Emsercota S.A.
EMPRESA DE SERVICIOS PÚBLICOS

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

1. INTRODUCCIÓN

La implementación de la política establecida por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC exige a EMSERCOTA S.A. E.S.P. adoptar un modelo que garantice la seguridad y la privacidad de la información pública y privada que administra, de conformidad con lo dispuesto en el Decreto 1008 de 2018 y las disposiciones contenidas en el Decreto Único Reglamentario 1078 de 2015, Capítulo 1, Título 9, Parte 2, Libro 2.

Este marco normativo tiene como propósito promover y fortalecer el uso seguro y responsable de las Tecnologías de la Información y las Comunicaciones, de manera que estas se conviertan en un habilitador del crecimiento institucional, la eficiencia operativa y el fortalecimiento de la relación con los usuarios de los servicios públicos que presta la Empresa.

El presente documento ha sido elaborado como una guía para EMSERCOTA S.A. E.S.P., con el fin de establecer los lineamientos necesarios para el diagnóstico, la planeación, la implementación, la gestión y el mejoramiento continuo del Plan de Seguridad y Privacidad de la Información, en concordancia con la estrategia definida por el MinTIC y el Modelo de Gobierno Digital.

El Modelo de Seguridad y Privacidad de la Información – MSPI, establecido por el MinTIC, orienta a la Entidad hacia la protección de la confidencialidad, integridad y disponibilidad de la información, así como a la garantía de la privacidad de los datos personales y sensibles que administra. Lo anterior se logra mediante la aplicación de un enfoque de gestión del riesgo, que permite generar confianza y asegurar una adecuada administración de los activos de información de la Empresa.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Definir el plan de acción para implementar la seguridad y la privacidad de la información en EMSERCOTA S.A. E.S.P., de acuerdo con las normas establecidas por el MinTIC y la política de Gobierno Digital, con el propósito de proteger y preservar la confidencialidad, integridad y disponibilidad de la información institucional, teniendo en cuenta las capacidades técnicas, operativas y presupuestales de la Empresa, y fortaleciendo la confianza de los usuarios y demás partes interesadas.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar e implementar los medios, controles y mecanismos necesarios para proteger los activos de información digital de EMSERCOTA S.A. E.S.P., con base en los principios de confidencialidad, integridad y disponibilidad.
- Gestionar adecuadamente los riesgos digitales asociados al uso de las TIC, con el fin de mantenerlos en niveles aceptables y controlados.
- Sensibilizar y capacitar al personal administrativo, operativo y a los contratistas de la Empresa sobre la importancia del Plan de Seguridad y Privacidad de la Información, promoviendo una cultura de protección de los activos críticos de información.
- Realizar seguimiento permanente al cumplimiento de los estándares de seguridad de la información, haciendo uso de herramientas de diagnóstico y evaluación.
- Identificar, implementar y evaluar acciones correctivas y de mejora, que permitan fortalecer de manera continua el Plan de Seguridad y Privacidad de la Información de EMSERCOTA S.A. E.S.P.

3. ALCANCE

La implementación del Plan de Seguridad y Privacidad de la Información en EMSERCOTA S.A. E.S.P. está orientada al fortalecimiento de la seguridad informática y la protección de los datos que soportan todos los procesos de la Empresa, en cumplimiento de las normas, lineamientos y políticas establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

El alcance del plan comprende los activos de información, sistemas, equipos, redes, servicios tecnológicos y el talento humano que interviene en la gestión y uso de la información, buscando garantizar la continuidad de los servicios públicos, la protección de los datos de los usuarios y el cumplimiento de los principios de transparencia, legalidad y buen gobierno.

