PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION PSPI

TELEVISION REGIONAL DEL ORIENTE LTDA
CANAL TRO

CONTENIDO

INTRODUCCIÓN

Toda organización, independientemente de su tamaño y naturaleza, debe comprender los riesgos que plantea la variedad actual de amenazas a la privacidad y la seguridad de la información, que, cuando se materialicen, no solo generarán costos financieros o sanciones legales; esto afecta no solo su imagen y reputación, sino también la continuidad del negocio. Lo anterior, combinado con un entorno de tecnología de seguridad y administración cada vez más complejo, significa que la seguridad de la información se está convirtiendo cada vez más parte de los objetivos y planes estratégicos de una organización. Por lo tanto, las autoridades de una organización responsables de proteger y asegurar sus recursos, infraestructura e información deben adoptar, implementar y mejorar las medidas de seguridad para prevenir y/o detectar riesgos que puedan comprometer la disponibilidad. Administrar la integridad y confidencialidad de los activos de información de una empresa, ya sea corporativa o personal, pública o privada.

En la medida que las organizaciones tengan una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad tanto de la información del negocio como los datos de carácter personal de sus empleados, usuarios y partes interesadas. Es indispensable que las organizaciones realicen una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riegos que pueden afectar su seguridad, con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

Para el Canal TRO es fundamental garantizar y proteger la seguridad y protección de la información y los datos personales de toda la comunidad institucional, entendiendo que la protección de su información es esencial para avalar una adecuada gestión financiera, administrativa y operativa y, por lo tanto, se requiere la implementación de un marco regulatorio de seguridad de la información que incluya políticas, responsabilidades y obligaciones para la seguridad y privacidad de la información.

Este documento incluye el plan de seguridad y privacidad de la información para el Canal TRO, que tendrá como referencia el modelo de seguridad y privacidad de la estrategia de gestión en línea y la norma ISO 27001, los cuales suministran un marco metodológico basado en buenas prácticas para la implantación de un modelo de gestión de la seguridad

y privacidad de la información en todo tipo de organizaciones, que permita su gestión efectiva y asegure su continuidad y adecuado desarrollo.

1. JUSTIFICACIÓN

Para Canal TRO es importante la protección de la información, con el fin de crear una cultura diseñada para minimizar y eliminar el riesgo de los activos informáticos y sistemas de información. El Plan de Seguridad y Privacidad de la Información (PSPI) está basado en un enfoque de planificación de la gestión de riesgos y tomar decisiones sobre el impacto del mismo donde se debe implementar estrategias que permitan el diagnóstico, evaluación, ejecución y luego el desarrollo de la gestión de eventos que afectan la continuidad de la información y las contramedidas para reducir la probabilidad de la ocurrencia.

2. OBJETIVOS

Generar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad de la información, estableciendo las estrategias y actividades que están contempladas en el Plan de Seguridad y Privacidad de la Información, alineadas con la norma ISO 27001, la Política de Seguridad Digital y Continuidad del servicio.

Objetivos específicos

- 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.

- Optimizar la gestión de la seguridad de la información al interior del CANAL TRO.

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

3. ALCANCE

Esto se aplica a todos los niveles del Canal TRO y todos sus empleados, contratistas, operadores y todas las personas o terceros cuya información se comparte, utiliza, recopila, procesa, intercambia o se accede en el desempeño de sus funciones y como entidad de control. Asimismo, este plan se aplica a toda la información generada, procesada o utilizada por el Canal TRO, independientemente de su medio, formato, imágenes o ubicación.

4. DEFINICIONES

ACTIVO DE INFORMACIÓN: Aquello que es de alta validez y que contiene información de la empresa que debe ser protegida.

AMENAZA: Es la causa potencial de un daño a un activo de información.

ANÁLISIS DE RIESGO: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

CAUSA: Razón por la cual el riesgo sucede.

