El servicio público es de todos

Función Pública

FUNCIÓN PÚBLICA

Manual Gobierno de Datos

Seguimiento y evaluación

VERSIÓN 1

Diciembre 2021

Versión	Fecha de versión (aaaa-mm-dd)	Descripción del cambio
1	2021-12-15	Creación del documento

Contenido

Tabla de tablas

Tabla de Gráficos

Introducción

Gobernar los datos es un proceso que busca administrar la disponibilidad, usabilidad, integridad y seguridad de los datos, basado en lineamientos y estándares que garantizan que los datos de una organización sean coherentes y confiables para una toma de decisiones asertiva, basada en evidencia, rompiendo silos de información y que la organización tenga una visión única a través de procesos armonizados entre sistemas y bajo una arquitectura que propende por la calidad y el correcto uso de la información.

Entendiendo lo anterior, Función Pública presenta este manual con el fin de entregar lineamientos para la administración y gestión de los diferentes componentes de información que orienten a la Entidad sobre la forma de implementar, mantener y mejorar un programa de gobierno de datos, con el fin de aportar al avance en la madurez en la gestión de datos, priorizando los datos maestros a gobernar según el flujo de información presente en diferentes procesos y procedimientos.

Este manual se estructura en 5 capítulos, los dos primeros hacen referencia a los conceptos, términos y normatividad aplicable, los restantes definen las políticas aplicables al Departamento Administrativo de la Función Pública y los procedimientos requeridos para la gestión de datos en la Entidad teniendo en cuenta lo establecido en la Guía G. INF. 06 Guía Técnica de Información – Gobierno de Datos elaborado por Ministerio de Tecnologías de la Información y las Comunicaciones MinTic (MinTIC, 2014) y el DAMA -DMBOOK (Beach, 2009).

Objetivo general

Establecer e implantar lineamientos y políticas para la administración y gestión de los diferentes componentes de información de la Entidad en el marco de los componentes de arquitectura empresarial de gobierno de datos con el fin de garantizar la calidad y oportunidad de los datos para la toma de decisiones asertivas.

Objetivos específicos

1. Establecer una cultura para la gestión y calidad de los datos
2. Gestionar la información a partir de estándares de calidad que faciliten su análisis y tratamiento
3. Identificar todos y cada uno de los componentes de información de la Entidad y los datos que los componen y sus diferentes flujos.
4. Contar con información homologada en los diferentes sistemas de información.
5. Gestionar los componentes de información de la entidad con el fin de asegurar su disponibilidad, seguridad y privacidad de acuerdo con la normatividad vigente.

Glosario

Arquitectura del dato: es el componente del dominio de información asociado con la coordinación de la estructura, semántica, y calidad del dato desde el origen, así mismo, participando en el diseño de los modelos y flujos de datos de las aplicaciones (Mintic. Guia del Dominio de Información G.IN.01, 2019)

Bodega de datos: es una colección de datos orientada a un determinado ámbito (institución, ciudadano, etc.), integrado, no volátil y variable en el tiempo, que ayuda a la toma de decisiones en la institución en la que se utiliza (Mintic. Guía Técnica de la información - Gobierno del dato G.INF.06, 2019)

Calidad de datos: es el componente del dominio de información asociado con procesos de ajuste y depuración de datos masivos, y definición, medición y mejora continua de los indicadores de calidad del dato (Mintic. Guía Técnica de la información - Gobierno del dato G.INF.06, 2019)

Ciclo de vida del dato: proceso que emprende el dato desde su creación y almacenamiento inicial, hasta el momento cuando se convierte en obsoleto y es eliminado (Mintic , 2019)

Componente de información: es el término agrupador utilizado para referirse al conjunto de los datos, entidades de negocio, unidades de información, los servicios de información y los flujos de información bajo un único nombre (Mintic. Guía técnica de información - Administración del dato maestro G.INF.02, 2019)

Conjunto de datos: unidad mínima de información sujeta a carga, publicación, transformación y descarga (Documento CONPES 3920, 2018)

Dato: representación simbólica, numérica, algorítmica, alfabética que describe un hecho empírico, un suceso, es la información que recibe el computador a través de distintos medios y que es manipulada mediante el procesamiento de los algoritmos de programación (Editorial Etecé , 2021).

Dato maestro: es el dato transversal a toda la organización que describe las entidades de negocio como ciudadano, institución, trámite, entre otros, resultado de la unificación de visión, y normalización de registros. Estos son compartidos por los diferentes sistemas de información de la institución. (Mintic. Guía técnica de información - Administración del dato maestro G.INF.02, 2019)

Diccionario de datos: listado de datos organizado, que se desarrolla de manera estricta, cuenta con características lógicas y puntuales de tal manera que se encuentren elementos comunes para el entendimiento de la base de datos y se utiliza en un sistema de información. Este hace parte de la documentación técnica en el desarrollo y mantenibilidad de los sistemas de información. (Catastro Distrital, 2019)

Gestión de datos: es la actividad que debe asegurar, mantener y proveer instituciones de datos, unificando datos maestros y regularizando registros en los sistemas fuente. Esta actividad involucra la identificación de los requerimientos que mantienen repositorios centrales del dato, los que determinan la asociación con procesos claves que usan el dato y los que definen los tipos de aprovisionamiento de datos a gestionar (reactivo, proactivo, administrado, optimizado y autoservicio) (Mintic. Guía Técnica de la información - Gobierno del dato G.INF.06, 2019)

Gobierno de datos: es una disciplina clave para controlar el uso de los datos maestros del sector público, además de abordar con éxito las renovaciones, migraciones, integraciones en sistemas y organizaciones asociadas con el dato. El gobierno aborda los ámbitos de arquitectura, calidad, custodia, aprovisionamiento y gestión de la demanda del dato. (Mintic. Guía Técnica de la información - Gobierno del dato G.INF.06, 2019)

Interoperabilidad: habilidad de transferir y utilizar información de manera uniforme y eficiente entre varias organizaciones y sistemas de información (Mintic, 2016)

Infraestructura de TIC: conjunto de elementos que sirven de soporte para la prestación de servicios informáticos. Está compuesta por servidores, computadores, sistemas de almacenamiento, dispositivos de red, canales de comunicación, sistemas de digitalización, dispositivos de seguridad, entre otros.

