DANE
INFORMACIÓN PARA TODOS

REVISIÓN DE REFERENTES INTERNACIONALES

El futuro es de todos
Gobierno de Colombia

DIRECCIÓN DE REGULACIÓN, PLANEACIÓN, ESTANDARIZACIÓN Y NORMALIZACIÓN (DIRPEN)

REVISIÓN DE REFERENTES INTERNACIONALES

1. **Buenas prácticas en el marco de gestión documental para los sistemas de almacenamiento (*backup*) y seguridad informática.**

2. **Buenas prácticas de las Instituciones Públicas para garantizar la propiedad intelectual sobre la divulgación de productos de investigación, desarrollo e innovación.**

3. **Reseña del documento Directrices Para La Elaboración De Una Estrategia De Comunicación.**

4. **Evento de la 70.ª sesión plenaria de la Conferencia de Estadísticos Europeos.**

5. **Evento de la 19.ª reunión del Comité de Estadística y Política Estadística – CSSP.**

Junio de 2022

Tabla de contenido

Lista de tablas

Lista de ilustraciones

Introducción

Este reporte tiene el propósito de apoyar el conocimiento, la generación de capacidades, brindar recomendaciones y propiciar acciones acordes a las necesidades temáticas relevantes del Departamento Administrativo Nacional de Estadística - DANE y del Sistema Estadístico Nacional - SEN. A partir de una revisión prospectiva que involucra referentes internacionales de diferente naturaleza y el rol en el ecosistema de datos, incluyendo, oficinas nacionales de estadística - ONE, organizaciones no gubernamentales e institutos de investigación, ente otros.

Con ello, se busca enriquecer los trabajos que se vienen desarrollando al interior de las diferentes áreas técnicas del DANE y las instancias de coordinación del SEN considerados prioritarios en concordancia con el Plan Estratégico Institucional, las agendas de trabajo e investigación y la captura de necesidades temáticas.

Para tal fin, la revisión de referentes constituye una investigación prospectiva de la práctica internacional, en función del tema de análisis, de organizaciones de diferente naturaleza y rol en un ecosistema de datos estadísticos, incluyendo: institutos u oficinas nacionales de estadística, organizaciones no gubernamentales e instituciones académicas o de investigación. Los temas que se abordan en cada reporte mensual se priorizan, considerando la urgencia de la necesidad, de una lista de temas construida a partir de la consulta directa realizada a los directivos DANE, directores técnicos y coordinadores de las mesas estadísticas del SEN. La profundidad y detalle de las revisiones está asociada a las preguntas clave, perspectivas y el alcance y disponibilidad de información; si bien se pretende dar una adecuada respuesta y generar valor.

En esta edición del reporte se abordan cinco temáticas: (1) Buenas prácticas en el marco de gestión documental para los sistemas de almacenamiento (back up) y seguridad informática, cuyo objetivo es conocer las buenas prácticas a nivel nacional e internacional de los sistemas de gestión documental y seguridad en el marco de los sistemas de almacenamiento; (2) Buenas prácticas de las Instituciones Públicas para garantizar la propiedad intelectual sobre la divulgación de productos de investigación, cuyo objetivo es brindar un panorama del manejo actual de las instituciones públicas para garantizar la propiedad intelectual sobre los productos de investigación, desarrollo e innovación; (3) Reseña del documento Directrices Para La Elaboración De Una Estrategia De Comunicación, el cual expone la importancia de la comunicación de estadísticas oficiales y propone una estrategia para una comunicación integral, por medio de un conglomerado de instrucciones, consejos y recursos; (4) Evento de la 70.ª sesión plenaria de la Conferencia de Estadísticos Europeos en el cual se presenta la posición del DANE, los temas clave y las próximas tareas frente a las temáticas abordadas en el evento y (5) Evento de la 19.ª reunión del Comité de Estadística y Política

Estadística – CSSP en el cual se presenta también la posición del DANE, los temas clave y las próximas tareas frente a las temáticas abordadas en la conferencia.

Por cada uno de los temas se incluyen un resumen con la necesidad y objetivo de la revisión, una tabla de síntesis asociada al hallazgo principal o respuesta a la pregunta clave, la revisión de cada referente y las conclusiones y recomendaciones en las que se identifican tendencias o buenas prácticas que pueden ser de utilidad para el tema en el DANE y/o el SEN.

1. Buenas prácticas en el marco de gestión documental para los sistemas de almacenamiento (*backup*) y seguridad informática.

1.1 Resumen

En la actualidad los avances tecnológicos de la información y la transformación digital son necesarios para el apoyo, sostenibilidad y crecimiento de las entidades; requieren de nuevas prácticas y formas de gestionar los documentos que permitan el acceso, consulta, transparencia, optimización y disponibilidad de la información de manera segura.