CICLO DE DEMING: Modelo mejora continua para la implementación de un sistema de mejora continua.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible a personas no autorizadas.

CONTROLES: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

DISPONIBILIDAD: Propiedad que determina que la información se accesible y utilizable por aquellas personas debidamente autorizadas.

IMPACTO: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

INCIDENTE: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos
.
PROBABILIDAD DE OCURRENCIA: Posibilidad de que se presente una situación o evento específico.

RESPONSABLE DEL ACTIVO: Persona responsables del activo de información.

RIESGO: Grado de exposición de un activo que permite la materialización de una amenaza.

RIESGO INHERENTE: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

RIESGO RESIDUAL: Nivel de riesgo remanente como resultado de la aplicación de medida de seguridad sobre el activo.
SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27001:2013).

SGSI: Sistema de Gestión de Seguridad de la Información.

SGSI: Sistema que permite establecer, implementar, mantener y mejora continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

VULNERABILIDAD: Debilidad de una activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad se caracteriza por ausencia en controles de seguridad que permite ser explotada.

5. RESPONABILIDADES

La Alta Dirección del CANAL TRO se compromete coordinar, hacer seguimiento y verificación de la estabilidad y mejora del plan, garantizando los recursos suficientes (tecnológicos y talento humano calificado), así mismo incluirá dentro de las decisiones estratégicas y la seguridad de la información.

Proceso de Gestión Técnica y Emisión es el responsable de emitir las normas, manuales, guías y la metodología de implementación del Plan de tratamiento de riesgos.

Los procesos de Planeación y Control Interno, es responsable del control y evaluación del tratamiento de riesgos de seguridad y privacidad de la información, como también proporcionar los recursos y estrategias para el desarrollo del plan realizando seguimiento y verificación de la implementación.

6. COMUNICACIÓN DEL PLAN

A continuación, se presentan algunas pautas para la distribución y comunicación en el plan general establecido en el SIG de Gestión de comunicaciones:

Publicación de información de manera continua y accesible.

- Boletines internos de comunicación a fin de establecer conciencia sobre la importancia del tema.
- Comunicación de la Alta Dirección. Como líderes de la entidad y del proceso de Contingencia de TI, los líderes, al menos una vez al año, comunicar a los contratistas su compromiso de salvaguardar la información y el plan de contingencias de la entidad, para lo cual utilizará cualquier medio de los mencionados anteriormente.

7. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

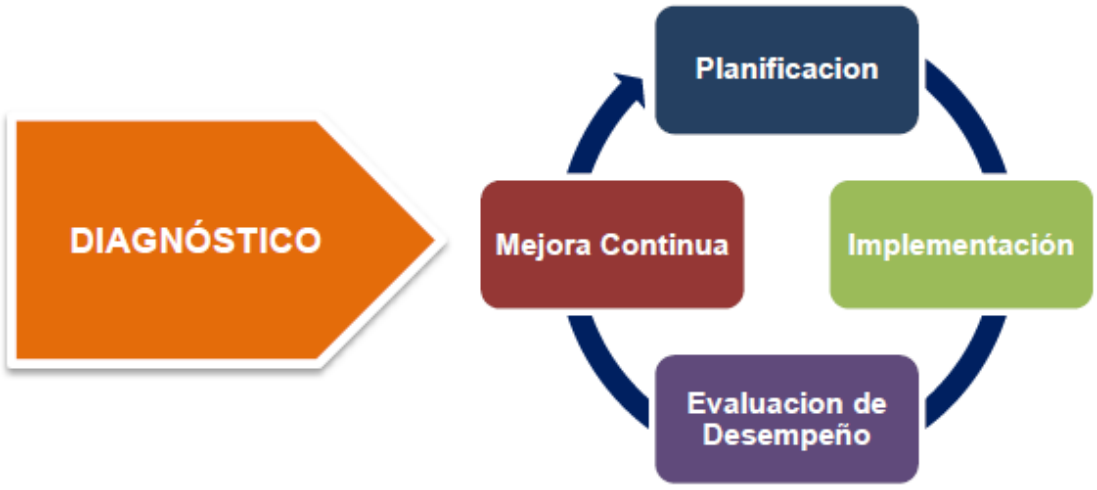
La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales,

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.

