BOLETÍN DE CUMPLIMIENTO 2026

PROTECCIÓN DE DATOS PERSONALES Y SAGRILAFT

UNIVERSIDAD SANTO TOMÁS

BOLETÍN DE CUMPLIMIENTO 2026
PROTECCIÓN DE DATOS PERSONALES Y SAGRILAFT
UNIVERSIDAD SANTO TOMÁS

1. INTRODUCCIÓN

La transformación digital se consolida como una realidad operativa que impacta de manera transversal los procesos académicos, administrativos, tecnológicos y de relacionamiento institucional. En este contexto, el tratamiento de datos personales, especialmente a través de sistemas automatizados e inteligencia artificial, representa uno de los principales retos para las instituciones de educación superior.

La protección de datos personales se integra y fortalece como un elemento esencial de la gobernanza institucional, la ética organizacional y la gestión del riesgo, directamente relacionado con la confianza de estudiantes, docentes, egresados, colaboradores y aliados estratégicos.

Durante la vigencia 2026, la Universidad Santo Tomás adelanta su gestión en un entorno normativo caracterizado por una mayor exigencia regulatoria, la adopción de modelos de responsabilidad demostrada (*accountability*), la supervisión de la Superintendencia de Industria y Comercio, la regulación emergente sobre inteligencia artificial y las reformas en curso al régimen de protección de datos personales en Colombia.

En este marco, el presente Boletín de Cumplimiento 2026 tiene por objeto exponer los ejes estratégicos en materia de protección de datos personales, orientados a anticipar riesgos, fortalecer la gobernanza de la información y consolidar un modelo de cumplimiento proactivo, alineado con las mejores prácticas nacionales e internacionales.

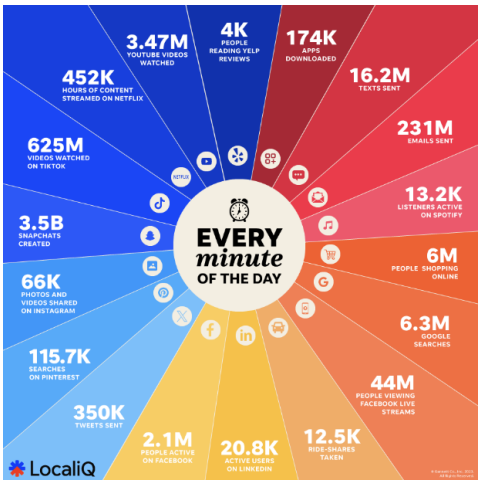
PARTE I - PROTECCIÓN DE DATOS PERSONALES

2. PANORAMA 2026

En este escenario, la gestión de la protección de datos personales opera durante 2026 como un eje transversal de la toma de decisiones institucionales y del fortalecimiento de los esquemas de cumplimiento y control.

Desde esta perspectiva, la Superintendencia de Industria y Comercio fortalece su enfoque de supervisión, privilegiando modelos de responsabilidad demostrada (accountability) y cumplimiento proactivo. Como reflejo de esta tendencia, durante el año 2025 la autoridad de control impuso sanciones por un valor aproximado de $2.168 millones de pesos, lo que refuerza la necesidad institucional de de adoptar y mantener medidas técnicas, administrativas y organizacionales efectivas que garanticen la protección de los derechos de los titulares y la sostenibilidad del cumplimiento normativo.

3. EL MINUTO DE INTERNET Y LA PROTECCIÓN DE DATOS PERSONALES[1]



Infografía What Happens in an Internet Minute?, LocaliQ, Susie Marino, actualización 14 de enero de 2026. Disponible en: https://localiq.com/blog/what-happens-in-an-internet-minute/

Cada minuto en internet se generan millones de interacciones en redes sociales, buscadores, plataformas digitales y comercios electrónicos. Cada una de estas acciones implica el tratamiento de datos personales, como información de identificación, contacto, hábitos, preferencias y ubicación, muchas veces de forma automatizada y a gran escala.

Este alto nivel de actividad digital incrementa los riesgos asociados al uso indebido de la información, accesos no autorizados y pérdida de control por parte de los titulares.

En este contexto, las instituciones tienen una responsabilidad reforzada de garantizar un tratamiento de datos personales legal, seguro, transparente y acorde con la finalidad informada, como base de la confianza y del cumplimiento normativo.

