos relacionados con los sistemas de información debe complementarse con un enfoque de privacidad para garantizar tanto la protección de los derechos a la intimidad y el buen nombre o la salvaguarda de secretos profesionales, industriales o de información privilegiada de particulares en poder de la administración como el acceso a la información pública cuando esta no se encuentre sometida a reserva. Para ello se requiere dotar al modelo de seguridad de la información de un componente específico relacionado con la privacidad.

Para que los servidores públicos entiendan mejor el concepto de privacidad, hay que tener claro que diferentes procesos relacionados con la recolección y uso de información son susceptibles de ser objeto de implementación de medidas de privacidad, como puede ser:

- ✓ La Implementación de un sistema de información que tenga la posibilidad de recolectar datos personales, tal como un sistema de seguridad a través de video vigilancia que capture imágenes, datos biométricos, etc
- ✓ El Diseño y ejecución de un sistema de gestión documental
- ✓ El Desarrollo de políticas que impliquen la necesidad de recolectar y usar información personal, como por ejemplo políticas de atención de PQR´s
- ✓ La Transferencia de información a terceros (otras entidades o países).

Para ello la entidad debe tener en cuenta los siguientes temas.

Contar con una herramienta de análisis sobre impacto en la privacidad

El MSPI es el instrumento que se pone a disposición de las entidades con el fin de realizar el análisis de impacto que en la privacidad de la información pueda presentarse a partir del desarrollo de las funciones administrativas o el desarrollo misional de cada entidad, teniendo como referente:

- ✓ El marco legal vigente.
- ✓ Las necesidades de los clientes internos y externos de la entidad.
- ✓ La identificación de los posibles problemas recurrentes relacionados con la privacidad.

Descripción de los flujos de información

La descripción de los flujos de información sirve para saber qué información está siendo recolectada, con qué propósito, cómo, en qué cantidad y si la misma es objeto de divulgación.

La fase de diagnóstico de privacidad puede servir como insumo al poder identificar qué información se tiene, dónde y en cabeza de quién. Este ejercicio tiene que ser complementado con la documentación de los procesos relacionados con gestión de la información que la entidad haya levantado, para poder hacer una valoración sobre la circulación de la información, identificando que en la misma no se afecten derechos de los titulares de información o se ponga en riesgo su privacidad.

Identificar los riesgos de privacidad

Los riesgos en relación con la privacidad pueden ser de varios tipos:

- ✓ En relación con la información personal de los individuos
  - ➢ Se expone información clasificada (datos personales no públicos) sin que medie autorización para ello.

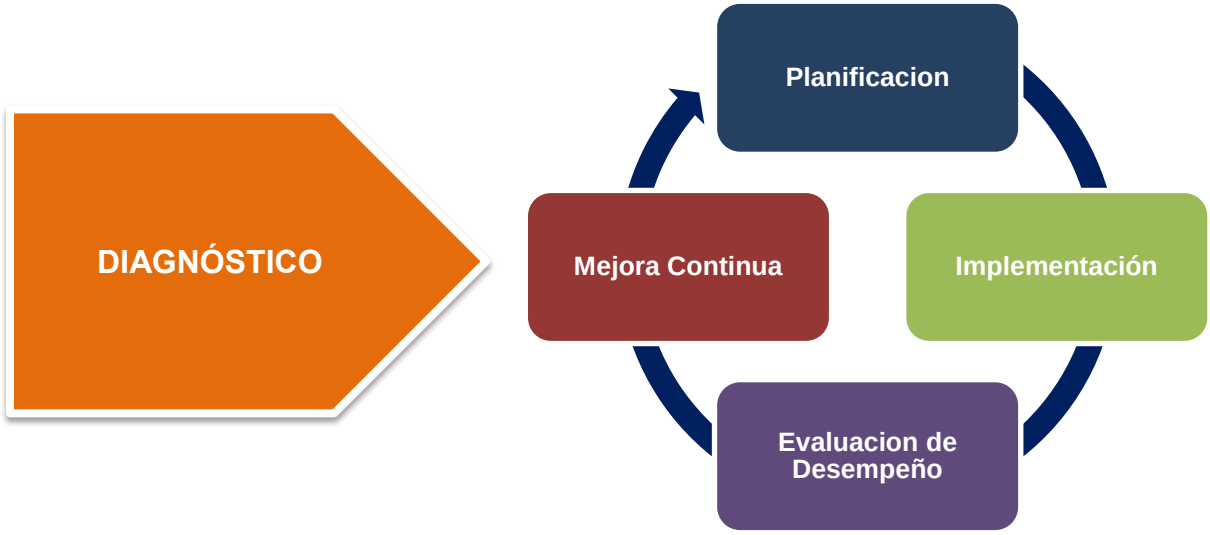
- Uso de sistemas de información o aplicaciones en la interacción con los ciudadanos que pueden ser intrusivos sobre su privacidad sin advertir previamente a los usuarios sobre ello (geolocalización)
- Información que permanece en poder de la entidad por más tiempo de la vigencia que tiene la base de datos o en contra del ejercicio de derecho de supresión por parte del titular-ciudadano.