Metadatos: son datos sobre los datos. Los metadatos articulan un contexto para determinados objetos de interés (recursos), en forma de descripción de recursos (Mintic. Guía Técnica de la información - Gobierno del dato G.INF.06, 2019)

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas (ISO 27001, 2005)

1. Marco legal

Ley 1581 de 2012, disposiciones generales para la protección de datos personales: La ley tiene como objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma (Función Pública, 2021).

Ley 1712 de 2014, Ley de transparencia y del derecho de acceso a la información pública nacional: La ley tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información y cuyo principio dictamina que toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con ley expuesta (Función Pública, 2021).

Normas ISO: dentro de las normas ISO se encuentra la ISO/IEC 38505-1 relacionada el gobierno de datos. Esta norma proporciona guías para aplicar el enfoque basado en principios de la norma ISO/IEC 38500 a los datos, incrementando su valor al interior de la organización a la vez que disminuye el riesgo involucrado en datos. Por otro lado, la ISO/IEC 38505-2 examina implicaciones para la gestión de datos, la estrategia de datos del consejo, además de como la estrategia difunde las políticas, procesos y controles relativos a los datos (ISO, 2017).

Por otro lado, la familia ISO 8000 está compuesta por conceptos generales, gestión de calidad de datos donde se proporciona un modelo de referencia de procesos y un modelo de evaluación de la madurez, información de

ingeniería como guía para la aplicación de calidad de los datos del producto y datos maestros donde se trata el intercambio de datos. (ISO 8000, 2018)

Directiva 002 de 2000, en ella se señala, "Las Tecnologías de la Información son herramientas que permiten el desarrollo de una nueva economía, la construcción de un Estado más moderno y eficiente, la universalización del acceso a la información, y la adquisición y eficaz utilización del conocimiento, todos estos elementos fundamentales para el desarrollo de la sociedad moderna". Por ello, se diseñó el marco de la Agenda de Conectividad, "como una Política de Estado, que busca masificar el uso de las Tecnologías de la Información en Colombia y con ello aumentar la competitividad del sector productivo, modernizar las instituciones públicas y socializar el acceso a la información" (Presidencia de la Republica, 2000).

G.INF.06 Guía Técnica de Información - Gobierno del dato guía técnica del Gobierno del Dato: en ella se soportan los componentes necesarios para la implementación de los lineamientos asociados a: registro y mantenimiento de información, establecimiento de los mecanismos de actualización de los componentes informacionales, la creación y mantenimiento del repositorio unificado de datos con el fin de realizar adecuado gobierno del dato en las organizaciones (MinTIC, 2014).

G.INF.02 Guía técnica de Información- Administración del dato maestro: donde se enmarcan un conjunto de pasos y actividades para una adecuada administración de datos maestros, y se aporta en la definición de procesos que permitan apoyar la mejora de la calidad de los datos, a partir del gobierno de datos (MinTIC, 2014).

Política de Gobierno Digital: define los lineamientos, estándares y proyectos estratégicos, que permiten llevar a cabo la transformación digital del Estado, a fin de lograr una mejor interacción con ciudadanos, usuarios y grupos de interés; permitiendo resolver necesidades satisfactoriamente, resolver problemáticas públicas, posibilitar el desarrollo sostenible y en general, crear valor público. (Mintic, 2021).

Política de Gestión de la Información Estadística: busca que las entidades generen y dispongan la información estadística, así como la de sus registros administrativos, de acuerdo con los lineamientos establecidos por el líder de Política, para mejorar la efectividad de su gestión y planeación basada en evidencias; garantizando una continua disponibilidad de información de calidad a lo largo del ciclo de la política pública; fomentando el diálogo social con la ciudadanía y los grupos de interés, en el marco de la construcción participativa de las soluciones sociales, y generando una herramienta de control político y social que permita la transparencia de las actuaciones del Estado. (Función Pública - Manual Operativo MIPG, 2021)

Política de Seguridad de la información: busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de las entidades del Estado, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado. (Función Pública - Manual Operativo MIPG, 2021)

Protocolo para la gestión de información estadística: proceso de gestión de información estadística, que se fundamenta en el diseño y ejecución eficiente de actividades entre dependencias y la adopción de estándares y buenas prácticas estadísticas. (Función Pública, 2021)

Resolución 110 de 2020: Comité Interno de Gestión de Información Estratégica que propende por la articulación, armonización y estandarización de la producción y consolidación de información estadística de carácter estratégico a interior de la entidad (Función Pública, 2021)

2. Roles de gobierno de datos

2.1. Roles de autoridad y responsabilidad

La estructura organizacional es vital para la ejecución de un programa de gobierno de datos, esta garantiza una distribución tanto para la toma de decisiones como la operatividad del programa. La estructura definida para el gobierno de datos en Función Pública tiene tres niveles, la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC participa activamente en la estructura puesto que participa desde el aspecto operativo en cuanto a la administración del sistema de información hasta niveles estratégicos a nivel de soporte tecnológico.

***Gráfica 1**. Roles para el gobierno de datos*

Fuente: Elaboración propia- Oficina Asesora de Planeación Función Pública

Nivel estratégico

La formalización de un consejo de gobierno proporciona supervisión del programa de gobierno de datos, tomando decisiones a nivel estratégico, se encargan de la aprobación de políticas y de asignación de los recursos necesarios para su cumplimiento. Función Pública cuenta con un comité interno de gestión de

información estratégica, el cual tiene las funciones establecidas para el consejo de gobierno, y asume el rol de rector según el "*protocolo para la gestión de información estadística*" de la Entidad.

Tabla 1. Rol consejo de gobierno

Rol	Consejo de Gobierno (Comité Interno de Gestión de Información Estratégica)
Actor	Dirección General Subdirección Direcciones Técnicas Oficinas de Apoyo
Responsabilidades	1 definir políticas o lineamientos estratégicos en programa del gobierno de datos. 2. Gestionar los recursos necesarios para el cumplimiento de las estrategias que se planteen. 3. Revisar y aprobar el plan operativo del programa de gobierno de datos 4. Establecer, en caso de requerirse, el nivel de participación de las dependencias involucradas en la atención de la necesidad del usuario. 5. Definir, en caso de requerirse, la dependencia responsable (única) para cada fuente de información 6. Designación de roles y responsabilidades para el gobierno de datos 7. Definir, conjuntamente con el productor, la periodicidad de la información
Nivel Decisorio	Estratégico
Cargo Servidor	Director General Subdirector Directores Técnicos Jefes de Oficina

El gerente de gobierno de datos y equipo de gobierno de datos tiene la visión del programa, propenden por una gestión adecuada de la información y es el articulador entre consejo de gobierno y el nivel operativo. Por otro lado, la Oficina Asesora de Planeación – OAP tiene el rol de coordinador según el "protocolo para la gestión de información estadística" de la Entidad lo que indica su participación activa en el equipo de gobierno de datos, todo esto al tener responsabilidades que se enmarcan en liderar la centralización de información estadística, apoyar el análisis y apoyar técnicamente bajo la perspectiva estadística a las dependencias.