4. MARCO NORMATIVO

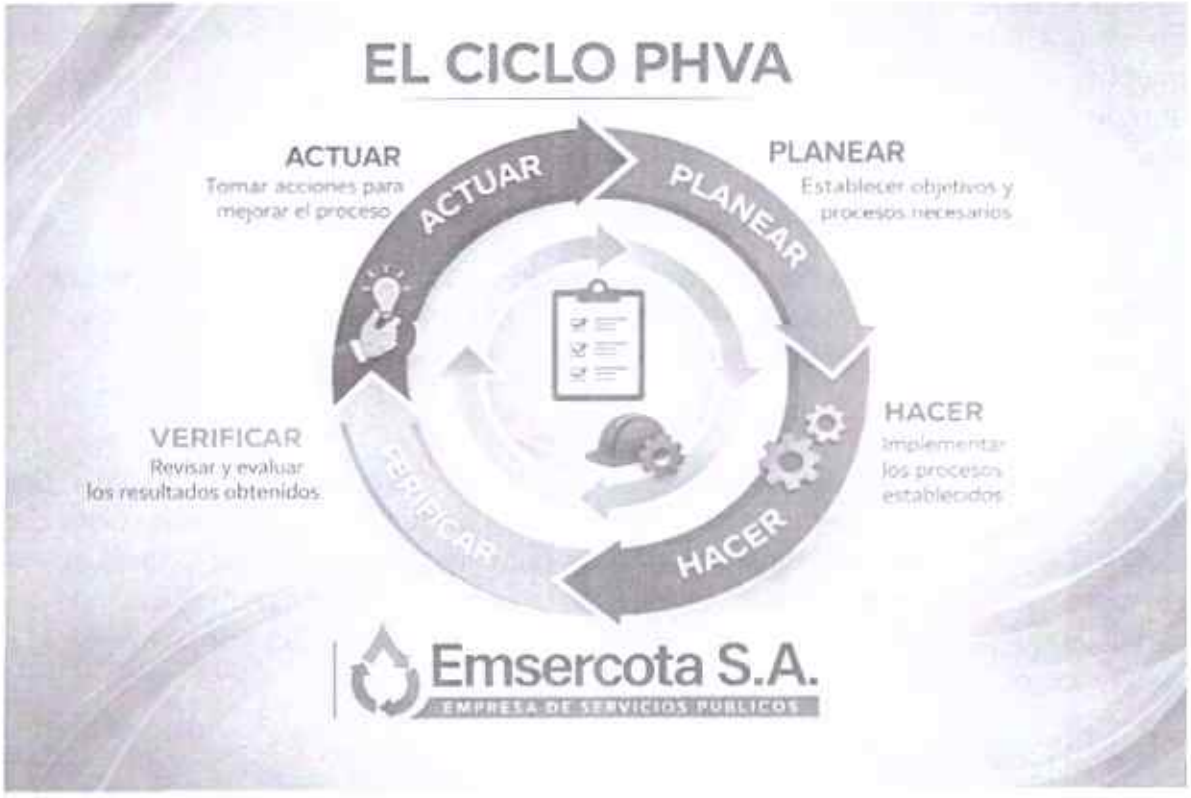
MARCO NORMATIVO	AÑO	DESCRIPCIÓN
CONSTITUCIÓN POLÍTICA DE COLOMBIA – ARTÍCULO 15	1991	Reconoce el derecho fundamental a la intimidad, el buen nombre y la protección de los datos personales, así como el acceso a la información.
LEY 1273	2009	Modifica el Código Penal y crea nuevos tipos penales relacionados con la protección de la información y los datos (delitos informáticos).
LEY ESTATUTARIA 1581	2012	Establece el régimen general de protección de datos personales y los principios para su tratamiento.
LEY 1712	2014	Crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
LEY 1928	2018	Aprueba el Convenio sobre la Ciberdelincuencia (Convenio de Budapest), fortaleciendo la cooperación y el marco penal en materia de delitos informáticos.
DECRETO 1078	2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
DECRETO 103	2015	Reglamenta parcialmente la Ley 1712 de 2014 en materia de acceso a la información pública.
CONPES 3854	2016	Define la Política Nacional de Seguridad Digital en Colombia.
DECRETO 1008	2018	Establece los lineamientos generales de la Política de Gobierno Digital.
DECRETO 338	2022	Fortalece la gobernanza de la seguridad digital y crea el Modelo y las instancias de Gobernanza de Seguridad Digital.
RESOLUCIÓN 1519	2020	Define estándares y directrices para la publicación de información pública, accesibilidad web, seguridad digital y datos abiertos.
RESOLUCIÓN 500	2021	Adopta el Modelo de Seguridad y Privacidad de la Información como habilitador de la Política de Gobierno Digital.
RESOLUCIÓN 746	2022	Fortalece el Modelo de Seguridad y Privacidad de la Información y define lineamientos adicionales.
RESOLUCIÓN 02277	2025	Actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI), alineándolo con la norma ISO/IEC

MARCO NORMATIVO	AÑO	DESCRIPCIÓN
		27001:2022 y consolidando los lineamientos vigentes en seguridad y privacidad de la información.

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

El Plan de Implementación del Modelo de Seguridad y Privacidad de la Información de EMSERCOTA S.A. E.S.P. se fundamenta en el Ciclo PHVA (Planear – Hacer – Verificar – Actuar), el cual es una herramienta reconocida de mejora continua ampliamente utilizada en los sistemas de gestión.

La aplicación de este modelo permite a EMSERCOTA fortalecer de manera integral sus procesos, garantizando una gestión más eficiente y segura de la información, mejorando la calidad de los servicios públicos prestados, optimizando los recursos institucionales y fortaleciendo la confianza de la comunidad y de las partes interesadas.



