Alcaldía de Manizales

MANUAL DE OPERACIÓN DE LAS POLÍTICAS DE MIPG

DIMENSIÓN GESTIÓN CON VALORES PARA RESULTADOS

POLÍTICA DE SEGURIDAD DIGITAL

2023

INTRODUCCION

La Alcaldía de Manizales, mediante el Decreto 0419 del 5 de septiembre de 2023, implementó el Modelo Integrado de Planeación y Gestión en la entidad con el fin de orientar, fortalecer, articular, alinear y dirigir la gestión institucional mejorando la interacción de la entidad y la ciudadanía.

Este proceso ha permitido agilizar su implementación en la entidad, el cual consiste en procesos como el ciclo PHVA, incluyendo con esto la mejora continua; es así como se estableció la responsabilidad para la implementación, desarrollo y control y mejora del esquema operativo de MIPG, dejando la estructura de las políticas, y líneas de acción.

Cada política será trabajada a través de mesas técnicas, con planes de trabajo anuales, estas mesas tendrán que reunirse periódicamente con carácter obligatorio, deberán reportar los avances, de las actividades al Comité de Desempeño Institucional con el fin de que se tomen las decisiones, atendiendo la implementación y operación del modelo.

Finalmente, la Unidad de Transparencia y Gobierno Abierto, adscrita a la secretaria de Servicios Administrativos, como Líder de MIPG, desarrolló conjuntamente con los funcionarios enlaces de cada dependencia la compilación y expedición de este Manual, buscando con ello promover la gestión y eficiencia de la entidad manteniendo su vigencia.

El Manual Operativo, que presentamos se ha desarrollado de acuerdo con el Modelo Integrado de Planeación y Gestión, describiendo los diferentes mecanismos a través de los cuales se deben dinamizar cada una de las 19 políticas, en el marco del direccionamiento y la planeación estratégica de la Alcaldía de Manizales, con la siguiente estructura:

- Objetivo general
- Objetivos específicos
- Marco legal,
- Definiciones
- Líneas de acción
- Responsables
- Seguimiento

Este manual, podrá ser consultado en la sede electrónica de la Alcaldía de Manizales en el botón de transparencia y acceso a la información pública, así mismo, debe ser objeto de socialización a los funcionarios de la administración municipal con el fin de que en sus actuaciones administrativas estén inmersas los lineamientos descritos en este documento.

7. OPERACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

7.1. Objetivo General

Identificar, gestionar y mitigar los riesgos de seguridad digital que puedan afectar la confianza de los ciudadanos y la calidad de datos que se gestionan por ambas partes.

7.2. Objetivos Específicos

- Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y el MinTIC para el Tratamiento de Riesgos de Seguridad Digital.
- Actualizar el Modelo de privacidad y seguridad de la información y aplicar los lineamientos allí establecidos para garantizar un entorno de confianza digital de manera articulada con la política de Gobierno Digital.
- Promover en los usuarios internos y externos el uso y comportamiento responsable, en el entorno digital, de forma que no afecten la seguridad de los activos digitales de la Entidad.
- Establecer los mecanismos de aseguramiento físico, digital y de cultura organizacional, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la Información de la Administración Municipal.

7.3. Marco Legal

NORMA	DESCRIPCION
Ley 23 1.982	Sobre Derechos de Autor
Ley 80 1993	Por la cual se expide el Estatuto General de Contratación de la Administración PÚBLICA
Ley 1341 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones
Ley 1347 2011	Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. - Utilización de Medios Electrónicos en el Procedimiento Administrativo.
Ley 1581 2012	Por el cual se dictan disposiciones generales para la protección de datos personales. HABEAS DATA
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Modificado en el artículo 2.2.9.1.1.3., incluye la seguridad de la información entre los principios de las Políticas de Gobierno Digital y Seguridad Digital; de igual manera, en el artículo 2.2.9.1.2.1. se establece que las Políticas de Gobierno Digital y Seguridad Digital - ÚLTIMA FECHA DE ACTUALIZACIÓN: 22 DE AGOSTO DE 2023
Decreto 1414 de 2017	A través del cual se modificó la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones, asignando a la Dirección de Gobierno Digital, antes "Dirección de Gobierno en Línea"
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. - Manual de Gobierno Digital

