Universidad de Santander
UDES

VIGILADA MINEDUCACIÓN | SNIES 2832

POLÍTICA INSTITUCIONAL
DE GOBIERNO DE DATOS



POLÍTICA INSTITUCIONAL DE GOBIERNO DE DATOS

1. CONTEXTO

En el marco de la transformación digital de la educación superior y de las exigencias del sistema de aseguramiento de la calidad, la gestión estratégica de los datos se ha convertido en un factor determinante para el cumplimiento de las funciones misionales y el logro de los propósitos formativos definidos en el Proyecto Educativo Institucional (Universidad de Santander, 2023a).

En la Universidad de Santander, el crecimiento sostenido de los sistemas de información, la diversificación de las fuentes de datos académicos y administrativos, y el fortalecimiento de los procesos de analítica institucional han incrementado la disponibilidad de información para la toma de decisiones; sin embargo, este avance no siempre ha estado acompañado de una estructura formal de gobierno que garantice su gestión integral, estandarizada y orientada a la generación de valor (Decreto 1389, 2022).

La situación actual evidencia la existencia de múltiples repositorios, aplicaciones y procesos que producen y consumen datos en los diferentes niveles organizacionales, lo que genera retos asociados a la calidad, trazabilidad, oportunidad, interoperabilidad y seguridad de la información. Esta condición limita, en algunos casos, la consolidación de reportes institucionales confiables, el seguimiento sistemático a los resultados de aprendizaje de los estudiantes, el monitoreo de los indicadores del Plan de Desarrollo Institucional (Universidad de Santander, 2023b) y la medición del impacto de los egresados y de la Universidad en el desarrollo regional.

En el contexto de los procesos de autoevaluación, autorregulación y acreditación, esta situación representa un desafío, dado que la disponibilidad de información pertinente, consistente y verificable es un requisito fundamental para la evaluación de las condiciones de calidad, la toma de decisiones basada en evidencia y el mejoramiento continuo. Asimismo, la ausencia de lineamientos institucionales unificados para la gestión de los datos dificulta la definición clara de responsabilidades, la priorización de información estratégica y la consolidación de una cultura organizacional orientada al uso analítico de la información.

Adicionalmente, las tendencias globales asociadas a la computación en la nube (Parra-González et al., 2023), el internet de las cosas (Mieles Mieles & Navia Mendoza, 2026) y el análisis de grandes volúmenes de datos han ampliado las oportunidades para el aprovechamiento académico, investigativo y administrativo de la información, pero también han incrementado la necesidad de establecer mecanismos de dirección, control y seguimiento desde los órganos de gobierno institucional, que permitan maximizar su valor y mitigar los riesgos relacionados con su uso inadecuado o con la exposición de datos sensibles (International Organization for Standardization [ISO] & International Electrotechnical Commission [IEC], 2017).

Ante esta realidad, se hace necesaria la implementación de un modelo institucional de Gobierno de Datos que articule los procesos académicos y administrativos con la planeación estratégica, el Sistema Interno de Aseguramiento de la Calidad y la analítica institucional, definiendo principios, roles, responsabilidades y lineamientos para la gestión integral del ciclo de vida de los datos.

En este proceso intervienen como actores estratégicos el Consejo Superior y la alta dirección, responsables de orientar la gobernanza de la información; la Secretaría General, como líder de la política; las dependencias académicas y administrativas, en su calidad de productoras y usuarias de datos; la Oficina de Tecnologías de la Información, como soporte de la infraestructura tecnológica; y la comunidad universitaria, beneficiaria de la mejora en los procesos de toma de decisiones, la calidad académica y el impacto institucional en el entorno.

De esta manera, el Gobierno de Datos se configura como un habilitador para el fortalecimiento del modelo educativo centrado en el estudiante, el seguimiento a los resultados de aprendizaje, el cumplimiento de las metas del Plan de Desarrollo Institucional, la consolidación de los procesos de autoevaluación y acreditación, y la medición del aporte de la Universidad al desarrollo regional.

2. JUSTIFICACIÓN

El crecimiento de los sistemas de información institucionales, la transformación digital de los procesos académicos y administrativos, las exigencias del aseguramiento de la calidad y la consolidación de la analítica institucional hacen necesaria la implementación de un modelo formal de Gobierno de Datos en la Universidad de Santander. Esta política busca garantizar la gestión integral, confiable y oportuna de la información como soporte para la toma de decisiones y el fortalecimiento de las funciones misionales (DAMA International, 2017).

El Gobierno de Datos permitirá disponer de información trazable y de alta calidad para el seguimiento al desempeño académico, favoreciendo la permanencia, la graduación y el éxito estudiantil. Asimismo, facilitará la evaluación y actualización de los planes de estudio mediante analítica académica, orientando el desarrollo de estrategias pedagógicas y curriculares hacia el logro de los propósitos formativos.

En términos institucionales, contribuirá a una planeación estratégica sustentada en evidencia, al fortalecimiento de los procesos de autoevaluación, autorregulación y acreditación, al mejoramiento de la gestión académica y administrativa y al monitoreo oportuno de los indicadores del Plan de Desarrollo Institucional.

Frente al impacto de los egresados, posibilitará el seguimiento a su trayectoria académica y laboral, la valoración de su aporte al entorno social y productivo y la retroalimentación de la oferta académica de acuerdo con las necesidades del contexto. En relación con el desarrollo regional, proporcionará información pertinente para la formulación de proyectos con enfoque territorial, la medición del impacto de la investigación, la extensión y la proyección social, y la definición de acciones orientadas al desarrollo sostenible en las regiones donde la Universidad tiene presencia.

Adicionalmente, el Gobierno de Datos favorece el cumplimiento de la normativa nacional en materia de gestión de la información, fortalece la cultura institucional basada en el uso estratégico de los datos y genera valor académico, investigativo y administrativo. De esta manera, se articula con el Proyecto Educativo Institucional y el Plan de Desarrollo Institucional, apoyando el logro de los propósitos formativos, la calidad académica y el impacto institucional.

3. ESTRATEGIA DE INTERVENCIÓN

La alternativa de intervención seleccionada consiste en implementar un modelo institucional de Gobierno de Datos de carácter centralizado con ejecución descentralizada. Este modelo ordena, estandariza y controla la gestión de la información; define una dirección institucional común y distribuye la ejecución en las dependencias académicas y administrativas, de acuerdo con sus responsabilidades y dominios de datos.

La intervención es aceptable porque se articula con la normativa y los instrumentos institucionales vigentes; eficaz porque orienta la gestión al mejoramiento de la calidad, la seguridad, la disponibilidad y la interoperabilidad; eficiente porque reduce duplicidades y facilita la integración de sistemas; pertinente porque responde a las necesidades de los procesos académicos, administrativos, investigativos y de extensión; y sostenible porque fortalece capacidades, roles, mecanismos de seguimiento y una cultura institucional basada en datos.

