POLÍTICA DE GOBIERNO DE DATOS E INFORMACIÓN DE LA CORPORACIÓN PARA EL DESARROLLO SOCIAL Y CULTURAL DEL VALLE DEL CAUCA – CORPOVALLE

1. OBJETIVO

Establecer las directrices en relación a la gestión y el gobierno de datos que permita a Corpovalle proveer las reglas, criterios y estándares para asegurar la Accesibilidad, Calidad, Consistencia, Seguridad y Auditabilidad de los datos durante su ciclo de vida; con el fin de promover la gestión adecuada de la información que permita obtener un nivel de madurez superior, al igual que el fortalecimiento de la gestión del conocimiento. De esta forma se incrementa la eficiencia operacional y se podrá convertir la información en uno de los activos más importantes, lo cual permitirá facilitar la toma de decisiones en la Corporación.

2. ALCANCE

La presente política y documentos anexos aplican para todos los procesos y procedimientos en los que las diferentes subdirecciones de Corpovalle participen, a sus colaboradores, contratistas, aliados estratégicos, y en general a los grupos de interés que se relacionen con la gestión y el gobierno de datos de la corporación.

3. DESCRIPCIÓN

Actualmente el Gobierno de Datos es percibido por las organizaciones como un propulsor para mejorar la eficiencia operacional y el fortalecimiento de la gestión de conocimiento. Además, puede ser entendido como garantía para los procesos de transformación descritos a continuación:

- Conocimiento de los datos: Visión integrada y unificada 360º de los grupos de interés, planes, programas y proyectos mejor orientados, convergencia, control de datos sensibles y coherencia de datos.
- Uso de información: Se refiere al uso de información de calidad en los procesos o iniciativas de planes, programas y proyectos, lo cual permitirá mejor la toma de decisiones, además de mejorar aspectos técnicos como migración/fusión de datos orientando a una corporación convergente, multicanal y con una oferta simplificada. Facilitando con esto la gestión de la transformación.
- Eficiencia operativa: Flujos de datos e información más eficientes, menos incidencias y rechazos por calidad de datos; trazabilidad, reutilización de componentes, robustez de las soluciones tecnológicas y mejor rendimiento.

4. ARTICULACIÓN DE LA POLÍTICA DE GOBIERNO DE DATOS E INFORMACIÓN

La presente Política, se encuentra alineada con el Programa de Integral de Gestión de Datos Personales y se complementa con las demás políticas y manuales de la Corporación que contengan aspectos relacionados con la protección de los datos que trata la Corporación.

5. GLOSARIO

Con el fin de adquirir dominio sobre los términos utilizados frecuentemente en materia de Gobierno de datos e información y la apropiación de los mismos; a continuación, se exponen las siguientes definiciones:

Gobernanza de datos: Es un **conjunto de procesos, funciones, normas, políticas y mediciones que garantizan el uso eficiente y eficaz de la información, proporcionando un enfoque holístico para administrar, mejorar y aprovechar la información** de forma que pueda ayudarnos a generar confianza en decisiones y operaciones. Además, permite abordar la gestión de los **datos** como **un activo de gran valor.**
Estructura de datos: Medio para gestionar datos de manera eficiente para usos tales como: bases de datos, bodegas de datos y servicios de indexación.
Propietario de dominio: Rol que puede autorizar o denegar el acceso a ciertos datos, es el responsable de su calidad, integridad, disponibilidad, seguridad, tratamiento y uso.
Oficina Gobierno de Datos: Área encargada de orientar a la organización en la gestión de datos.
Accesibilidad de datos: Garantiza que los usuarios puedan acceder a los datos que necesitan en el momento adecuado, encontrándolos en condiciones de formato adecuadas.
Accesibilidad de datos: Garantiza que los usuarios puedan acceder a los datos que necesitan en el momento adecuado, encontrándolos en condiciones de formato adecuadas.
Seguridad de datos: Garantiza que sólo los usuarios autorizados puedan acceder a los datos. **Consistencia de datos:** Datos sin duplicidad, libres de redundancias y en condiciones de racionalización de cada versión de los mismos.
Auditabilidad de datos: Capacidad de explicar el origen de los datos y de aportar información suficiente sobre su linaje y propósito.
Calidad de datos: Se refiere a los procesos y técnicas enfocadas a mejorar la eficacia de los datos existentes en las diferentes bases de datos de la organización.
Integración de datos: Es la práctica de combinar datos que se encuentran en diferentes fuentes para permitirle al usuario final tener una vista unificada de los mismos para una accesibilidad idónea, que sirva a las necesidades de negocio.
Integridad de datos: atributo o cualidad que es inherente al dato cuando se considera exacta, completa, homogénea, sólida y coherente con la intención de los creadores.
Disponibilidad de datos: propiedad que tiene el da la información sea accesible y utilizable por solicitud de una entidad autorizada.
Tratamiento de datos: Es cualquier operación o conjunto de operaciones efectuadas sobre datos personales, mediante procedimientos manuales o automatizados relacionadas con la obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales.
Migración de datos: Es el proceso necesario para transferir datos de una base de datos (fuente) a otra (destino).

