# Plan de Seguridad
# &
# Privacidad de la Información



## ALCALDÍA DE MONTERÍA

Alcaldía de
MONTERÍA
Gobierno de la GENTE

WWW.MONTERIA.GOV.CO

2021

VERSIÓN 1.0

## Tabla de versiones

| Versión | Fecha | Autor |
|---|---|---|
| **1.0 – Versión final 2021** | 27 de enero de 2021 | Oficina TIC |

## Tabla de contenido


***Introducción*** ..... ***3***

***Objetivo*** ..... ***4***

***Política de seguridad de la información*** ..... ***5***

**Objetivos de la política** ..... **5**

***Alcance del documento*** ..... ***6***

***Términos y definiciones*** ..... ***7***

***Contexto normativo*** ..... ***9***

***Comité de seguridad de la información*** ..... ***11***

***Plan de implementación del modelo de seguridad y privacidad de la información*** ..... ***12***

# Introducción

El plan de desarrollo 2020 - 2023 “Gobierno de la gente”, establece la implementación de la política de Gobierno Digital, de tal manera que la administración pública esté preparada para un contexto de economía digital y tiene como línea de acción estratégica el desarrollo de alianzas para formación en Gestión Tecnologías de la Información, Seguridad y Privacidad de la Información.

La política de gobierno digital precisa que se debe preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos. Esta política es un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual se ha articulado con el Modelo Integrado de Planeación y Gestión, como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual se ha articulado con el Modelo Integrado de Planeación y Gestión, como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia.

La oficina TIC de la Alcaldía de Montería, considera la información como un activo valioso de la institución, el cual se debe proteger. Es por eso que se ha implementado un Plan de seguridad y privacidad de la información (2021 -2023).

# Objetivo

El plan de seguridad y privacidad de la información tiene como objetivo establecer un plan de acción para la implementación del modelo de seguridad y privacidad de la información y describir cada una de las actividades con las cuales se busca desarrollar, verificar y aplicar la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI de la Alcaldía Municipal de Montería alineados con NTC/IEC ISO 27001:2013.

# Política de seguridad de la información

La política de seguridad de la información se encuentra basadas en la Norma NTC/ISO IEC 17799 con su equivalente NTC/ISO/ IEC 27001,27002 como un marco de referencia para la gestión de la seguridad de la información en la Alcaldía de Montería.

La Alcaldía de Montería, se compromete a administrar los riesgos de seguridad de la información para generar, implementar y monitorear los controles que permitan mantener la confidencialidad, integridad y disponibilidad de sus activos de información en cumplimiento de los requisitos aplicables.

La Norma ISO/IEC 27001 avala la adecuada implantación, gestión y operación de todo lo relacionado con un SGSI, siendo la norma más completa que existe en la implantación de controles, métricas e indicadores que permiten establecer un marco adecuado de gestión de la seguridad de la información para las organizaciones.

Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación y operación, seguimiento, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma adopta el modelo de procesos “Planificar, Hacer, Verificar, Actuar (PHVA) que aplica para estructurar todos los procesos del SGSI.

## Objetivos de la política

1. Administrar los eventos de seguridad de la información de la Alcaldía de Montería
2. Fortalecer la seguridad y disponibilidad de la información y plataforma tecnológica acorde con la declaración de aplicabilidad aprobada.
3. Cumplir con los requisitos legales aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información.
4. Fomentar una cultura de seguridad de la información en los servidores públicos (funcionarios, contratistas, pasantes, judicantes y personal en comisión de la Alcaldía de Montería).
5. Fortalecer el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

# Alcance del documento

El alcance del Plan de Seguridad y Privacidad de la Información se aplica a los procesos, funcionarios y contratistas de la Alcaldía de Montería, en concordancia con Sistema de Gestión de la Seguridad de la Información y el Plan de Desarrollo 2020 - 2023 “Gobierno de la gente”, con el objetivo de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Alcaldía.