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.

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. Estas, contienen objetivos, metas y herramientas que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible en el CANAL TRO:



Ciclo de operación del Modelo de Seguridad y Privacidad de la Información
http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

7.1 FASE DE DIAGNÓSTICO

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,

DIAGNÓSTICO			
Metas	**Resultados**	**Instrumentos MSPI[1]**	**Alineación MRAE[2]**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Guía No 1 - Metodología de Pruebas de Efectividad[3]	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			
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.			

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.

[1] MSPI: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

[2] Los lineamientos por Dominio del Marco de referencia de Arquitectura Empresarial de MINTIC en los cuales se basan las políticas. https://www.mintic.gov.co/arquitecturaempresarial/portal/

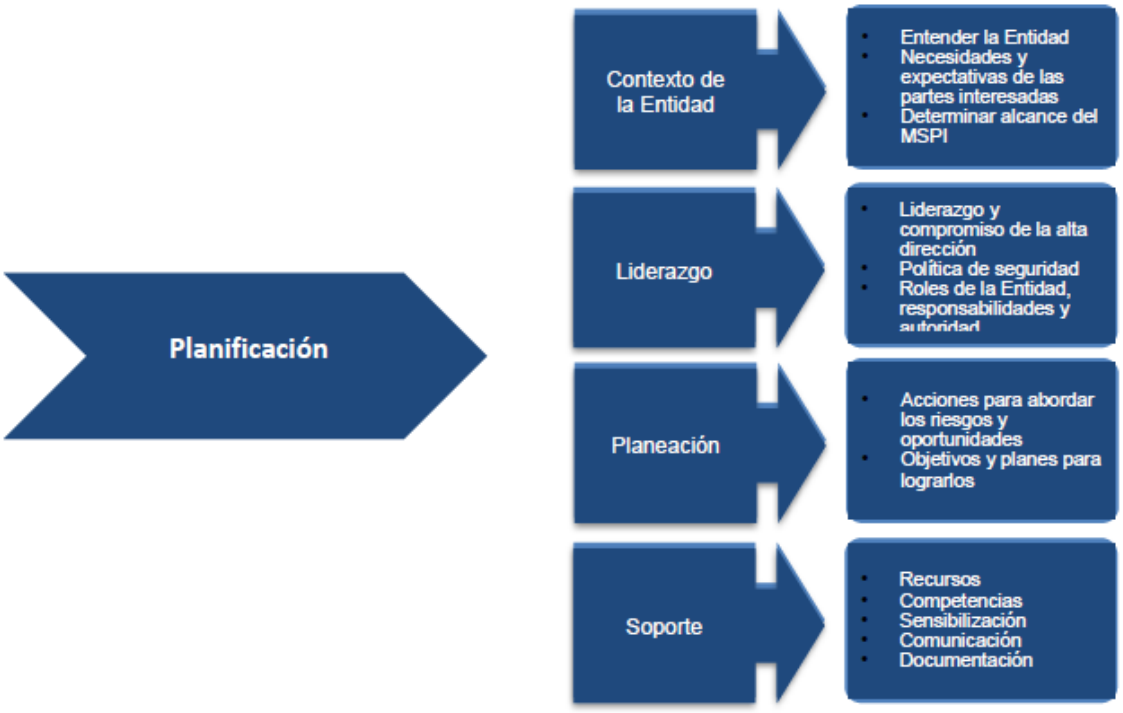
[3] Guía No. 1 Metodológica de Pruebas de Efectividad: https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

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.

7.2 FASE DE PLANIFICACIÓN

Para el desarrollo de esta fase el CANAL TRO 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 co
n otros procesos.