La implementación de un modelo institucional de Gobierno de Datos permitirá ordenar, estandarizar y controlar la gestión de la información en la Universidad, garantizando su calidad, seguridad, disponibilidad e interoperabilidad. Bajo esta intervención, se espera que la existencia de roles definidos, procesos unificados, arquitectura integrada y capacidades analíticas fortalecidas incremente significativamente el uso estratégico de los datos (ISO/IEC 38505-1, 2017), lo que conducirá a mejores decisiones institucionales, al fortalecimiento del aseguramiento de la calidad, al cumplimiento normativo y a la mejora sostenida del desempeño académico y administrativo.

En consecuencia, si la Universidad adopta y ejecuta de manera sistemática el modelo de Gobierno de Datos, se generarán las condiciones necesarias

para alcanzar los resultados, logros e impactos esperados, potenciando el desarrollo misional y la contribución de la UDES al entorno regional.

3.1. Modelo institucional de Gobierno de Datos

La Universidad de Santander adopta un Modelo de Gobierno de Datos de carácter centralizado con ejecución descentralizada. En este enfoque, las políticas, estándares, lineamientos y prioridades estratégicas son definidos por una instancia institucional única, responsable de establecer el marco rector para el Programa de Gobierno de Datos, así como para sus proyectos, actividades, roles y los indicadores de resultado, logro e impacto.

La implementación de estas directrices se desarrolla de manera descentralizada en las diversas dependencias académicas y administrativas, garantizando la articulación con los criterios institucionales previamente definidos.

Este modelo asegura la existencia de un marco común para la gestión de los datos, promoviendo su alineación con el direccionamiento estratégico institucional y permitiendo la estandarización de prácticas relacionadas con la calidad, seguridad, interoperabilidad y aprovechamiento de la información como un activo estratégico. Asimismo, fortalece la toma de decisiones basada en evidencia, impulsa el desarrollo de capacidades en analítica institucional y contribuye a consolidar una cultura organizacional orientada al uso responsable, ético y eficiente de los datos.

El Gobierno de Datos se organiza en tres niveles de actuación: estratégico, táctico y operacional, los cuales permiten:

- Definir políticas institucionales y prioridades estratégicas.
- Convertir dichas políticas en planes, lineamientos y mecanismos de implementación.
- Asegurar su ejecución efectiva en los procesos académicos y administrativos.

De esta manera, la estructura del modelo permite una gestión coherente, articulada y sostenible del ciclo de vida de los datos dentro de la Universidad.

3.2. Niveles de actuación, roles y responsabilidades

La estructura organizacional del Gobierno de Datos de la Universidad se define en tres niveles de actuación (Estratégico, táctico y operacional) que permiten la dirección, coordinación e implementación del modelo institucional, en coherencia con lo establecido en el marco nacional de gobernanza de la infraestructura de datos.

3.2.1. Nivel estratégico

El nivel estratégico es la instancia responsable de definir las políticas, los lineamientos generales, las prioridades institucionales y la asignación de recursos para el desarrollo del Gobierno de Datos.

Comité de Gobierno de Datos

El Comité de Gobierno de Datos es la máxima instancia de orientación y supervisión del modelo institucional. Tiene a su cargo la aprobación, actualización y seguimiento de la Política de Gobierno de Datos, del Plan Estratégico de Gobierno de Datos y de los estándares asociados a la gestión de la información.

Asimismo, define las prioridades institucionales en materia de dominios de datos, establece los lineamientos para la seguridad, privacidad e intercambio de información, actúa como instancia de resolución de conflictos y promueve la consolidación de una cultura institucional basada en datos.

3.2.2. Nivel táctico

El nivel táctico es responsable de convertir las directrices estratégicas en planes, programas, procesos y lineamientos operativos, así como de realizar el seguimiento a su cumplimiento y de soportar la toma de decisiones institucional.

Administrador del Gobierno de Datos

El Administrador del Gobierno de Datos, equivalente al rol de Chief Data Officer, coordina integralmente el modelo institucional, lidera la ejecución del Plan Estratégico de Gobierno de Datos, realiza el seguimiento a los indicadores de desempeño y

actúa como articulador entre el nivel estratégico y el nivel operacional.

Desde este rol se promueve la visión institucional de los datos como activo estratégico, se coordinan los programas de calidad de datos y de analítica institucional, se gestionan los acuerdos entre dependencias y se canalizan hacia el Comité las situaciones que requieren decisiones de carácter estratégico.

Administrador de Seguridad y Privacidad de la Información

Es responsable de definir y aplicar los lineamientos para la clasificación, protección y control de acceso a los datos, gestionar los riesgos asociados a su tratamiento y asegurar el cumplimiento de la normativa vigente en materia de seguridad y protección de datos personales.

Líderes de proceso

Los líderes de las dependencias académicas y administrativas garantizan la articulación de sus procesos con el modelo institucional, identifican los datos críticos para la toma de decisiones, definen los elementos de datos clave y disponen los recursos necesarios para la implementación de los lineamientos de Gobierno de Datos en su ámbito de gestión.

3.2.3. Nivel operacional

El nivel operacional es el responsable de ejecutar los lineamientos, procedimientos y actividades definidos en los niveles estratégico y táctico, asegurando la gestión adecuada de los datos en los procesos institucionales.

Gestores de datos de dependencia

Son los encargados de implementar el modelo en cada unidad académica o administrativa, mantener actualizado el inventario de datos, apoyar los procesos de calidad de la información, aplicar los estándares definidos y actuar como enlace entre su dependencia y el equipo central de Gobierno de Datos.

Equipo técnico de Gobierno de Datos

Es el responsable de desarrollar las capacidades técnicas del modelo, incluyendo la gestión de la calidad de los datos, la arquitectura e integración de la información y el aprovechamiento analítico de los datos para la toma de decisiones institucional.

3.2.4. Equipo transversal de apoyo

El Gobierno de Datos cuenta con el apoyo de dependencias institucionales que, desde su ámbito de competencia, contribuyen a su implementación y sostenibilidad. La Oficina Jurídica orienta el cumplimiento normativo y la gestión de riesgos legales; la Oficina de Comunicaciones apoya los procesos de apropiación y cultura institucional basada en datos; y Talento Humano lidera las estrategias de formación y gestión del cambio organizacional.

Estas instancias no constituyen un nivel de gobernanza, sino que actúan como soporte especializado para el fortalecimiento del modelo institucional.

3.3. Ciclo de vida de los datos

El ciclo de vida de los datos en la Universidad comprende un proceso integral y continuo que inicia con la planeación, etapa en la que se definen las políticas, necesidades y lineamientos para asegurar una gestión adecuada y estratégica de la información.

Posteriormente, se avanza a la recopilación, donde los datos se recolectan conforme a los objetivos institucionales y bajo criterios de calidad definidos.

Una vez obtenidos, los datos pasan al procesamiento, fase en la que son depurados, organizados y estructurados para permitir su uso confiable en el seguimiento y la gestión institucional.

