

# POLÍTICA DE GOBIERNO DE DATOS DRC - COLOMBIA

## Índice de Contenido

Índice de Contenido.....	1
<b>1. INTRODUCCIÓN.....</b>	<b>2</b>
1.1 ¿Qué es el gobierno de datos?.....	2
1.2 Objetivos de la Política del Gobierno de datos .....	2
1.3 Alcance .....	3
1.4 Definiciones.....	3
1.5 Metodología .....	4
<b>2. CALIDAD DE LOS DATOS .....</b>	<b>4</b>
2.1 Enfoque de gestión de calidad de datos .....	5
2.2 Cultura de calidad de datos.....	5
2.3 Dimensiones de la calidad de datos .....	6
2.4 Administración de datos .....	6
2.5 Resumen del proceso de calidad de datos.....	7
<b>3. SEGURIDAD DE DATOS .....</b>	<b>9</b>
3.1 Requisitos de seguridad de datos .....	9
3.2 Política de seguridad de datos .....	9
<b>3.2.1</b> Administración de usuarios, contraseñas y accesos .....	9
3.3 Acceso y clasificación de los datos .....	10
3.4 Auditorias .....	10
<b>4. DISPOSICIONES FINALES PARA EL CUMPLIMIENTO DE LA POLÍTICA.....</b>	<b>11</b>
4.1 Estructura administrativa para el cumplimiento de la política de Gobierno de Datos.....	11
<b>4.1.1</b> Detalle de los roles .....	11

## 1. INTRODUCCIÓN

La digitalización es una gran tendencia global que está transformando las sociedades, las organizaciones, las economías y los gobiernos. Tiene el potencial de facilitar un cambio real y positivo, pero también puede conducir a un aumento de la represión, inestabilidad y exclusión de los grupos marginados a causa de la brecha digital, incluidas las personas afectadas por el desplazamiento forzado; ello obedece a la falta de productos o servicios asequibles o pertinentes, o a factores políticos, sociales o económicos que impiden la incorporación equitativa.

DRC al incluir el fortalecimiento de la digitalización como una prioridad de su Estrategia 2025, reconoce que su capacidad futura para el logro de su visión y de su misión dependerá de la capacidad para multiplicar las oportunidades digitales como parte de intervenciones de alta calidad que les aporten un valor agregado a las comunidades de desplazados. Para materializar esta meta, DRC fortalecerá su capacidad para utilizar las tecnologías digitales, analizar disyuntivas y mitigar los posibles riesgos.

DRC se dará a conocer por su enfoque realista, ambicioso, ético y centrado en las personas en lo que respecta a la digitalización. En lugar de desarrollar una estrategia independiente, la digitalización la incorporarán minuciosamente en sus objetivos e iniciativas generales.

### 1.1 ¿Qué es el gobierno de datos?

El Gobierno de datos es la capacidad de una organización para gestionar el conocimiento que tiene sobre su información de forma que pueda responder a preguntas tales como ¿qué sabemos sobre nuestra información?, ¿de dónde provienen esos datos?, ¿están estos datos alineados con nuestra política de empresa?

El gobierno de datos en cualquier organización permite establecer la información como un activo y tratarla como tal, verificando su ciclo de vida. Mantener la información disponible, con calidad, son condiciones necesarias para la toma de decisiones en las organizaciones

### 1.2 Objetivos de la Política del Gobierno de datos

Como parte integral de la programación general de la oficina del Consejo Danés para Refugiados (DRC) en Colombia, esta política tiene como objetivo establecer e implementar lineamientos para la administración y gestión de los diferentes componentes de información de la organización 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. [Por lo anterior, el presente documento busca dar a conocer a todas las partes interesadas un lineamiento de la herramienta diseñada respecto al gobierno de datos.](#)

Así, los objetivos específicos de la política son:

- ✓ Establecer una cultura para la gestión y calidad de los datos.
- ✓ Gestionar la información a partir de estándares de calidad que faciliten su análisis y tratamiento.