PLANIFICACIÓN			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación 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.[4]	LI.ES.02 LI.ES.06 LI.ES.07 LI.ES.08 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
	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.	
	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.[5]	
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.[6]	

[4] Guía No 2 – Política General MSPI: https://gobiernodigital.mintic.gov.co/692/articles-5482_G2_Politica_General.pdf

[5] Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información: https://gobiernodigital.mintic.gov.co/692/articles-5482_G3_Procedimiento_de_Seguridad.pdf

[6] Guía No 4 – Roles y responsabilidades de seguridad y privacidad de la información: https://gobiernodigital.mintic.gov.co/692/articles-5482_G4_Roles_responsabilidades.pdf

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.[7]	LI.UA.05 LI.UA.06
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Guía No 6 - Gestión Documental.[8]	
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 - Gestión de Riesgos.[9] Guía No 8 - Controles de Seguridad.[10]	
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan de comunicación,	

[7] Guía No 5 - Gestión De Activos: https://gobiernodigital.mintic.gov.co/692/articles-5482_G8_Controles_Seguridad.pdf
[8] Guía No 6 - Gestión Documental: https://gobiernodigital.mintic.gov.co/692/articles-5482_G6_Gestion_Documental.pdf
[9] Guía No 7 - Gestión de Riesgos: https://gobiernodigital.mintic.gov.co/692/articles-5482_G7_Gestion_Riesgos.pdf
[10] Guía No 8 - Controles de Seguridad: https://gobiernodigital.mintic.gov.co/692/articles-5482_G8_Controles_Seguridad.pdf

		sensibilización y capacitación.[11]	
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.[12]	

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

[11] Guía No 14 - Plan de comunicación, sensibilización y capacitación: https://gobiernodigital.mintic.gov.co/692/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf
[12] Guía No 20 - Transición IPv4 a IPv6: https://gobiernodigital.mintic.gov.co/692/articles-5482_G20_Transicion_IPv4_IPv6.pdf

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, así 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 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.

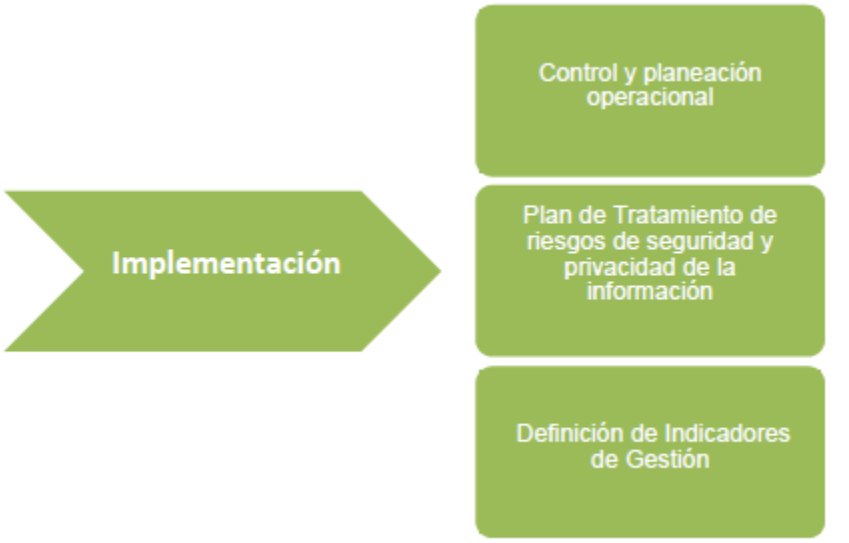
Plan de Comunicaciones.
La Entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros)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

7.3 FASE DE IMPLEMENTACIÓN

Esta fase le permitirá a la Entidad, llevar a cabo la implementación de la planificación realizada en la fase anterior del MSPI. (ISO IEC 27001 Capítulo 8, que permite orientar como se desarrolla la implementación del MSPI).