Directiva presidencial de 2019	Simplificación de la interacción digital entre los ciudadanos y el estado
Decreto 2106 de 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública
CONPES 3995 de 2020	POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL
Resolución 2893 2020	"Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPAs y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado Colombiano, y se dictan otras disposiciones"
Resolución 1519 2020	"Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos
Decreto 338 2022	Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 767 de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 88 de 2022	"Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los articulas 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea"
Resolución 460 de 2022	Por lo cual se expide el plan nacional de infraestructura de datos y su hoja de ruta en el desarrollo de la política de gobierno digital y se dictan los lineamientos generales para su implementación.
Decreto 1263 2022	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública
Ley 2294 2023	Por la cual se expide el Plan Nacional de Desarrollo 2022-2026 "Colombia Potencia Mundial de la Vida" establece en su artículo 43 las medidas que implementará el Ministerio de las Tecnologías de la Información y las comunicaciones entre las que se encuentra el Fortalecimiento del Gobierno digital para "tener una relación eficiente entre el Estado y el ciudadano, que lo acerque y le solucione sus necesidades, a través del uso de datos y de tecnologías digitales para mejorar la calidad de vida

7.4. Definiciones

Amenaza cibernética: aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (Documento CONPES 3854)

Ataque cibernético: acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio. (Documento Modelo Nacional Riesgo de Seguridad Digital)

Ciberdefensa: es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. (Documento CONPES 3854).

Ciberespionaje: es el acto o práctica de obtener secretos sin el permiso del dueño de la información (personal, sensible, propietaria o de naturaleza clasificada) para ventaja personal, económica, política o militar en el Ciberespacio, a través del uso de técnicas malintencionadas. (Documento CONPES 3854).

Ciberterrorismo: es el uso del Ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado trayendo. (Documento CONPES 3854).

Cibercrimen (delito cibernético): conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio. (Documento CONPES 3854).

Ciberlavado: es el uso del Ciberespacio, en cualquiera de sus formas, para dar apariencia de legalidad a bienes obtenidos ilícitamente o para ocultar dicha ilicitud ante las autoridades

Ciberseguridad: es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio. (Documento CONPES 3854).

Entorno digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

Entorno digital abierto: entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica.

Gestión de riesgos de seguridad digital: es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades.

Incidente digital: evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos.

Infraestructura crítica cibernética nacional: aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (Documento CONPES 3854).

Riesgo: es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

Riesgo de seguridad digital: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital.

Resiliencia: es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (Documento CONPES 3854).

Seguridad de la información: "Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua, con miras a preservar la confidencialidad, integridad, y disponibilidad de la información" (ISO/IEC 27000).

Seguridad digital o ciberseguridad: Conjunto de medidas de "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (Documento CONPES 3854).

7.5. Líneas de Acción

- **Fortalecimiento De Las Capacidades En Seguridad Digital De Los Ciudadanos, De Los Servidores Públicos Y Del Sector Privado Para Aumentar La Confianza Digital En La Administración Municipal**

Adoptar las estrategias diseñadas por el gobierno nacional, para la formación en materia de seguridad digital

Establecer la articulación con las autoridades definidas por el gobierno nacional en la identificación, prevención y gestión de incidentes de seguridad digital que puedan afectar a la Administración Municipal.

- **Actualizar El Marco De Gobernanza En Materia De Seguridad Digital Para Aumentar Su Grado De Desarrollo Y Mejorar El Avance En Seguridad Digital De La Administración Municipal**

Definir los objetivos, alcance, roles, responsabilidades y competencias tanto de las diferentes instancias encargadas de la seguridad digital en la Administración Municipal, como las correspondientes a una unidad de política de ciberseguridad, de acuerdo con el protocolo nacional.

Estandarizar un mecanismo de reporte periódico de incidentes y vulnerabilidades cibernéticas que permita identificarlos, evaluarlos y comunicarlos a los interesados y servir de fuente para la toma de decisiones por parte de la Administración Municipal.

- **Analizar La Adopción De Modelos, Estándares Y Marcos De Trabajo En Materia De Seguridad Digital, Con Énfasis En Nuevas Tecnologías Para Preparar Al País A Los Desafíos De La Cuarta Revolución Industrial (4ri)**

  - Definir el alcance de los modelos y estándares a adoptar por parte de la entidad, donde se tenga la capacidad de analizar el impacto de la implementación de las nuevas tecnologías.

- Adquirir dispositivos que permitan proteger la información digital de la Institución.
- Actualizar la infraestructura tecnológica con el fin de disminuir las vulnerabilidades derivadas de la obsolescencia tecnológica y así favorecer la seguridad digital en la Administración Municipal.

❑ Generar Indicadores Que Permitan Realizar El Seguimiento Periódico Al Cumplimiento De Las Acciones Y Actividades Derivadas De La Política Operativa De Seguridad Digital

- Disponer de un repositorio de gestión de incidentes desde el cual se puedan recopilar datos para alimentar los indicadores.
- Llevar a cabo reuniones periódicas programadas para revisar los indicadores y proponer planes de acción y actividades que faciliten una gestión efectiva de los incidentes relacionados con la seguridad digital.