En la etapa de análisis, la información resultante es interpretada para generar conocimiento y orientar la toma de decisiones. Cuando estos productos de información están listos, se procede a la publicación, garantizando que sean divulgados en formatos accesibles y pertinentes para los diferentes usuarios.

A continuación, la preservación asegura su almacenamiento seguro, manteniendo la

disponibilidad, integridad y trazabilidad en el tiempo. Finalmente, cuando los datos cumplen su periodo de utilidad, se realiza su eliminación de manera segura, conforme a las políticas institucionales de retención, protección y privacidad de la información.

3.4. Principios éticos del buen Gobierno de Datos

Los principios éticos del buen gobierno constituyen la base para una gestión pública íntegra, transparente y orientada al interés general.

La responsabilidad implica que quienes administran información y recursos actúen con rigor, asumiendo las consecuencias de sus decisiones y garantizando un desempeño íntegro y orientado al servicio público, en consonancia con los marcos éticos del buen gobierno que promueven la integridad y la rendición de cuentas.

La calidad se manifiesta en la obligación de asegurar que los datos y procesos institucionales sean precisos, consistentes y confiables, de modo que soporten decisiones fundamentadas y eficaces, un principio ampliamente reconocido en los estándares de gestión pública responsable.

La transparencia demanda que la información institucional sea accesible, verificable y comprensible, favoreciendo la confianza ciudadana y la apertura de los actos administrativos en línea con los principios consolidados en los códigos de buen gobierno y las políticas de acceso a la información.

La accesibilidad garantiza que los datos y servicios puedan ser consultados por los usuarios autorizados sin barreras técnicas o administrativas, promoviendo instituciones inclusivas y eficaces según los estándares éticos contemporáneos.

La interoperabilidad, por su parte, se refiere a la capacidad de los sistemas para intercambiar información de manera segura y eficiente, permitiendo la integración de procesos y una gestión coherente de los datos, como recomiendan los marcos modernos de gobernanza y arquitectura institucional.

Asimismo, los principios de confidencialidad, integridad y disponibilidad operan como salvaguardas esenciales para la gestión responsable de la información. La confidencialidad protege los datos sensibles y evita accesos no autorizados; la integridad vela por que la información se mantenga exacta y completa durante todo su ciclo de vida; y la disponibilidad garantiza que la información esté accesible cuando se requiera, asegurando la continuidad de la operación institucional. Estos tres elementos conforman la base reconocida internacionalmente para la protección y el uso ético de los datos en organizaciones públicas y privadas, al promover entornos seguros, confiables y orientados al bienestar colectivo.

3.5. Administración y servicios de gestión de datos

La Administración y los Servicios de Gestión de Datos comprenden el conjunto de capacidades, procesos y funciones que garantizan el manejo adecuado, seguro y eficiente de la información institucional a lo largo de su ciclo de vida.

En primer lugar, la arquitectura de datos establece la estructura, los estándares y los modelos que permiten organizar, relacionar y armonizar los datos provenientes de diferentes sistemas, asegurando coherencia y consistencia en todo el ecosistema informacional. Complementariamente, la seguridad de la información vela por la protección de los datos frente a accesos no autorizados, pérdidas, alteraciones o incidentes, implementando controles que garanticen confidencialidad, integridad y disponibilidad.

El almacenamiento y respaldo de la información constituye otro componente esencial, ya que garantiza que los datos se preserven de manera segura, con mecanismos de respaldo y recuperación que protejan la operación institucional ante contingencias. A su vez, la integración y transformación de datos permite unificar información proveniente de diversas fuentes, depurarla y prepararla para su análisis, facilitando su uso en procesos académicos, administrativos y estratégicos. La gestión de metadatos complementa esta labor al documentar el significado, origen, estructura y uso de los datos, promoviendo la trazabilidad y facilitando su reutilización.

La calidad del dato es un servicio transversal que

busca asegurar que la información sea exacta, completa, consistente y oportuna, permitiendo que las decisiones institucionales se fundamenten en evidencia confiable. De manera relacionada, la gestión y evaluación de riesgos de datos identifica amenazas y vulnerabilidades que podrían afectar la información institucional y establece acciones de mitigación para protegerla. En concordancia con las normativas vigentes, la privacidad y protección de datos personales garantiza el tratamiento adecuado de la información sensible, asegurando que su uso cumpla con principios éticos y obligaciones legales.

Asimismo, el cumplimiento normativo y la ética institucional aseguran que todos los procesos relacionados con los datos respondan a leyes, lineamientos internos, estándares sectoriales y principios rectores del buen gobierno. La analítica institucional y el reporte integran la interpretación, visualización y comunicación de la información, generando análisis, indicadores y reportes que apoyan la toma de decisiones, la planeación estratégica y la mejora continua en todos los niveles de la Universidad.

3.6. Grupos de interés

El Gobierno de Datos de la Universidad identifica a sus grupos de interés como los actores que participan, influyen o se ven impactados por la gestión institucional de los datos. Estos grupos se clasifican en internos y externos, atendiendo a su relación directa con los procesos académicos, administrativos y de aseguramiento de la calidad.

Entre los grupos de interés internos se encuentran los órganos de dirección y decisión estratégica, como el Consejo Superior, el Consejo Académico y el Comité Rectoral, cuyas funciones requieren información confiable para orientar el rumbo institucional. También hacen parte las decanaturas, las direcciones de programa, los estudiantes, los graduados, así como las unidades administrativas y unidades de apoyo, que generan, administran y utilizan datos esenciales para el funcionamiento académico y operativo de la Universidad.

En cuanto a los grupos de interés externos, el Gobierno de Datos reconoce la interacción con entidades del entorno regulatorio y social, entre ellas el Ministerio de Educación Nacional (MEN), que exige reportes y estructuras de información para el cumplimiento normativo, así como otras dependencias no gubernamentales que requieren o aportan datos en el marco de procesos de cooperación, evaluación, investigación o relacionamiento institucional.

Esta identificación de actores permite garantizar que la gestión de los datos responda a las necesidades, responsabilidades y expectativas de cada grupo, fortaleciendo la transparencia, la calidad de la información y la toma de decisiones basada en evidencia.

3.7. Gestión del conocimiento, comunicación, métricas y gerencia del cambio

Gestión del conocimiento y la comunicación

La Gestión del Conocimiento y la Comunicación en el marco del Gobierno de Datos comprende la generación y disponibilidad de información confiable y estandarizada que facilite la comprensión, uso y aprovechamiento institucional de los datos. Esto incluye la definición de datos estandarizados, la elaboración de informes y consultas que apoyen los procesos de análisis y decisión, así como el diseño de una estrategia de comunicación que garantice la divulgación efectiva de lineamientos, buenas prácticas y resultados. Asimismo, incorpora un plan de capacitación orientado a fortalecer las competencias de los diferentes actores institucionales en el uso, interpretación y gestión del dato.

