

**CORPORACIÓN AUTÓNOMA REGIONAL
DEL QUINDÍO**

**PLAN DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACIÓN**

VERSION 04

ENERO 2023

CONTROL DE CAMBIOS

Versión	Fecha (dd/mm/aaaa)	Descripción
01	20/01/2020	Versión inicial del documento.
02	25/01/2021	Actualización del documento y del plan de acuerdo con los lineamientos de Gobierno Digital.
03	25/01/2022	Actualización del documento de acuerdo con las guías de MINTIC.
04	30/01/2023	Actualización del documento para la vigencia 2023 de acuerdo las últimas actualizaciones realizadas a las guías emitidas por MINTIC.

APROBACIÓN

Aprobó	Revisó	Elaboró
Nombre: Víctor Hugo González Giraldo Jefe Oficina Asesora de Planeación	Nombre: Víctor Hugo González Giraldo Jefe Oficina Asesora de Planeación	Nombre: Richard Edwin Camarillo Osorio - Técnico Operativo

TABLA DE CONTENIDO

1. INTRODUCCIÓN	4
2. OBJETIVO	5
2.1. OBJETIVOS ESPECÍFICOS	5
3. ALCANCE	6
4. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	7
4.1. DIAGNÓSTICO	9
4.2. PLANIFICACIÓN	9
4.3. OPERACIÓN	10
4.4. EVALUACIÓN DE DESEMPEÑO.....	11
4.5. MEJORAMIENTO CONTÍNUO.....	12
5. CRONOGRAMA DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	13

1. INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones, 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 Digital, 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 transparente.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en la CRQ estará determinado por las necesidades y objetivos, los requisitos de seguridad y la estructura de procesos.

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 de Gobierno Digital.

2. OBJETIVO

Definir las actividades a realizar en la CRQ para la implementación del Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

2.1. OBJETIVOS ESPECÍFICOS

Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información que se gestiona en la CRQ, de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información de Gobierno Digital y la norma ISO 27001.

Definir los lineamientos para el manejo de la información digital en el marco las políticas de Seguridad y Privacidad de la Información.

3. ALCANCE

Aplica para todas las dependencias, funcionarios y contratistas de la CRQ, y para toda persona natural o jurídica que por sus funciones hagan uso de la información digital de la Entidad sin importar la ubicación, medio o formato.

4. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Siguiendo los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la información definido por el Ministerio TIC, el plan de Seguridad y Privacidad de la información para la CRQ se desarrollará en cinco fases, teniendo en cuenta los 6 niveles de madurez de la implementación del Modelo de Seguridad y Privacidad de la Información.

El Sistema de seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno digital, permitirá preservar la confidencialidad, integridad y disponibilidad 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 Plan de Seguridad y Privacidad de la Información se implementa en cinco fases, planificación, implementación, evaluación del desempeño y mejora continua.