7. RETOS CLAVE EN PROTECCIÓN DE DATOS PARA LA UNIVERSIDAD

7.1 AUTORIZACIONES Y FINALIDADES DEL TRATAMIENTO

Uno de los principales focos de riesgo identificados por la autoridad de control se relaciona con el tratamiento de datos personales sin autorización válida o para finalidades no informadas al titular. Las autorizaciones incompletas, desactualizadas o genéricas continúan siendo una de las principales causas de sanción en Colombia.

Reto 2026: Fortalecer los mecanismos de obtención, gestión, actualización y trazabilidad de las autorizaciones, garantizando que el uso de la información sea coherente con las finalidades

[1] https://localiq.com/blog/what-happens-in-an-internet-minute/

informadas y con el principio de transparencia.

7.2 RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

La legislación colombiana distingue dos figuras jurídicas en el tratamiento de datos personales. La primera, es denominada **responsable del tratamiento,** y la segunda, **encargado del tratamiento** (Ley 1581- Art. 3).

Responsable	Encargado
Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

Los aspectos particulares de estas figuras, es que el Encargado no decide en ningún momento el tratamiento que dará a los datos que trate, pues todo lo realiza bajo las indicaciones e instrucciones que otorga el responsable. Por lo que, cualquier operación que realice el encargado, se entiende efectuada bajo una especie de mandato o encargo del responsable.

Por regla general, cuando un encargado desarrolla operaciones con un responsable, se suele suscribir un contrato de transmisión de datos.

En este sentido, ***el Responsable del tratamiento*** es quien define de manera autónoma las finalidades y los medios del tratamiento de los datos personales, mientras que ***el Encargado del tratamiento*** actúa exclusivamente por cuenta del responsable, siguiendo sus instrucciones y sin poder decidir de forma independiente sobre el uso de la información.

Cualquier actuación realizada por el Encargado se entiende jurídicamente efectuada bajo el ámbito de responsabilidad del Responsable, sin perjuicio de las obligaciones propias que la ley asigna a cada una de estas figuras.

7.3 DERECHO DE IMAGEN

En el tratamiento de imágenes de personas naturales, es fundamental distinguir entre dos categorías jurídicas que, aunque relacionadas, no son equivalentes: Por un lado, el dato personal (cuando la imagen permite identificar a la persona se entenderá dato personal), y por otro, el derecho fundamental a la imagen, que tiene contenido y protección propia.

Conforme al literal c del artículo 3 de la Ley 1581 de 2012, un dato personal es “cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”, y, según el artículo 5 ibídem, la imagen puede ser considerada un dato sensible cuando contiene información biométrica que permite identificar físicamente a una persona.

Así lo ha reconocido la Superintendencia de Industria y Comercio:

> *"Algunas fotos captan la imagen de la cara de las personas u otras partes de su cuerpo que permiten identificarlas. Estas imágenes se consideran información biométrica… y, por tanto, datos sensibles".*

Por otro lado, el derecho a la imagen es un derecho fundamental autónomo, protegido por los artículos 14 y 15 de la Constitución Política, que reconoce a toda persona la facultad de autorizar o no el uso, reproducción o divulgación de su imagen en medios físicos, digitales, publicitarios o institucionales. La Corte Constitucional ha señalado que este derecho constituye una expresión directa de la individualidad e identidad de la persona y es exigible de manera independiente, aun cuando pueda relacionarse con otros derechos como la intimidad o el buen nombre.

- ***Autorización para el tratamiento del dato personal (imagen como rasgo identificable):*** Debe ser previa, expresa e informada, conforme al artículo 9 de la Ley 1581 de 2012.
- ***Autorización para el uso de imagen con fines específicos (reproducción, circulación, promoción, etc.):*** Debe ser clara, voluntaria e inequívoca, en función de los usos que se pretenden.

En este sentido, una fotografía o video puede contar con una doble protección jurídica: como dato personal y como manifestación del derecho a la imagen. En consecuencia, el uso institucional o publicitario de imágenes requiere la obtención de autorizaciones diferenciadas, aunque estas puedan otorgarse en un mismo instrumento, tanto para el tratamiento del dato personal como para la utilización de la imagen conforme a la finalidad informada.

Incluso cuando una persona consiente la captura de su imagen, dicho consentimiento no habilita de forma automática su uso público o promocional, por lo que resulta indispensable contar con autorizaciones claras, específicas y coherentes con los fines para los cuales se pretende utilizar la imagen, especialmente en contextos de alta visibilidad o proyección institucional.