Métricas

De manera complementaria, el componente de Métricas se orienta al desarrollo de análisis, indicadores y sistemas de monitoreo que permitan evaluar el desempeño institucional. Esto abarca la producción de análisis y estadísticas, la construcción de métricas de desempeño, y el seguimiento de indicadores estratégicos relacionados con la gestión, control y cumplimiento de metas institucionales. Finalmente, este proceso impulsa la mejora continua, asegurando que la información generada contribuya a optimizar los procesos, fortalecer la toma de decisiones basada en evidencia y promover una cultura institucional orientada al aprendizaje permanente.

Gerencia del cambio

La gerencia del cambio en el marco del buen gobierno garantiza que la adopción de nuevas prácticas, procesos y sistemas se realice de manera ordenada, responsable y participativa. Este proceso inicia con la evaluación del impacto y la preparación, que permite anticipar efectos, necesidades y ajustes organizacionales. Posteriormente, la alineación del liderazgo asegura que directivos y responsables impulsen el cambio con coherencia, transparencia y compromiso. La gestión de las partes interesadas promueve el diálogo, la participación y la corresponsabilidad de los diferentes grupos que intervienen en la transformación. A ello se suman las listas de verificación para la planificación e implementación, que facilitan la organización de acciones, el cumplimiento de responsabilidades y el control de riesgos. Finalmente, la transición hacia la sostenibilidad garantiza que los cambios implementados se consoliden, permanezcan en el tiempo y aporten valor institucional, fortaleciendo la toma de decisiones basada en evidencia y la cultura del buen gobierno.

4. DECLARACIÓN DE LA POLÍTICA

La Política de Gobierno de Datos de la Universidad de Santander tiene como propósito establecer los principios, lineamientos, roles y mecanismos institucionales para la gestión integral de los datos como activo estratégico. Garantiza su calidad, seguridad, disponibilidad, integridad, interoperabilidad y aprovechamiento para la toma de decisiones basada en evidencia. Además, busca el fortalecimiento de las funciones misionales y el cumplimiento del direccionamiento estratégico institucional. Esta Política aplica a todos los procesos académicos, administrativos, investigativos y de extensión. También se aplica a los colaboradores, directivos y demás actores responsables de la generación, gestión, análisis, custodia y uso de la información institucional. Se articula con el Plan de Desarrollo Institucional, las políticas de transformación digital, seguridad de la información, calidad, transparencia y gobernanza institucional. La Universidad orientará la gestión de los datos bajo los principios de confiabilidad, trazabilidad, ética, responsabilidad, interoperabilidad y protección de la información, promoviendo una cultura institucional basada en el uso estratégico de los datos y exigiendo el cumplimiento de estándares y buenas prácticas para su administración, uso y protección, prohibiendo actuaciones que comprometan la veracidad, seguridad, confidencialidad o uso adecuado de la información institucional.

La Universidad de Santander reconoce los datos como un activo estratégico para la gestión institucional, la toma de decisiones basada en evidencia, el fortalecimiento de las funciones misionales y el cumplimiento del direccionamiento estratégico (Universidad de Santander, 2023b).

Mediante la presente política se establecen los principios, la estructura organizacional, los roles, los lineamientos y los mecanismos de gestión necesarios para garantizar la calidad, seguridad, disponibilidad, integridad, interoperabilidad y aprovechamiento estratégico de los datos en todos los niveles de la Institución (véase el Anexo 1).

4.1. Alcance

La Política de Gobierno de Datos de la Universidad de Santander aplica a todas las dependencias académicas y administrativas, a la totalidad de los campus y a todos los procesos institucionales, tanto estratégicos como misionales, de apoyo y de evaluación. Sus disposiciones involucran a directivos, docentes, personal administrativo, estudiantes y a los terceros que, en el desarrollo de sus funciones o mediante vínculos contractuales, gestionen, produzcan, transformen, almacenen o utilicen datos institucionales.

En cuanto al ámbito de la información, esta política regula la gestión de datos estructurados, semiestructurados y no estructurados, así como de los datos maestros, transaccionales y derivados que se generan en el desarrollo de las actividades académicas, administrativas, investigativas y de extensión.

La presente política no sustituye la Política de Tratamiento de Datos Personales de la Universidad (Universidad de Santander, 2021); por el contrario, se articula con ella de manera complementaria, garantizando una gestión integral de los datos en coherencia con el marco normativo vigente y con los lineamientos institucionales en materia de

seguridad y privacidad de la información.

4.2. Propósito

Establecer el marco institucional de Gobierno de Datos de la Universidad de Santander, definiendo la estructura, los lineamientos, los roles y los mecanismos que permitan gestionar los datos como activos estratégicos para la generación de valor institucional y el mejoramiento continuo.

5. DESARROLLO DE LA POLÍTICA

La Política Institucional de Gobierno de Datos se operacionaliza mediante el Programa 1. Gobierno de Datos, integrado por dos proyectos y nueve actividades. Su ejecución se orienta al logro de resultados, logros e impactos verificables, con metas previstas al año 2028.

a. Programa 1. Gobierno de Datos

i. Proyecto 1.1. Gobernanza, seguridad y cumplimiento del dato

Actividad 1.1.1. Conformación e institucionalización de estructuras de gobierno

- **Responsables:** Comité de Gobierno de Datos, Secretaría General, Vicerrectoría Administrativa y Financiera y Talento Humano.
- **Indicador de resultado:** Porcentaje de dependencias con gestor/a de datos designado. **Meta 2028:** ≥95 % de dependencias con gestor/a de datos designado.
- **Indicador de logro:** Comité de Gobierno de Datos sesionando trimestralmente y Equipo Técnico de Gobierno de Datos operando formalmente. **Meta 2028:** 100 % de estructuras conformadas y activas.
- **Indicador de impacto:** Nivel de madurez institucional en Gobierno de Datos (escala 1–5). **Meta 2028:** ≥3,5/5 en nivel de madurez institucional.

Actividad 1.1.2. Gestión del cambio organizacional y apropiación cultural

- **Responsables:** Administrador de Gobierno de Datos, Oficina de Comunicaciones, Talento Humano y Gestores de Datos de Dependencia.
- **Indicador de resultado:** Número de campañas institucionales de sensibilización ejecutadas. **Meta 2028:** ≥6 campañas institucionales ejecutadas.
- **Indicador de logro:** Nivel institucional de adopción del modelo de Gobierno de Datos. **Meta 2028:** ≥80 % de adopción institucional del modelo.
- **Indicador de impacto:** Reducción de la resistencia organizacional frente al modelo de Gobierno de Datos. **Meta 2028:** ≥60 % de reducción frente a la línea base 2026.