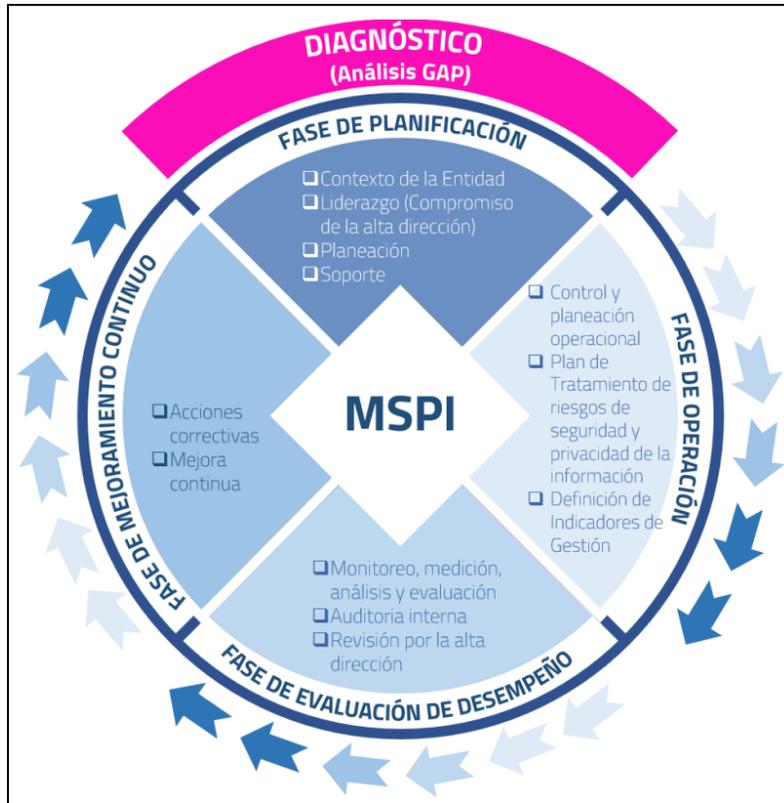


Figura 1. Ciclo del Modelo de Seguridad y Privacidad de la Información

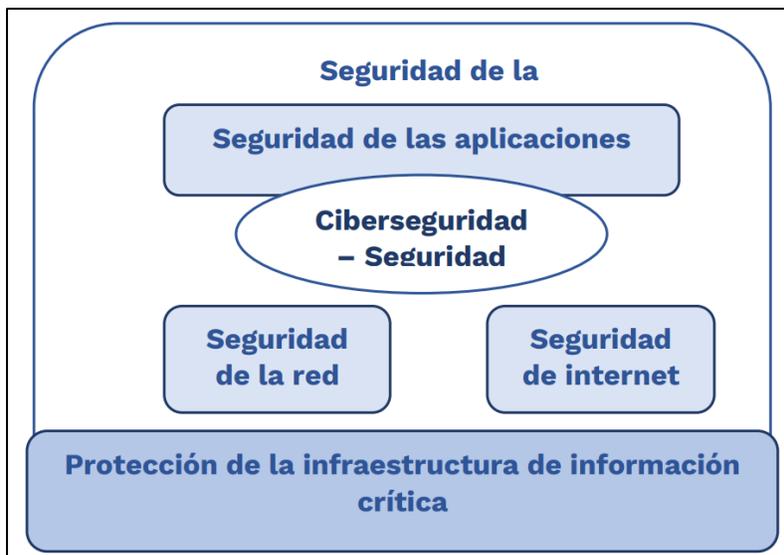


Figura 2. Relación entre la ciberseguridad y otros ámbitos de la seguridad. (Fuente: ISO/IEC 27032)

4.1. DIAGNÓSTICO

Se debe iniciar con un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.

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	

4.2. PLANIFICACIÓN

Determina las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

Planificación			
Metas	Resultados	INSTRUMENTO	
		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
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

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.	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
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.	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
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 - Gestión 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 - Gestión 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	

4.3. OPERACIÓN

La entidad implementa los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

Operación			
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.	
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

4.4. EVALUACIÓN DE DESEMPEÑO

La entidad determina de qué manera va a ser evaluado la adopción del modelo.

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 Auditorías	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.	

4.5. MEJORAMIENTO CONTÍNUO

Se establecen procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

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

5. CRONOGRAMA DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA VIGENCIA 2023

ETAPAS / ACTIVIDADES	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	
Diagnóstico													
Realizar el diagnóstico utilizando la herramienta establecida por Mintic		■											
Identificar vulnerabilidades administrativas y documentar los hallazgos		■											
Identificar vulnerabilidades técnicas y documentar los hallazgos (se podrá hacer uso de metodologías de Ethical Hacking, pruebas de Ingeniería Social, entre otras)		■											
Planificación													
Establecer la Política de Seguridad y Privacidad de la Información							■						
Realizar el Manual de Políticas de Seguridad y Privacidad de la Información							■						
Diseñar los procedimientos de seguridad de la información		■											
Definir los roles y responsabilidades de seguridad y privacidad de la información		■											
Realizar el Inventario de activos de información		■											
Integración del MSPi con el Sistema de Gestión documental		■											
Identificación, Valoración y tratamiento de riesgos de Seguridad de la información							■						
Elaborar el Plan de Comunicaciones		■											
Elaborar el Plan de diagnóstico de transición de IPv4 a IPv6		■											
Implementación													
Definir la estrategia de planificación y control operacional							■						
Implementar el plan de tratamiento de riesgos							■						
Realizar la medición de los Indicadores De Gestión							■						
Implementar el Plan de Transición de IPv4 a IPv6							■						
Evaluación del Desempeño													
Plan de revisión y seguimiento a la implementación del MSPi		■											
Plan de Ejecución de Auditorías		■											
Mejora Continua													
Plan de mejora continua		■											