Tabla 2.Rol gerente y equipo de gobierno

Rol	Gerente de gobierno de datos y equipo de Gobierno de Datos
Actor	Oficina Asesora de Planeación Oficina de Tecnologías de la información

Responsabilidades	1. Coordina el proceso del gobierno de datos 2. Convoca y lidera sesiones de comité de gobierno de datos 3. Realiza un seguimiento de las métricas 4. Gestiona las comunicaciones internas 5. Realizar evaluaciones periódicas al programa en materia de políticas dispuestas, calidad de datos, riesgos de privacidad, entre otros 6. Desarrollar estrategias de gobernanza y su plan de implementación 7. Determinar las estrategias más adecuadas de divulgación o socialización de las decisiones tomadas en todo lo relacionado a gobierno de datos.
Nivel Decisorio	Estratégico
Cargo Servidor	Jefe Oficina Asesora de Planeación Jefe Oficina Tecnologías de la Información

Nivel táctico

Roles con conocimiento del negocio, con capacidades técnicas y habilidades analíticas e informáticas conforman este segundo nivel, deben tener una constante comunicación con el nivel estratégico y operativo para la toma de decisiones tácticas para una gestión adecuada de la información en el ciclo de vida del dato.

El nivel táctico comprende los roles descritos a continuación

Tabla 3. Rol Arquitecto de datos

Rol	Arquitecto de datos
Actor	Oficina de Tecnologías de la información
Responsabilidades	1. Arquitectura de datos y la integración de los mismos 2. desarrollo, mantenimiento y aprovechamiento del modelo de datos empresarial.
Nivel Decisorio	Táctico
Cargo Servidor	Administrador de base de datos

Tabla 4. Rol Administrador de datos en seguridad de la información

Rol	Administrador del dato en seguridad de la información
Actor	Oficina Asesora de Planeación

Responsabilidades	1. Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información. 2. Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. 3. Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora 4. Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. 5. Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información. 6. Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.
Nivel Decisorio	Táctico
Cargo Servidor	Oficial de seguridad de la información

Tabla 5. Rol líder de procesos y procedimientos

Rol	Líder de procesos y procedimientos
Actor	Direcciones Técnicas
Responsabilidades	1. apoyar la articulación de los procesos y procedimientos con la gestión de información y el gobierno de datos 2. Designar los responsables temáticos por dependencia para implementación y seguimiento al gobierno de datos
Nivel Decisorio	Táctico
Cargo Servidor	Directores técnicos

Nivel operacional

Es vital para el desarrollo del programa de gobierno de datos tanto el gestor del dato como su administrador funcional son responsables de la calidad de los datos, debe tener conocimiento en los procesos que intervienen con el dato a gobernar, está conformado por miembros representantes de las dependencias que producen información y que en el marco del protocolo comprenden el rector de productor.

Tabla 6. Rol gestor del dato

Rol	Gestor del dato (Data steward)
Actor	Direcciones Técnicas
Responsabilidades	1. Producir información estadística de calidad para satisfacer las necesidades del usuario. 2. Propender por el mejoramiento continuo de la información estadística que produce. 3. Reportar hallazgos al administrador de gobierno de datos 4. Definir el flujo de datos en los procesos y los sistemas de información 5. Comunicar y promover el valor de la información. 6. Monitorear y hacer cumplir las políticas y prácticas de datos en su dependencia.
Nivel Decisorio	Operacional
Cargo Servidor	Directores técnicos Analista de datos dependencia

Para el nivel operacional se cuenta con el apoyo de Oficina de Tecnologías de la Información y las Comunicaciones – OTIC encargada de la administración del componente tecnológico del sistema de información que centraliza el dato a gobernar, además se cuenta con el apoyo temático de la dependencia técnica.

Tabla 7. Rol administrador del dato técnico

Rol	Administrador del dato técnico
Actor	Oficina de Tecnologías de la información
Responsabilidades	1. Aplicar las políticas y lineamientos de gobierno de datos a los sistemas de información 2. Apoyar en la definición y ajuste de problemas de datos y alternativas de solución. 3. Apoyar en la definición de políticas y estándares de gestión de datos. 4. Apoyar a comprender las necesidades de información. 5. Participar en el modelado y la arquitectura de datos. 6. Apoyar en las definiciones y requisitos de calidad de los datos
Nivel Decisorio	Operacional
Cargo Servidor	Jefe Oficina Tecnologías de la Información Administrador del sistema de información

2.2. Roles de acceso a los datos

Cada uno de los sistemas de información de la Entidad tienen identificados roles y permisos de acceso, de acuerdo con lo definido por el usuario funcional y técnico y a la documentación correspondiente que comprende

la matriz de roles y responsabilidades, manual de usuario y manual técnico, por lo tanto, para el gobierno de datos de Función Pública en lo que se refiere a los sistemas de información los roles serán los mismos que ya se encuentran establecidos. De otra parte, para la consulta y acceso de los datos maestros identificados en el software o aplicativo definido por la entidad se tendrán en cuenta los siguientes roles:

Propietario: el cual estará a cargo del usuario funcional o responsable del dato a gobernar y tendrá acceso a consulta sin restricciones

Administrador: el cual estará a cargo de equipo de gobierno de datos de Función Pública y tendrá acceso a consultas y modificaciones sin ningún tipo de restricción.

Consulta: a este rol tendrán acceso todos los usuarios de la información de la entidad el cual se podrá configurar de acuerdo con la necesidad especifica de cada uno

3. Lineamientos y políticas de gobierno de datos

3.1 Política de Seguridad de la información

Teniendo en consideración los principios legales identificados en las normas aplicables al tratamiento de datos personales y la política de gobierno digital se hace necesario consolidar los principios aplicables a la arquitectura de la seguridad digital institucional priorizando aquellos orientados a la preservación de la privacidad de los datos personales. Sin desconocer la importancia de los diferentes principios analizados, a continuación, se agrupan los principios de la arquitectura de seguridad digital para gobierno de datos.