Actividad 1.1.3. Formalización de roles, lineamientos y mecanismos de escalamiento

- **Responsables:** Comité de Gobierno de Datos, Secretaría General, Oficina Jurídica y Administrador de Gobierno de Datos.
- **Indicador de resultado:** Porcentaje de lineamientos y roles formalizados institucionalmente. **Meta 2028:** 100 % de lineamientos y roles formalizados.
- **Indicador de logro:** Porcentaje de dependencias que aplican los lineamientos de Gobierno de Datos. **Meta 2028:** ≥85 % de dependencias aplicando lineamientos institucionales.
- **Indicador de impacto:** Nivel de estandarización institucional de los procesos de gestión de datos. **Meta 2028:** ≥80 % de estandarización institucional de procesos asociados al dato.

Actividad 1.1.4. Actualización de procedimientos de clasificación y control de acceso

- **Responsables:** Administrador de Seguridad y Privacidad de la Información, Oficina TIC, Oficina Jurídica y Gestores de Datos.

- **Indicador de resultado:** Porcentaje de procedimientos críticos actualizados y vigentes. **Meta 2028:** 100 % de procedimientos críticos actualizados.

- **Indicador de logro:** Porcentaje de sistemas críticos con controles RBAC implementados. **Meta 2028:** ≥90 % de sistemas críticos con controles RBAC implementados.

- **Indicador de impacto:** Reducción de incidentes de acceso no autorizado. **Meta 2028:** Reducción ≥50 % de incidentes frente a la línea base 2026.

Actividad 1.1.5. Gestión integral de riesgos de datos

- **Responsables:** Administrador de Seguridad y Privacidad, Comité de Gobierno de Datos, Oficina Jurídica y Equipo Técnico de Gobierno de Datos.

- **Indicador de resultado:** Porcentaje de riesgos críticos identificados y documentados. **Meta 2028:** 100 % de riesgos críticos identificados.

- **Indicador de logro:** Porcentaje de riesgos con plan de mitigación activo y seguimiento periódico. **Meta 2028:** ≥90 % de riesgos con plan de mitigación activo.

- Indicador de impacto: Reducción del nivel institucional de riesgo asociado al tratamiento de datos. **Meta 2028:** Nivel de riesgo institucional ≤2,0 en escala 1–5.

Actividad 1.1.6. Sensibilización y capacitación en seguridad y privacidad

- **Responsables:** Administrador de Seguridad y Privacidad, Oficina de Comunicaciones, Talento Humano y Oficina TIC.

- **Indicador de resultado:** Número de campañas y jornadas de capacitación ejecutadas. **Meta 2028:** ≥6 campañas institucionales ejecutadas.

- **Indicador de logro:** Porcentaje de funcionarios que aprueban evaluaciones institucionales de seguridad y privacidad. **Meta 2028:** ≥85 % de funcionarios aprobando evaluaciones.

- **Indicador de impacto:** Reducción de incidentes ocasionados por error humano. **Meta 2028:** Reducción ≥40 % de incidentes asociados a error humano.

ii. Proyecto 1.2. Calidad, integración y ciclo de vida del dato

Actividad 1.2.1. Definición de estándares del ciclo de vida y catalogación de datos

- **Responsables:** Administrador de Gobierno de Datos, Equipo Técnico de Gobierno de Datos, Gestores de Datos de Dependencia y Líderes de Proceso.

- **Indicador de resultado:** Porcentaje de etapas del ciclo de vida con estándares institucionales definidos. **Meta 2028:** 100 % de etapas del ciclo de vida estandarizadas.

- **Indicador de logro:** Porcentaje de dominios institucionales con inventario actualizado y metadatos completos. **Meta 2028:** ≥90 % de dominios con inventario y metadatos completos.
- **Indicador de impacto:** Índice institucional de completitud de metadatos. **Meta 2028:** ≥85/100 en el índice institucional de completitud de metadatos.

Actividad 1.2.2. Implementación de controles de calidad para elementos de datos clave (KDE)

- **Responsables:** Equipo Técnico de Gobierno de Datos – Gestor de Calidad, Líderes de Proceso, Gestores de Datos de Dependencia y Administrador de Gobierno de Datos.

- **Indicador de resultado:** Número de elementos de datos clave (KDE) identificados y con reglas de calidad activas. **Meta 2028:** ≥50 KDE con reglas activas.

- **Indicador de logro:** Porcentaje de KDE

monitoreados mediante controles automatizados de calidad. **Meta 2028:** ≥90 % de KDE monitoreados automáticamente.

- **Indicador de impacto:** Índice institucional de calidad del dato (0–100). Meta 2028: ≥90/100 en el índice institucional de calidad del dato.

Actividad 1.2.3. Integración y reducción de redundancia de datos

- **Responsables:** Equipo Técnico de Gobierno de Datos, Oficina TIC y Líderes de Proceso.
- **Indicador de resultado:** Porcentaje de sistemas institucionales integrados a la arquitectura central de datos. **Meta 2028:** ≥80 % de sistemas institucionales integrados.
- **Indicador de logro:** Porcentaje de procesos institucionales interoperables mediante integración de datos. **Meta 2028:** ≥85 % de procesos interoperables.
- **Indicador de impacto:** Reducción institucional de redundancia y duplicidad de datos críticos. **Meta 2028:** Reducción ≥40 % de redundancia de datos frente a la línea base 2026.

6. MARCO NORMATIVO

La Política de Gobierno de Datos de la Universidad de Santander se fundamenta en un marco normativo de carácter internacional, nacional e institucional. Este marco proporciona el sustento jurídico y conceptual necesario para la implementación exitosa de las disposiciones aquí contenidas.

6.1. Referentes internacionales

Como referentes técnicos de carácter internacional, se han incorporado diversos marcos y estándares reconocidos en la disciplina de la gestión y gobernanza de datos. Entre ellos se encuentra la serie ISO/IEC 38505 (2017), que establece lineamientos para el gobierno de datos dentro del marco de la gobernanza de TI y cuyo uso ha sido validado internacionalmente.

Asimismo, se ha considerado el DAMA-DMBOK, documento aceptado a nivel global y publicado por DAMA International (2017), que reúne principios, prácticas y áreas funcionales esenciales para la administración de datos en organizaciones. De igual manera, se incorporan los principios y lineamientos de gobernanza de datos de la OCDE (2021), los cuales orientan a los gobiernos y organizaciones en el uso responsable, ético y eficiente de los datos, incluyendo directrices recientes en materia de acceso, intercambio y ética en el manejo de información.

6.2. Normativa nacional

En el ámbito nacional, como referencia está la Ley 1581 de 2012, que establece el régimen general de protección de datos personales (Congreso de la República de Colombia, 2012), y su Decreto Reglamentario 1377 de 2013, mediante los cuales se definen los principios, alcances y procedimientos para el tratamiento adecuado de la información personal (Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC], 2013). De igual forma, es vinculante el Decreto 1389 de 2022, que fija el marco de gobernanza de la infraestructura de datos en Colombia y constituye un referente clave para la estructuración del presente modelo (MinTIC, 2022).