- ✓ Identificar todos y cada uno de los componentes de información de la Organización y los datos que los componen y sus diferentes flujos.
- ✓ Contar con información homologada en los diferentes sistemas de información.
- ✓ Gestionar los componentes de información de la organización con el fin de asegurar su disponibilidad, seguridad y privacidad de acuerdo con la normatividad vigente.

### **1.3 Alcance**

La Política de Gestión de Datos es una herramienta participativa e inclusiva, donde se espera que el personal de DRC, socios de la organización o cualquier persona responsable de la obtención, clasificación, almacenamiento, circulación, uso y disposición final de los datos y la información de la organización puedan tener un lineamiento claro que responda a los retos organizacionales y permita el buen gobierno de los datos y la información, de cara a la necesidad de fortalecer la toma de decisiones, la rendición de cuentas y las necesidades diarias para el buen funcionamiento de DRC Colombia.

Así mismo, la presente política se articula con las disposiciones descritas en los siguientes documentos, que colectivamente operacionalizan el gobierno de datos e información:

- IT security at DRC, version 1.0
- IT Operations Handbook
- General Data Protection Regulation (GDPR)
- Protection Information Management (PIM)

### **1.4 Definiciones**

**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. Guía 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).

## 1.5 Metodología

A continuación, se describen las metodologías y estándares que dan lineamiento sobre las buenas prácticas frente a la gestión de los datos y la información de la organización:

**Metodología DAMA:** Marco de referencia para la administración de los datos a través de un conjunto de áreas de conocimiento. Se articula con las demás normas y cuenta con un marco de excelencia y buenas prácticas siendo referencia en todo el mundo.

**ISO 27000:** Es el conjunto de estándares del Sistema de Gestión de Seguridad de la Información en las organizaciones, reúne las buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información mediante buenas prácticas.

## 2. CALIDAD DE LOS DATOS

La gestión de la Calidad de Datos (DQM) es un proceso de apoyo crítico en la gestión del cambio organizacional. La calidad de los datos es sinónimo de calidad de la información. La formalización de los procesos de supervisión de calidad de datos, la gestión y mejora depende de la identificación de las necesidades de calidad de datos del negocio y de determinar las mejores formas de medir, monitorear, controlar e informar sobre la calidad de los datos.

## **2.1 Enfoque de gestión de calidad de datos**

Cuando se aplica la calidad de los datos dentro del marco de los ANS de calidad de datos definidos, se involucra:

- Planeación del diagnóstico de la situación y la identificación de indicadores clave para medir la calidad de datos actual.
- Implementación de procesos para medir y mejorar la calidad de los datos.
- Seguimiento y medición de los niveles en relación con las expectativas definidas por el negocio.
- Actuar para resolver los problemas identificados para mejorar la calidad de los datos y satisfacer de una mejor manera las expectativas de negocio.

## **2.2 Cultura de calidad de datos**

La cultura incluye relacionar impactos materiales significativos a los problemas de datos, asegurando enfoques sistemáticos de supervisión de la calidad de los datos de la organización, y socializar el concepto de que los problemas de calidad de datos no pueden ser exclusivamente dirigidas por soluciones tecnológicas.

Algunas tareas de DQM relacionadas con Gobierno de Datos incluyen:

- Involucrar a socios de negocios que trabajarán con el equipo de calidad de los datos y patrocinarán el programa de DQM.
- Identificar los roles y responsabilidades de propiedad de datos, incluyendo la junta de gobierno de datos y de administradores de datos.
- Asignación de responsabilidad de los elementos de datos críticos y de DQM.
- Identificar las áreas de calidad de datos clave para abordar y dar directrices para la organización en torno a estas áreas clave.
- Sincronizar los elementos de datos usados en todas las líneas de negocio y proporcionar definiciones claras, sin ambigüedades, el uso de los valores de dominios y reglas de calidad de datos.
- Informar continuamente sobre la medición de los niveles de la calidad de datos.
- Introducir los conceptos de análisis de los requerimientos de datos como parte del ciclo de vida de desarrollo de los sistemas.
- Relacionar la alta calidad de los datos a los objetivos del desempeño individual.