El DANE cuenta con el Programa de Gestión Documental – PDG, desarrollado por el Archivo General de la Nación – AGN, el cual es un instrumento archivístico que le permite al DANE "*formular y documentar, a corto, mediano y largo plazo, el desarrollo sistemático de los procesos de la gestión documental, encaminados a la planificación, procesamiento, manejo y organización de la documentación producida y recibida, desde su origen hasta su destino final, para facilitar su uso, conservación y preservación*". El PDG identifica dentro de los procesos de la entidad la información producida y su valor legal, administrativo, financiero, técnico, estratégico y de gestión.

Asimismo, el PDG reconoce la necesidad del DANE en la digitalización de sus documentos, así como de la producción digital de estos, por medio de un Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA en el que independientemente de su forma de creación, ingreso o captura de los documentos, se pueda conformar un expediente utilizando un gestor documental, con todas las características y componentes de archivo; en el que refleje la totalidad de los documentos que hacen parte de un mismo trámite.

En este momento el DANE cuenta con ciento noventa y un (191) sistemas de información que soportan la operación misional y administrativa de la entidad, todos los sistemas generan información asociada a las Operaciones Estadísticas - OOEE, Operaciones Censales - OOCC y gestión administrativa en general (jurídica/legal, contable/financiera, administrativa, entre otras); que se encuentran de manera desarticulada y no toda se registra de manera electrónica, tal y como se define en la funcionalidad principal del SGEDA.

Sin embargo, hasta el momento la entidad solo ha identificado los requerimientos funcionales para establecer un SGDEA, a pesar de que en el Plan Estratégico de Tecnologías de la Información – PETI 2019-2022 se encuentra registrado el proyecto Implementación del Sistema de Información de Gestión Documental que tiene dentro de sus objetivos específicos: i) "*Apoyar el fortalecimiento de la capacidad institucional para que su gestión documental sea más efectiva y transparente*" y ii) "*Permitir que los expedientes documentales estén disponibles e integrados a los diferentes procesos y sistemas de información de la entidad*", no obstante, el proyecto no ha podido ser ejecutado por restricciones presupuestales.

Por otro lado, con respecto a los temas relacionados con back up y seguridad informática, el DANE cuenta con la adopción de las políticas de Seguridad Digital (RES.602 de 2021), el modelo de Seguridad y Privacidad de la información (RES 0738 de 2020, RES 0667 de 2020, RES 1241 de 2021 y RES 0644 de 2022), los subprocesos de Gestión de Servicios de TI (GTE-030) y de Seguridad Informática (GET-040); los cuales aseguran la adopción y desarrollo de actividades para asegurar la seguridad informática, de acuerdo con las políticas impartidas a través del MIPG-MECI y los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI, Gestión y Gobierno de TI, Arquitectura Empresarial del Estado Colombiano, Gestión de Proyectos de TI, los Marcos de Referencia de Interoperabilidad y de Transformación Digital de MINTIC.

No obstante, a pesar de la adopción progresiva de las medidas agrupadas en los anteriores documentos normativos y de asegurar un ambiente de control, el pasado mes de noviembre del 2021, los sistemas del DANE fueron objeto de un ataque informático, los controles dispuestos por la plataforma tecnológica fueron vulnerados, afectando la disponibilidad de los servicios tecnológicos, por lo que se tuvo que recurrir a mecanismos alternos y contingencias que permitieron la continuidad de las operaciones, garantizando que la información estadística clave se pudiera publicar al país oportunamente.

Un factor que ha impactado los respaldos de información y seguridad informática es la disponibilidad de recursos para poder realizar una renovación tecnológica adecuada, en especial sobre aquellos componentes críticos y directamente relacionados con estos. Para la ejecución del proyecto de inversión de "Fortalecimiento y modernización de las Tecnologías de la información y las Comunicaciones - TIC que respondan a las necesidades de la entidad a nivel nacional" no se han contado con los recursos suficientes.

Para el año 2022 el DANE solicitó un presupuesto de 104.256 millones de pesos al Ministerio de Hacienda, de los cuales fueron asignados 14.700 millones de pesos, por lo que la Oficina de Sistemas – OSIS está implementando los proyectos para la continuidad operativa, relacionados con la actualización de las soluciones de seguridad informática y habilitación de sus respectivos servicios, el fortalecimiento de la infraestructura, la adquisición de los componentes y subcomponentes de los controles de seguridad informática de manera paulatina y acorde con los recursos asignados.

Dado lo anterior, la Oficina de Sistemas plantea la necesidad de contar con una revisión de referentes internacionales sobre buenas prácticas en el marco de gestión documental para los sistemas de almacenamiento (*backup*) y seguridad informática, que le permita obtener una visión más amplia de los sistemas y procesos usados en la actualidad para este fin, dando como resultado un panorama que sirva de guía para tomar decisiones sobre las actualizaciones de las soluciones de seguridad informática y la habilitación de sus respectivos servicios, por medio del fortalecimiento de la

infraestructura y los componentes asociados a los controles de seguridad informática. Para ello se solicitó abordar en el informe los siguientes referentes:

- MinTIC.
- Archivo General de la Nacion.
- OECD.
- Banco Interamericano de Desarrollo.
- Agencia de Ciberseguridad e infraestructura del gobierno americano – CISA.
- Agencia de Ciberseguridad de la Unión Europea – ENISA.
- Gartner.
- Normas ISO 22301, 27001, 27002, 270131, 27701.
- Marco COBIT.
- Critical Security Controls – CIS.
- Marco HITRUST CSF.
- Marco COSO.