Ciclo de vida de datos: Es el proceso a través del cual se define el flujo que tendrá el dato desde su generación o captura, almacenamiento, acceso y uso hasta su eliminación o destrucción, durante todo este flujo deberán ser custodiados los datos.
Custodia de datos: Hace referencia a la supervisión que se realiza sobre los datos, los cuales son la combinación de personal humano y herramientas tecnológicas que permitan al acceso y uso de dichos datos de acuerdo a las definiciones preestablecidas por la corporación.
Administración de datos maestros: Es un método que **permite relacionar todos los datos críticos en un solo archivo o base de datos llamado repositorio de datos maestros**, de forma que se obtiene un punto de referencia común para los datos más importantes, simplificando además el intercambio de datos entre personal y departamentos. Para lograr un MDM es necesario alinear **metodologías, herramientas y procesos, necesarios para crear y mantener conjuntos precisos y consistentes de datos maestros.** De esta forma se identifica la información más importante de una empresa, creando una **única fuente de la verdad,** que permite a la organización mejorar sus procesos empresariales.
Cliente Único: Es un modelo conceptual y repositorio que contiene los datos maestros de clientes y proveedores que provienen de los principales sistemas de información que posee la organización.
Grupos de interés: Es un conjunto de personas o empresas, las cuales son gestionadas de acuerdo a las necesidades o intereses de la corporación.

6. LOS DATOS COMO UN ACTIVO EMPRESARIAL: DATOS, INFORMACIÓN, CONOCIMIENTO

Los datos son la representación de hechos como texto, números, gráficos, imágenes, sonido o vídeo. Técnicamente, datos es el plural de la palabra proveniente del latín datum, que significa "un hecho". Sin embargo, la gente comúnmente utiliza el término como una cosa singular. Los hechos son capturados, almacenados y se expresan como datos.

La información son datos en un contexto. Sin contexto, los datos no tienen:

- El significado que tienen los elementos de datos para el negocio y términos relacionados.
- El formato en que se presentan los datos.
- El periodo de tiempo representado por los datos.
- La importancia de los datos para un uso determinado.

A su vez, los datos son la materia prima que interpretamos como consumidores de datos para crear continuamente la información, como se muestra en la Figura 1. La información resultante guía nuestras decisiones.

FIGURA 1. DATOS, INFORMACIÓN Y CONOCIMIENTO

Los significados formales o términos comúnmente utilizados también representan un valioso recurso de la empresa, contribuyendo a un entendimiento compartido de información relevante. Las definiciones de datos son sólo algunos de los muchos tipos diferentes de "datos sobre datos", conocido como metadatos. Los metadatos, incluyendo las definiciones de datos empresariales, ayuda a establecer el contexto de los datos y así la gestión de metadatos contribuye directamente a mejorar la calidad de la información. La gestión de los activos de información incluye la gestión de datos y sus metadatos.

La información contribuye al conocimiento. El conocimiento es la comprensión, conciencia, conocimiento y el reconocimiento de una situación y su familiaridad con su complejidad. El conocimiento es información en perspectiva, integrado desde un punto de vista basado en el reconocimiento y la interpretación de los patrones, como las tendencias, formado con otra información y experiencia. También puede incluir hipótesis y teorías sobre las causas. El conocimiento puede ser explícito, lo que una empresa o comunidad acepta como verdadero o tácita-dentro de las cabezas de las personas. Ganamos en conocimiento cuando entendemos la importancia de la información.

Al igual que los datos y la información, el conocimiento también es un recurso empresarial. Los trabajadores del conocimiento deben ganar experiencia a través de la comprensión de la información, y luego aplicar esa experiencia tomando decisiones y acciones informadas y conscientes. Los trabajadores del conocimiento pueden ser expertos funcionarios, gerentes o ejecutivos. Una organización que aprende es aquella que busca en forma proactiva aumentar el conocimiento colectivo y la sabiduría de sus trabajadores del conocimiento.

La gestión del conocimiento propende por generar el aprendizaje organizacional y la gestión del capital intelectual como un recurso de empresa. Tanto la gestión del conocimiento y gestión de datos, dependen de los datos e información de alta calidad.