Por último, el comité de supervisión de calidad de datos en DRC conformado por Gerente MEAL/IM, TL MEAL y TL IM es responsable de las políticas y procedimientos para la supervisión de calidad de los datos, por tal motivo, la orientación del comité incluye:

- Establecer prioridades para la calidad de los datos.
- Desarrollar y mantener los estándares de calidad de datos.
- Informar mediciones pertinentes de calidad de los datos en toda la empresa.
- Proporcionar orientación que facilite la participación del personal necesario.
- Establecer mecanismos de comunicación para el intercambio de conocimiento.

- Desarrollar y aplicar políticas de certificación y cumplimiento.
- Seguimiento y presentación de informes sobre el rendimiento.
- Identificación de oportunidades de mejora y la construcción de consensos para su aprobación.
- Resolución de variaciones y conflictos.

### **2.3 Dimensiones de la calidad de datos**

- **Completitud:** Los datos que se requieren están completos en cuanto a sus características.
- **Consistencia:** Los datos se representan de forma coherente en todo el conjunto de datos.
- **Exactitud:** Los datos representan con precisión los valores reales de la información.
- **Pertinencia temporal:** Los datos están disponibles en el momento requerido.
- **Unicidad:** Los datos se identifican y registran correctamente solo una vez.
- **Validez:** Los datos se ajustan a la sintaxis (formato, tipo, rango) de su definición.

### **2.4 Administración de datos maestros**

Los datos se clasifican en Datos Maestros. A continuación, presentamos las consideraciones frente a esta clasificación:

**Datos Maestros:** datos que son usados para consolidar los datos de los beneficiarios para un proyecto específico, llevándolo así al desarrollo de una aplicación en Power Apps para consulta rápida en la búsqueda de la información.

Para el caso de DRC, los datos maestros son parte fundamental de su operación en todos los países y para el caso específico de la sede Colombia, los datos maestros se comparten con muy poco personal y siguiendo procesos estrictos para su tratamiento. En este proceso intervienen áreas como IM para todo lo relacionado con cruces de bases de datos a partir de datos maestros y MEAL, área que se encarga del reporting asociado a esta información.

Consideraciones frente a Datos Maestros:

- No son de naturaleza transaccional, pero describen transacciones.
- Son compartidos por los diferentes sistemas de información de la organización para un fin común y adicionalmente realizar una buena atención a los beneficiarios.
- Requieren consolidación para visualizar toda la información de un beneficiario durante la vigencia del proyecto.
- Requieren de limpieza y estandarización mediante los procesos establecidos para garantizar la calidad de los datos.
- Deben gobernarse para mitigar el riesgo de incumplimiento frente a la ley de Protección de Datos Personales y la duplicidad de información.
- Deben tener una estrategia para ser desplegados a los diferentes procesos (estratégicos, tácticos y operativos) que así lo requieran.

## **2.5 Resumen del proceso de calidad de datos**

Si bien sólo se han mencionado al detalle algunas actividades relevantes dentro del proceso de calidad de datos, la siguiente tabla muestra los entregables, roles responsables, roles de aprobación y roles de contribución para cada actividad en la función de gestión de operaciones de datos:

Actividades	Entregables	Roles responsables	Roles aprobados	Roles contribuyentes
Desarrollar y promover la cultura de Calidad de los Datos (O)	Entrenamiento en calidad de datos Procesos de gobierno de datos comité de gobierno de datos	Gerente MEAL/IM	Head of Programme (HoP)	Team Leader IM (TL IM)
Definir los requerimientos de calidad de datos ((D)	Documento de requerimientos de la calidad de datos	Team Leader IM (TL IM)	Gerente MEAL/IM	Team Leader MEAL (TL MEAL)
Perfilar, analizar y evaluarla calidad de datos(D)	Informe de diagnóstico de calidad de datos	Oficial IM	Gerente MEAL/IM Team Leader IM (TL IM)	Team Leader MEAL (TL MEAL)
Definir métricas e indicadores de calidad de los datos (P)	Documento de Métricas e indicadores de calidad de datos	Gerente MEAL/IM Team Leader IM (TL IM)	Head of Programme (HoP)	Team Leader MEAL (TL MEAL)
Definir las reglas del negocio de la calidad de los datos (P)	Reglas de negocio de calidad de datos	Team Leader IM (TL IM)	Gerente MEAL/IM	Team Leader MEAL (TL MEAL)
Probar y validar requerimientos de la calidad de los datos (D)	Casos de prueba de calidad de datos	Team Leader IM (TL IM)	Gerente MEAL/IM	Team Leader MEAL (TL MEAL)
Establecer y evaluar los niveles de servicio de Calidad de los Datos (P)	Niveles de servicio de calidad de datos	Team Leader IM (TL IM) Team Leader MEAL (TL MEAL)	Gerente MEAL/IM	Oficial IM Oficial MEAL
Medir y monitorear Continuamente la calidad de datos (C)	Informes de calidad de datos	Oficial IM Oficial MEAL	Team Leader IM (TL IM) Team Leader MEAL (TL MEAL)	Asistente IM Asistente MEAL



### 3. SEGURIDAD DE DATOS

La seguridad de los datos incluye las acciones de planear, desarrollar y ejecutar políticas y procedimientos de seguridad en términos de autenticación, autorización y acceso a la data. El objetivo de las prácticas de seguridad es garantizar que los activos de la información bajo custodia de una organización cumplan con ciertas normas de privacidad y confidencialidad, pero para que estas normas se puedan cumplir, existen cuatro requisitos, que son: las preocupaciones de los grupos de interés, la normativa gubernamental, las necesidades de acceso de las organizaciones y las preocupaciones empresariales legítimas.

#### 3.1 Requisitos de seguridad de datos

Los requisitos de seguridad de datos y los procedimientos para cumplir con estos requisitos se pueden clasificar en cuatro grupos básicos (los cuatro de A):

- **Autenticación:** Validar los usuarios son quienes dicen que son.
- **Autorización:** Identificar a las personas adecuadas y les conceda los privilegios correctos para visitas específicas, adecuadas de datos.
- **Acceso:** Habilitar estas personas y sus privilegios en forma oportuna.
- **Auditoría:** acciones de seguridad de la opinión y la actividad del usuario para garantizar el cumplimiento de la normativa y la conformidad con la política y las normas.

#### 3.2 Política de seguridad de datos

La política de seguridad de datos debe definir los controles y procedimientos de seguridad de datos siendo esto la principal responsabilidad del área de Information Technology (IT).

##### 3.2.1 Administración de usuarios, contraseñas y accesos

Los requisitos típicos de complejidad de contraseña requieren una contraseña para:

- Contener al menos 8 caracteres.
- Contener una letra mayúscula y un número.
- No ser el mismo que el nombre de usuario.
- No ser las mismas que las 5 contraseñas anteriores utilizadas.
- No contienen palabras completas en cualquier idioma.
- No ser incrementales (Password1, Contraseña2, etc.).
- No tener dos caracteres repetidos secuencialmente.
- Evite el uso de caracteres adyacentes en el teclado.
- Si el sistema es compatible con un espacio en las contraseñas, a continuación, un "frase de paso" se puede utilizar.

**Contraseñas:** El área de IT como principal y directo responsable debe divulgar las recomendaciones establecidas y/o actualizaciones frente a los cuidados en la creación de las contraseñas por parte de cada personal de DRC en Colombia.