1.2 Síntesis de hallazgos

La Tabla 1. Principales hallazgos sobre los lineamientos en materia de gestión documental en el marco de sistemas de almacenamiento (*backup*) Presenta una breve descripción de los principales hallazgos de la revisión de referentes internacionales en los organismos internacionales, entidades públicas y privadas que han desarrollado lineamientos o buenas prácticas en el marco de gestión documental para los sistemas de almacenamiento.

Tabla 1. Principales hallazgos sobre los lineamientos en materia de gestión documental en el marco de sistemas de almacenamiento (*backup*)

Referente	¿Qué lineamientos o buenas prácticas existen en el marco de gestión documental para los sistemas de almacenamiento (*backup*)?, ¿tienen en cuenta esquemas de seguridad que permitan cumplir con auditorias de control interno?
OECD	La OCDE presenta en el 2021 la Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la información, en ella se establece el marco GSI con acuerdos de gobernanza, políticas, procedimientos, prácticas y controles de seguridad; además de presentar los pasos para crear un GSI basado en la ISO 27001, enmarcado en el ciclo PDCA; se profundiza en los requisitos específicos relacionados con los sistemas y protección de la información.

Referente	¿Qué lineamientos o buenas prácticas existen en el marco de gestión documental para los sistemas de almacenamiento (*backup*)?, ¿tienen en cuenta esquemas de seguridad que permitan cumplir con auditorias de control interno?
BID	Se destacan 5 normas ISO; la 22301 por su Sistema de Gestión de Continuidad del Negocio – SGCN, que permite garantizar la continuidad de las operaciones en las organizaciones por su dependencia de las tecnologías de la información y las comunicaciones; la 27001 por su Sistema de Gestión de Seguridad de la Información, que presenta unas fases para su implementación, identificación de riesgos y realización de autorías internas y externas; la 27002 cuenta con una guía de implementación del SGSI planteado en la norma 27001 y en su última versión se plantea la necesidad de analizar la ciberseguridad e identificación de riesgos en la conservación de la información; la 27032 trata sobre la gestión de la ciberseguridad, como marco para mantener la confidencialidad, integridad y disponibilidad de la seguridad de la información, de las redes, del internet y la infraestructura; y la 27701 establece el sistema de gestión de la privacidad de la información como complemento de las normas 27001 y 27002.
ISO	Se destacan 5 normas ISO; la 22301 por su Sistema de Gestión de Continuidad del Negocio – SGCN, que permite garantizar la continuidad de las operaciones en las organizaciones por su dependencia de las tecnologías de la información y las comunicaciones; la 27001 por su Sistema de Gestión de Seguridad de la Información, que presenta unas fases para su implementación, identificación de riesgos y realización de autorías internas y externas; la 27002 cuenta con una guía de implementación del SGSI planteado en la norma 27001 y en su última versión se plantea la necesidad de analizar la ciberseguridad e identificación de riesgos en la conservación de la información; la 27032 trata sobre la gestión de la ciberseguridad, como marco para mantener la confidencialidad, integridad y disponibilidad de la seguridad de la información, de las redes, del internet y la infraestructura; y la 27701 establece el sistema de gestión de la privacidad de la información como complemento de las normas 27001 y 27002.
Archivo General de la Nación	El Archivo General de la Nación – AGN desarrolló el Programa de Gestión Documental – PDG, el cual es un instrumento archivístico que establece una línea estratégica de ocho procesos de gestión documental (planeación, producción, gestión y trámite, organización, transferencia, disposición de documentos, preservación a largo plazo y valoración), los cuales tienen la finalidad de garantizar la integridad, disponibilidad, fiabilidad y usabilidad de los documentos como fuente de historia y de hechos que dan soporte para continuar con las misiones y obligaciones del AGN.