✓ En relación con la información de usuarios institucionales
- Se divulga información que puede ser clasificada como secreto industrial o que pone en riesgo la imagen corporativa.

✓ En relación con los sistemas de información y programas usados o los procedimientos y procesos relacionados con la gestión administrativa a cargo.
- Procesos no ajustados al sistema de gestión documental que garanticen medidas de protección sobre la información.
- Adquisición de programas que no garanticen un nivel adecuado de privacidad, por ejemplo que permitan recolección masiva de datos sin conocimiento de los usuarios.
- Indebida utilización de datos personales en ejercicios de divulgación tales como procesos de rendición de cuentas, publicación de información en la página web, etc.

El análisis debe reflejarse en una matriz de riesgos ponderando la probabilidad de su ocurrencia (ejemplo: baja-intermedia-alta) y el impacto que puede generar su causación (se sugiere utilizar una tabla numérica, por ejemplo - 1 ningún impacto a 10 impacto considerable).

La implementación del componente de privacidad sigue el mismo ciclo de operación adoptado para seguridad de la información consistente en cinco fases o etapas así: diagnóstico, planeación, implementación, gestión y mejora continua.



10.1 Fase Diagnostico

En esta fase es necesario que las entidades identifiquen cómo se está garantizando la privacidad sobre todo el ciclo de la información que tienen en su poder verificando la implantación o no de medidas que den cumplimiento a los requerimientos de las normas sobre protección de datos personales y que, adicionalmente contribuya a identificar la información pública sometida a reserva o clasificada en los términos de la Ley.

Para ello se pone a disposición de las entidades, el instrumento de diagnóstico y seguimiento a la implementación. A través del diligenciamiento de este instrumento se podrá conocer la realidad de la información relacionada con el manejo de los activos de la información que reposen en bancos de datos o archivos y a partir de allí determinar las medidas a nivel procedimental que deben adelantar las entidades para otorgar un nivel adecuado de protección a esta información.

Tabla 7 - Metas, Resultados e Instrumentos de la Fase de Diagnostico

Diagnostico			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Diagnostico	Realizar el diagnóstico de las condiciones en que se encuentran los activos de información administrados por la entidad. Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	
	Documento con el resultado del diagnóstico realizado por la entidad con la clasificación y distinción de los activos de información teniendo en cuenta la información con datos personales y aquellos que no lo son identificando la criticidad de la información clasificada o reservada.		

Con el resultado del diagnóstico se puede contar con un insumo frente a la identificación de aquella información que debe ser manejada como privada (clasificada en los términos de la Ley) para a partir de allí incorporar las medidas de seguridad proporcionales a su naturaleza como los procedimientos que lleven al cumplimiento de la normatividad de protección de datos, transparencia y acceso a la información pública soportado todo ello en la incorporación de un sistema de privacidad por diseño que responda a la realidad presupuestal, humana y técnica de cada entidad.

Para construir los instrumentos de gestión de la información pública, las entidades pueden remitirse a la Guía sobre Instrumentos de Gestión de la Información Pública de la Secretaría de Transparencia de la Presidencia de la República.

10.2 Fase Planificación

En esta segunda etapa se debe trazar la estrategia con el objetivo de organizar el trabajo adelantado por la entidad a partir de las características recogidas en la fase de diagnóstico, para acercarlas a un nivel de cumplimiento adecuado para salvaguardar la información privada y de manera concomitante responder a los retos de disponibilidad a la información pública por parte de la ciudadanía, así

como para ajustar los roles del personal designado para cumplir con las responsabilidades de seguridad y privacidad de la información.

Para ello deben ajustarse las políticas, los procesos y procedimientos ya definidos en el modelo de seguridad con el fin de incorporar la privacidad con el alcance mencionado.