### **3.3 Acceso y clasificación de los datos**

Dentro de las metas en seguridad de datos está el permitir el apropiado acceso y evitar el inapropiado acceso a los activos de datos de la organización, para ello es importante que se reduzcan riesgos, cumpliendo no sólo los requisitos de ley, sino también las políticas y prácticas establecidas. Es importante que estas políticas y prácticas se divulguen dentro de DRC ya que todos los colaboradores en las que se gestiona la data no las conocen a profundidad, por eso es importante establecer procesos de capacitación.

DRC debe garantizar la seguridad de la información clasificando los datos de la organización para identificar qué datos requieren protección y que nivel de confidencialidad necesitan. Inicialmente, deben identificar y clasificar activos de datos confidenciales, incluyendo identificación personal, financiera, entre otros, como segundo paso, DRC debe localizar datos confidenciales en toda la organización, el almacenar una cantidad significativa de datos en un solo lugar permite un alto riesgo, como tercer paso, la organización debe determinar cómo debe proteger cada dato, las medidas pueden variar según el contenido de los datos y el tipo de tecnología, y por último, identificar cómo interactúa esta información con los procesos internos.

### **3.4 Auditorías**

Las auditorías de seguridad de datos incluyen:

- Analizar las políticas y normas con las mejores prácticas y las necesidades de seguridad de los datos.
- El análisis de los procedimientos de ejecución y las prácticas reales para garantizar la coherencia con los objetivos de seguridad de datos, políticas, normas, lineamientos y resultados deseados.
- Evaluar si las normas y procedimientos existentes son adecuados y en alineación con los requerimientos del negocio y de la tecnología.
- Verificación de la organización cumple con los requisitos reglamentarios.
- Revisión de la fiabilidad y exactitud de los datos de auditoría de seguridad de datos.
- Evaluar los procedimientos de escalamiento y mecanismos de notificación en caso de un fallo de seguridad de datos.
- Revisar los contratos, acuerdos de intercambio de datos y las obligaciones de seguridad de datos de proveedores subcontratados y externas, garantizando que cumplan con sus obligaciones y que garanticen la organización cumple sus obligaciones para los datos de origen externo.
- Informar a la alta dirección, los administradores de datos y otros interesados en el "Estado de seguridad de datos" dentro de la organización y la madurez de sus prácticas.

Recomendar diseño de seguridad de datos, mejoras operativas y de cumplimiento.

## 4. DISPOSICIONES FINALES PARA EL CUMPLIMIENTO DE LA POLÍTICA

### 4.1 Estructura administrativa para el cumplimiento de la política de Gobierno de Datos

Por medio de la presente política se establece: comité estratégico de información, Team Leader IM (Chief Data Officer), oficial IT (Chief Information Officer), mesas de trabajo, administradores de datos, custodios de datos, guardianes de datos, consumidores de datos, grupos de trabajo, reporteros de datos, arquitectos de datos y oficial de protección de datos personales.

#### 4.1.1 Detalle de los roles

Comité estratégico de información está integrado por:

- Gerente MEAL/IM
- Team Leader IM
- Team Leader MEAL
- Oficial IT

#### Responsabilidades:

- Aprobar la viabilidad e implementación de los métodos de visualización y consolidación de datos de la organización, para asegurar y garantizar la trazabilidad del dato, los responsables y la finalidad de la información procesada.
- Desarrollar en conjunto con las áreas programáticas y transversales, estrategias encaminadas a capacitar a las personas en el adecuado manejo de datos, así como impulsar el análisis y la gestión de los datos mejorando la calidad y el valor de los activos estratégicos de información.
- Liderar la estrategia de datos, información y analítica del Consejo Danés para Refugiados en Colombia, para lograr el máximo aprovechamiento de la información que se pueda generar.
- Promover una cultura basada en datos sostenible que promueva el uso de los datos como activos que respalden la Estrategia 2025 y la toma de decisiones en DRC fomentando un impacto en el ciclo de vida de los datos.
- Delegar los recursos humanos o materiales requeridos para la ejecución de las actividades planteadas en la estrategia de gobierno de datos e información.
- Responder por los datos producidos en el área que lideran al más alto nivel, tanto en la entrega de la información requerida por los entes de control y la generada por DRC como parte del proceso de rendición de cuentas.
- Establecer los lineamientos para el desarrollo de auditorías de control y aseguramiento de calidad de la información para garantizar el efectivo cumplimiento de la presente política.
- Promover el uso de los sistemas de gestión oficiales de la organización para garantizar la confidencialidad, disponibilidad e integridad de los datos.
- Garantizar el cumplimiento de la política de tratamiento de datos personales para garantizar los derechos de los titulares de los datos y evitar multas y/o sanciones, así como el cumplimiento de los acuerdos establecidos con los donantes.

## **TL IM – Chief Data Officer**

Responsable de la estrategia de gestión de los datos y la información, el control y desarrollo de políticas para la toma de decisiones organizacionales estratégicas y reportes ante entes internos y externos.

### **Responsabilidades:**

- Establecer una estrategia y una hoja de ruta para la maduración de la gestión de los datos y la información en DRC.
- Formar alianzas estratégicas con el área de IT y Comunicaciones como con las otras áreas de la organización, para la gestión de los datos y la información.
- Garantizar que la gestión de los datos y la información de DRC en Colombia estén alineados a las directrices desde la sede principal.
- Diseñar e implementar estrategias de datos para los diferentes dominios en conjunto con los Administradores de datos.
- Garantizar el cumplimiento de la Política de Tratamiento de Datos Personales en el uso de los datos para cumplir con lo relacionado por la normatividad vigente.
- Crear una cultura basada en datos en el staff de DRC.

## **Oficial IT – Chief information Officer**

Responsable de definir, dirigir y controlar la gestión de innovación en tecnologías de información, mediante la planificación estratégica de TI, generando la creación y desarrollo de proyectos y planes orientados a la modernización administrativa y optimización de las capacidades de la infraestructura misma mediante el uso de tecnologías de información, estándares y mejores prácticas de TI, para soporte a las funciones sustantivas de acuerdo con las nuevas tendencias y lineamientos de la sede principal de DRC a nivel global.

### **Responsabilidades:**

- Definir la arquitectura de sistemas de información garantizando integración de las tecnologías, seguridad en las aplicaciones e integridad de la información con el fin de apalancar las funciones de negocio y los datos necesarios para soportar las funciones de todas las áreas de la organización.
- Asegurar la definición de procesos y la información de negocios requeridos para soportar a la organización y crear procesos adecuados y arquitecturas de datos. Planificar, diseñar, ejecutar y monitorear la estrategia de tecnologías de información.
- Definir como se custodian los tipos de información estructurada y no estructurada tanto si se produce interna o externamente con el fin de soportar la toma de decisiones, los procesos institucionales y los servicios digitales de la organización.
- Desarrollar estrategias que abarquen el desarrollo y la promoción de la estrategia y las políticas que cubren el diseño de estructuras y taxonomías de datos y la información, promoviendo el cumplimiento de la legislación que regula todos los aspectos de la propiedad, el tratamiento y la divulgación de datos.
- Establecer políticas, estándares, indicadores, lineamientos y directrices tecnológicas que soporten la gestión de los datos y la información con el fin de garantizar la calidad y

seguridad de la información cubriendo el diseño de estructuras y taxonomías de los datos y la información.

- Evaluar y contratar Servicios de Tecnologías de información y comunicaciones (TICs) asegurando la calidad, cumplimiento funcional, adecuado soporte técnico, garantía y actualizaciones.
- Administrar y controlar las redes e infraestructura tecnológica de la organización, con el fin de asegurar la disponibilidad y rendimiento de los sistemas de información de DRC.