3.1.1 Principios y controles de seguridad para el tratamiento de datos personales

3.1.1.1 Principio de veracidad o calidad: la información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Tratamiento de datos personales

Control: política de tratamiento de datos personales. De acuerdo con los requisitos de la ley 1581 de 2012, la entidad cuenta con una política de protección de datos personales que garantiza a los titulares de los datos personales el ejercicio de su derecho de hábeas data. Ver: Política de tratamiento de datos personales

Uso aceptable de los activos de información

Control: lineamientos de gestión de activos de información en Función Pública.

- Todos los servidores públicos, contratistas y pasantes de Función Pública deben aplicar los controles de seguridad de la información definidos por la entidad para garantizar la preservación de la confidencialidad, integridad, disponibilidad de los activos de información institucionales.

- Los propietarios de los activos de información son responsables de su uso y protección mientras estén en su custodia ya sea física o electrónica. Así mismo, son responsables de informar a los jefes inmediatos de cualquier incidente de seguridad que se pueda presentar, tales como: uso indebido, alteración y/o divulgación no autorizados. Ver: Políticas técnicas de seguridad de la información Función Pública

Gestión de cambios sobre los activos de información

Control: procedimiento de control de cambios. Los cambios en la infraestructura tecnológica y servicios de información en Función Pública se deben realizar de acuerdo con el procedimiento establecido por la Oficina de Tecnologías de la Información y las Comunicaciones. Ver: Gestión de Cambios

3.1.1.2 Principio de acceso y circulación restringida: el Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones legales y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas por la ley;

Restricciones de acceso a la información

Control: Lineamientos para el control de acceso a la información

- La Oficina de Tecnologías de la Información y las Comunicaciones es la responsable de implementar controles de acceso a los servicios de información e infraestructura tecnológica. Es responsabilidad de los dueños de los servicios de información restringir el acceso a los servidores públicos, pasantes y contratistas de acuerdo con las funciones y/o actividades a realizar.

- Las áreas responsables de la administración de los sistemas de información, aplicaciones y portales de Función Pública con el apoyo de la Oficina de Tecnologías de la Información y las Comunicaciones son responsables de mantener actualizados los privilegios de acceso a los sistemas de información de sus usuarios.

3.1.1.3 Principio de seguridad: la información sujeta a Tratamiento por el responsable del tratamiento o encargado del tratamiento, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

Modelo de seguridad y privacidad de la información institucional

Control: Política institucional de la seguridad de la información. En su condición de Entidad cabeza del Sector responsable de la formulación de las políticas generales de Administración Pública, en especial de materias relacionadas con el Empleo Público, Organización Administrativa, Control Interno y Racionalización de Trámites, el Departamento Administrativo de la Función Pública, está comprometido con preservar la

confidencialidad, Integridad, disponibilidad y veracidad de sus activos de información, reduciendo los riesgos de seguridad digital a través del mejoramiento continuo de los controles en sus procesos, planes y proyectos, el cumplimiento de la normatividad vigente, la aplicación de lineamientos de la Política de Gobierno Digital y la adopción de buenas prácticas de seguridad de la información que contribuyan al logro de los objetivos institucionales y faciliten el aprovechamiento de las tecnologías de la información y las Comunicaciones para que la entidad constantemente sea más proactiva e innovadora.
Ver: Manual del Sistema Integrado de Planeación y Gestión
Ver: Políticas técnicas de seguridad de la información Función Pública

3.1.1.4 Principio de confidencialidad: todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.
Aplicando el principio nueve de OEA sobre tratamiento de datos personales sensibles la Entidad acepta que: algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos. En ese sentido el DAFP aplica la normatividad vigente en Colombia sobre la protección de datos personales.

Clasificación de la información

Control: lineamiento de gestión de activos de información

- La calificación e inventario de la información se realiza a través del procedimiento de calificación de información.
- La identificación de riesgos de seguridad digital contempla la identificación de los activos de información calificados como reservados o clasificados.
- La información calificada como datos abiertos es evaluada por el proceso de gestión documental para autorizar su publicación en el portal datos.gov.co
- La calificación de la información se debe tener en cuenta al momento de autorizar el acceso a los diferentes activos de información institucionales
- El índice de información clasificada y reservada debe ser verificado al momento de autorizar acceso o transferencia de información con todas las partes interesadas y grupos de valor.

Ver: Políticas técnicas de seguridad de la información Función Pública

Lineamientos para la transferencia e intercambio de información

Control: acuerdos de confidencialidad

- La Función Pública establece acuerdos de confidencialidad e intercambio de información con terceros que manipulen, requieran o provean información física y/o digital de carácter reservado.

- El grupo de Grupo de Gestión Contractual es el responsable de realizar el acompañamiento a las diferentes áreas de la entidad para que se garantice la inclusión de los acuerdos de confidencialidad en los contratos o convenios que lo requieran

Ver: Políticas técnicas de seguridad de la información Función Pública

3.1.2 Principios de seguridad para el tratamiento de información pública

Todos los grupos de valor tiene derecho a conocer la información que reposa en las instituciones públicas con las limitaciones que la constitución o la ley impongan, es ese sentido, el Departamento administrativo de la función pública adopta políticas, procesos, procedimientos y controles que garantizar a los ciudadanos el acceso a la información pública, garantizando en todo momento la integridad y disponibilidad de la misma.

3.1.2.1 Principio de máxima publicidad para el titular universal: Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con los requisitos legales.

Principio de transparencia: Principio conforme al cual toda la información en poder de los sujetos obligados definidos en la ley 1712 de 2014 se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en la ley.

Principio de buena fe: En virtud del cual todo sujeto obligado, al cumplir con las obligaciones derivadas del derecho de acceso a la información pública, lo hará con motivación honesta, leal y desprovista de cualquier intención dolosa o culposa.

Clasificación de la información

Control: lineamiento de gestión de activos de información

- La información calificada como datos abiertos es evaluada por el proceso de gestión documental para autorizar su publicación en el portal datos.gov.co

Ver: Políticas técnicas de seguridad de la información Función Pública

3.1.3 Principios de seguridad para la interoperabilidad

Como lo establece el manual del marco de interoperabilidad de MINTIC, la interoperabilidad busca facilitar el acceso a los grupos de valor de los servicios ciudadanos digitales de las entidades del Estado de manera completa, adecuada, minimizando los pasos y evitando el desplazamiento del ciudadano a diversas entidades para obtener la información necesaria de una entidad y acceder así a sus derechos y obligaciones con el Estado, pero este valor agregado obliga a la implementación de servicios y controles de seguridad que garanticen al ciudadano que la información que consulta o los servicios que demanda protegen sus derechos fundamentales, contemplan principios y controles de seguridad y privacidad, y sobre todo, son confiables. Para cumplir con estas expectativas, la gobernabilidad del dato en el Departamento Administrativo de la Función pública acoge principios de seguridad, protección y preservación.