En el contexto universitario, este derecho adquiere especial relevancia en el desarrollo de actividades académicas, eventos institucionales, prácticas, proyectos de proyección social y estrategias de divulgación, por lo que resulta indispensable asegurar que el uso de imágenes se encuentre debidamente autorizado, sea coherente con la finalidad informada y respete la dignidad y los derechos fundamentales de las personas.

7.4 DATOS BIOMÉTRICOS

Los datos biométricos son aquellos datos personales referidos a las características físicas, fisiológicas o conductuales de una persona natural, que permiten su identificación o autenticación de manera única y medible. Debido a su naturaleza, estos datos suelen calificarse como datos sensibles, por cuanto su uso indebido puede afectar de forma significativa los derechos fundamentales del titular.

El tratamiento de datos biométricos debe sujetarse estrictamente a los principios de necesidad y proporcionalidad, lo que implica que solo podrán ser recolectados y utilizados cuando resulten indispensables para la finalidad legítima previamente informada, y siempre en la medida estrictamente necesaria para cumplir dicha finalidad, evitando tratamientos excesivos, invasivos o desproporcionados frente al objetivo perseguido.

En este sentido, la implementación de mecanismos biométricos debe estar debidamente justificada, demostrando que no existen otros medios menos intrusivos que permitan alcanzar el mismo fin, y garantizando la adopción de medidas técnicas, jurídicas y administrativas reforzadas para su protección.

Los datos biométricos presentan, entre otras, las siguientes características:

- **Universal**: existen en todas las personas sin distinción.
- **Único**: son distinguibles en cada individuo.
- **Permanente**: se mantienen de forma continua en el tiempo.

GRUPOS DE DATOS BIOMÉTRICOS:

1-CARACTERÍSTICAS FÍSICAS Y FISIOLÓGICAS

- Huella dactilar
- Reconocimiento facial
- Reconocimiento de iris
- Geometría de la mano
- Reconocimiento de retina
- Reconocimiento vascular

2-CARACTERÍSTICAS DEL COMPORTAMIENTO Y LA PERSONALIDAD

- Reconocimiento de firma
- Reconocimiento de escritura
- Reconocimiento de voz
- Reconocimiento de escritura de teclado
- Reconocimiento de la forma de andar

7.5 TRATAMIENTO DE DATOS DE NIÑOS, NIÑAS Y ADOLESCENTES

El tratamiento de datos personales de menores de edad está sujeto a una protección reforzada. La regulación vigente y los proyectos de reforma introducen mayores exigencias en materia de consentimiento, proporcionalidad y finalidad, así como restricciones expresas frente a la elaboración de perfiles.

En el entorno universitario, este riesgo se presenta especialmente en actividades académicas, de extensión, proyección social, eventos institucionales, prácticas, y el uso de plataformas digitales.

Reto 2026: Asegurar controles diferenciados para el tratamiento de datos de menores de edad, con especial atención a la obtención del consentimiento, la finalidad del tratamiento y la protección del interés superior del menor de edad.

PARTE II – SAGRILAFT

La lucha contra el Lavado de Activos y la Financiación del Terrorismo es una constante en los últimos años, lo que implica la necesidad de adoptar sistemas de prevención de riesgos, no sólo para evitar sanciones o dar cumplimiento a la normativa legal, sino para promover las buenas prácticas y limitar los efectos adversos que pueden provocar indistintamente estos delitos. En armonía con su contexto, la Universidad Santo Tomás, comprendiendo que dentro del giro ordinario de sus operaciones existe cierto nivel de riesgo reputacional, financiero y legal, prevé la adopción de un sistema **SAGRILAFT** al interior de la Institución y de alcance multicampus. De esta manera la Universidad cuenta con un mayor respaldo en cuanto a la implementación de políticas y procedimientos que le permiten actuar con prevención e identificar alertas tempranas cuya intención será siempre la detección anticipada de riesgos y la toma de decisiones mejor informadas, basadas en el conocimiento de sus contrapartes.

11. PANORAMA GENERAL SAGRILAFT 2026

La gestión del riesgo de lavado de activos, financiación del terrorismo y proliferación de armas de destrucción masiva continúa siendo una prioridad para las autoridades de supervisión. En 2026 se mantiene la tendencia hacia una mayor exigencia en la debida diligencia, la identificación del beneficiario final y la efectividad de los controles internos.