También son relevantes la Ley 1712 de 2014, que regula la transparencia y el acceso a la información pública, fijando obligaciones de divulgación y apertura de datos por parte del Estado (Congreso de la República de Colombia, 2014), así como el Decreto 1078 de 2015 del sector TIC, que incorpora lineamientos asociados a la política de Gobierno Digital (MinTIC, 2015). A ello se suma la Directiva Presidencial 04 de 2012, orientada a promover la eficiencia administrativa y la política de "cero papel", directriz que guía la gestión documental y el uso racional de recursos en las entidades públicas (Presidencia de la República de Colombia, 2012).

En este marco normativo, se consideran además:

- Ley 1581 de 2012 – Protección de datos personales.
- Decreto 620 de 2020 – Lineamientos para el uso y aprovechamiento de los datos (MinTIC, 2020).

- Lineamientos generales para el uso de tecnologías emergentes – MinTIC (2022).
- Documento CONPES en materia de Inteligencia Artificial, que orienta el desarrollo y adopción responsable de esta tecnología en el país (Departamento Nacional de Planeación, 2025).
- Norma Técnica de la Calidad del Proceso Estadístico NTCPE 1000, aplicable a procesos institucionales que involucren producción y gestión de información estadística (Departamento Administrativo Nacional de Estadística [DANE], 2020).
- Norma Técnica Colombiana NTC-ISO-IEC 27001(2013-12-11). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (ICONTEC, 2013).

6.3. Marco institucional

En el ámbito interno de la Universidad, esta política se articula con la normatividad institucional vigente y debe interpretarse en concordancia con la Política de Seguridad de la Información de la UDES y la Política de Tratamiento de Datos Personales. Asimismo, mantiene coherencia con los objetivos y estrategias definidos en el Plan de Desarrollo Institucional, El Proyecto Educativo Institucional y con los lineamientos del Sistema de Gestión de la Calidad implementado en la Universidad.

Documentos institucionales relacionados:

- Universidad de Santander. (2026). Política de tratamiento de datos personales (REG-PI-001-UDES).
- Universidad de Santander. (2025). Organización de archivos de gestión y transferencias documentales (GED-GU-003-UDES).
- Universidad de Santander. (2025). Organización de archivo central y disposición final de los documentos (GED-IN-005-UDES).
- Universidad de Santander. (s.f.). Respaldo y restauración de la información (SEI-PR-003-UDES).
- Universidad de Santander. (2025). Uso adecuado y protección de la información (GED-PC-001-UDES).
- Universidad de Santander. (s.f.). Plan estratégico TIC: Gestión TIC.
- Universidad de Santander. (2021). Políticas y lineamientos institucionales de seguridad informática (VAF-PI-001-UDES).

7. DEFINICIONES

Para efectos de la correcta interpretación y aplicación de la presente política, se adoptan las siguientes definiciones que constituyen el glosario fundamental del Gobierno de Datos institucional.

- **Accesibilidad:** Condición que garantiza que los datos estén disponibles de forma oportuna para los usuarios autorizados, mediante mecanismos que faciliten su consulta y uso responsable, sin barreras tecnológicas o informativas innecesarias.
- **Calidad de Datos:** Grado en que los datos satisfacen los requisitos y expectativas de sus usuarios. Se evalúa mediante dimensiones como exactitud, completitud, consistencia, oportunidad y validez.
- **Ciclo de Vida de los Datos:** Conjunto de etapas por las que transitan los datos desde su creación o captura inicial hasta su archivo o eliminación definitiva. Incluye planificación, captura, almacenamiento, uso, mantenimiento, archivo y disposición final.
- **Curaduría de contenidos:** Proceso obligatorio de revisión, validación, edición y contextualización realizado por una persona sobre los resultados generados con apoyo de herramientas de Inteligencia Artificial, con el fin de garantizar su veracidad, calidad académica, pertinencia institucional y coherencia ética (CONPES 4144, 2025).
- **Dato:** Representación simbólica (numérica, alfabética, algorítmica, espacial u otra) que describe atributos o variables cuantitativas o cualitativas asociadas a hechos o entidades del mundo real o del quehacer institucional.
- **Datos Derivados:** Datos calculados o agregados a partir de datos maestros

o transaccionales, como indicadores, estadísticas, reportes consolidados y tableros de control.

- **Datos de Entrenamiento (Training Data):** Activos de información institucional o externa utilizados para enseñar, ajustar o validar un modelo de IA. En la UDES, el uso de estos datos está supeditado a los niveles de calidad y privacidad definidos en la Política de Gobierno de Datos.
- **Datos Maestros:** Datos fundamentales del negocio que se comparten entre múltiples sistemas y procesos, manteniendo su identidad y coherencia en toda la organización. Ejemplos: estudiantes, docentes, programas académicos.
- **Datos Transaccionales:** Datos generados por las operaciones diarias de la Universidad, que registran eventos o actividades específicas como inscripciones, calificaciones, pagos o asistencias.
- **Dominio de Datos:** Agrupación lógica de datos relacionados por área temática, proceso institucional o función organizacional. Ejemplos: dominio académico, dominio financiero, dominio de investigación.
- **Elemento de Dato Clave (Key Data Element:** KDE): Dato crítico cuya calidad afecta de manera significativa la operación institucional, la toma de decisiones o el cumplimiento de obligaciones normativas. Requiere controles reforzados por su alto nivel de riesgo o impacto.
- **Fuente Autorizada:** Sistema, repositorio o proceso designado formalmente como origen oficial y confiable de un conjunto específico de datos. Es responsable de su creación, actualización y mantenimiento.
- **Gobierno de Datos:** Conjunto articulado de normas, políticas, estándares, roles y responsabilidades que permiten gestionar, controlar y aprovechar los datos como activos estratégicos de la organización.
- **Infraestructura de Datos:** Conjunto de recursos tecnológicos, organizacionales y estandarizados que habilitan la provisión continua de datos para generar valor académico, investigativo y administrativo.
- **Interoperabilidad:** Capacidad de distintos sistemas, plataformas u organizaciones para intercambiar datos de manera efectiva, permitiendo su uso compartido y superando barreras tecnológicas, semánticas u organizacionales.
- **Metadatos:** Datos que describen otros datos, aportando información sobre su significado, estructura, origen, uso y relaciones. Facilitan su comprensión, localización y reutilización.
- **Múltiples partes interesadas:** conjunto de actores internos y externos que dependen del entorno digital y del uso de los datos para el desarrollo de sus funciones misionales e institucionales, entre ellos los órganos de gobierno, directivos, dependencias académicas y administrativas, docentes, estudiantes, graduados, aliados del sector público y privado y la comunidad en general.