3.1.3.1 Seguridad, protección y preservación de la Información: Deberán aplicarse medidas y controle que aseguren, protejan, preserven y mantengan la privacidad de la información susceptible de interoperar generando un entorno seguro y de confianza que permita transmitir a los ciudadanos una sensación de seguridad, donde se vela por sus intereses y se cuida la privacidad de la información y se respeta plenamente la normativa aplicable cada vez que interactúan con el Estado.

Aquellos datos que pertenezcan a ciudadanos y cuya pérdida y/o alteración pueda significar algún tipo de inconveniente para ellos con el Estado, deberán ser especialmente protegidos evitando el uso no autorizado y garantizando su integridad, disponibilidad y resguardo. Los ciudadanos y empresas tendrán el derecho a conocer, actualizar y rectificar la información que se haya recogido las entidades, así como demás derechos, libertades o garantías relacionadas con la recolección, tratamiento y circulación de datos personales. En términos de preservación de la información para las consultas históricas de los servicios de intercambio de información, las entidades deberán considerar el almacenamiento de históricos de los datos y ofrecer servicios interoperables para que se pueda acceder a la información compartida o intercambiada durante un período de tiempo determinado.

Modelo de seguridad y privacidad de la información institucional

Control: política institucional de la seguridad de la información

En su condición de Entidad cabeza del Sector responsable de la formulación de las políticas generales de Administración Pública, en especial de materias relacionadas con el Empleo Público, Organización Administrativa, Control Interno y Racionalización de Trámites, el Departamento Administrativo de la Función Pública, está comprometido con preservar la confidencialidad, Integridad, disponibilidad y veracidad de sus activos de información, reduciendo los riesgos de seguridad digital a través del mejoramiento continuo de los controles en sus procesos, planes y proyectos, el cumplimiento de la normatividad vigente, la aplicación de lineamientos de la Política de Gobierno Digital y la adopción de buenas prácticas de seguridad de la información que contribuyan al logro de los objetivos institucionales y faciliten el aprovechamiento de las tecnologías de la información y las Comunicaciones para que la entidad constantemente sea más proactiva e innovadora.
Ver: Manual del Sistema Integrado de Planeación y Gestión
Ver: Políticas técnicas de seguridad de la información Función Pública

3.1.3.2 Neutralidad tecnológica y adaptabilidad: El desarrollo de servicios de intercambio de información se deberá orientar en la atención de las necesidades manifiestas de los ciudadanos y empresas; por lo tanto, la construcción de estos servicios deberá orientarse por la funcionalidad y no por la tecnología que ofrezca una herramienta o proveedor en particular. Las decisiones de tecnología, durante el desarrollo de un servicio de intercambio de información, deberán guiarse por el uso de especificaciones que faciliten su interconexión con el mayor número de sistemas que conforman el ecosistema de soluciones con el que interopera. Los servicios de intercambio de información no deberán exigir, por parte de las entidades, ninguna tecnología exclusiva o limitada al ámbito de un proveedor o plataforma, así mismo, las entidades públicas deben dar acceso a sus servicios de intercambio de información con independencia de cualquier tecnología o producto concreto y permitir su reutilización.

Control: lineamientos de seguridad para intercambio de información

Con el fin de adoptar lineamientos que se deben aplicar al momento de realizar intercambios de información con otras entidades con el fin de habilitar el cumplimiento de obligaciones misionales y, facilitar la prestación

de servicios o mejorar la entrega de valor, la entidad adopta el documento de "Lineamientos de seguridad para el intercambio, transferencia o transmisión de datos personales". Disponible en el sistema integrado de planeación y gestión de la entidad.

3.2 Política de gestión de la continuidad para el gobierno de datos

La gestión de la continuidad de negocio para el modelo de gobierno de datos del Departamento Administrativo de la Función Pública se fundamenta en la estrategia de continuidad de negocio institucional que se puede consultar en: Documento técnico - Plan de Continuidad[1]

Con el fin de garantizar la disponibilidad y continuidad de las actividades de gobierno de datos, se aplican los siguientes lineamientos:

1. Identificación y gestión de riesgos de continuidad de negocio: los riesgos asociados a la pérdida de continuidad de los servicios de gobierno de datos se gestionan mediante la metodología de gestión de riesgos institucional. Los riesgos de continuidad de negocio se clasifican como riesgos de seguridad digital y para los riesgos identificados se identifican planes de tratamiento

2. Copia de respaldo: la información dentro del alcance del programa de gobierno de datos se salvaguarda mediante copias de respaldo siguiendo la política institucional disponible en: Políticas de respaldo, custodia y recuperación de la información.[2]

3. Recuperación ante desastres: los sistemas de información responsables de las actividades de gobierno de datos, se deben incluir en la estrategia de recuperación antes desastres tecnológicos institucional disponible en: Plan de recuperación de desastres tecnológicos.[3]

4. Las actividades de procesamiento de información involucradas en el gobierno de datos, cuentan con procedimientos alternos de operación basados en la estrategia de trabajo remoto en caso de materialización de los escenarios de emergencia social, emergencia sanitaria, colapso de infraestructura y desastre tecnológico. Ver (Plan alterno de operación medición del desempeño institucional)

[1] Documento técnico - Plan de Continuidad: https://www.funcionpublica.gov.co/documents/418537/528603/documento-tecnico_plan_continuidad.pdf/ea6ead0c-0cc6-f5bf-9e5d-c374770ae902?t=1605278309908

[2] Políticas de respaldo, custodia y recuperación de la información: https://www.funcionpublica.gov.co/documents/34645357/34703081/Politicas_respaldo_custodia_informacion.pdf/cdadd3ea-31f5-4154-be6a-f8227b3cc47e?t=1544198825391

[3] Plan de recuperación de desastres tecnológicos: https://www.funcionpublica.gov.co/documents/418537/528603/plan-recuperacion-desastres-tecnologicos-version-clasificada.pdf/1db3db38-3123-c70a-1887-89c9f348290?t=1606856665039

5. Verificación, revisión y evaluación de la continuidad: anualmente se deben realizar verificaciones de los procedimientos de operación alterna, evaluación del estado de riesgos de continuidad y pruebas de la estrategia de continuidad de las actividades de gobierno de datos.