IMPLEMENTACIÓN			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación 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.	LI.ES.09 LI.ES.10 LI.GO.04 LI.GO.09 LI.GO.10

		Documento con la declaración de aplicabilidad.	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 LI.ST.13 LI.UA.01
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.[13]	
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.[14]	

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

[13] Guía No 9 - Indicadores de Gestión SI: https://gobiernodigital.mintic.gov.co/692/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

[14] Guía No 19 – Aseguramiento del Protocolo IPv6: https://gobiernodigital.mintic.gov.co/692/articles-5482_G19_Aseguramiento_protocolo.pdf

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 debe 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”.

7.4 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.

IMPLEMENTACIÓN			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación 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.[15]	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.[16]	

Plan de revisión y seguimiento a la implementación del MSPI.
En esta actividad la entidad debe crear un plan que contemple las siguientes actividades:

[15] Guía No 16 – Evaluación del desempeño: https://gobiernodigital.mintic.gov.co/692/articles-5482_G16_evaluaciondesempeno.pdf
[16] Guía No 15 – Guía de Auditoría: https://gobiernodigital.mintic.gov.co/692/articles-5482_G15_Auditoria.pdf

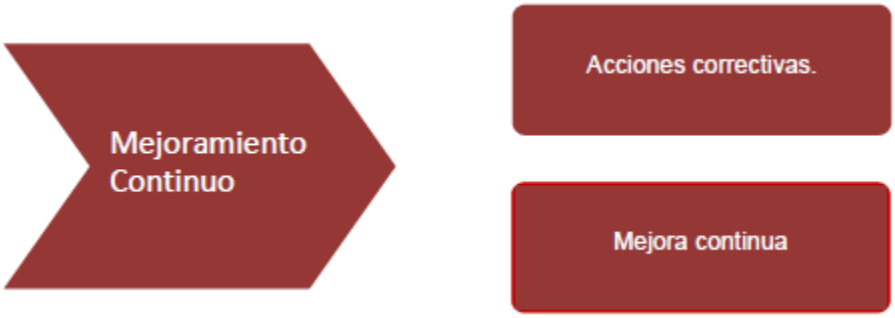
- Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- Seguimiento a la programación y ejecución de las 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.

7.5 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.



IMPLEMENTACIÓN			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación 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.[17]	

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:

[17] Guía No 17 – Mejora Continua: https://gobiernodigital.mintic.gov.co/692/articles-5482_G17_Mejora_continua.pdf

- 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.

8. HOJA DE RUTA.

ACTIVIDADES	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
Diagnostico												
Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.												
Planificación												
Revisar Política de Seguridad y Privacidad de la Información												
Revisar Manual de Políticas de Seguridad y Privacidad de la Información												
Definir y Asignar Roles y responsabilidades de seguridad y privacidad de la información.												
Actualizar Inventario de activos de información.												
Actualizar Plan de Tratamiento al riesgo												
Integrar al Plan de Comunicaciones del SIG												
Plan de diagnóstico de IPv4 a IPv6.												
Implementación												
Actualización de Políticas												
Actualización del Manual de Políticas												
Implmentación del Manual de Políticas												
Definir Indicadores de Gestión												
Definir Plan de Transición de IPv4 a IPv6												
Evaluación												
Seguimiento a la implementación del MSPI												
Mejora Continua												
Propuesta de Mejora Continua												

9. CONTROL DE CAMBIOS.

Versión	Descripción del cambio	Fecha
01	Versión inicial	Enero 25 de 2023
02	Se modifica el plan desde introducción objetivos hasta fase de mejora continua con el fin de definir y establecer la metodología e implementación del plan.	Diciembre 19 de 2023
03	Se modifica el plan teniendo en cuenta la inclusión de la hoja de ruta para la vigencia 2024	Enero 30 de 2024

Elaboró	Aprobó
Líder del proceso de Técnica	Comité de Gestión y desempeño Institucional.