8. ARTICULACIÓN CON EL PEI Y EL PDI

El Gobierno de Datos converge con el Proyecto Educativo Institucional (PEI 2023) al aportar los fundamentos técnicos y metodológicos que soportan la cultura de autorregulación, el aseguramiento de la calidad y la toma de decisiones basadas en evidencia. Mientras el PEI establece que la Universidad debe sustentar sus decisiones en información válida, análisis riguroso y procesos permanentes de autoevaluación, el Gobierno de Datos garantiza la disponibilidad, calidad, estandarización e interoperabilidad de los datos necesarios para medir el aprendizaje, evaluar la efectividad curricular, comprender el impacto social y fortalecer los procesos de investigación y extensión.

En coherencia con la misión, visión y principios institucionales, también materializa valores como la responsabilidad en el uso ético del dato, la excelencia reflejada en la confiabilidad de la información, y la cooperación mediante la articulación entre dependencias.

De manera complementaria, el Gobierno de Datos se alinea con el Plan de Desarrollo Institucional

2024–2028, orientado a la transformación educativa y digital de la Universidad. El PDI destaca la importancia de contar con sistemas de información robustos, capacidades de analítica avanzada y modelos de automatización que permitan caracterizar a los estudiantes, monitorear sus trayectorias académicas, medir el valor agregado institucional y hacer seguimiento a los indicadores estratégicos.

En este sentido, el Gobierno de Datos actúa como soporte estructural de dicha transformación al definir estándares, roles y procesos que aseguran gobernanza, trazabilidad y consistencia en la gestión de los datos. Asimismo, contribuye a la sostenibilidad y la transparencia institucional al proporcionar información confiable para la rendición de cuentas, la toma de decisiones estratégicas y la articulación con actores externos.

A ello se suma el Plan Estratégico de Gestión TIC, que establece la infraestructura tecnológica, los sistemas de información y los lineamientos operativos necesarios para garantizar la calidad, seguridad, disponibilidad e interoperabilidad de los datos.

Este plan, alineado con el PEI y el PDI, impulsa la modernización de centros de datos, la estandarización del cableado y equipamiento de red, la actualización de plataformas y el fortalecimiento de los subprocesos de sistemas, infraestructura y seguridad informática; elementos que constituyen la base operativa sobre la cual el Gobierno de Datos ejerce su función.

El Gobierno de Datos se articula con la Política de Seguridad y Privacidad de la Información (SEI) al asegurar que los datos institucionales se gestionen como activos protegidos bajo criterios de integridad, disponibilidad, confidencialidad y cumplimiento normativo. Mientras la Política SEI establece los lineamientos, controles y prácticas de seguridad, el Gobierno de Datos complementa estas disposiciones definiendo roles adicionales relacionados con la custodia, administración, calidad y operación del dato, y armonizando sus modelos con los requisitos de protección de datos personales y las buenas prácticas de seguridad.

En conjunto, ambos instrumentos garantizan que los flujos de información institucional sean seguros, trazables, confiables y responsables, fortaleciendo así el ecosistema de información que soporta la función misional y el desarrollo estratégico de la Universidad.

9. COMPROMISO CON LOS ODS

La Política de Gobierno de Datos de la Universidad de Santander contribuye al cumplimiento de los Objetivos de Desarrollo Sostenible al fortalecer la toma de decisiones basada en evidencia, el aseguramiento de la calidad académica, la innovación institucional y la transparencia en la gestión.

En particular, aporta al ODS 4: Educación de calidad, al facilitar el seguimiento a los resultados de aprendizaje, la permanencia y graduación estudiantil y el mejoramiento continuo de los procesos formativos, en coherencia con las metas 4.3 (acceso a la educación superior de calidad), 4.4 (desarrollo de competencias para el empleo y el emprendimiento) y 4.7 (educación para el desarrollo sostenible).

Asimismo, contribuye al ODS 9: Industria, innovación e infraestructura, mediante la consolidación de la infraestructura de datos, la interoperabilidad de los sistemas de información y el fortalecimiento de las capacidades analíticas para la investigación, la innovación y la transformación digital institucional, en correspondencia con las metas 9.5 (fomento de la investigación y la innovación) y 9.c (acceso y uso de las tecnologías de la información y las comunicaciones).

En relación con el ODS 16: Paz, justicia e instituciones sólidas, el Gobierno de Datos promueve la transparencia, la trazabilidad de la información y la gestión eficiente y responsable de los datos como activos institucionales, aportando a las metas 16.6 (instituciones eficaces y transparentes) y 16.10 (acceso a la información).

Finalmente, se articula con el ODS 17: Alianzas para lograr los objetivos, al facilitar el intercambio seguro y estandarizado de información con entidades del sector público, el sector productivo, redes

académicas y aliados estratégicos, contribuyendo a la meta 17.18 (fortalecimiento de la disponibilidad de datos oportunos y de calidad) y al desarrollo de procesos colaborativos basados en información confiable.

10. DOCUMENTOS DE REFERENCIA (SI APLICA)

Congreso de la República de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (2014). Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Consejo Nacional de Política Económica y Social. (2023). CONPES 4144. Política nacional de inteligencia artificial. Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf

DAMA International. (2017). DAMA-DMBOK: Data management body of knowledge (2.ª ed.). Technics Publications.

Departamento Administrativo Nacional de Estadística. (2020). Norma Técnica de la Calidad del Proceso Estadístico NTC PE 1000. DANE. https://www.dane.gov.co/files/sen/normatividad/NTC-Proceso-Estadistico-PE-1000-2020.pdf

Departamento Nacional de Planeación & Consejo Nacional de Política Económica y Social. (2025). Política Nacional de Inteligencia Artificial (Documento CONPES 4144). https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf

Instituto Colombiano de Normas Técnicas y Certificación. (2013). NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. ICONTEC. https://www.contaduria.gov.co/documents/115223/5709447/NTC +ISO +IEC +27001+2013.pdf/d25e4542-1170-2318-abe9-9e7702e66b79?t=1700170285016

International Organization for Standardization & International Electrotechnical Commission. (2017). Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data (ISO/IEC Standard No. 38505-1:2017). https://www.iso.org/obp/ui/#iso:std:iso-iec:38505:-1:ed-1:v1:en

Mieles, G., & Navia, M. (2026). Aplicación de la inteligencia artificial en el Internet de las Cosas: un estudio documental. MASKAY, 16(1), 1-8. https://doi.org/10.24133/maskay.v16i1.4161

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTic]. (2013). Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015). Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTic]. (2020). Decreto 620 de 2020. Por el cual se subroga el Capítulo 4 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, en relación con los lineamientos para el uso y operación de los datos abiertos. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=118337

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2022). Decreto 1389 de 2022. Por el cual se establece el marco de gobernanza de la infraestructura de datos en Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=191409

Organisation for Economic Co-operation and Development. (2021). Good practice principles for data ethics in the public sector. OECD. https://www.oecd.org/content/dam/oecd/

en/publications/reports/2021/03/oecd-good-practice-principles-for-data-ethics-in-the-public-sector_7a36f20d/caa35b76-en.pdf

Parra-González, E. F., Jaramillo-Avila, U., Salazar-Linares, P., & Lara-Álvarez, C. A. (2023). Tendencias y desafíos de la computación de alto rendimiento en la nube. Revista Ibérica de Sistemas e Tecnologias de Informação, (49), 131-146. https://doi.org/10.17013/risti.49.131-146

Presidencia de la República de Colombia. (2012). Directiva Presidencial 04 de 2012. Eficiencia administrativa y lineamientos de la política cero papel en la administración pública. Departamento Administrativo de la Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50155

Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial No. 48.834.