11.1 ALGUNAS SANCIONES QUE SE HAN IMPUESTO

RESOLUCIÓN	CONDUCTA SANCIONADA PRINCIPAL	SANCIÓN
2025-01-446210JUANCAMAR Y CIA S. EN C.	No implementó adecuadamente el SAGRILAFT; no realizó gestión de riesgos; omitió debida diligencia y no reportó operaciones sospechosas (ROS).	$98.712.000
240-301404 / 2025-01-009655PLAZA MAYOR DE MEDELLÍN CONVENCIONES Y EXPOSICIONES S.A.	Implementó extemporáneamente el SAGRILAFT (retraso de ocho meses en la adopción del manual y ejecución del sistema).	$15.000.000

240-300190 / 2024-01-951756METALES Y MADERAS DEL RISARALDA S.A	No cumplió el plazo para implementar el PTEE; no identificó, evaluó ni controló riesgos de soborno transnacional; no estableció procesos de debida diligencia.	$66.000.000
2024-01-637008 / 2025-01-037688 CONCENTRIX CVG CUSTOMER MANAGEMENT COLOMBIA S.A.S.	No diseñó ni aprobó el PTEE; incumplió órdenes sobre auditoría, capacitación, canales de denuncia y funciones del Oficial de Cumplimiento; sin procesos de debida diligencia frente a riesgos de corrupción y soborno transnacional.	$88.000.000
2023-01-917478KOPPS COMERCIAL S.A.S.	No aprobó el PTEE dentro del plazo; no implementó elementos mínimos; no identificó, evaluó ni controló riesgos de soborno transnacional.	$505.000.000
2024-01-277337 YARA COLOMBIA S.A.	No aprobó el PTEE conforme a los procedimientos; no realizó debida diligencia; omitió identificación y evaluación de riesgos de corrupción y soborno transnacional.	$100.000.000

12. RETOS SAGRILAFT PARA LA UNIVERSIDAD

AML Protektor. (s. f.). ¿Qué es y quiénes están obligados a implementar SAGRILAFT – Supersociedades? https://www.amlprotektor.com/que-es-y-quienes-estan-obligados-a-implementar-sagrilaft-supersociedades/

El análisis de los procesos sancionatorios recientes, así como la experiencia derivada de la gestión institucional del **SAGRILAFT,** permite identificar patrones reiterados de incumplimiento en organizaciones vigiladas, los cuales constituyen insumos clave para la

definición de retos estratégicos de cumplimiento.

En términos generales, las sanciones impuestas por las autoridades no se originan en la ausencia total del sistema, sino en fallas relacionadas con su implementación deficiente, aplicación tardía o falta de efectividad real.

12.1 DEBIDA DILIGENCIA DE TERCEROS

Financial Crime Academy. (2025, noviembre 27). *Tipos de diligencia debida sobre el cliente: Tipos importantes de* DDC https://financialcrimeacademy.org/es/tipos-de-diligencia-debida-sobre-el-cliente-tipos-importantes-de-ddc/

Un número significativo de sanciones se relaciona con deficiencias en los procesos de debida diligencia frente a proveedores, contratistas, aliados estratégicos, y contrapartes relevantes.

Reto 2026: robustecer los procedimientos de conocimiento, verificación y seguimiento de terceros, asegurando coherencia entre la información suministrada, la naturaleza de la relación y el nivel de riesgo identificado.

Este reto implica reconocer que los procesos de debida diligencia demandan una dedicación permanente de tiempo y recursos, especialmente en un entorno multicampus, en el que se requiere continuidad en el conocimiento de las relaciones contractuales ya suscritas y de aquellas que se proyectan celebrar.

12.2 IMPLEMENTACIÓN EFECTIVA Y TRANSVERSAL DEL SAGRILAFT

AQUIA. (2023, febrero 3). Obligación implementación SAGRILAFT en 2023 https://aquia.co/2023/02/03/obligacion-implementacion-sagrilaft-en-2023/

Uno de los principales motivos de sanción es la adopción meramente formal del **SAGRILAFT**, sin una aplicación real en los procesos organizacionales.

Reto 2026: Asegurar que el **SAGRILAFT** opere como un sistema efectivo, actualizado y transversal, integrado a los procesos académicos, administrativos, contractuales y de relacionamiento institucional.

12.3 GESTIÓN INTEGRAL Y DEMOSTRABLE DEL RIESGO LA/FT/FPADM

G5 Integritas. (2020, noviembre 13). *Los estándares internacionales sobre LA, FT y FPADM* https://g5integritasblog.wordpress.com/2020/11/13/los-estandares-internacionales-sobre-la-ft-y-fpadm/

Las autoridades han sancionado de manera reiterada a entidades que no identificaron, evaluaron ni controlaron adecuadamente los riesgos asociados a **LA/FT/FPADM**.