Referente	¿Qué lineamientos o buenas prácticas existen en el marco de gestión documental para los sistemas de almacenamiento (*backup*)?, ¿tienen en cuenta esquemas de seguridad que permitan cumplir con auditorias de control interno?
	Asimismo, AGN elaboró el documento *Guía de Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA*, el cual tiene como propósito establecer una estructura conceptual y una ruta de implementación del SGDEA en una organización, permitiendo gestionar tanto documentos de archivo (evidencias de las actividades de negocio) como documentos con un único valor informativo.
MINTIC	Dentro de la política de Gobierno Digital, el ministerio de las Tecnologías de la Información y las Comunicaciones expide el 15 de febrero de 2022 el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la política, donde se plantean difunden documentos que conforman los lineamientos o guía de buenas prácticas correspondiente a la construcción del Plan Nacional de Infraestructura de datos. Dentro de estos documentos guías se tratan temas como Gobierno de datos, Guía para el uso y aprovechamiento, marco de interoperabilidad, entre otros. En lo que respecta a los esquemas de seguridad que permitan cumplir con auditorias de control no se encuentra que el ministerio tenga documentación frente a esto. Sin embargo, en el marco de la Política de gobierno digital, uno de sus habilitadores transversales se enfoca en modelo de seguridad y privacidad de la información, en la cual se puede encontrar temáticas cercanas a la pregunta.
Departamento Nacional de Planeación	El Departamento Nacional de Planeación – DNP, desarrolló el Manual y Políticas de Seguridad de la información, con el objetivo de garantizar que los riesgos asociados a la seguridad de la información sean identificados, valorados, controlados y administrados en el marco de la protección de datos personales. En el manual se plantean lineamientos de buenas prácticas en cuanto a responsables del almacenamiento de información, ejecución correcta de los *backups*, restauración de copias de respaldo en ambientes de producción, periodicidad de los *backups*, etc. Además, indica que la información manejada por la entidad debe tener carácter auditable, aunque no explica ampliamente cómo se surte el proceso de auditoría, sí especifica que se debe diligenciar información en registros (logs) de auditoría.
Ministerio de Educación Nacional	El Ministerio de Educación Nacional, desarrolló el Programa de Gestión Documental. – PGD, que fortalece la cultura de gestión de los documentos electrónicos con política cero papel y fácil acceso a la información para usuarios externos e internos, preservando las buenas prácticas en el proceso. Dentro de las premisas del programa se presentan 1. La preservación de la documentación en formato físico, electrónico y digital en el largo plazo, elaborando e implementando el Sistema Integrado de Conservación y estableciendo políticas de *backups* y 2. El desarrollo de un programa

Referente	¿Qué lineamientos o buenas prácticas existen en el marco de gestión documental para los sistemas de almacenamiento (*backup*)?, ¿tienen en cuenta esquemas de seguridad que permitan cumplir con auditorias de control interno?
	de auditoría y control, que tiene como propósito la cultura de autocontrol en la administración de archivos y la producción documental.
Marco COBIT	COBIT es un marco que establece lineamientos de buenas prácticas dirigidos al gobierno y gestión de la información y la tecnología empresarial – TI, promovido desde su primera versión en 1996 por *Information Systems Audit and Control Association – ISACA* hasta la más reciente COBIT 2019, actualmente están disponibles los siguientes marcos: • Marco de Referencia COBIT 2019: Introducción y metodología, el cual presenta los conceptos clave de COBIT 2019 • Marco de Referencia COBIT 2019: Objetivos de gobierno y gestión, en el cual se exponen los 40 objetivos principales de gobierno y gestión y los procesos y componentes relacionados (esta guía también hace referencia a otros estándares y marcos relacionados). • Guía de diseño COBIT 2019: Diseño de una solución de Gobierno de Información y Tecnología, el cual investiga los factores de diseño que pueden influir en el gobierno y además incluye un flujo de trabajo para la planificación de un sistema de gobierno personalizado para la empresa. Guía de implementación de COBIT 2019: Implementación y optimización de una solución de gobierno de Información y Tecnología, el cual es la evolución de la guía COBIT 5 y desarrolla una hoja de ruta para la mejora continua del gobierno.
CIS	*Control of Internet Security – CIS* publica un documento donde se establece una guía de Controles de seguridad y privacidad para organizaciones y sistemas de información federales, donde se establecen un conjunto de medidas enfocadas a los sistemas de información del sector público. Es importante resaltar que este documento trae un mapeo de puntos en común, relacionadas desde el marco de seguridad de CIS y el Marco del Instituto Nacional de Estándares y Tecnología denominado – NIST.
ENISA	La Agencia de Ciberseguridad de la Unión Europea – ENISA contribuye a la política de cibernética de la UE, mejora la confiabilidad de los productos, servicios y procesos de las TIC con esquemas de ciberseguridad, coopera con los Estados Miembros y los organismos de la UE y ayuda a Europa a prepararse para los desafíos cibernéticos del mañana.

Referente	¿Qué lineamientos o buenas prácticas existen en el marco de gestión documental para los sistemas de almacenamiento (*backup*)?, ¿tienen en cuenta esquemas de seguridad que permitan cumplir con auditorias de control interno?
	ENISA, divulgó un informe sobre "*Protección de Datos de Ingeniería, de la teoría a la práctica*" donde se mencionan los principios de protección de datos, tal como se establece en el Reglamento General de Protección de Datos – RGPD, los objetivos que se deben alcanzar al considerar el diseño, la implementación y el despliegue de una operación de procesamiento. ENISA menciona una serie de tecnologías y técnicas, aplicables a la protección de datos, sin embargo, no es sencillo para los controladores y procesadores de datos cuál es aplicable y más adecuada para cada operación de procesamiento y para cada contexto. La comunidad investigadora debe continuar explorando el despliegue de técnicas y tecnologías (de seguridad) que puedan respaldar la implementación práctica de los principios de protección de datos, con el apoyo de las instituciones de la UE en términos de orientación política y financiación de la investigación.
Marco COSO	El Comité de Organizaciones Patrocinadoras del Treadway – COSO publicó una guía sobre Gestión de riesgos cibernéticos en la era digital que tiene como fin proporcionar una descripción general sobre la gestión del riesgo cibernético a través de los principios definidos en el Marco de gestión de riesgos empresariales. La Guía proporciona un contexto de los conceptos fundamentales de las técnicas de gestión de riesgos cibernéticos, sin embargo, no pretende ser una guía para desarrollar e implementar estrategias técnicas.