- **Etapa 0 – Diagnóstico**

En esta fase se identifica el estado actual de EMSERCOTA S.A. E.S.P. frente a los requerimientos del Modelo de Seguridad y Privacidad de la Información, permitiendo reconocer fortalezas, brechas y oportunidades de mejora en el manejo y protección de la información institucional.

- **Etapa 1 – Planificación (Planear)**

En esta etapa se establecen los objetivos, estrategias y acciones necesarias para fortalecer la seguridad y privacidad de la información, teniendo en cuenta las políticas institucionales y las necesidades de la comunidad. Durante esta fase se definen aspectos clave como: ¿qué se va a hacer?, ¿por qué?, ¿cuándo?, ¿dónde?, ¿quiénes serán responsables?, ¿cómo se realizará? y ¿con qué recursos?, convirtiéndose en una fase fundamental para el desarrollo exitoso de las siguientes etapas.

- **Etapa 2 – Implementación (Hacer)**

En esta fase se ejecutan las acciones previamente planificadas. Aquí se ponen en marcha los controles y medidas definidas, se identifican posibles dificultades durante la ejecución y se aprovechan las oportunidades de mejora para fortalecer el modelo y su aplicación en la empresa.

- **Etapa 3 – Evaluación (Verificar)**

En esta etapa se realiza el seguimiento y medición de las acciones implementadas, verificando el cumplimiento de los objetivos establecidos y evaluando su efectividad, de acuerdo con las políticas institucionales y la planeación inicial.

- **Etapa 4 – Mejora Continua (Actuar)**

En esta fase se adoptan las acciones necesarias para el mejoramiento continuo del desempeño de los procesos relacionados con la seguridad de la información. Se corrigen desviaciones, se estandarizan los cambios realizados, se fortalecen las competencias del personal mediante capacitaciones y se definen mecanismos de seguimiento que permitan reiniciar el ciclo de mejora continua con base en los resultados obtenidos.

A continuación, se detallan las actividades planeadas para cada una de las fases del Ciclo PHVA, así como el estado actual de su ejecución.

De acuerdo con los resultados obtenidos en las fases culminadas (diagnóstico y planificación), se incorporan acciones adicionales a la fase de implementación, con el fin de fortalecer continuamente el Modelo de Seguridad y Privacidad de la Información en EMSERCOTA S.A. E.S.P.

4.0 - FASE DE DIAGNOSTICO				
N°	DESCRIPCIÓN	RESPONSABLE	VIGENCIA DE IMPLEMENTACIÓN	SEGUIMIENTO
1	Conocer la situación actual de EMSERCOTA S.A. E.S.P. en materia de seguridad y privacidad de la información, identificando cómo se gestionan y protegen los datos dentro de la Empresa.	Personal Administrativo/ Contratista	Vigencia 2026	
2	Reconocer las debilidades técnicas y administrativas presentes en los procesos y sistemas de información de EMSERCOTA S.A. E.S.P., que sirvan como base para planear acciones de mejora.	Personal Administrativo	Vigencia 2026	
3	Verificar el cumplimiento de EMSERCOTA S.A. E.S.P. frente a la normativa vigente relacionada con la protección de los datos personales y la seguridad de la información.	Personal Administrativo/ Contratista	Vigencia 2026	
4	Identificar buenas prácticas en ciberseguridad que puedan ser aplicadas en EMSERCOTA S.A. E.S.P. para fortalecer la protección de la información institucional.	Personal Administrativo/ Contratista	Vigencia 2026	

4.1 - FASE DE PLANIFICACION (Planear)				
N°	DESCRIPCIÓN	RESPONSABLE	VIGENCIA DE IMPLEMENTACIÓN	SEGUIMIENTO
5	Definir y diseñar el manual de seguridad y privacidad de la información de EMSERCOTA S.A. E.S.P., asegurando su aprobación y socialización al interior de la entidad.	Personal Administrativo/ Contratista	Vigencia 2026	
6	POLITICA…Establecer y documentar los procedimientos necesarios para la gestión de la seguridad y privacidad de la información, garantizando su aprobación y divulgación entre las áreas responsables de EMSERCOTA S.A. E.S.P.	Personal Administrativo	Vigencia 2026	
7	Identificar, clasificar y asignar responsables sobre los activos de información de EMSERCOTA S.A. E.S.P., incluyendo software, hardware, redes, servicios de tecnologías de la información y servicios contratados, con el fin de asegurar su adecuada protección.	Personal Administrativo/ Contratista	Vigencia 2026	
8	Identificar, valorar y definir el tratamiento de los riesgos de seguridad digital desde el componente de seguridad informática, orientado a la protección de la información institucional de EMSERCOTA S.A. E.S.P.	Personal Administrativo/ Contratista	Vigencia 2026	