Tabla 8 - Metas, Resultados e Instrumentos de la Fase de Planificación

Planificación			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Planificación	Documento con la política de privacidad, debidamente aprobada por la alta dirección y socializada al interior de la entidad. Manual de políticas de seguridad y privacidad de la información, aprobada por la alta dirección y socializada al interior de la entidad. Documento con el plan de gestión de la privacidad sobre la información, aprobado por la alta dirección de la entidad. Definición de roles en relación con la Información. Procedimientos de privacidad. Plan de capacitación al interior de la entidad	Herramienta de diagnóstico. Guía No 4 - Roles y Responsabilidades de Seguridad y Privacidad de la Información. Guía No 2 – Política General.	

10.3 Fase de Implementación

En esta fase se deben ejecutar las acciones trazadas en la etapa previa de planeación de manera que la entidad diseñe un modelo de privacidad que le permita cumplir con los mínimos legales y generar una política privacidad que le permita la correcta gestión de la información.

De esta manera se da cumplimiento normativo, como: registro de bases de datos en el RNBD, índice de información clasificado y reservado revisado,

procedimiento interno ajustado a la gestión de la privacidad de la información diseñada.

Tabla 9 - Metas, Resultados e Instrumentos de la Fase de Implementación

Implementación			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Implementación	Documento con los riesgos contra la privacidad identificados y las medidas de solución adoptadas a partir de la implementación del plan de gestión de la privacidad de la información Documento que evidencie el registro de las Bases de datos, Documento con el índice de información clasificada, reservada, revisada y sus procedimientos ajustados	Herramienta de Diagnóstico. Guía No 7 – Gestion de Riesgos.	

10.4 Fase de Evaluación del desempeño

Una vez implementadas las anteriores actividades el modelo de privacidad se evalúa, para medir la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI y la aplicación de la Ley de Transparencia y Acceso a la Información Pública.

Tabla 9 - Metas, Resultados e Instrumentos de la Fase de Evaluación de Desempeño

Evaluacion de Desempeño			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Evaluación del desempeño	Documento con los resultados del plan de seguimiento Documento con el Plan de auditoría interna y resultados revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces Comunicación de los indicadores al público a través de la rendición de cuentas, informe a la PGN y al Congreso de la República.	Guía No 16 – Evaluación del Desempeño. Guía No 15 – Auditoria. Guía No 14 – Plan de Comunicación, sensibilización y capacitación.	

10.5 Fase de Mejora Continua

Una vez se tengan los resultados del componente de evaluación del desempeño se toman los resultados obtenidos y se preparan los correctivos necesarios que permitan a la misma crecer en el nivel de responsabilidad demostrada.

Tabla 10 - Metas, Resultados e Instrumentos de la Fase de Mejora Continua

Mejora Continua			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Mejora Continua	Documento con los resultados del plan de seguimiento Documento con los resultados del plan de mejoramiento revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces. Documento con el consolidado de las auditorias.	Guía No 16 – Evaluación del Desempeño. Guía No 17 - Mejora Continua.	

11. ADOPCIÓN DEL PROTOCOLO IPv6

En el presente capitulo se relacionan las fases para el proceso de transición del protocolo IPv4 a IPv6 que orientará a las entidades del gobierno y a la sociedad en general en el análisis, la planeación y la implementación del protocolo IPv6.

Figura 8 - Fases del proceso de transición del protocolo IPv4 al IPv6

11.1 FASE DE PLANEACIÓN

En esta fase, se debe definir el plan y la estrategia de transición de IPv4 a IPv6, en procura de los resultados que permitan dar cumplimiento con la adopción del nuevo protocolo.

En la Tabla No 10 se describen las metas, entregables e instrumentos que pueden ser utilizados para cumplir esta actividad, de conformidad con la Guía de Transición de IPV4 a IPV6 para Colombia.

Tabla 11 - Metas, Resultados e Instrumentos de la Fase de Planeación

Planeacion			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Plan y estrategia de transición de IPv4 a IPv6.	Plan de diagnóstico que debe contener los siguientes componentes: Inventario de TI (Hardware y software) de cada Entidad diagnosticada, Informe de la Infraestructura de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones , de cómputo y almacenamiento con el cumplimiento de IPv6, plan de direccionamiento en IPv6, plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6, Informe de preparación (Readiness) de los sistemas de comunicaciones, bases de datos y aplicaciones. Documento que define la estrategia de para la implementación y aseguramiento del protocolo IPv6 en concordancia con la política de seguridad de las entidades.	Guía No 20 – Transición IPv4 a IPv6. Guía No 19 – Aseguramiento del protocolo IPv6. Circular 002 de 2011 del MinTIC.	