7. GOBIERNO DE DATOS E INFORMACIÓN

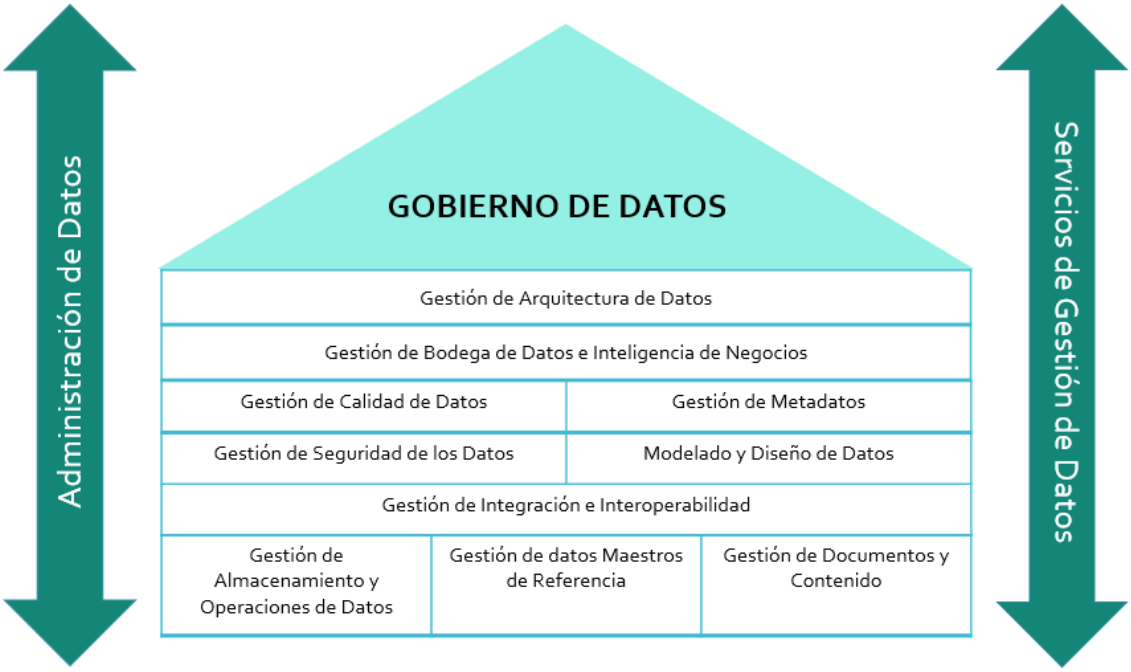


FIGURA 2. GOBIERNO DE DATOS

7.1. DIRECTRICES GENERALES

Es política de Corpovalle preservar los estándares, lineamientos, procesos, roles, responsabilidades y condiciones de legalidad que determinan el adecuado uso, desarrollo y gestión de los datos e información a nivel corporativo como un recurso de valor empresarial.

Para lograrlo se debe dar cumplimiento a las siguientes directrices:

- Todas las subdirecciones, áreas, unidades o divisiones, entre otros, que resulten en la Corporación, responsables de estructuras de datos que contengan información DE beneficiarios, clientes, proveedores y en general, de los distintos grupos de interés de la entidad, deben cumplir cinco principios para una efectiva gestión de datos: Accesibilidad, Calidad, Consistencia, Seguridad y Auditabilidad.
- Las estructura de datos que contengan información de los grupos de interés, deben dar cumplimiento a los derechos y condiciones de legalidad para el tratamiento de datos personales, como se especifica en la Ley Estatutaria 1581 de 2012 y Ley Estatutaria 1266 de 2008 y demás normas concordantes en la materia.
- Las solicitudes referentes a los derechos amparados por la Ley Estatutaria 1581 de 2012 y Ley Estatutaria 1266 de 2008 respecto a conocer, actualizar, rectificar, suprimir información y revocar

la autorización para tratamiento de datos, deben ser canalizadas de acuerdo a lo definido en la política de protección de datos a través del Oficial de Protección de Datos de la entidad.
- Corpovalle velará por el cumplimiento de lo dispuesto en la ley 1712 de 2014 – Transparencia y del derecho de acceso a la información pública.
- Es responsabilidad del Director y Subdirectores, garantizar el adecuado uso, gestión y tratamiento de los datos cuando se requiera.

Este numeral se rige por lo dispuesto en los siguientes documentos:

- Política de Protección de Datos Personales de Corpovalle.
- Política interna efectiva
- Política de Seguridad de la Información

7.2. ARQUITECTURA DE DATOS

La arquitectura de datos gestiona la definición de las necesidades de datos de la organización y el diseño de los planos maestros para satisfacer esas necesidades. Esta función incluye el desarrollo y mantenimiento de la arquitectura de datos empresariales, en el contexto de toda la arquitectura de la empresa y su conexión con las soluciones de sistemas de aplicaciones y proyectos.

La gestión de la Arquitectura de Datos es el proceso de definir y mantener especificaciones que:

- Proporcionan un vocabulario común de estándares de negocios;
- Expresan requisitos de datos estratégicos;
- Delinean diseños integrados en un alto nivel para cumplir con estos requisitos; y
- Alinean con la estrategia empresarial y arquitectura de negocios relacionada.

La arquitectura de Datos es un conjunto integrado de artefactos de especificación utilizados para definir requisitos de datos, guiar integración y control de los activos de datos, y alinear inversiones de datos con la estrategia empresarial. La arquitectura de Datos incluye nombres de datos formales, definiciones de datos completas, estructuras de datos eficaces, reglas de integridad de datos precisas, y documentación de datos robusta.

La Arquitectura de Datos es más valiosa cuando apoya las necesidades de información de la empresa entera y permite estandarización e integración de datos. Esta arquitectura hace parte de otra más grande. La Arquitectura empresarial integra datos, procesos, organizaciones, aplicaciones, y arquitectura de tecnología. Ésta ayuda a las organizaciones gestionar cambio y mejorar eficacia, agilidad, y rendición de cuentas.