Universidad de Santander. (2023a). Proyecto Educativo Institucional PEI 2023. https://repositorio.udes.edu.co/handle/001/10147

Universidad de Santander. (2023b). Plan de Desarrollo Institucional 2024-2028. https://udes.edu.co/images/la_universidad/documentos/plan-desarrollo-institucional-2024-2028-udes.pdf

Universidad de Santander. (2021). Resolución No 028. Por medio del cual se actualiza la Política de Tratamiento de Datos Personales de la Universidad de Santander. Secretaría General. https://udes.edu.co/images/2021/BUC/documentos/resolucion-politica-tratamiento-datos-personales-2021.pdf

Universidad de Santander. (s.f.-a). Política institucional de seguridad y privacidad de la información (SEI). https://udes.edu.co/images/micrositios/gestion-tic/seguridad_informatica/politicas_institucionales_SEI.pdf

Universidad de Santander. (2026). Política de tratamiento de datos personales (REG-PI-001-UDES).

Universidad de Santander. (2025). Organización de archivos de gestión y transferencias documentales (GED-GU-003-UDES).

Universidad de Santander. (2025). Organización de archivo central y disposición final de los documentos (GED-IN-005-UDES).

Universidad de Santander. (s.f.). Respaldo y restauración de la información (SEI-PR-003-UDES).

Universidad de Santander. (2025). Uso adecuado y protección de la información (GED-PC-001-UDES).

Universidad de Santander. (s.f.). Plan estratégico TIC: Gestión TIC.

Universidad de Santander. (2021). Políticas y lineamientos institucionales de seguridad informática (VAF-PI-001-UDES).

11. ANEXOS (SI APLICA)

Se incorpora como anexo la representación gráfica de la estructura institucional de Gobierno de Datos de la Universidad de Santander.

Universidad de Santander UDES
VIGILADA MINEDUCACIÓN | SNIES 2832

ACREDITADA ALTA CALIDAD
Ministerio de Educación Nacional
RES. 023456 15/12/21

ACREDITACIÓN INTERNACIONAL EQUAA
Education Quality Accreditation Agency

Estructura Gobierno de Datos

Es un conjunto de procesos, funciones, mediciones, normas, políticas y procedimientos que garantizan el uso seguro, eficaz y eficiente de la información para apoyar en la toma de decisiones de la Institución.

Estrategia

- Visión y mision
- Objetivos y metas institucionales
- Alineación con PEI - PDI
- Alineamiento con las operaciones institucionales
- Principios clave para el buen gobierno de datos

Instancias del modelo de la gobernanza de la infraestructura de datos

Nivel Estratégico

Define la dirección, las políticas y las prioridades institucionales

- Consejo Superior
- Rectoría General
- Comité Institucional de Gobierno de Datos

Nivel Táctico

Traduce la estrategia en planes, lineamientos y control de gestión

- Administrador del Gobierno de Datos – CDO
- Jefe de la Oficina de TI
- Líder de Seguridad y Privacidad de la Información
- Directores y Jefes de dependencia (Líderes de proceso)

Nivel Operativo

Implementa los lineamientos y gestiona los datos en los procesos

- Gestores de datos de las dependencias
- Equipo técnico de Gobierno de Datos:
  Calidad de datos
  Arquitectura e integración
  Analítica y explotación de datos

Soporte Transversal

Acompañan el cumplimiento normativo, la gestión del cambio y la cultura de datos.

- Jurídica
- Comunicaciones
- Talento Humano
- Comité de Bioética

Ciclo de vida de los datos

Planeación	Recopilación	Procesamiento	Análisis	Publicación	Preservación	Eliminación
Definir políticas, necesidades y lineamientos para la gestión institucional de los datos.	Recolección de datos según objetivos institucionales y criterios de calidad.	Depuración y estructuración de datos para su uso y seguimiento estratégico.	Interpretación de los datos para generar información y orientar decisiones institucionales.	Divulgación de información en formatos accesibles para diferentes usuarios.	Almacenamiento seguro para garantizar disponibilidad, integridad y trazabilidad en el tiempo.	Eliminación segura conforme a políticas de retención y protección de datos.

Administración y Servicios de Gestión de datos

- Arquitectura de datos
- Seguridad de la información
- Almacenamiento y respaldo de la información
- Integración y transformación de datosmiento nde datos
- Gestión de metadatos datos
- Calidad del dato
- Gestión y evaluación de riesgos de datos
- Privacidad y protección de datos personales
- Cumplimiento normativo y ética institucional
- Analítica institucional y reporte

Gerencia del cambio

- Evaluación de impacto y preparación
- Alineación de liderazgo
- Manejo de las partes interesadas
- Listas de verificación para planeación de cambios e implementación
- Transición a la sostenibilidad

Principios éticos del buen Gobierno

- Responsabilidad
- Calidad
- Transparencia
- Accesibilidad
- Interoperabilidad

→ Confidencialidad
→ Integridad
→ Disponibilidad

Gestión del Conocimiento y Comunicación

- Datos estandarizados
- Informes
- Consultas
- Estrategia de Comunicación
- Plan de capacitación

Grupos de Interés

Internos:
Consejo Superior
Consejo Académico
Comité Rectoral
Decanaturas
Direcciones de programas
Estudiantes
Graduados
Unidades administrativas
Unidades de apoyo

Externos:
Ministerio de Educación Nacional (MEN)
Otras dependencias no Gubernamentales

Marco Legal

ISO/IEC 38505-1 (2017)
ISO/IEC 27001
DAMA-DMBOK 2 (2017)
Ley 1581 de 2012
Ley 1712 de 2014
Decreto 1389 de 2022
Política de Tratamiento de Datos Personales – REG PI 001
Política Institucional de Seguridad y Privacidad de la Información – SEI
Plan de Desarrollo Institucional – PDI 2024–2028

Métricas

- Análisis y estadísticas
- Métricas de desempeño (Indicadores estratégicos de seguimiento, monitoreo y control a metas Institucionales)
- Mejora continua

Proyecto: Planeación Institucional 2026

Herramientas

SIGA UDES, SIGNP, moodle, KAWAK, +tableau, zenodo, MENDELEY, Canva, genially, koha, GitHub, Power BI, R Studio, DMP Tool, Office 365


Universidad de Santander
UDES
VIGILADA MINEDUCACIÓN | SNIES 2832