11.2 FASE DE IMPLEMENTACIÓN

En esta fase se realizan actividades tales como habilitación del direccionamiento de IPv6, montaje, ejecución y corrección de configuraciones para pruebas piloto,

activar las políticas de seguridad de IPv6, validar la funcionalidad de los servicios y aplicaciones de las entidades, entre otras.

En la Tabla No 12 se describen las metas, entregables e instrumentos que pueden ser utilizados para cumplir esta actividad, de conformidad con la Guía de Transición de IPV4 a IPV6 para Colombia

.

Tabla 12 - Metas, Resultados e Instrumentos de la Fase de Implementación.

Implementación			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Implementación del plan y estrategia de transición de IPv4 a IPv6.	Documento con el informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.	Guía No 20 – Guía Transición de IPv4 a IPv6 para Colombia Guía No 19 - Guía de Aseguramiento del Protocolo IPv6.	

11.3 FASE – PRUEBAS DE FUNCIONALIDAD

En esta fase se hacen pruebas de funcionalidad y/o monitoreo de IPv6, en sistemas de información, de almacenamiento, de comunicaciones y servicios; frente a las políticas de seguridad perimetral, de servidores de cómputo, equipos de comunicaciones, de almacenamiento, entre otros. Tener en cuenta que se debe elaborar un inventario final de servicios y sistemas de comunicaciones, bajo el nuevo esquema de funcionamiento de IPv6.

En la Tabla 13 se describen las metas, entregables e instrumentos que pueden ser utilizados para cumplir esta actividad, de conformidad con la Guía de Transición de IPV4 a IPV6 para Colombia.

Tabla 13 - Metas, Resultados e Instrumentos de la Fase de Pruebas de Funcionalidad.

Pruebas de Funcionalidad			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Plan de pruebas de funcionalidad de IPv4 a IPv6.	Documento con los cambios detallados de las configuraciones realizadas, previo al análisis de funcionalidad realizado en la fase II de Implementación. Acta de cumplimiento a satisfacción de la Entidad con respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos durante la fase II de la implementación. Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.	Guía No 20 – Guía Transición de IPv4 a IPv6 para Colombia Guía No 19 - Guía de Aseguramiento del Protocolo IPv6.	

12. PLAZOS

Los plazos para la implementación de las actividades se establecieron para el Manual de Gobierno en Línea, y a través del Decreto 1078 de 2015, en el Artículo 10. "Plazos. Los sujetos obligados deberán implementar las actividades establecidas en el Manual de Gobierno en Línea dentro de los siguientes plazos:

12.1 Sujetos Obligados del Orden Nacional

Componente/Año	2015	2016	2017	2018	2019	2020
TIC para ser servicios	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para Gobierno abierto	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	25%	50%	80%	100%	Mantener 100%	Mantener 100%
Seguridad y Privacidad de la Información	40%	60%	80%	100%	Mantener 100%	Mantener 100%

12.2 Sujetos Obligados del Orden Territorial

A. Gobernaciones de categoría Especial y Primera; alcaldías de categoría Especial, y demás sujetos obligados de la administración publica en el mismo nivel.

B. Gobernaciones de categoría segunda, tercera y cuarta; alcaldías de categoría primera, segunda y tercera y demás sujetos obligados de la Administración Pública en el mismo nivel.

C. Alcaldías de categoría cuarta, quinta y sexta y demás sujetos obligados de la Administración Pública en el mismo nivel.

Para las entidades agrupadas en A, B y C los plazos serán los siguientes:

Componente/Año	Entidades A (%)					
	2015	2016	2017	2018	2019	2020
TIC para ser servicios	70%	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%

TIC para Gobierno abierto	80%	95%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	20%	45%	80%	100%	Mantener 100%	Mantener 100%
Seguridad y Privacidad de la Información	**35%**	**50%**	**80%**	**100%**	**Mantener 100%**	**Mantener 100%**

Componente/Año	Entidades B (%)					
	2015	2016	2017	2018	2019	2020
TIC para ser servicios	45%	70%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para Gobierno abierto	65%	80%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	10%	30%	50%	65%	80%	100%
Seguridad y Privacidad de la Información	10%	30%	50%	65%	80%	100%

Componente/Año	Entidades C (%)					
	2015	2016	2017	2018	2019	2020
TIC para ser servicios	45%	70%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para Gobierno abierto	65%	80%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	10%	30%	50%	65%	80%	100%
Seguridad y Privacidad de la Información	10%	30%	50%	65%	80%	100%

12.3 Guías Modelo de Seguridad y Privacidad de la Información

Los siguientes documentos se diseñados para un mejor entendimiento de las entidades en la implementación el Modelo de Seguridad y Privacidad de la Información.