4.2 - FASE DE IMPLEMENTACION (Hacer)				
N°	DESCRIPCIÓN	RESPONSABLE	VIGENCIA DE IMPLEMENTACIÓN	SEGUIMIENTO
9	Realizar la planeación y el control operativo del Plan de Seguridad y Privacidad de la Información de EMSERCOTA S.A. E.S.P., asegurando su aplicación conforme a lo aprobado y socializado en la entidad.	Contratista	Vigencia 2026	
10	Implementar el plan de tratamiento de riesgos de seguridad de la información, de acuerdo con la matriz de riesgos aprobada, con el fin de reducir amenazas y fortalecer los controles definidos.	Personal Administrativo	Vigencia 2026	
11	Validar la aplicación de indicadores de gestión relacionados con la seguridad y privacidad de la información, verificando su correcta documentación, análisis y utilidad dentro del sistema integrado de gestión.	Personal Administrativo/ Contratista	Vigencia 2026	
12	Adoptar controles de seguridad informática orientados a la gestión de riesgos, asegurando su articulación con la matriz de riesgos y la generación de informes periódicos para el seguimiento correspondiente.		Vigencia 2026	

6. CONTROL OPERACIONAL AL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El control operacional en EMSERCOTA S.A. E.S.P. se enfoca en la aplicación diaria de prácticas y procedimientos orientados a proteger los activos de información de la entidad, garantizar el acceso adecuado a los sistemas y prevenir, detectar y atender eventos o incidentes de seguridad de la información.

Este control incluye la implementación y cumplimiento del plan de seguridad y privacidad de la información, el seguimiento a los accesos a los sistemas, la supervisión de los eventos de seguridad y la gestión oportuna de los incidentes que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Adicionalmente, contempla actividades como capacitaciones al personal, control de cambios y mejora de los procesos tecnológicos, con el propósito de fortalecer la cultura de seguridad de la información y asegurar la continuidad y confiabilidad de los servicios prestados por EMSERCOTA S.A. E.S.P.

ÁREA	CUMPLE/ NO CUMPLE	DESCRIPCIÓN
1. Análisis de riesgos:		
La entidad identifica la información más importante y analiza los riesgos que pueden afectar su seguridad.	NO CUMPLE	
2. Objetivos y metas:		
EMSERCOTA S.A. E.S.P. define metas claras para proteger la información y mejorar su gestión.	CUMPLE	
3. Políticas y procedimientos:		
Se cuenta con lineamientos y procedimientos que orientan el manejo seguro de la información.	NO CUMPLE	
Define procedimientos claros para la gestión de la información, el acceso, la transmisión y el almacenamiento seguro.	NO CUMPLE	
4. Concientización y capacitación		
Se realizan actividades para sensibilizar al personal sobre el cuidado de la información.	NO CUMPLE	
5. Control de acceso		
Solo el personal autorizado puede acceder a la información, con controles y revisiones periódicas.	CUMPLE	
6. Cumplimiento normativo		
Se verifica el cumplimiento de la normativa vigente sobre seguridad y protección de datos.	NO CUMPLE	

4.3 - FASE DE EVALUACIÓN (Verificar)				
N°	DESCRIPCIÓN	RESPONSABLE	VIGENCIA DE IMPLEMENTACIÓN	SEGUIMIENTO
17	Realizar auditorías de seguimiento para verificar la correcta implementación del Plan de Seguridad y Privacidad de la Información.	Jefe de oficina de control interno y calidad	2026	
18	Revisar y aprobar el plan de ejecución de auditorías, asegurando su cumplimiento.	Jefe de oficina de control interno y calidad	2026	
19	Analizar los planes de acción y verificar el avance y cumplimiento de las acciones definidas.	Jefe de oficina de control interno y calidad	2026	

4.4 - FASE DE MEJORA CONTINUA (Actuar)				
N°	DESCRIPCIÓN	RESPONSABLE	VIGENCIA DE IMPLEMENTACIÓN	SEGUIMIENTO
20	Definir y socializar el plan de mejora continua, incorporando las acciones necesarias para fortalecer la seguridad y privacidad de la información en EMSERCOTA S.A. E.S.P.	Jefe de oficina de control interno y calidad	2026	

FUNCIONARIO	NOMBRE Y CARGO	FIRMA
PROYECTÓ	Yamir Geovanny Quevedo Agudelo – Técnico en Sistemas – EMSERCOTA S.A E.S.P.	
REVISÓ	Sandra Lorena Mondragón H- Jefe de Oficina de Control Interno- – EMSERCOTA S.A E.S.P.	
APROBÓ	Andrés Felipe Rincón Damián – Gerente- EMSERCOTA S.A E.S.P.	