6. Capacitación en procedimientos de operación alterna: anualmente se deben realizar actividades de socialización de la estrategia de continuidad de negocio y procedimientos alternos de operación.

7. Redundancias: la infraestructura de procesamiento de datos requerida para las operaciones de gobierno de datos se soporta en equipos con redundancias a nivel de potencia eléctrica, equipos de procesamiento de datos y almacenamiento en nube.

3.3 Arquitectura TIC

Según el Data Management Body of Knowledge- DAMA -DMBOK[4], el objetivo de la Arquitectura es ser un puente entre la estrategia del negocio y la ejecución de la tecnología, porque la Arquitectura TIC es más valiosa cuando apoya completamente las necesidades de toda la empresa (Beach, 2009).

La arquitectura se refiere a una disposición organizada de elementos componentes destinados a optimizar la función, el rendimiento, la viabilidad, el coste y la estética de una estructura o sistema global. Dentro del mundo de los datos más específicamente, hablamos de arquitectura, cuando, tenemos que lidiar, gestionar, mitigar toda la complejidad de la información.

Teniendo en cuenta lo anterior para el desarrollo de la arquitectura de datos en Función Pública se tendrán cuatro momentos así:

- **Levantamiento de requerimientos**: esta fase se centra en la identificación, captura, documentación y priorización de requisitos sobre los procesos y la información asociada. Es fundamental documentar en esta fase las políticas de calidad de los datos, así como las fuentes y/o sistemas de información, archivos. Por otro lodo en lo que se refiere a los datos externos solo podrán complementar la información, pero no podrán ser tenidos en cuenta para análisis de calidad.

- **Diseño:** es la etapa más compleja de la arquitectura de datos, ya que es el momento en el que se definen las estructuras que la componen hay que elegir las tecnologías que se utilizarán para la transmisión, gestión, el almacenamiento y el tratamiento de datos.

- **Documentación**. Tras la creación del diseño de la arquitectura socializarlo en las mesas operativas y tácticas.

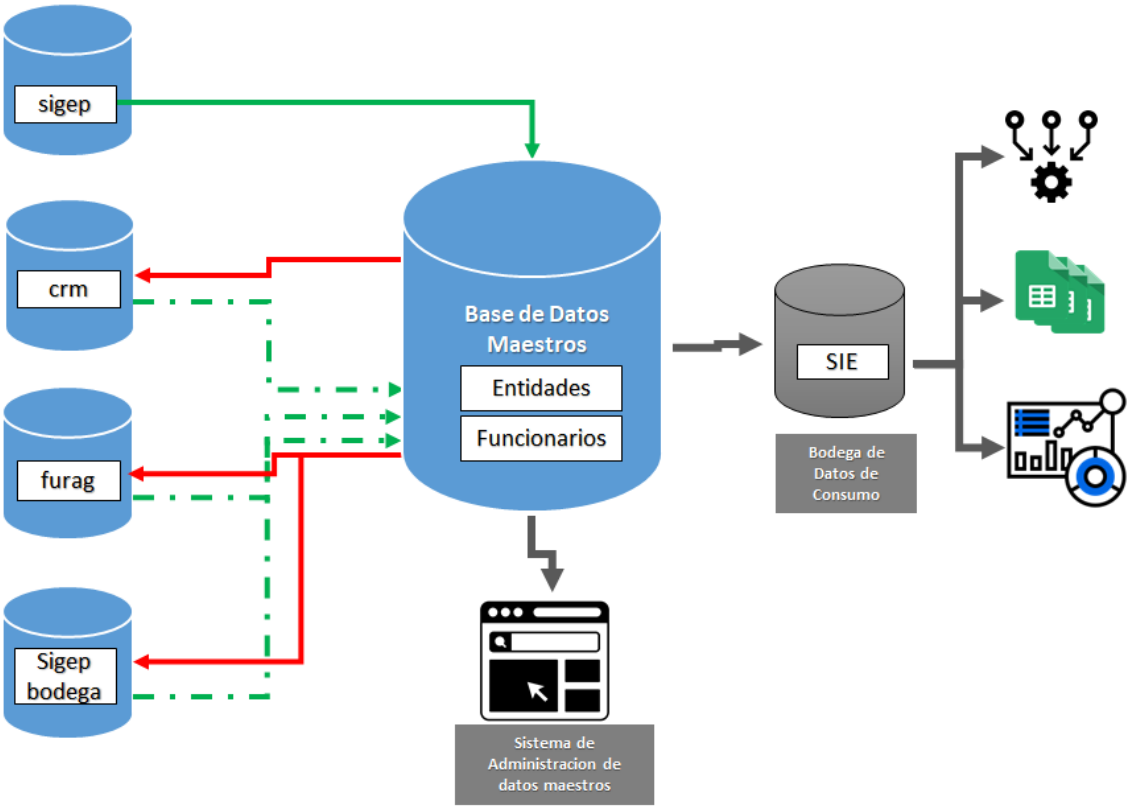
[4] El DAMA -DMBOK recomienda redactar un documento de diseño de la Arquitectura de Datos. Es un modelo formal de datos de la empresa, que contiene nombres de datos, definiciones completas de datos y metadatos, entidades y relaciones conceptuales y lógicas, y reglas de negocio. Se incluyen modelos de datos físicos, pero como producto del modelado y diseño de datos, en lugar de la Arquitectura de Datos

- **Evaluación:** después de la etapa de documentación, es importante evaluar el diseño para identificar posibles problemas, en esta fase es importante definir el alcance en cuanto a sensibilidad de los datos y consume de información.

Como resultado de la ejecución de los momentos descritos anteriormente y desde el punto de vista de infraestructura el gobierno de datos de Función Pública inicia desde la identificación del procedimiento, los sistemas de información involucrados y los administradores del dato técnicos y funcionales. Como se observa en el Diagrama de arquitectura se relacionan las fuentes de información o sistemas origen, cuyo funcionamiento no son impactados por esta estrategia, se busca mediante mecanismos de extracción cargar la información de Datos Maestros definidos previamente.

El repositorio de datos maestros, que se observa en la parte central del diagrama, contiene 4 grandes procesos de información donde se encargaran de ejecutar las políticas de calidad, almacenamiento de los datos, gestión de usuarios del sistema de gestión de Datos Maestros y políticas de perfilamiento.