	Modelo de Seguridad y Privacidad de la Información
	Instructivo Herramienta de Diagnostico
	Herramienta de Diagnostico
	Guía Mi pymes

Guía 1	Metodología de pruebas de efectividad
Guía 2	Política General MSPI v1
Guía 3	Procedimientos de Seguridad y Privacidad de la Información
Guía 4	Roles y responsabilidades de seguridad y privacidad de la información
Guía 5	Gestión de Activos
Guía 6	Gestión Documental
Guía 7	Gestión de Riesgos
Guía 8	Controles de Seguridad
Guía 9	Indicadores Gestión SI
Guía 10	Continuidad de TI
Guía 11	Impacto Negocio
Guía 12	Seguridad en la Nube
Guía 13	Guía De Evidencia Digital
Guía 14	Plan de comunicación, sensibilización y capacitación
Guía 15	Auditoria
Guía 16	Evaluación del Desempeño
Guía 17	Mejora Continua
Guía 18	Lineamientos terminales de áreas financieras entidades públicas
Guía 19	Aseguramiento del protocolo IPV6
Guía 20	Transición IPv4_IPv6
Guía 21	Gestión de Incidentes

12.4 Guías Marco de Referencia de Arquitectura Empresarial

REFERENCIA	LINEAMIENTO	DESCRIPCIÓN
LI.ES.01	**Entendimiento estratégico - LI.ES.01**	Las instituciones de la administración pública deben contar con una estrategia de TI que esté alineada con las estrategias sectoriales, el Plan Nacional de Desarrollo, los planes sectoriales, los planes decenales - cuando existan- y los planes estratégicos institucionales. La estrategia de TI debe estar orientada a generar valor y a contribuir al logro de los objetivos estratégicos.
LI.ES.02	**Definición de la Arquitectura Empresarial - LI.ES.02**	Cada sector e institución, mediante un trabajo articulado, debe contar con una Arquitectura Empresarial que permita materializar su visión estratégica utilizando la tecnología como agente de transformación. Para ello, debe aplicar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI del país, teniendo en cuenta las características específicas del sector o la institución.

LI.ES.06	**Políticas y estándares para la gestión y gobernabilidad de TI - LI.ES.06**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar y definir las políticas y estándares que faciliten la gestión y la gobernabilidad de TI, contemplando por lo menos los siguientes temas: seguridad, continuidad del negocio, gestión de información, adquisición, desarrollo e implantación de sistemas de información, acceso a la tecnología y uso de las facilidades por parte de los usuarios. Así mismo, se debe contar con un proceso integrado entre las instituciones del sector que permita asegurar el cumplimiento y actualización de las políticas y estándares de TI.
LI.ES.07	**Plan de comunicación de la estrategia de TI - LI.ES.07**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir el plan de comunicación de la estrategia, las políticas, los proyectos, los resultados y los servicios de TI.
LI.ES.08	**Participación en proyectos con componentes de TI - LI.ES.08**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe participar de forma activa en la concepción, planeación y desarrollo de los proyectos de la institución que incorporen componentes de TI. Así mismo, debe asegurar la conformidad del proyecto con los lineamientos de la Arquitectura Empresarial definidos para la institución.
LI.ES.09	**Control de los recursos financieros - LI.ES.09**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar de manera periódica el seguimiento y control de la ejecución del presupuesto y el plan de compras asociado a los proyectos estratégicos del PETI.
LI.ES.10	**Gestión de proyectos de inversión - LI.ES.10**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe ser la responsable de formular, administrar, ejecutar y hacer seguimiento de las fichas de los proyectos de inversión requeridos para llevar a cabo la implementación de la Estrategia TI. El proceso de gestión de proyectos de inversión debe cumplir con los lineamientos que para este efecto establezca el Departamento Nacional de Planeación (DNP).
LI.ES.12	**Evaluación de la gestión de la estrategia de TI - LI.ES.12**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar de manera periódica la evaluación de la gestión de la Estrategia TI, para determinar el nivel de avance y cumplimiento de las metas definidas en el PETI.
LI.ES.13	**Tablero de indicadores - LI.ES.13**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un tablero de indicadores sectorial y por institución, que permita tener una visión integral de los avances y resultados en el desarrollo de la Estrategia TI.
LI.GO.01	**Alineación del gobierno de TI - LI.GO.01**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar un esquema de Gobierno TI que estructure y direccione el flujo de las decisiones de TI, que garantice la integración y la alineación con la normatividad vigente, las políticas, los procesos y los servicios del Modelo Integrado de Planeación y Gestión de la institución.
LI.GO.03	**Conformidad - LI.GO.03**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir y realizar actividades que conduzcan a evaluar, monitorear y direccionar los resultados de las soluciones de TI para apoyar los procesos internos de la institución. Debe además tener un plan específico de atención a aquellos procesos que se encuentren dentro de la lista de no conformidad del marco de las auditorías de control interno y externo de gestión, a fin de cumplir con el compromiso de mejoramiento continuo de la administración pública de la institución.
LI.GO.04	**Cadena de Valor de TI - LI.GO.04**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el macro-proceso de gestión de TI, según los lineamientos del Modelo Integrado de Planeación y Gestión de la institución, teniendo en cuenta el Modelo de gestión estratégica de TI.
LI.GO.05	**Capacidades y recursos de TI - LI.GO.05**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir, direccionar, evaluar y monitorear las capacidades disponibles y las requeridas de TI, las cuales incluyen los recursos y el talento humano necesarios para poder ofrecer los servicios de TI.