Fuente: DANE a partir de las revisiones de referentes.

1.3 Revisión de referentes

En esta sección se presentan, de forma sintetizada, la revisión de referentes en: i) tres organismos internacionales, ii) uno perteneciente a la unión europea, iii) tres instituciones privadas y iv) cuatro entidades públicas nacionales, los cuales han desarrollado lineamientos o buenas prácticas en el marco de gestión documental para los sistemas de almacenamiento (*backup*).

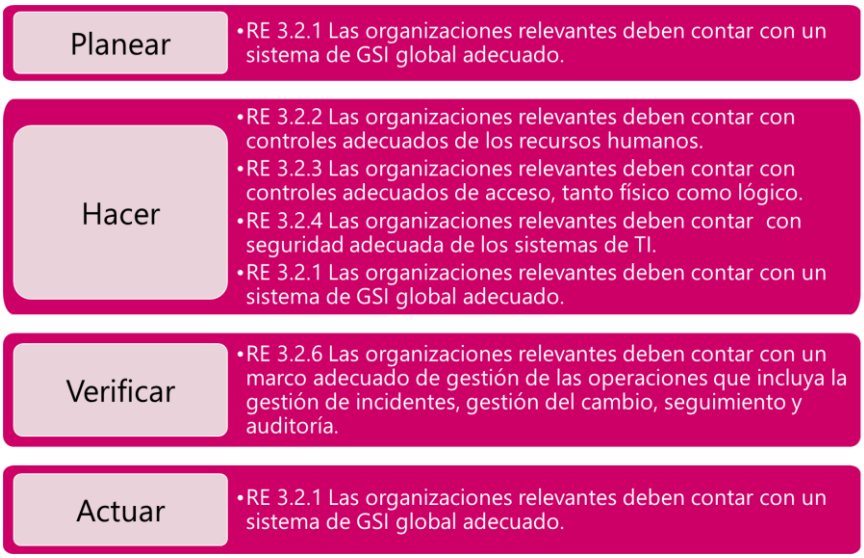
1.3.1 OECD

Desde el Foro Global sobre Transparencia e intercambio de información con fines fiscales, la OCDE presenta la Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información[1], con el fin de ayudar a las administraciones tributarias de todos los países en desarrollo a mejorar los elementos para el marco de la Gestión de la Seguridad de la Información – GSI y el intercambio de acuerdo con los acuerdos internacionales. La guía maneja una estructura que se ajusta a los requisitos de confidencialidad y protección de datos del Estándar del Intercambio Automático de Información – AEOI.

Un marco GSI presenta acuerdos de gobernanza, políticas, procedimientos, prácticas y controles de seguridad, que se debe complementar con el Estándar AEOI; con el fin de complementar la sensibilidad de la información, grandes volúmenes de datos y medios electrónicos.

A continuación, se presentan los pasos claves para la implementación de un marco de GSI en un país en desarrollo; paso 1, delimitar el alcance del marco de GSI; paso 2, definir una política de GSI; paso 3, identificar los riesgos para la seguridad; paso 4, establecer políticas, procesos y procedimientos específicos en los ámbitos relevantes; Paso 5, formar al personal; y paso 6, verificar la adopción efectiva del sistema de GSI. Cada uno de estos pasos se encuentra relacionado con el ciclo PDCA (*Plan, Do, Check, Act*) como se evidencia en la Ilustración 1.

Ilustración 1. Estructura del Requisito Principal (Marco GSI)



Fuente: OCDE, 2021

[1] Disponible en https://www.oecd.org/tax/transparency/documents/confidentiality-ism-toolkit_es.pdf

Adicionalmente, la OCDE proporcionan un mapeo general del Sistema de Gestión de la Seguridad de la Información aplicando los estándares de la ISO 27001, como se muestra en la Ilustración 2, cada uno de requisitos específicos son el complemento para lograr el requisito principal; sin embargo, en este informe se profundiza en el requisito 3.2.4 Seguridad del sistema de TI.

Ilustración 2. Mapeo general del RP 3.2 (marco GSI) con el estándar ISO/IEC 27001

Fuente: OCDE, 2021

Como parte integral de la Guía, se encuentran algunas políticas que presentan una administración tributaria para implementar procesos, procedimientos y controles; en este caso cada requisito específico cuenta con una política como se presenta en la Tabla 2.

