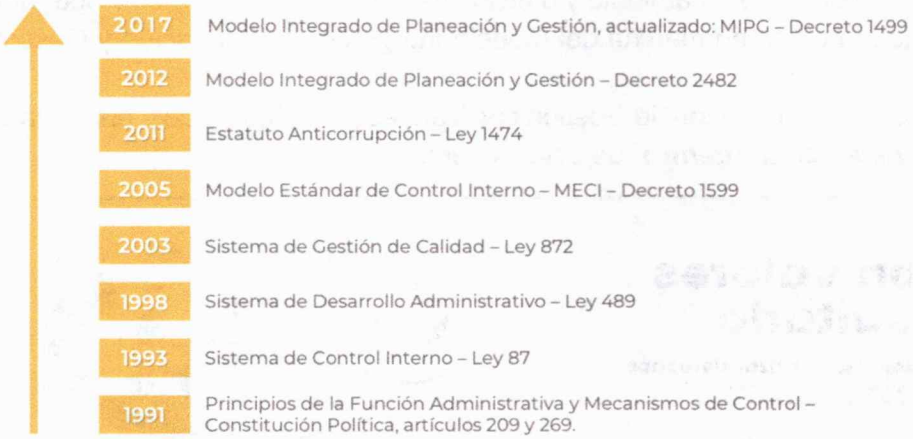
MIPG se entiende como un: Marco de referencia que le facilita a las entidades públicas:


## MARCO NORMATIVO DE MIPG




**Componentes del Modelo Integrado de Planeación y Gestión**




Calle 51C Carrera 15B Barrio La Asunción.
Manizales, Colombia
PBX: (606) 8928057
www.loteriademanizales.com

Línea de Atención al Cliente 018000188057
emsa.loteriademanizales@gmail.com
notificacionesjudiciales@loteriademanizales.com

## Introducción

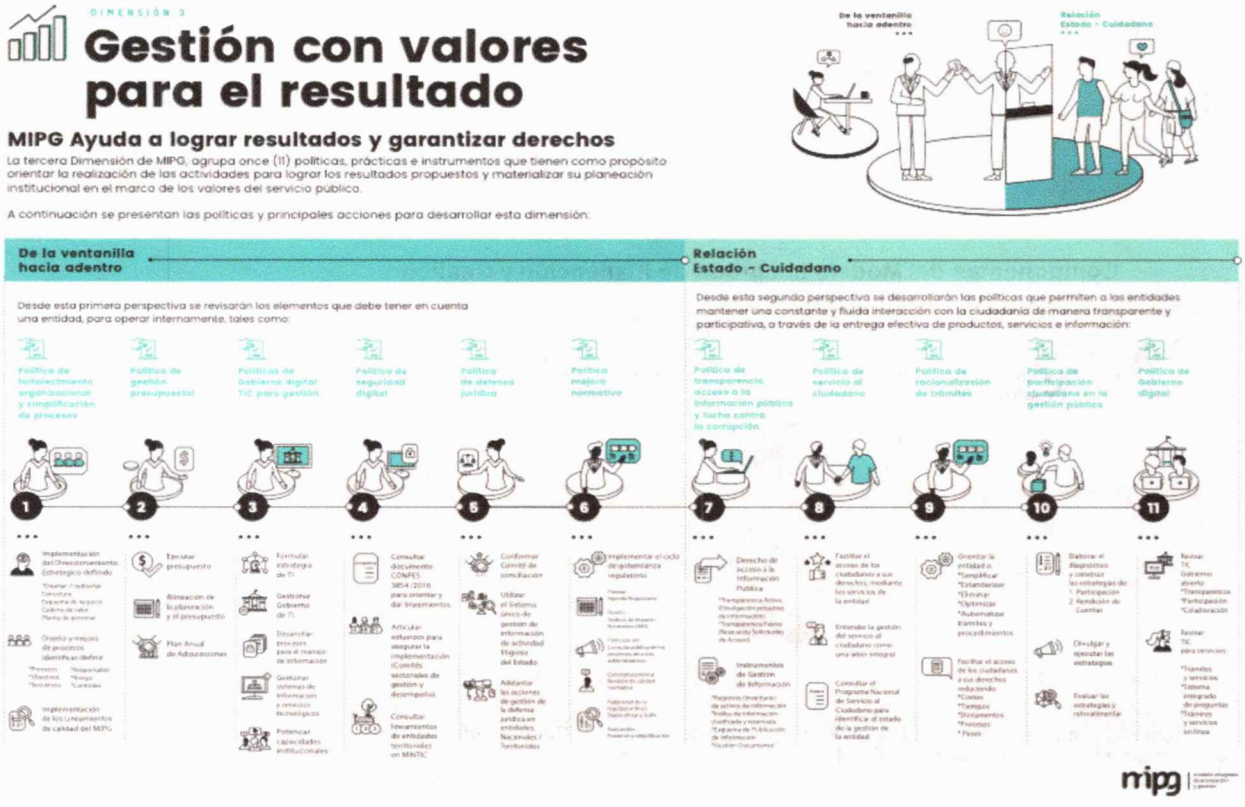
A partir del artículo 133 de la Ley 1753 de 2015 y del Decreto 1499 de 2017, el Modelo Integrado de Planeación y Gestión (MIPG) integró los sistemas de gestión de la calidad de la Ley 872 de 2003 y de Desarrollo Administrativo de que trataba la Ley 489 de 1998 y fueron derogados los artículos del 15 al 23 de la Ley 489 de 1998 y la Ley 872 de 2003.