LI.GO.07	**Criterios de adopción y de compra de TI - LI.GO.07**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios y métodos que direccionen la toma de decisiones de inversión en Tecnologías de la Información (TI), buscando el beneficio económico y de servicio de la institución. Para todos los proyectos en los que se involucren TI, se deberá realizar un análisis del costo total de propiedad de la inversión, en el que se incorporen los costos de los bienes y servicios, los costos de operación, el mantenimiento, el licenciamiento, el soporte y otros costos para la puesta en funcionamiento de los bienes y servicios por adquirir. Este estudio debe realizarse para establecer los requerimientos de financiación del proyecto. Debe contemplar los costos de capital (CAPEX) y los costos de operación (OPEX).
LI.GO.08	**Retorno de la inversión de TI - LI.GO.08**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe establecer la relación costo-beneficio y justificar la inversión de los proyectos de TI. Para establecer el retorno de la inversión, se deberá estructurar un caso de negocio para el proyecto, con el fin de asegurar que los recursos públicos se utilicen para contribuir al logro de beneficios e impactos concretos de la institución. Debido a la imposibilidad de obtener retorno monetario en algunos casos, ya que se trata de gestiones sin ánimo de lucro, los beneficios deben contemplar resultados de mejoramiento del servicio, de la oportunidad, de la satisfacción del ciudadano y del bienestar de la población, entre otros.
LI.GO.09	**Liderazgo de proyectos de TI - LI.GO.09**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe liderar la planeación, ejecución y seguimiento a los proyectos de TI. En aquellos casos en que los proyectos estratégicos de la institución incluyan componentes de TI y sean liderados por otras áreas. La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, deberá liderar el trabajo sobre el componente de TI conforme con los lineamientos de la Arquitectura Empresarial de la institución.
LI.GO.10	**Gestión de proyectos de TI - LI.GO.10**	El gerente de un proyecto, por parte de la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, deberá evaluar, direccionar y monitorear lo relacionado con TI, incluyendo como mínimo los siguientes aspectos: alcance, costos, tiempo, equipo humano, compras, calidad, comunicación, interesados, riesgos e integración. Desde la estructuración de los proyectos de TI y hasta el cierre de los mismos, se deben incorporar las acciones necesarias para gestionar los cambios que surjan.
LI.GO.11	**Indicadores de gestión de los proyectos de TI - LI.GO.11**	El gerente de un proyecto, por parte de la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe monitorear y hacer seguimiento a la ejecución del proyecto, por medio de un conjunto de indicadores de alcance, tiempo, costo y calidad que permitan medir la eficiencia y efectividad del mismo.
LI.GO.12	**Evaluación del desempeño de la gestión de TI - LI.GO.12**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar el monitoreo y evaluación de desempeño de la gestión de TI a partir de las mediciones de los indicadores del macro-proceso de Gestión TI.
LI.GO.13	**Mejoramiento de los procesos - LI.GO.13**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar áreas con oportunidad de mejora, de acuerdo con los criterios de calidad establecidos en el Modelo Integrado de Planeación y Gestión de la institución, de modo que pueda focalizar esfuerzos en el mejoramiento de los procesos de TI para contribuir con el cumplimiento de las metas institucionales y del sector.
LI.GO.14	**Gestión de proveedores de TI - LI.GO.14**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe administrar todos los proveedores y contratos para el desarrollo de los proyectos de TI. Durante el proceso contractual se debe aplicar un esquema de dirección, supervisión, seguimiento, control y recibo a satisfacción de los bienes y servicios contratados.
LI.GO.15	**Transferencia de información y conocimiento - LI.GO.15**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe gestionar la transferencia de conocimiento asociado a los bienes y servicios contratados por la institución. Además debe contar con planes de formación y de transferencia de conocimiento en caso de cambios del recurso humano interno.