Tabla 2. Políticas de seguridad

Requisito	Política
RE 3.2.1.5	Política de continuidad del negocio
RE 3.2.2	Política de seguridad de los recursos humanos
RE 3.2.3	Política de gestión de accesos
RE 3.2.3.1 y 3.2.3.2	• Política de acceso físico
RE 3.2.3.3 y 3.2.3.4	• Política de acceso lógico
RE 3.2.4.2	Política de seguridad de TI
	• Política de protección frente a un software malicioso (*malware)*
	• Política de registro y seguimiento

Requisito	Política
RE 3.2.4.3	Política de gestión de activos
RE 3.2.5	Política de clasificación de la información
RE 3.2.5	• Política de "escritorio limpio/despejado"
RE 3.2.5	Política de criptografía
RE 3.2.6.5	Política de gestión del cambio
RE 3.2.6.6	Política de gestión de incidentes

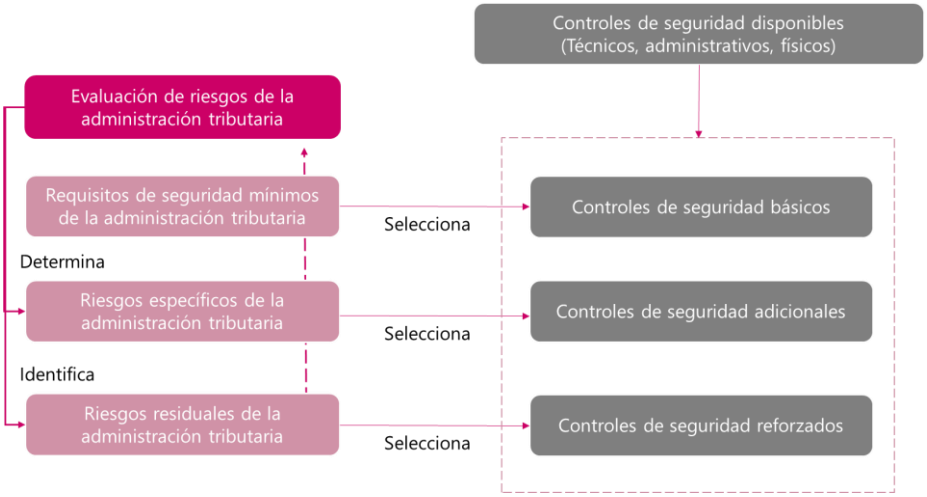
Fuente: OCDE, 2021

Requisito específico 3.2.4 Seguridad del sistema de TI

El requisito específico 3.2.4 Seguridad del sistema de TI, se refiere a la protección de la información mediante la protección de la infraestructura (tanto del software como del hardware) en la que se conserva la información, se consulta y se utiliza; se establecen unas acciones específicas para protección de la información:

- RE 3.2.4.1: Hagan que la seguridad forme parte de la prestación de servicios de TI en apoyo de las funciones del negocio, adopten un plan de seguridad para las aplicaciones del negocio y armonicen sus sistemas con la seguridad.
- RE 3.2.4.2: Implanten una serie adecuada de controles de seguridad de TI. Esto se establece según la función informática y se evalúan diferentes controles, **Error! Reference source not found.**, esta estructura debe quedar documentada; con el fin de mantener una trazabilidad por parte del equipo encargado y registrar los ajustes y cambios producidos en el sistema. Algunos ejemplos de estos controles se evidencian en la Tabla 3.

Ilustración 3. Tipos de controles de seguridad



Fuente: OCDE, 2021

Tabla 3. Ejemplos de controles básicos, adicionales y reforzados

Control	Ejemplo	Ejemplo	Ejemplo
Básico	Antivirus, registro y Seguimiento.	CCTV, sistema de iluminación.	Política de contraseñas.
Adicional	Autenticación de múltiples factores.	Vallas, trampas.	Política de formación sobre sensibilización.
Reforzado	Sistemas de prevención de pérdida de datos, Centro de Operaciones de Seguridad interno y continuo.	Centro de datos de nivel 1, sitio de respaldo (*hot site)* activo/ replicación activa.	Política "Trae tu propio dispositivo", política de cifrado reforzado para información muy sensible.

Fuente: OCDE, 2021

- RE 3.2.4.3: Gestionen debidamente sus activos de TI.
- RE 3.2.4.4: Gestionen debidamente la prestación de servicios por parte de los proveedores.
- RE 3.2.4.5: Garanticen la continuidad de los servicios de TI y su resiliencia ante fallos.