❑ Documentación Que Se Deben Tener En Cuenta En El Desarrollo De La Política

- Modelo de Seguridad y Privacidad de la Información: Actualizar el MSPI mínimo una vez al año.
- **PESI:** Plan estratégico de seguridad de la información
- Plan de Tratamiento de Riesgos de seguridad y privacidad de la Información
-

7.6. Responsabilidades de la Operación de la Política

La responsabilidad de la implementación, desarrollo, control y mejora de las políticas de Gobierno Digital y Seguridad Digital y su marco de referencia se encuentra a cargo de los siguientes servidores públicos:

Responsable Institucional de la Política de Gobierno Digital: es el representante legal, responsable de coordinar, hacer seguimiento y verificar la implementación de la Política de Gobierno Digital.

Responsable de orientar la implementación de la Política de Gobierno Digital: es el Comité Institucional de Gestión y Desempeño, de que trata el artículo 2.2.22.3.8 del Decreto 1083 de 2015. Esta instancia será la responsable de orientar la implementación de la política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.

Responsable de liderar la implementación la Política de Gobierno Digital: La Secretaría de Tic y Competitividad y la Secretaría de Servicios Administrativos son las encargadas de coordinar, orientar y promover la articulación de los actores institucionales para la óptima implementación de las Políticas.

Los líderes de proceso dentro del rol que les corresponde deben liderar, impulsar, apoyar, evaluar y hacer seguimiento al cumplimiento en concordancia con sus competencias y nivel de responsabilidad, así como generar las recomendaciones de mejoramiento pertinentes.

Los servidores públicos que tienen a su cargo cada plan, programa, proyecto o estrategia, son los responsables de realizar el seguimiento y la evaluación de los resultados institucionales, y definir las acciones de corrección o prevención de riesgos.

Los servidores públicos de la entidad que no se encuentren inmersos en los roles anteriores y los terceros vinculados con ella, son responsables de aplicar lo establecido en el Modelo Integrado de Planeación y Gestión y su marco de referencia, en el desarrollo de sus funciones u obligaciones a su cargo.

POLITICA	SECRETARIAS LIDER	LIDER TEMATICO	GESTOR
Seguridad Digital	Servicios Administrativos con el apoyo de Competitividad, Movilidad, Hacienda, Salud, Planeación, Educación	Líder de Proyecto – Unidad de Gestión Tecnológica	Profesional Especializado Unidad Administrativa de Planeación y Control Para la Movilidad - Profesional Especializado Unidad de Planeación Estratégica - Profesional Especializado de Fomento Empresarial - Profesional Universitario Unidad de TIC Profesional Universitario Estadística - Salud Profesional Universitario -líder Cobertura Educación Profesional Universitario tecnología Educación Líder de Proyecto – Unidad de Gestión Tecnológica Profesional Universitario – Unidad de Gestión Tecnológica Hacienda

7.7. Seguimiento de la Operación de la Política

Se crea la Mesa Técnica de Transformación Digital para que sea la instancia encargada de la actualización de la política y el desarrollo de las actividades derivadas de la misma.

Secretarías que componen la mesa técnica:

- Secretaría de Servicios Administrativos
- Secretaría de TIC y Competitividad
- Secretaría de Educación
- Secretaría de Salud Pública
- Secretaría de Planeación
- Secretaría de Hacienda
- Secretaría de Movilidad

Dentro del seguimiento a la operación, la identificación de activos tecnológicos es fundamental para que una entidad pueda comprender cuáles son los recursos, datos e información críticos para su operación y, así, protegerlos de manera adecuada.

Una vez que se han identificado estos activos, es necesario evaluar los riesgos que podrían afectarlos. Esto implica analizar las amenazas potenciales, establecer la matriz de riesgos, las acciones de mitigación y el manejo de los mismos, de igual manera cuantificar y determinar el impacto y las vulnerabilidades que podrían ser explotadas.

Una vez que se han identificado los riesgos, es fundamental implementar acciones de mitigación. Estas acciones pueden incluir la aplicación de medidas de seguridad técnicas, como firewalls, sistemas de detección de intrusiones y actualizaciones regulares de software, así como la implementación de políticas y procedimientos para concientizar a los funcionarios y contratistas sobre las mejores prácticas de seguridad.

De igual forma, es importante tener un plan de respuesta a incidentes en su lugar para abordar rápidamente cualquier problema de seguridad que pueda surgir.

Documento socializado por los representantes de cada Mesa técnica de Política de MIPG en sesión del día jueves 23 de noviembre de 2023 al Comité Institucional de Gestión y Desempeño mediante acta de reunión.