LI.INF.01	**Responsabilidad y gestión de Componentes de información - LI.INF.01**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir las directrices y liderar la gestión de los Componentes de información durante su ciclo de vida. Así mismo, debe trabajar en conjunto con las dependencias para establecer acuerdos que garanticen la calidad de la información.
LI.INF.02	**Plan de calidad de los componentes de información - LI.INF.02**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un plan de calidad de los componentes de información que incluya etapas de aseguramiento, control e inspección, medición de indicadores de calidad, actividades preventivas, correctivas y de mejoramiento continuo de la calidad de los componentes.
LI.INF.09	**Canales de acceso a los Componentes de información - LI.INF.09**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe garantizar los mecanismos que permitan el acceso a los servicios de información por parte de los diferentes grupos de interés, contemplando características de accesibilidad, seguridad y usabilidad.
LI.INF.10	**Mecanismos para el uso de los Componentes de información - LI.INF.10**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe impulsar el uso de su información a través de mecanismos sencillos, confiables y seguros, para el entendimiento, análisis y aprovechamiento de la información por parte de los grupos de interés.
LI.INF.11	**Acuerdos de intercambio de Información - LI.INF.11**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe establecer los Acuerdos de Nivel de Servicio (ANS) con las dependencias o instituciones para el intercambio de la información de calidad, que contemplen las características de oportunidad, disponibilidad y seguridad que requieran los Componentes de información.
LI.INF.13	**Hallazgos en el acceso a los Componentes de información - LI.INF.13**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe generar mecanismos que permitan a los consumidores de los Componentes de información reportar los hallazgos encontrados durante el uso de los servicios de información.
LI.INF.14	**Protección y privacidad de Componentes de información - LI.INF.14**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar, en los atributos de los Componentes de información, la información asociada con los responsables y políticas de la protección y privacidad de la información, conforme con la normativa de protección de datos de tipo personal y de acceso a la información pública.
LI.INF.15	**Auditoría y trazabilidad de Componentes de información - LI.INF.15**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los Componentes de información. Estos mecanismos deben ser considerados en el proceso de gestión de dicho Componentes. Los sistemas de información deben implementar los criterios de trazabilidad y auditoría definidos para los Componentes de información que maneja.
LI.SIS.01	**Definición estratégica de los sistemas de información - LI.SIS.01**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir la arquitectura de los sistemas de información teniendo en cuenta las relaciones entre ellos y la articulación con los otros dominios del Marco de Referencia.
LI.SIS.11	**Ambientes independientes en el ciclo de vida de los sistemas de información - LI.SIS.11**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe disponer de ambientes independientes y controlados destinados para desarrollo, pruebas, operación, certificación y capacitación de los sistemas de información, y debe aplicar mecanismos de control de cambios de acuerdo con las mejores prácticas.
LI.SIS.22	**Seguridad y privacidad de los sistemas de información - LI.SIS.22**	En el diseño de sus sistemas de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar aquellos componentes de seguridad para el tratamiento de la privacidad de la información, la implementación de controles de acceso, así como los mecanismos de integridad y cifrado de la información.
LI.SIS.23	**Auditoría y trazabilidad de los sistemas de información - LI.SIS.23**	En el diseño de sus sistemas de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios.