Requisito específico 3.2.5 Protección de la información

El requisito específico 3.2.5 la "Protección de la información", protege los distintos tipos de información en papel y digital que manejan las administraciones tributarias, si se encuentran en reposo, en uso o en movimiento entre entornos y lugares de trabajo, con controles acordes a su

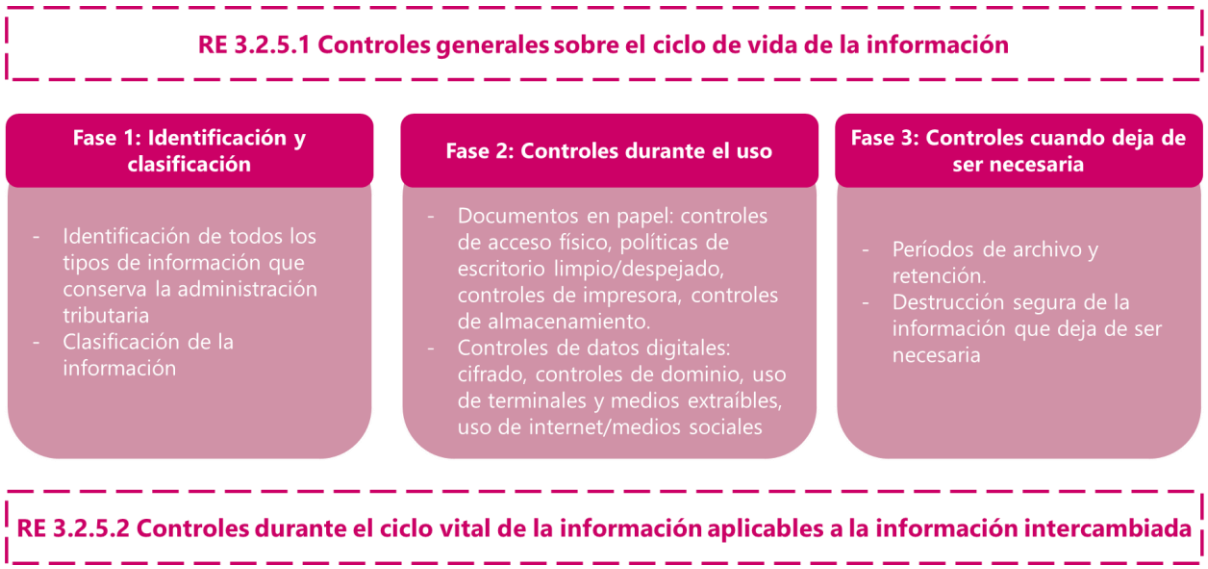
clasificación con respecto a su sensibilidad y confidencialidad. Los controles en el ciclo de vida de la información incluyen:

- Políticas de escritorio limpio/despejado.
- Controles de impresora.
- Mecanismos de almacenamiento físico y digital de la información.
- Controles de cifrado y dominio.
- Controles de medios seguros para soportes de información tales como dispositivos periféricos.
- Controles al finalizar el ciclo de vida, tales como políticas de eliminación de información.

En la

Ilustración 4, se presenta los controles de la información (digital o en papel), con las tres fases generales del ciclo de vida de gestión de la información, según la práctica en las administraciones tributarias, se recomienda aplicar controles reforzados sobre la información intercambiada.

Ilustración 4. Ciclo vital de la gestión de la información



Fuente: OCDE, 2021

Directrices para la seguridad de sistemas y redes de información

Por otra parte, la OCDE ha creado unas directrices para la seguridad de sistemas y redes de información[2], con el propósito de promover una cultura de seguridad entre todos los participantes como medio de proteger los sistemas y redes de información; promover el conocimiento en materia de seguridad como un objetivo importante a lograr entre todos los participantes involucrados en el desarrollo y ejecución de normas técnicas.

Adicionalmente, presenta nueve principios inmersos en la concienciación, educación, intercambio de información y capacitación, con el fin de tener un mejor entendimiento de la seguridad y de las prácticas requeridas. Estos principios se presentan en la Ilustración 5, los cuales son complementarios entre sí y se interpretan como un todo.

Ilustración 5. Principios de las directrices para la seguridad de sistemas y redes de información

Fuente: DANE a partir de la OCDE

1.3.2 Banco Interamericano de Desarrollo – BID

[2] Disponible en https://www.oecd-ilibrary.org/docserver/9789264065819-es.pdf?expires=1655766552&id=id&accname=guest&checksum=15BF18F76376FAEAAC034BD4FB406615

El Banco Interamericano de Desarrollo es una de las principales fuentes de financiamiento a largo plazo para proyectos económicos, sociales e institucionales en América Latina y el Caribe. Además de préstamos, donaciones y garantías de crédito, el BID realiza proyectos de investigación de vanguardia para brindar soluciones innovadoras y sostenibles a los problemas más urgentes de nuestra región.

La Organización de los Estados Americanos – OEA y el Banco Interamericano de Desarrollo – BID lanzaron el estudio conjunto "*Ciberseguridad: riesgos, progreso y el camino a seguir en América Latina y el Caribe*"[3]. Esta es la segunda edición de un informe que evalúa el estado de la ciberseguridad en la región.

Según el informe, desde el último estudio realizado en 2016, más de la mitad de los países de la región han mejorado su disposición hacia la ciberseguridad al desarrollar e implementar estrategias nacionales y/o marcos legales que permiten una mejor respuesta a las *ciberamenazas*, incluyendo mayor protección de los datos personales de los ciudadanos.