Gráfica 2. Arquitectura de datos maestros



Fuente: Elaboración Propia

Por otra parte, el sistema de gestión de datos maestros permite al usuario administrador gestionar las políticas definidas y aprobadas en el Consejo de Gobierno, y contar con una interfaz gráfica donde se podrán administrar

las políticas de los datos maestros, definir modelos de datos, crear reglas para actualizar los mismos y controlar quién actualiza los datos.

En cuanto a la trasmisión de datos de los sistemas de información internos y la base de datos maestros se realizará de acuerdo con los lineamientos aplicables de cada sistema de información y los protocolos para el intercambio de datos aprobado por la Entidad.

3.4 Política de calidad

Para el modelo de gobierno de datos de Función Pública se tienen en cuenta los lineamientos impartidos por el Ministerio de Tecnologías de la Información y las Comunicaciones. Los datos son un activo de información para la entidad e insumo fundamental para la toma de decisiones, desde el gobierno de datos de Función Pública se tienen en cuenta los siguientes criterios de calidad que buscan asegurar el ciclo de vida del dato de acuerdo con lo establecido en la ISO / IEC 25012: 2008

- **Completitud:** grado en el que los datos asociados con una entidad tienen valores para todos los atributos esperados e instancias de entidades relacionadas en un contexto de uso específico.
- **Consistencia**: grado en el que los datos están libres de contradicción y son coherentes con otros datos en un contexto de uso específico. Puede ser analizada en datos que se refieran tanto a una como a varias entidades comparables.
- **Exactitud:** grado en el que los datos representan correctamente el verdadero valor del atributo deseado de un concepto o evento en un contexto de uso específico.
- **Credibilidad:** grado en el que los datos tienen atributos que se consideran ciertos y creíbles en un contexto de uso específico. La credibilidad incluye el concepto de autenticidad (la veracidad de los orígenes de datos, atribuciones, compromisos).
- **Conformidad**: grado en el que los datos tienen atributos que se adhieren a estándares, convenciones o normativas vigentes y reglas similares referentes a la calidad de datos en un contexto de uso específico.
- **Confidencialidad:** grado en el que los datos tienen atributos que aseguran que los datos son sólo accedidos e interpretados por usuarios autorizados en un contexto de uso específico. La confidencialidad es un aspecto de la seguridad de la información
- **Trazabilidad:** grado en el que los datos tienen atributos que proporcionan un camino de acceso auditado a los datos o cualquier otro cambio realizado sobre los datos en un contexto de uso específico.
- **Compresibilidad**: grado en el que los datos tienen atributos que permiten ser leídos e interpretados por los usuarios y son expresados utilizando lenguajes, símbolos y unidades apropiados en un contexto de uso específico. Cierta información sobre la comprensibilidad puede ser expresada mediante metadatos.

Adicionalmente, con el fin de asegurar la calidad del dato se deberán llevar a cabo las siguientes actividades, que se encuentra descritas en el flujo del proceso de datos en el procedimiento de calidad de datos, y que facilitan la mejora de estos en los diferentes sistemas de información de acuerdo con los roles y responsabilidades establecidos:

1. Definir y documentar las reglas de negocio de la calidad del dato a gobernar, para lo cual se debe establecer las reglas validación y consistencia de las: tablas, registro, campo, integridad creación, actualización, borrado o modificación de tablas, relaciones y acceso a la información.
2. Establecer los criterios de validación u homologación para los datos: Identificar, actualizar o documentar los procesos y procedimientos necesarios para determinar las condiciones de calidad de los datos, sus indicadores y acuerdo de niveles de servicio.
3. Realizar el diagnóstico de la calidad de los datos y de las fuentes de información: Una vez definidas las reglas de negocio es necesario realizar un análisis del estado actual de la información con el fin de identificar diferencias entre los distintos sistemas de información e inconsistencias de estos.
4. Identificar las causas y problemas de la calidad de los datos: Documentar los principales razones y problemas por las cuales los datos no poseen calidad e implementar estrategias y objetivos que permitan la mejora continua de los datos.
5. Crear los planes de trabajo que permitan mejorar la calidad del dato: Definir el plan de mejoramiento con actividades, responsables y tiempos para garantizar la mejora de los datos.
6. Certificar la calidad del dato: Se debe velar por el cumplimiento de los todos los criterios establecidos en los procedimientos definidos y en las reglas de negocio

Teniendo en cuenta que la Entidad dispone del el “Protocolo para la gestión de información estadística” donde establece lineamientos para lograr una planeación, administración, difusión y uso de la información estadística que permita el aprovechamiento de ésta, los directores de cada dependencia y demás miembros del consejo de gobierno de datos deben propender por la adopción y aplicación del mismo por parte de funcionarios, contratistas y pasantes según sus funciones y en aras de una gestión eficiente de la información estadística, apoyados también por el gestor del dato (Data steward).

3.4.1 Actividades preventivas y correctivas

Se deben implementar metodologías para el análisis identificación y mitigación de no conformidades que afecten el buen desempeño del modelo de gobierno de datos por lo tanto se sugieren las siguientes actividades preventivas:

- Medir y validar la calidad del dato a gobernar y el cumplimiento de las reglas de negocio a través de la generación de informes de calidad en los cuales se pueda establecer que los datos están completos son consistentes, entre otras características.
- Realizar campañas de depuración y limpieza de los datos en los sistemas de información con el fin de hacer verificaciones periódicas y monitoreo continuo.

Así mismo como acciones correctivas se aplica:

- Diseñar e implementar planes de mejora derivados de los hallazgos o inconsistencias de las revisiones de calidad de las bases de datos.
- Identificar oportunidades de mejora del dato a gobernar.

3.4.2 Indicadores de calidad

Con el fin de realizar monitoreo y seguimiento a la implementación del modelo de gobierno de datos en la entidad se establecen los siguientes indicadores con los cuales se medirá la calidad de los datos a gobernar.