Existen tres conjuntos de grandes de componentes de diseño:

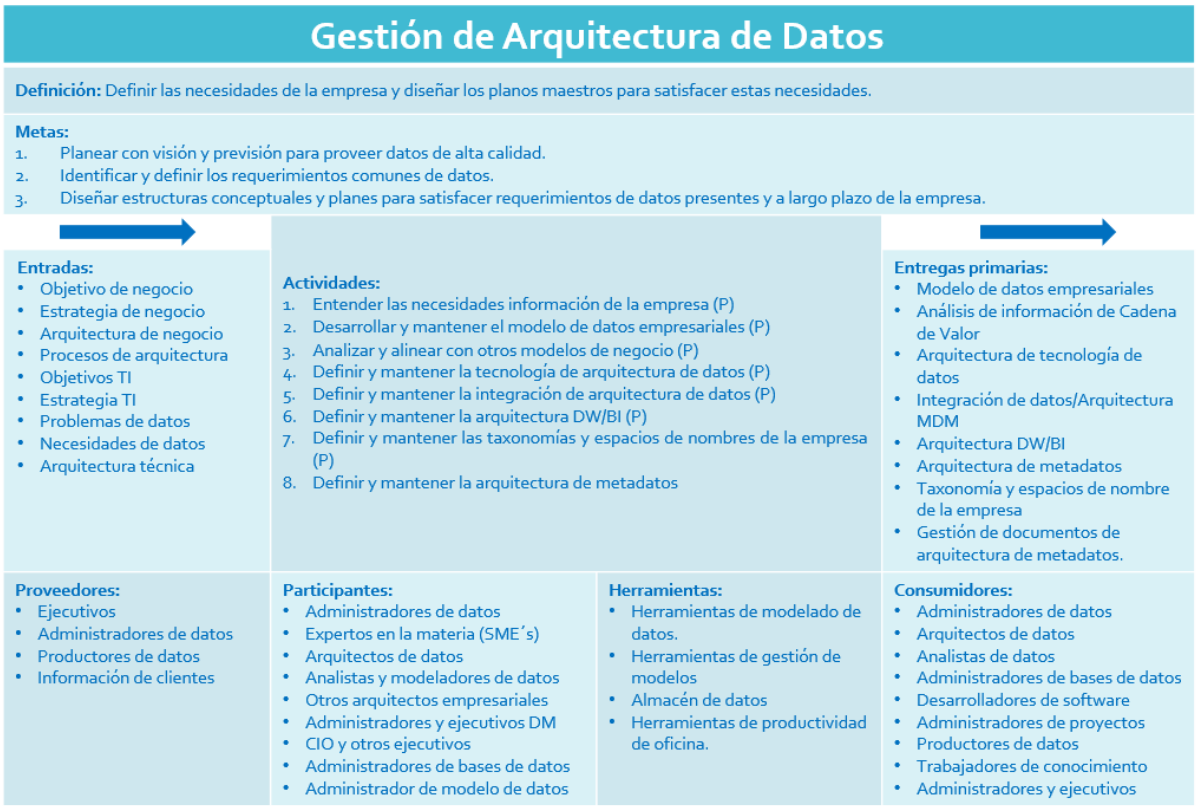
i. Un modelo de datos de la empresa, áreas temáticas identificables, entidades de negocios, reglas de negocios que rigen las relaciones entre entidades, y los atributos de datos esenciales de la empresa.
ii. El análisis de la cadena de valor de información que alinea componentes del modelo de datos,

ej., áreas temáticas y entidades de negocios, con procesos de negocios y otros componentes de la arquitectura empresarial. Estos pueden incluir organizaciones, papeles, aplicaciones, metas, estrategias, proyectos, y plataformas tecnológicas.

iii. La arquitectura de entrega de datos que incluye la arquitectura de tecnología de datos, arquitectura de integración de datos, almacenamiento de datos, la arquitectura de inteligencia de negocios, taxonomías empresariales para gestión de contenidos, y arquitectura de metadatos.

A continuación se presentan unos artefactos para iniciar su implementación:

- Vista del Planeador (Contextos de Alcance): Una lista de áreas temáticas y entidades empresariales.
- Vista del Propietario (Conceptos de Negocios): Modelos de datos conceptuales que se muestran las relaciones entre entidades.
- Vista del Diseñador (Lógico de Sistema): Modelos de datos lógicos, normalizados totalmente y atribuidos.
- Vista del Generador (Física de Tecnología): Modelos de datos físicos optimizados para limitar la tecnología.
- Vista del Implementador (Asambleas de Componente): Representaciones detalladas de estructuras de datos definidas normalmente en “SQL” Lenguaje de Definición de Datos (DDL).
- Empresa en Funcionamiento: Casos implementados operan dentro de la empresa.



Actividades: Planeación (P) – Control (C) – Desarrollo (D) — Operacional (O)

PRINCIPIOS RECTORES

La aplicación de la función de gestión de la arquitectura de datos en organizaciones sigue ocho principios básicos:

i. La arquitectura de datos es un conjunto integrado de artefactos de especificación (planes maestros) utilizados para definir requisitos de datos, guiar integración de datos, controlar activos de datos, y alinear inversiones de datos con estrategia de negocios.
ii. La arquitectura de datos forma parte de la estructura empresarial general, junto con arquitectura de procesos, arquitectura de negocios, la arquitectura de sistemas, y la de tecnología.
iii. La arquitectura de datos incluye tres grandes categorías de especificaciones: modelo de datos empresarial, análisis de cadena de valor de información, y la arquitectura de entrega de datos.
iv. La arquitectura de datos abarca más datos. Ayuda a establecer una base semántica de la empresa, utilizando vocabulario de negocios común.