LI.ST.05	**Continuidad y disponibilidad de los Servicios tecnológicos - LI.ST.05**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe garantizar que sus Servicios Tecnológicos estén respaldados con sistemas de alimentación eléctrica, mecanismos de refrigeración, soluciones de detección de incendios, sistemas de control de acceso y sistemas de monitoreo de componentes físicos que aseguren la continuidad y disponibilidad del servicio, así como la capacidad de atención y resolución de incidentes.
LI.ST.06	**Alta disponibilidad de los Servicios tecnológicos - LI.ST.06**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar capacidades de alta disponibilidad que incluyan balanceo de carga y redundancia para los Servicios Tecnológicos que afecten la continuidad del servicio de la institución, las cuales deben ser puestas a prueba periódicamente.
LI.ST.08	**Acuerdos de Nivel de Servicios - LI.ST.08**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe velar por el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) para los Servicios Tecnológicos.
LI.ST.10	**Planes de mantenimiento - LI.ST.10**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar un plan de mantenimiento preventivo sobre toda la infraestructura y los Servicios Tecnológicos.
LI.ST.12	**Gestión preventiva de los Servicios tecnológicos - LI.ST.12**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe asegurarse de que la infraestructura que soporta los Servicios Tecnológicos de la institución cuente con mecanismos de monitoreo para generar alertas tempranas ligadas a los umbrales de operación que tenga definidos.
LI.ST.13	**Respaldo y recuperación de los Servicios tecnológicos - LI.ST.13**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un proceso periódico de respaldo de la configuración de sus Servicios Tecnológicos, así como de la información almacenada en la infraestructura tecnológica. Este proceso debe ser probado periódicamente y debe permitir la recuperación íntegra de los Servicios Tecnológicos.
LI.ST.14	**Análisis de vulnerabilidades - LI.ST.14**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el análisis de vulnerabilidades de la infraestructura tecnológica, a través de un plan de pruebas que permita identificar y tratar los riesgos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI.
LI.ST.15	**Monitoreo de seguridad de infraestructura tecnológica - LI.ST.15**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar controles de seguridad para gestionar los riesgos asociados al acceso, trazabilidad, modificación o pérdida de información que atenten contra la disponibilidad, integridad y confidencialidad de la información.
LI.ST.16	**Tecnología verde - LI.ST.16**	La institución debe implementar un programa de correcta disposición final de los residuos tecnológicos, incluyendo las opciones de reutilización a través de otros programas institucionales con los que cuente el gobierno nacional.
LI.UA.01	**Estrategia de Uso y apropiación - LI.UA.01**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de definir la estrategia de Uso y Apropiación de TI, articulada con la cultura organizacional de la institución, y de asegurar que su desarrollo contribuya con el logro de los resultados en la implementación de los proyectos de TI.
LI.UA.02	**Matriz de interesados - LI.UA.02**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con una matriz de caracterización que identifique, clasifique y priorice los grupos de interés involucrados e impactados por los proyectos de TI.
LI.UA.03	**Involucramiento y compromiso - LI.UA.03**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de asegurar el involucramiento y compromiso para llamar a la acción de los grupos de interés, partiendo desde la alta dirección hacia al resto de los niveles organizacionales, de acuerdo con la matriz de caracterización.
LI.UA.04	**Esquema de incentivos - LI.UA.04**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de identificar y establecer un esquema de incentivos que, alineado con la estrategia de Uso y Apropiación, movilice a los grupos de interés para adoptar favorablemente los proyectos de TI.
LI.UA.05	**Plan de formación - LI.UA.05**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de asegurar que el plan de formación de la institución incorpora adecuadamente el desarrollo de las competencias

		internas requeridas en TI.
LI.UA.06	**Preparación para el cambio - LI.UA.06**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de elaborar un plan de gestión del cambio para facilitar el Uso y Apropiación de los proyectos de TI. Este plan debe incluir las prácticas, procedimientos, recursos y herramientas que sean necesarias para lograr el objetivo.
LI.UA.07	**Evaluación del nivel de adopción de TI - LI.UA.07**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con indicadores de Uso y Apropiación para evaluar el nivel de adopción de la tecnología y la satisfacción en su uso, lo cual permitirá desarrollar acciones de mejora y transformación.
LI.UA.08	**Gestión de impactos - LI.UA.08**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de administrar los efectos derivados de la implantación de los proyectos de TI.
LI.UA.10	**Acciones de mejora - LI.UA.10**	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe diseñar acciones de mejora y transformación a partir del monitoreo de la implementación de su estrategia de Uso y Apropiación y de la aplicación de mecanismos de retroalimentación.