Reto 2026: Fortalecer la metodología de identificación, medición, control y monitoreo del riesgo, garantizando su actualización periódica y la existencia de evidencia clara y verificable de su aplicación.

En el contexto institucional, este reto se acentúa por la necesidad de consolidar la identificación y evaluación de los riesgos específicos de cada área, dependencia y sede, teniendo en cuenta las particularidades operativas del modelo multicampus y la incorporación de nuevas actividades y relaciones institucionales.

12.4 IDENTIFICACIÓN DEL BENEFICIARIO FINAL

Bresciani, P. (2023, agosto 31). *Beneficiario Final, ¿Qué es?, ¿Por qué?, ¿Para qué?* LinkedIn. https://www.linkedin.com/pulse/beneficiario-final-qu%C3%A9-es-por-para-pablo-bresciani/

La falta de identificación adecuada y actualizada del beneficiario final constituye una infracción recurrente en los procesos sancionatorios.

Reto 2026: Garantizar la obtención, verificación y actualización de la información del beneficiario final en las relaciones jurídicas que así lo exijan, conforme a la normativa vigente.

12.5 REPORTE DE OPERACIONES SOSPECHOSAS (ROS)

Moreno López, I. (2025, noviembre 11). *Señales de alerta temprana: KPI´s clave de actividad anómala*. UBT Compliance. https://ubtcompliance.com/blog/indicadores-para-detectar-actividades-sospechosas-y-protocolos-de-respuesta/

La omisión en el reporte de operaciones sospechosas es considerada una de las conductas más graves por las autoridades de supervisión.

Reto 2026: Fortalecer la cultura institucional de reporte, asegurando que las áreas y colaboradores conozcan los canales internos, los criterios de alerta y la relevancia del ROS como herramienta preventiva.

12.6 EVIDENCIA, TRAZABILIDAD Y SOSTENIBILIDAD DEL SISTEMA

Affirma Legal, SAGRILAFT: ¿Qué es y cómo debe ser implementado por las empresas?, junio de 2025. https://www.affirmalegal.com/blog/que-es-sagrilaft-y-como-debe-ser-implementado/

Las autoridades han incrementado sus exigencias en materia de soportes, trazabilidad y demostración del cumplimiento.

Reto 2026: Fortalecer los mecanismos de documentación, archivo y trazabilidad de las actuaciones del **SAGRILAFT**, garantizando la sostenibilidad del sistema y su capacidad de respuesta ante requerimientos de supervisión.

12.7 CULTURA ORGANIZACIONAL Y ENFOQUE PREVENTIVO EN SAGRILAFT

Cámara de Comercio de Pereira, Programas de Prevención de Lavado de Activos (SAGRILAFT) y de Transparencia y Ética Empresarial (PTEE), 26 de octubre de 2021. https://www.camarapereira.org.co/es/programas-de-prevencion-de-lavado-de-activos-sagrilaft-y-de-transparencia-y-etica-empresarial-ptee-una-obligacion-que-no-puede-pasar-desapercibida-EV2612

La efectividad del **SAGRILAFT** no depende únicamente del diseño del sistema o de la adopción de políticas, sino de su apropiación real por parte de la comunidad institucional.

Reto 2026: Fortalecer una cultura organizacional con enfoque preventivo frente a los riesgos de **LA/FT/FPADM,** promoviendo la corresponsabilidad de las áreas y colaboradores en la identificación temprana de alertas y el uso de los canales de reporte.

Durante la vigencia 2026, la gestión **SAGRILAFT** se apoya en la ejecución de jornadas de preauditoría en las sedes y seccionales, la normalización de políticas y lineamientos pendientes, y la realización de consultas masivas de información contenida en las bases de datos institucionales, como herramientas clave para el fortalecimiento preventivo del sistema.

13. CONCLUSIÓN

La Universidad Santo Tomás reafirma su compromiso con una cultura institucional de cumplimiento, fundamentada en la legalidad, la transparencia y la gestión preventiva de riesgos. La adecuada protección de los datos personales y la implementación efectiva del **SAGRILAFT** constituyen elementos esenciales para el fortalecimiento de la confianza, la sostenibilidad institucional y el desarrollo responsable de sus actividades académicas, administrativas y de relacionamiento, en coherencia con el marco normativo vigente y las buenas prácticas de gobierno institucional.