v. Un modelo de datos empresarial es integrado y orientado al sujeto. Define datos esenciales que se utilizan por la organización entera. El modelo de empresa de datos es construido en capas: vista de áreas temáticas general, vistas conceptuales de entidades y sus relaciones con áreas temáticas, y vistas más detalladas, parcialmente atribuidas de estas áreas temáticas.
vi. La información de análisis de cadena de valor define las relaciones críticas entre datos, procesos, funciones, organizaciones, y otros elementos de la empresa.
vii. La entrega de datos define el plan maestro para cómo fluyen los datos a través de bases de datos y aplicaciones. Esto garantiza la calidad y la integridad de datos que apoya procesos de negocios transaccionales, informes de inteligencia de negocios, y análisis.
viii. Los marcos de arquitecturas como TOGAF y el Marco de Zachman ayudan a organizar el pensamiento colectivo acerca de la arquitectura. Esto permite a los grupos con diferentes objetivos y perspectivas trabajar juntos para satisfacer intereses comunes.

7.3. CALIDAD DE DATOS

La Gestión de la Calidad de Datos (GCD) es un proceso de apoyo crítico en la gestión del cambio organizacional. Cambiar el enfoque de negocios, estrategias de integración de negocios, fusiones, adquisiciones y asociaciones puede obligar a combinar fuentes de datos, poblar retrospectivamente o integrar los datos.

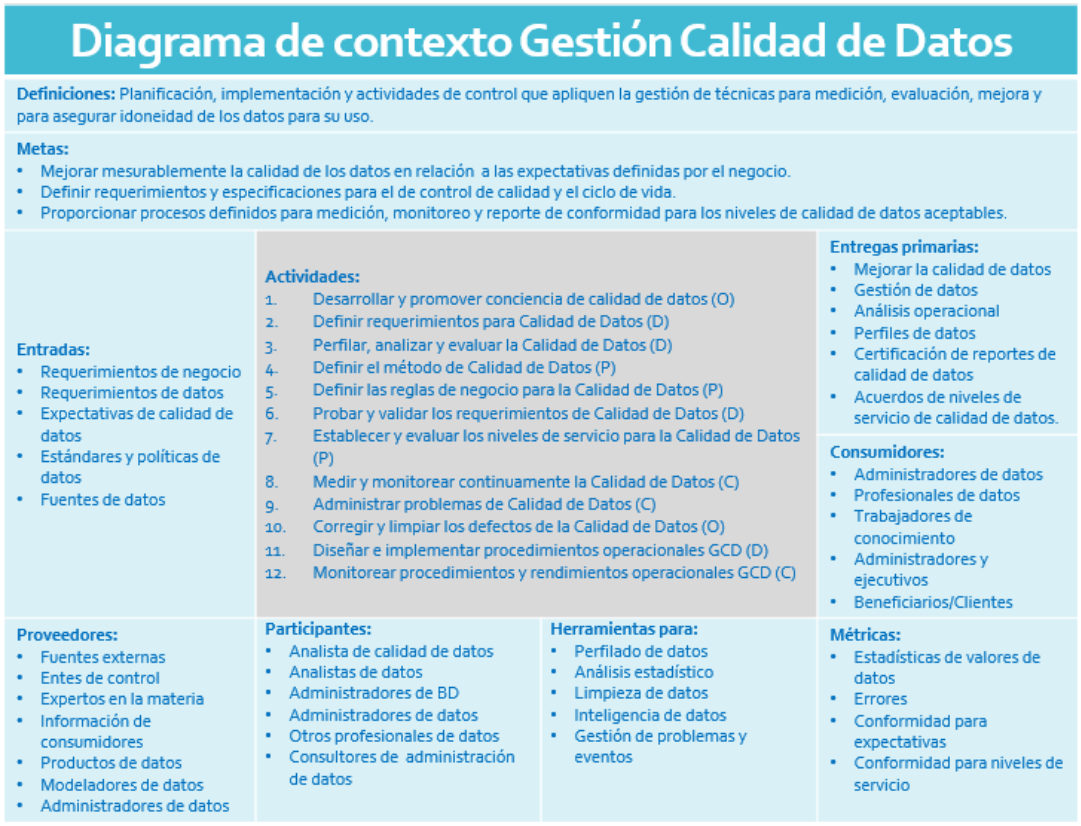
La calidad de los datos es sinónimo de calidad de la información ya que los malos resultados de calidad de datos conllevan a información inexacta y un bajo rendimiento del negocio. La limpieza de datos puede dar lugar a mejoras costosas de corto plazo que no abordan las causas raíz de los defectos de datos. Un programa más riguroso de calidad de datos es necesario para proporcionar una solución más económica para la mejora de la calidad y la integridad de los datos.

Estos problemas implican más que sólo corrección de datos, implican la gestión del ciclo de vida para la creación de datos, transformación y transmisión de los datos para asegurar que la información resultante satisfaga las necesidades de todos los consumidores de datos dentro de la corporación.

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. Después de identificar los problemas en los flujos de procesamiento de datos, notificar a los administradores de datos apropiados para tomar las medidas correctivas que permitan la eliminación de su causa raíz.