# Términos y definiciones

- Administración de Riesgos. Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podría afectar a la información.
- Autenticidad. Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- Confiabilidad de la Información. Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de la misiones y funciones.
- Confidencialidad. Se garantiza que la información se accesible solo a aquellas personas autorizadas a tener accesos a la misma.
- Disponibilidad. Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que requieran.
- Evaluación de Riesgos. Se entiende a la amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma. La probabilidad de que ocurran y su potencial impacto en la operatoria de la Alcaldía.
- Información. Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, graficas cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en pape, en pantallas de computadoras, audiovisual u otro.
- Incidente de Seguridad. Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, la integridad o disponibilidad, la legalidad y confiabilidad de la información. Pude ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenazas de romper los mecanismos de seguridad existentes.
- Integridad. Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- Legalidad. Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a la que está sujeta la Alcaldía.

- Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.
- Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

# Contexto normativo

A continuación, se relaciona normativa clave que puede servir como guía a las entidades en la identificación de esta para la estructuración del Plan de seguridad y privacidad de la información.

| MARCO NORMATIVO | DESCRIPCIÓN |
|---|---|
| **Decreto 1078 de 2015** | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. |
| **NTC / ISO 27001:2013** | Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. |
| **NTC/ISO 27002:2013** | Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información. |
| **Conpes 3854 Política Nacional de Seguridad Digital de Colombia, del 11 de abril de 2016** | El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo |

| MARCO NORMATIVO | DESCRIPCIÓN |
|---|---|
| **Ley 527 de 2099** | Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones. |
| **Ley 1266 de 2008.** | Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. |

# Comité de seguridad de la información

El Comité de Seguridad de la Información, es creado en la Alcaldía de Montería respondiendo a la dependencia de la Oficina TIC y el cual tiene dentro de sus funciones la de impulsar, hacer seguimiento y/o verificación de la implementación del Sistema de Gestión de Seguridad de la Información - SGSI, de la Alcaldía de Montería.

Está conformado por:

- El alcalde de la ciudad de Montería o su delegado quien lo presidirá.
- Secretario de Gobierno Municipal o su delegado
- Secretario General Municipal o su delegado
- El jefe de la oficina TIC / Sistemas
- El jefe de la Oficina de Control Interno de la Alcaldía Municipal de Montería
- El Coordinador del Grupo de Gestión Documental.

# Plan de implementación del modelo de seguridad y privacidad de la información

| ACTIVIDAD | PRODUCTO | FECHA DE INICIO | FECHA DE TERMINACIÓN |
|---|---|---|---|
| Definir lineamientos para el levantamiento de activos de información | Actualización de metodología e instrumento de levantamiento de activos de información | Enero 2021 | Diciembre 2021 |
| Levantamiento de activos de información | Informe de activos de información consolidados | Enero 2021 | Diciembre 2021 |
| Gestionar el respaldo de los activos de información disponibles en medio digital | Copias de Seguridad o Backup | Enero 2021 | Diciembre 2021 |
| Divulgar y socializar las políticas de seguridad de la información | Informe de funcionarios y contratistas informados | Enero 2021 | Diciembre 2021 |
| Realizar sesiones de sensibilización sobre seguridad de la información y controles del sistema de gestión de seguridad de la información institucional para el equipo de contratistas de la Entidad | Informe de resultados de la implementación del plan de sensibilización en seguridad de la información | Enero 2021 | Diciembre 2021 |

| | | | |
|---|---|---|---|
| Gestión de Usuarios de los Sistemas de Información | Acceso seguro y controlado a los Sistemas de Información | Enero 2021 | Diciembre 2021 |
| Gestionar contratos para la actualización de las licencias de Antivirus y de dispositivos de Seguridad Perimetral | Licencias Actualizadas | Enero 2021 | Diciembre 2021 |
| Gestionar contrato de Soporte y mantenimiento de dispositivos de Seguridad Perimetral | Dispositivos de seguridad perimetral cubiertos con soporte y mantenimiento | Enero 2021 | Diciembre 2021 |
| Adelantar una Actualización del Inventario de Activos de información | Inventario Actualizado | Julio 2021 | Diciembre 2021 |
| Adelantar las actividades para el cumplimiento de la Fase de Planificación del Modelo de Seguridad y Privacidad de la Información. | Fase Planificación del MSPI cumplida.<br><br>Políticas, procedimientos, protocolos, registros y manuales del MSPI | Abril 2021 | Diciembre 2021 |
| Adelantar las actividades de la fase de implementación del MSPI | Fase de Implementación Iniciada | Abril 2021 | Diciembre 2021 |
| Acciones para apoyar la transición de IPv4 a IPv6 de la plataforma tecnológica de la entidad. | | Mayo 2021 | Diciembre 2021 |