El Modelo Integrado de Planeación y Gestión MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio.

MIPG busca mejorar la capacidad del Estado para cumplirle a la ciudadanía, incrementando la confianza de la ciudadanía en sus entidades y en los servidores públicos, logrando mejores niveles de gobernabilidad y legitimidad del aparato público y generando resultados con valores a partir de una mejor coordinación interinstitucional, compromiso del servidor público, mayor presencia en el territorio y mejor aprovechamiento y difusión de información confiable y oportuna es una de los objetivos de la puesta en marcha del Modelo Integrado de Planeación y Gestión MIPG.

Esta Política está asociada en la Dimensión de Gestión con Valores para Resultados, enmarcada en el concepto de "***Ventanilla hacia Adentro***" de esta Dimensión.





## ALCANCE:

La Política de Seguridad Digital, busca proteger la información, minimizar los riesgos y asegurar la continuidad del servicio en de La Empresa Municipal para la Salud – Lotería de Manizales, aplica a todos Servidores Públicos y en general todas aquellas personas naturales y jurídicas, que realicen cualquier actividad en la Entidad.

Con la política de Seguridad Digital se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia; Contribuyendo así a mejorar las capacidades institucionales y del gobierno central para atender los distintos tipos de ataques a la seguridad de la información.

La Empresa Municipal para la Salud – Lotería de Manizales pretende que sus funcionarios utilicen correctamente las herramientas tecnológicas como el uso de internet, las páginas sociales, el uso del papel y de la tinta de las impresoras, así mismo el uso de los equipos de cómputo, programas y todos los accesorios que se conecten a estos y que complementan su funcionamiento de modo que se garantice la protección, seguridad y privacidad de la información, por tanto es responsabilidad de todos, que se involucre la participación y el soporte de cada uno de los funcionarios de la Lotería que estén involucrados con el manejo de información y con sistemas de información, así como es un compromiso de cada persona usuario de un computador y de las redes conocer esta política y acatarla durante el desarrollo de sus actividades.



## MARCO NORMATIVO

- Constitución Política de Colombia 1991: El artículo 15 define el derecho a la intimidad y al buen nombre
- Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1581 de 2012: Se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la ley 1266 de 2008, excepto los principios.
- Ley 962 2005: Simplificación y Racionalización de Tramite. Atributos de seguridad en la información electrónica de entidades públicas.
- Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Decreto 4632 de 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

## POLITICAS DE SISTEMAS EMSA

**Propósito:**

- Asegurar la integridad, confidencialidad de la información y los recursos relacionados.
- Investigar posibles incidentes de seguridad para garantizar el cumplimiento de las políticas de seguridad de la empresa.
- Monitorear las actividades relacionadas con los sistemas de usuarios cuando se considere apropiado

## ALCANCE DE LAS POLÍTICAS

Describir las políticas de sistemas, anuncia los principales lineamientos en relación con aspectos generales de la informática con sistemas de información que apoyan la gestión administrativa, equipos de cómputo y seguridad informática.

Esta política aplica a todos funcionarios que utilizan tecnologías de información y de comunicaciones y aplica a los equipos y software propios de la entidad



## RESPONSABLE

El profesional de Sistemas será el responsable del mantenimiento y revisión periódica de este documento de tal forma que tenga en cuenta cambios tecnológicos y los cambios que ocurra en la organización o nuevas normas jurídicas que afecten las políticas aquí enunciadas.

## POLITICA DE INFORMATICA Y COMUNICACIONES

- Mejorar el efecto de la función de los sistemas y los recursos informáticos en las actividades propias de la empresa. Es compromiso de cada funcionario usuario de un computador, de los servicios y de las redes, conocer estas políticas y acatarlas durante el desarrollo de sus funciones.

- Debe existir la cultura informática en la empresa, para lograr que los usuarios tomen conciencia de que los documentos críticos desde el punto de vista del negocio, deben residir en un directorio de su PC en Mis documentos\EMSA ## (## Numero que tiene asignado el usuario).

## POLITICA DE ACCESO A LA INFORMACIÓN

- Todos los funcionarios de EMSA deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades.
- Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la Entidad, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Entidad.
- Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.
- Todas las prerrogativas para el uso de los sistemas de información de la Entidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad.

## POLITICA DE ADMINISTRACION DE CAMBIOS



- Los cambios en la plataforma tecnológica deben solicitarse a la Gerencia para su presupuesto.
- Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.
- Los servicios informáticos se brindarán en función de los recursos disponibles y las prioridades establecidas por la directiva Gerencial.
- El profesional sistemas definirá un esquema para la recepción y atención de las solicitudes de servicios que tengan que ver con recursos informáticos y de comunicaciones.
- EMSA velara través de sistemas por el buen funcionamiento de los recursos informáticos.