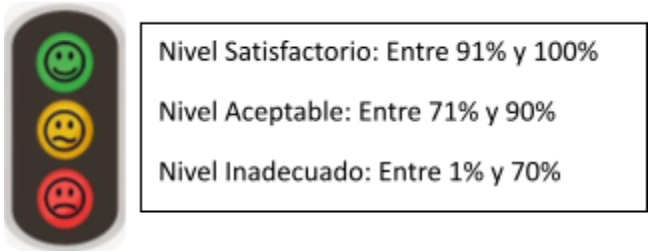
La Gestión de Calidad de Datos es también un proceso continuo para definir los parámetros y especificar los niveles aceptables de calidad de datos para satisfacer las necesidades del negocio y de garantizar que la calidad de datos cumple con estos niveles adecuados. Esto implica realiza análisis, identificación de anomalías, definición de los requerimientos del negocio y las correspondientes reglas de negocio para definir la calidad de los datos requeridos. La Gestión de Calidad de Datos implica instituir procesos de inspección y control para vigilar el cumplimiento de las reglas de calidad de datos definidas, así como perfilados de datos, la normalización, la limpieza y consolidación, cuando sea necesario. Por último, es necesario incorporar temas de seguimiento de incidentes como una forma de

controlar el cumplimiento de los acuerdos de nivel de servicio de calidad de datos definidos.



PRINCIPIOS RECTORES

i. Corpovalle define el índice de calidad de datos, de acuerdo a la siguiente gráfica:



ii. Los propietarios de dominio de las Subdirecciones, deben garantizar que la recolección y actualización de datos se genere en los formularios físicos y/o virtuales definidos y aprobados por la Corporación.

iii. Es responsabilidad de todas las Subdirecciones que hacen gestión de datos mantener la calidad del conjunto de datos de sus sistemas de información, basada en el Instructivo "*Estándares de Calidad para la Elaboración de Formularios.*"

iv. Los cargos o personas que se designen como propietarios de dominio (dominio de datos) deberán garantizar que las estructuras de datos que tienen a cargo mantengan un nivel de calidad igual o superior al 71%.

v. Todo requerimiento de calidad de datos y/o integración de datos de bases de datos que contengan información de los grupos de interés, debe ser efectuado a través de una solicitud con aprobación del jefe inmediato, utilizando el procedimiento vigente.

vi. El líder de gestión de datos de la corporación deberá presentar un informe semestral de los índices de calidad de las estructuras de datos definidas por la alta dirección.

Este numeral se rige por lo dispuesto en los siguientes documentos:

- Estándar para la elaboración de formularios y registro de datos.

7.4. CICLO DE VIDA DE LOS DATOS

Al igual que cualquier activo, los datos tienen un ciclo de vida para gestionar los activos de datos. Los datos son creados o adquiridos, almacenados y mantenidos, son utilizados y en ocasiones destruidos. En el curso de su vida, los datos pueden ser extraídos, exportados, importados, migrados, validados, editados, actualizados, limpiados, transformados, convertidos, integrados, segregados, agregados, referenciados, revisados, informados, analizados, minados, resguardados, restaurados, archivados y recuperados antes de ser eventualmente eliminados.

Los datos fluyen dentro y fuera de los almacenes de datos y se empaquetan para su entrega en productos de información. Se almacena en formatos estructurados en bases de datos y archivos planos, y en formatos menos estructurados como correo electrónico y otros documentos electrónicos, documentos de papel, hojas de cálculo, informes, gráficos, archivos de imágenes electrónicas, grabaciones de audio y vídeo. Por lo general, el 80% de los activos de datos de una organización reside en formatos relativamente no estructurados.

Los datos sólo tienen valor cuando se utilizan realmente, o quedan disponibles para ser útiles en el futuro. Todas las etapas del ciclo de vida de datos tienen costos y riesgos asociados, pero sólo la etapa de "utilización" agrega valor al negocio.

Cuando se gestiona con eficacia, el ciclo de vida de datos comienza incluso antes de la adquisición de datos, con la planificación o arquitectura que la corporación defina para los datos, la especificación de los datos y la habilitación de la captura de datos, entrega, almacenamiento y controles.

El Ciclo de Vida de Desarrollo de Sistemas (SDLC), que se muestra en la Figura 3, no es el mismo que el ciclo de vida de datos. El SDLC describe las etapas de un proyecto, mientras que el ciclo de vida de los datos describe los procesos realizados para gestionar los activos de datos.