Tabla 8. Indicador completitud de la información

Elemento	Descripción
Aspecto para medir	**Completitud de la información**
Tipo de indicador:	Operativo
Objetivo:	Medir el grado en que las bases de datos reflejan la totalidad de información requerida por el negocio
Fórmula:	Total de datos nulos o campos vacíos/Total de datos sistema de información *100
Meta	0%
Nivel de referencia	Aceptable: 0%
Periodicidad de medición	Semestral
Responsable de medición	Oficina Asesora de Planeación

Tabla 9. Indicador conformidad de la información

Elemento	Descripción
Aspecto para medir	**Conformidad de la información**
Tipo de indicador:	Operativo
Objetivo:	Medir el grado en que la información es aceptada por el negocio
Fórmula:	Total de datos que no cumplen con el dominio o formato definido/Total de datos sistema de información *100

Meta	0%
Nivel de referencia	Aceptable: 0%
Periodicidad de medición	semestral
Responsable de medición	Oficina Asesora de Planeación

Tabla 10. Consistencia de la información

Elemento	Descripción
Aspecto para medir	**Consistencia de la información**
Tipo de indicador:	Operativo
Objetivo:	Medir que la información sea la misma en todas las áreas o sistemas
Fórmula:	Total, de fuentes o atributos **diferentes** en todos los sistemas de información/Total fuentes y atributos de todos los sistemas de información *100
Meta	0%
Nivel de referencia	Aceptable: 0%
Periodicidad de medición	semestral
Responsable de medición	Oficina Asesora de Planeación

Tabla 11 Indicador duplicidad de la información

Elemento	Descripción
Aspecto para medir	**Duplicidad de la información**
Tipo de indicador:	Operativo
Objetivo:	Medir e identificar múltiples instancias que son innecesarias frente al mismo objeto

Fórmula:	Total de registros duplicados/Total de registros del sistema de información*100
Meta	0%
Nivel de referencia	Aceptable: 0%
Periodicidad de medición	Semestral
Responsable de medición	Oficina Asesora de Planeación

Tabla 12. Indicador duplicidad de la información

Elemento	Descripción
Aspecto para medir	**Duplicidad de la información**
Tipo de indicador:	Operativo
Objetivo:	Medir e identificar múltiples instancias que son innecesarias frente al mismo objeto
Fórmula:	Total de registros duplicados/Total de registros del sistema de información*100
Meta	0%
Nivel de referencia	Aceptable: 0%
Periodicidad de medición	Semestral
Responsable de medición	Oficina Asesora de Planeación

Tabla 13. Indicador exactitud de la información

Elemento	Descripción

Aspecto para medir	**Exactitud de la información**
Tipo de indicador:	Operativo
Objetivo:	Medir el grado en que la información refleja lo que está pasando en el negocio
Fórmula:	Total de registros inexactos o inconsistentes/Total de registros del sistema de información*100
Meta	0%
Nivel de referencia	Aceptable: 0%
Periodicidad de medición	Semestral
Responsable de medición	Oficina Asesora de Planeación

3.5 Política de gestión del cambio

Para Función Pública es indispensable contar con información verídica, confiable, oportuna y de calidad que le apoye en la toma de decisiones a todo nivel, por tanto, la implementación del programa de gobierno de datos y modelo de datos maestros es una estrategia que le permitirá una gestión asertiva de los datos. Para asegurar que este programa se mantenga en el tiempo es indispensable crear estrategias de sensibilización con todos los servidores públicos, contratistas y pasantes de la entidad con el fin de fomentar una cultura de calidad de los datos, así como, con los usuarios y/o grupos de valor que diligencian los diferentes aplicativos o sistemas de información para incurrir en menos errores.

Teniendo en cuenta lo anterior y con el fin de crear una cultura de calidad de los datos se debe:

1. La Oficina Asesora de Planeación con el apoyo del profesional de gestión del cambio incluir en la estrategia anual de formación y capacitación temáticas relacionadas con gobierno de datos y datos maestros.
2. Las dependencias técnicas que tengan a cargo sistemas de información deben incluir programas de sensibilización con usuarios con el fin de mejorar la calidad de los datos desde la captura.
3. Elaborar estrategias de difusión de las políticas y estándares definidas o actualizadas en el marco del programa de gobierno de datos.
4. Evaluar la adopción y apropiación de conceptos y lineamientos para el uso adecuado de la información producida y administrada por la Entidad.

4. Procedimiento de uso de datos

4.1 Definición de datos críticos o datos maestros

Es necesario definir los datos que se requieren gobernar para esto se deben llevar a cabo las siguientes actividades, dando línea al procedimiento de datos maestros establecido en la Entidad para una identificación y gestión del dato critico o maestro:

- El consejo de gobierno define según el impacto, misionalidad y transversalidad el dato que quiere gobernar.
- Para cada uno de los datos críticos se debe documentar, sus reglas de validación, ajustes o cambios realizados, reglas de datos sensibles, y datos relacionados en múltiples fuentes
- Se debe actualizar el diccionario de datos y metadatos según los criterios y el mecanismo definido por la Entidad.
- Definir el repositorio central para el almacenamiento y administración de los datos a gobernar en la Entidad.

5. Bibliografía

Beach, B. (2009). *The DAMA Guide to The Data Management Body of Knowledge.*

Documento CONPES 3920. (2018).

Función Pública - Manual Operativo MIPG. (2021). Obtenido de Micrositio MIPG: https://www.funcionpublica.gov.co/documents/28587410/38054865/Manual+Operativo+del+Modelo+Integrado+de+Planeaci%C3%B3n+y+Gesti%C3%B3n+MIPG+-+Versi%C3%B3n+4+-+Marzo+2021.pdf/89cdee1e-2670-829b-d9d1-f1999abd1789?t=1620912368879

Función Pública. (2021). Obtenido de Gestor Normativo: https://www.funcionpublica.gov.co/web/eva/gestor-normativo

ISO 27001. (2005).

ISO 8000. (2018). Obtenido de ISO 8000: http://iso8000.es/normas-iso-8000

Mintic. (2021). Obtenido de https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

Mintic. Guia del Dominio de Información G.IN.01. (2019).

Mintic. Guía técnica de informción - Administración del dato maestro G.INF.02. (2019).

Mintic. Guía Técnica de la información - Gobierno del dato G.INF.06. (2019).

Norma Técnica de Calidad del Proceso Estadístico - DANE. (2020).

Presidencia de la Republica. (2000). *Directiva Presidencial 02 de 2000*. Obtenido de https://intranet.secretariajuridica.gov.co/node/2233

Manual Gobierno de Datos

VERSIÓN 1
Seguimiento y evaluación
DICIEMBRE
2021

Departamento Administrativo de la Función Pública
Carrera 6 n.º 12-62, Bogotá, D.C., Colombia
Conmutador: 7395656 Fax: 7395657
Web: www.funcionpublica.gov.co
eva@funcionpublica.gov.co
Línea gratuita de atención al usuario: 018000 917770
Bogotá, D.C., Colombia.