## POLITICA DE SEGURIDAD DE LA INFORMACION

- Los funcionarios públicos y el proveedor de software son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

- Los funcionarios EMSA y el proveedor, no deben suministrar información de la entidad a ningún ente externo sin las autorizaciones respectiva de la Gerencia.
- Todo funcionario que utilice los recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje.
- Los funcionarios y el proveedor cuando dejen de prestar sus servicios a la Entidad, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez retirado el funcionario y/o proveedor, deben comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los funcionarios públicos que detecten el mal uso de la información están en la obligación de reportar el hecho a la Oficina Jurídica de la entidad.
- El profesional de Sistemas no violará el derecho a la privacidad y confidencialidad de los datos colocados en los sistemas de información en general en la empresa, solo se permitirá el acceso a la información propia de los usuarios cuando se solicitado de manera formal por una un funcionario competente con la respectiva justificación.
- Sistemas velara por que se establezcan sistemas de protección, sistemas de detección de ataques informáticos y la creación de procedimientos de recuperación de los sistemas en caso de ocurrencia de incidentes.



## POLITICA DE SEGURIDAD PARA LOS SERVICIOS INFORMATICOS

- El sistema de correo electrónico y grupos de charla de la entidad deben ser usados únicamente para el ejercicio de las funciones de competencia de cada funcionario.
- Los funcionarios EMSA y/o proveedores que hayan recibido aprobación para tener acceso a Internet a través de las facilidades de la entidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.
- Si los usuarios sospechan que hay infección por un virus, deben inmediatamente informar al profesional de sistemas y no utilizar el computador.

## POLITICA DE SEGURIDAD EN RECURSOS INFORMATICOS

- Administración de usuarios: Establecer como deben ser utilizadas las claves de ingreso a los recursos informáticos. Dar los parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas.

- Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles.
- El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.
- Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos, son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.
- Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.
- Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.
- Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.
- El profesional de sistemas definirá el esquema para garantizar el mantenimiento de los PCs e impresoras.
- La infraestructura tecnológica que soporta los servicios telemáticos y los sistemas de información de apoyo a la gestión administrativa será administrada por el profesional de sistemas.



## POLITICA DE SEGURIDAD EN COMUNICACIONES

- Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratados como información confidencial.
- Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la entidad, deben pasar a través Firewall, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.
- Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la Entidad e Internet deberá estar cifrada

## POLITICA DE SOFTWARE UTILIZADO

- Todo software que utilice EMSA será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.
- Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios, de las implicaciones que tiene el instalar software ilegal en los computadores de EMSA.
- Los sistemas de información de apoyo a gestión administrativa están regidos por los derechos de autor que se lleve a cabo entre las partes.

## POLITICA DE ACTUALIZACION DE HARDWARE

- Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del Profesional de sistemas.
- La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.
- Los equipos (PC, servidores, LAN etc.) no deben moverse o reubicarse sin la aprobación previa del profesional de sistemas.
- EMSA debe tener un proveedor del servicio de Internet para toda la entidad.
- El esquema de las redes LAN será definido por EMSA.



## POLITICA DE ALMACENAMIENTO Y RESPALDO

- La información que es soportada por la infraestructura de sistemas deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.
- Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.
- La entidad definirá la custodia de los respaldos de la información que se realizará externamente.
- El almacenamiento de la información deberá realizarse interna y/o externamente a la Entidad, de acuerdo con la importancia de la información.
- El área dueña de la información en conjunto con la oficina Sistemas definirán la estrategia a seguir para el respaldo de la información.

- Los funcionarios de EMSA son responsables de los respaldos de su información en los PCs, siguiendo las indicaciones técnicas dictadas por la oficina de Sistemas. La oficina de Sistemas será la autorizada para realizar el seguimiento y control de esta política.

## POLITICA DE CONTINGENCIA

- La Entidad debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, incendio, explosión, terrorismo, inundación etc.

## POLITICA DE SEGURIDAD FISICA

- La Entidad deberá contar con los mecanismos de control de acceso como: puertas de seguridad, sistema de alarmas y cámaras en las dependencias que la entidad considere críticas.
- El área de Sistemas es de acceso restringido y cualquier persona que ingrese a ella deberá estar acompañada permanentemente por el personal que labora cotidianamente en este lugar.
- Los equipos de cómputo (PCs, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa de Sistemas.
- Los funcionarios públicos se comprometen a **NO** utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que genere caídas de la energía.



Actualización de esta política de Seguridad Digital, Manizales, 19 de julio de 2023

**JORGE ANDRES ARTEAGA MARTINEZ**
Gerente

**NÉSTOR FABIO VALENCIA TORRES**
Profesional Especializado
Gestión Jurídica

**WILIAM ANDRES VASCO PINEDA.**
Profesional Universitario
Gestión Administrativa

**JOHN JAIRO ZULUAGA HENAO**
Profesional Universitario Sistemas
Vo.Bo.