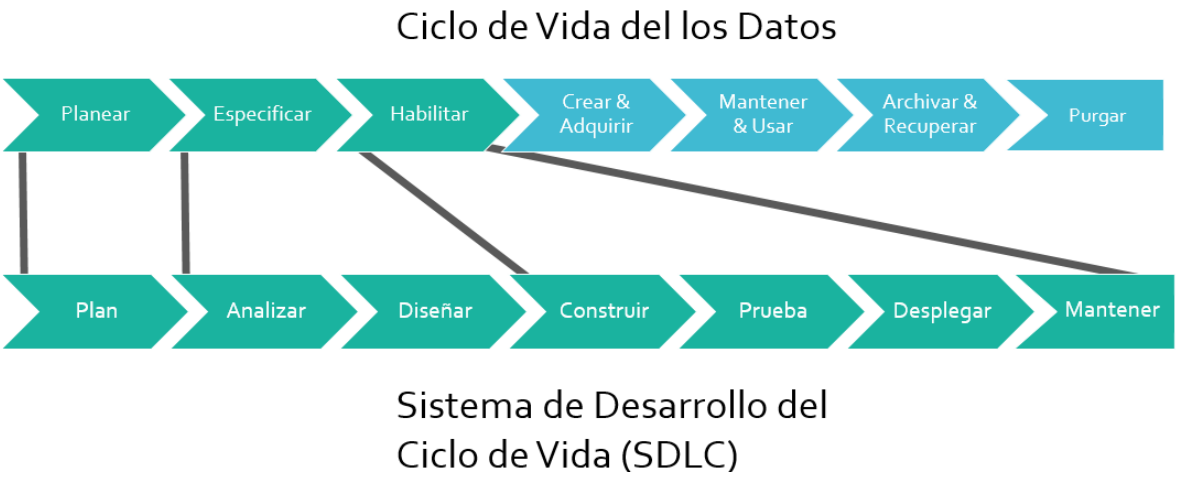


FIGURA 3. EL CICLO DE VIDA DE LOS DATOS Y EL CICLO DE VIDA DE DESARROLLO DE SISTEMAS

Sin embargo, los dos ciclos de vida están estrechamente relacionados porque las actividades de planificación de datos, especificación y de habilitación son partes integrales del SDLC. Otras actividades SDLC son operativas o de supervisión por naturaleza.

PRINCIPIOS RECTORES

i. Las áreas responsables de la gestión de datos deberán alinear sus procesos para cumplir con una Estrategia de Actualización de Datos Corporativa y lo dispuesto en el Estándar para la elaboración de formularios y registro de datos.
ii. Todas las áreas que requieran capturar o actualizar datos de los grupos de interés deben solicitar al responsable de gestión de datos el acompañamiento para lograr el desarrollo y ejecución de esta actividad.
iii. Las áreas responsables de datos y el líder de gestión de datos definirán en conjunto el ciclo de vida de los datos de acuerdo a las necesidades de negocio y la naturaleza de los proyectos a través de los cuales se haga la vinculación de datos.

Este numeral se rige por lo dispuesto en los siguientes documentos:
- Estándar para la elaboración de formularios y registro de datos.

7.5. SEGURIDAD DE DATOS

7.5.1. ACTIVIDADES Y CONCEPTOS

El objetivo final de la gestión de la seguridad de datos es proteger los activos de información en línea con las regulaciones de privacidad, confidencialidad y requerimientos del negocio. Estos requisitos

provienen de varias fuentes diferentes, muy importantes:

- Gestión de los interesados: Se deben reconocer las necesidades de privacidad y confidencialidad de sus partes interesadas, incluidos los clientes, beneficiarios, ciudadanos, proveedores o socios de negocios. Los interesados son los propietarios finales de los datos sobre ellos y todos en la organización deben ser un administrador responsable de estos datos.
- Regulaciones Gubernamentales: Las regulaciones gubernamentales protegen algunos de los intereses de seguridad de los interesados. Algunas regulaciones restringen el acceso a la información, mientras que otras normativas garantizan la apertura, la transparencia y la rendición de cuentas.
- Preocupación comercial de dominio privado: Cada organización tiene sus propios datos, los cuales debe proteger; asegurar la ventaja competitiva proporcionada por la propiedad intelectual y el conocimiento íntimo de las necesidades del cliente y las relaciones con los socios de negocios es una piedra angular de cualquier plan de negocios.
- Necesidades acceso legítimo: los ejecutores de seguridad de datos también deben entender las necesidades legítimas de acceso a datos. Estrategia empresarial, normas y los procesos requieren que las personas en ciertos roles a asumir la responsabilidad por el acceso y el mantenimiento de ciertos datos.

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

- **Autenticación:** Validar los usuarios son quienes dicen ser.
- **Autorización:** Identificar a las personas adecuadas y conceder los privilegios correctos.
- **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.

7.5.2. GESTIÓN DE SEGURIDAD DE DATOS

Comprender las necesidades de seguridad de datos y los requisitos reglamentarios

- Definición de la Política de Seguridad de Datos
- Definir Estándares de Seguridad de Datos
- Definir los Controles y Procedimientos de Seguridad de Datos
- Administrar Usuarios, Contraseñas y membresía de Grupos
- Gestionar las vistas y permisos a los datos
- Monitorear la autenticación de usuario y el comportamiento de acceso
- Clasificar la confidencialidad de la información
- Auditar la seguridad de los datos
- Las herramientas utilizadas para administrar la seguridad de datos.
- Normas y mecanismos de cifrado de datos.

- Directrices de acceso a proveedores y contratistas externos.
- Protocolos de transmisión de datos a través de Internet.
- Los requisitos de documentación.
- Estándares de acceso remoto.
- Violación de la seguridad, incidente y procedimientos de información.

7.5.3. NORMAS Y PROCEDIMIENTOS CONTRASEÑA

Las contraseñas son la primera línea de defensa para proteger el acceso a los datos. Cada cuenta de usuario debe ser forzada a tener una contraseña (propietario de la cuenta) con un nivel suficiente de complejidad, conocido comúnmente como contraseñas "fuertes". No permitir contraseñas en blanco. 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.

