CORPORACIÓN AUTÓNOMA REGIONAL DEL QUINDÍO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VERSION 01

ENERO 2021

TABLA DE CONTENIDO

LISTA DE FIGURAS

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.

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

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 más 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 que están contempladas en el Modelo de Seguridad y Privacidad de la Información de la Política de Gobierno Digital para la Corporación Autónoma Regional del Quindío.[1]

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 física y digital en el marco de una Gestión Documental basada en 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 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. Fases de Implementación del Modelo de Seguridad y Privacidad de la Información

Para la fase de **Diagnóstico**, inicialmente se toma como base el

autodiagnóstico realizado por la Entidad en el Modelo Integrado de Planeación y Gestión, dando como resultado lo siguiente:

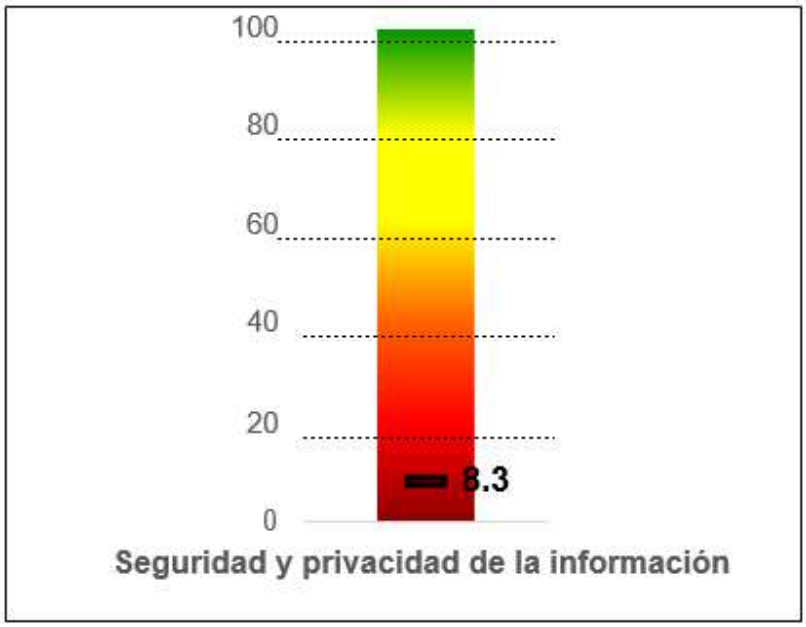

Figura 2. Calificación Componente Seguridad y Privacidad de la Información

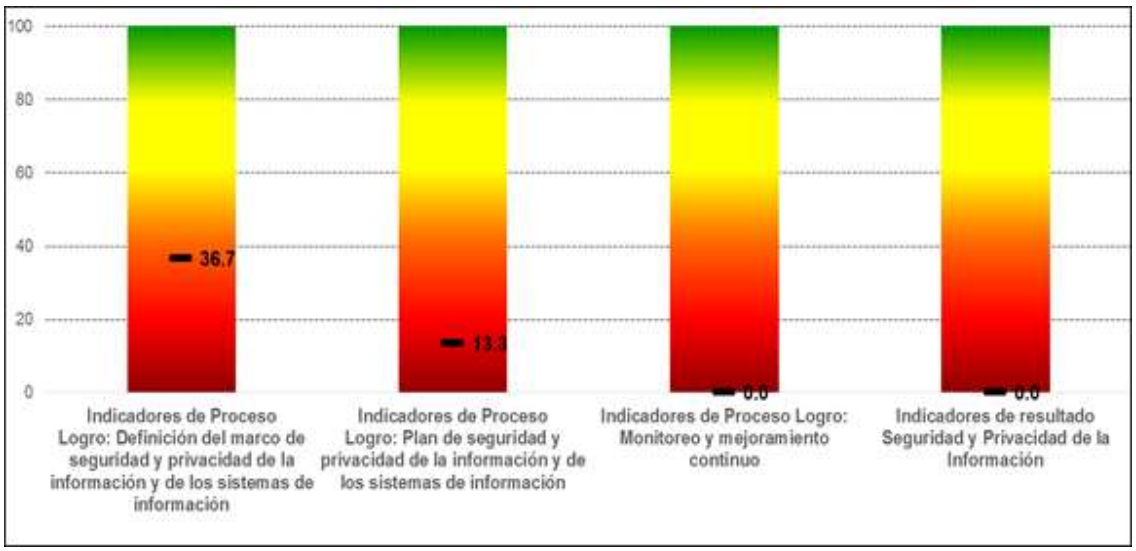

Figura 3. Calificación categorías del Componente "Seguridad y Privacidad de la Información"

Como se puede observar y de acuerdo con el esquema de madurez del Modelo de Seguridad y Privacidad de la Información, se determina que el nivel de madurez para la CRQ es "INICIAL" de acuerdo con la descripción

de la siguiente tabla:

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.

Figura 4. Niveles de Madurez

Con estos resultados se tiene una línea base para plantear el plan de implementación.

5. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ACTIVIDAD	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Diagnóstico												
Determinar el estado actual de la entidad y el nivel de madurez												
Identificar vulnerabilidades técnicas y administrativas (realizar pruebas 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 Privacidadde la Información												
Diseñar los procedimientosde seguridad de la información												
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												
Plan de Comunicaciones												
Implementación												
Planificación y Control Operacional												
Implementación del plan de tratamiento de riesgos												
Indicadores De Gestión												
Plan de Transición de IPv4 a IPv6												
Evaluación del Desempeño												
Plan de revisión y seguimiento a la implementación del MSPI												
Plan de Ejecución de Auditorias												
Mejora Contínua												
Plan de mejora continua												