### **Mesas de trabajo**

Responsables de apoyar la adopción del modelo de gestión de datos e información permanente en DRC, garantizando la integridad, disponibilidad, confidencialidad, privacidad de la información y el uso ético de los datos. Habilitando a la organización para gestionar los datos como un activo estratégico, focalizándose en disponer de datos con la calidad requerida.

**Perfil de integrantes:** Colaboradores que poseen el conocimiento funcional del ciclo de vida de los datos (captura, procesamiento, transformación, distribución, almacenamiento, recuperación y eliminación), y están en la capacidad de aplicar las reglas y las políticas del modelo de gobierno de datos.

### **Responsabilidades:**

- Crear y gestionar los datos, mediante la construcción o actualización del glosario organizacional, el inventario de bases de datos y sistemas de gestión.
- Gestionar la calidad, seguridad y privacidad del dato.
- Adoptar el modelo de gestión de datos e información permanente: principios, políticas, procesos y procedimientos.
- Liderar las actividades operativas para cumplir con los objetivos propuestos por el Comité Estratégico de Información.

### **Grupos de Trabajo**

Designados por los integrantes de las mesas de trabajo, se les asignarán labores y tareas específicas a cumplir en un tiempo determinado.

### **Responsabilidades:**

- Ejecutar las labores y tareas específicas asignadas por las Mesas de trabajo dentro del tiempo establecido en el plan de trabajo.
- Entregar el informe final respectivo, que dé cuenta de los logros alcanzados en la labor asignada.
- Ejecutar las actividades operativas con el fin de cumplir con los objetivos propuestos por el Comité Estratégico de Información.

### **Administradores de datos**

Tienen un conocimiento profundo de su dominio de datos y toman decisiones sobre el tratamiento de los datos. Funcionarios que dentro de sus responsabilidades administran al menos un segmento

de los Datos Institucionales. Son responsables de aprobar las solicitudes de acceso y establecer la calidad de los datos que requiere y que circula.

**Responsabilidades:**

- Identificar cuáles son los datos necesarios para la correcta gestión del dominio del cual es experto, definiéndolos de forma clara en el glosario organizacional.
- Establecer la calidad mínima necesaria que deban tener los datos con base en las dimensiones establecidas en la presente política.
- Tomar decisiones en lo referente a la forma de capturar los datos y del plan de remediación en caso de que se presenten incidencias.

**Custodios de datos**

Funcionarios que tienen la responsabilidad a nivel operativo de la captura, almacenamiento, uso, circulación y disposición final de Datos Organizacionales. Los custodios son designados y generalmente informan a los administradores de datos. Están autorizados a otorgar acceso a elementos dentro del dominio de datos por los que el administrador es responsable.

**Responsabilidades:**

- Mantener la calidad con base en las dimensiones definidas por el administrador de datos.

**Guardianes de datos**

Funcionarios del área de IT o IM que tienen la responsabilidad de configurar, mantener y dar soporte a la infraestructura tecnológica para los Datos Organizacionales. Serán los encargados de brindar soporte a los administradores y custodios de datos.

**Consumidores de datos**

Funcionarios autorizados por los custodios de datos de DRC para que accedan a los Datos organizacionales en el desempeño de sus funciones asignadas en nombre de DRC.

**Reporteros de datos**

Funcionarios que dentro de sus responsabilidades están autorizados para reportar o divulgar información organizacional ante entes internos y externos.

**Responsabilidades:**

- Garantizar la calidad de los informes.
- Decidir los criterios que se deben utilizar a la hora de elaborar un informe.
- Controlar el acceso y distribución de los informes.

**Arquitectos de datos:** colaboradores del área de IM encargados de garantizar la calidad de datos, gestión de la ficha técnica de los datos y la integración de los sistemas de información.