7.5.4. MONITOREAR LA AUTENTICACIÓN DEL USUARIO Y COMPORTAMIENTO DE ACCESO

Autenticación de Monitoreo y comportamiento de acceso es fundamental porque:

- Proporciona información acerca de quién se está conectando y acceder a los activos de información, lo cual es un requisito básico para la auditoría de cumplimiento.
- Alerta a los administradores de seguridad de situaciones imprevistas, compensando descuidos en la planificación de la seguridad de datos, diseño y puesta en práctica.

7.5.5. MONITOREO (AUDITORIA)

Las declaraciones de política de seguridad de datos, documentos estándares, guías de implementación, solicitudes de cambio, registros de monitoreo de acceso, salidas de informes y otros registros (copia electrónica o impresa) forman la base del monitoreo. Además de examinar la evidencia existente, también se pueden incluir la realización de pruebas y comprobaciones.

Los cuales son:

- Analizar las políticas y normas con las mejores prácticas y las necesidades de seguridad de los datos.
- Revisión 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.
- Verificar que la organización cumple con los requisitos reglamentarios.
- Revisar 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.

7.5.6. CONFIDENCIALIDAD DE INFORMACIÓN CLASIFICADA

Corpovalle deberá clasificar los datos y productos de información mediante un sencillo esquema de clasificación de la confidencialidad. La mayoría de las organizaciones clasifican el nivel de confidencialidad de información que se encuentra dentro de los documentos, incluidos los informes. Un esquema de clasificación típico puede incluir los siguientes niveles de clasificación de confidencialidad:

- Para Audiencias Generales: Información disponible para cualquier persona, incluido el público en general.
- Sólo para uso interno: Información limitado a empleados o miembros, pero con un riesgo mínimo si se comparten.
- Confidencial: La información que no debe ser compartida fuera de la organización.
- Confidencial Restringido: Información limitada a individuos que realizan ciertas funciones con la "necesidad de conocer".
- confidencial que cualquiera que acceda a la información debe firmar un acuerdo legal para acceder a los datos y asumir la responsabilidad de su carácter secreto.

La gestión de seguridad de los datos es la planificación, desarrollo y ejecución de las políticas y procedimientos para proporcionar la debida autenticación, autorización, acceso y auditoría de datos y activos de información de seguridad.

Las políticas y procedimientos de seguridad de datos eficaces aseguran que las personas adecuadas pueden utilizar y actualizar los datos de la manera correcta y que todo el acceso inapropiado está restringido. Entender y cumplir con los intereses de privacidad, confidencialidad está en el mejor interés de la corporación.

Una función eficaz de gestión de la seguridad de datos establece los mecanismos de gobernanza juiciosas que son bastante fáciles de cumplir en una base operativa diaria de todos los interesados. El contexto de la gestión de la seguridad de datos se muestra en la siguiente gráfica.

Actividades: Planeación (P) – Control (C) – Desarrollo (D) — Operacional (O)

PRINCIPIOS RECTORES

La aplicación de la función de gestión de la seguridad de datos sigue doce Principios básicos:

i. Ser un administrador responsable de información, comprendiendo y respetando las necesidades de privacidad y confidencialidad de todos los interesados ya sean clientes, beneficiarios, ciudadanos, proveedores o socios de negocios.
ii. Entender y cumplir con todos los reglamentos y directrices pertinentes.
iii. Identificar los requisitos detallados de seguridad de aplicaciones en la fase de análisis de todos los proyectos que se desarrollen en la corporación.
iv. Clasifica todos los datos de la corporación y productos de información en contra de un sencillo esquema de clasificación de la confidencialidad.
v. Cada cuenta de usuario debe tener una contraseña definida por el usuario siguiendo una serie de pautas de complejidad de contraseña y que expira cada 45 días.
vi. Crear grupos de funciones; definir privilegios de papel y conceder privilegios a los usuarios mediante la asignación al grupo de función apropiada. Siempre que sea posible, asignar a

cada usuario a un solo grupo de funciones.

vii. Para evitar problemas de integridad de datos con la información de acceso, se deben gestionar de forma centralizada los datos de identidad de usuario y datos de los miembros del grupo.

viii. Utilice vistas de base de datos relacional para restringir el acceso a las columnas sensibles y/o filas específicas en tablas y bases de datos.

ix. Reducir al máximo y considerar cuidadosamente cada uso de cuentas compartidas o usuario del servicio.

x. Monitorear acceso de datos a cierta información activa y tomar foto instantáneas periódicas de la actividad de acceso a datos para comprender las tendencias y comparar con los criterios de normalización.

xi. Realizar periódicamente las auditorías de seguridad de datos para verificar el cumplimiento de las normas. Además, para analizar la eficacia y la madurez de las políticas y prácticas de seguridad de datos.

xii. En un entorno externalizado, asegúrese de definir claramente las funciones y responsabilidades en materia de seguridad de los datos y comprender la "cadena de custodia" de datos a través de las organizaciones y los roles.

Este numeral se rige por lo dispuesto en los siguientes documentos:

- Política de seguridad de la información.

--- Fin del documento ---