Sin embargo, el informe también revela que aún se necesitan más esfuerzos para fortalecer la ciberseguridad en la región. Actualmente, más de las tres cuartas partes de los países observados en este informe carecen de los planes de ciberseguridad necesarios para la protección de su infraestructura crítica, un hecho particularmente preocupante en el contexto del COVID-19. La mayoría de los países de la región también necesitan capacidades más sistemáticas y eficientes para monitorear y responder a los incidentes de ciberseguridad, así como la creación de organismos centrales encargados de coordinar las actividades de seguridad informática.

El documento destaca la necesidad de una cooperación más activa entre todas las partes interesadas, que permita fortalecer la capacidad de prevención de amenazas cibernéticas, así como la posibilidad de abordar algunos de los incidentes más comunes como el cibercrimen, las intrusiones en redes críticas y las operaciones cibernéticas políticamente motivadas.

"El mensaje de este informe es claro: América Latina y el Caribe necesitan hacer más para mejorar su situación de ciberseguridad", dijo Ana María Rodríguez, vicepresidenta de sectores y conocimiento del BID. "Los hallazgos son cruciales para guiar los esfuerzos de los gobiernos de la región, especialmente ahora que la crisis del COVID-19 ha acelerado nuestra dependencia de las plataformas digitales en nuestra vida profesional y personal".

[3] Disponible en https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

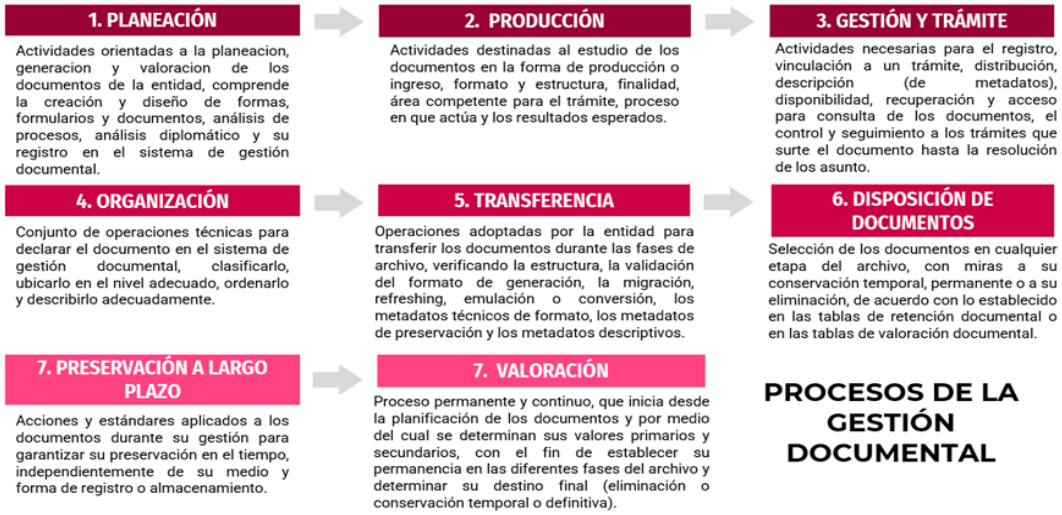
Para Farah Diva Urrutia, secretaria de Seguridad Multidimensional de la OEA, "este informe puede servir de hoja de ruta para los Estados Miembros e instituciones interesadas que continuamente buscan formas de adaptarse a las amenazas de ciberseguridad emergentes que afectan a nuestra región. Aunque todavía queda trabajo por hacer, estamos orgullosos de apoyar el desarrollo de capacidades a través de nuestro Programa de ciberseguridad y seguiremos promoviendo la concientización sobre este tema, junto con socios tan importantes como el BID.

1.3.3 Archivo General de la Nación

El Programa de Gestión Documental[4] – PDG es el instrumento archivístico que establece una línea estratégica de ocho procesos de gestión documental (Ver

Ilustración 6), los cuales tienen la finalidad de garantizar la integridad, disponibilidad, fiabilidad y usabilidad de los documentos como fuente de historia y de hechos que dan soporte para continuar con las misiones y obligaciones del Archivo General de la Nación – AGN.

Ilustración 6. Descripción de los Procesos de Gestión Documental



Fuente DANE a partir de AGN[5]

El documento detalla las actividades adelantadas durante el periodo 2014-2018 y otras programadas para ser ejecutadas y controladas en el periodo 2018-2022; así mismo, el PGD permite al AGN

4 Disponible en https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/2_Politica_archivistica/Instrumentos_Archivisticos/PGD/PGD_AGN_2018.pdf

5 Disponible en https://www.archivogeneral.gov.co/Politica/procesos

formular y documentar a corto (1 año), mediano (2 años) y largo (3 y 4 años) plazo el desarrollo sistemático de los procesos de gestión documental, "*encaminados a la planificación, procesamiento, manejo y organización de la documentación producida y recibida, desde su origen hasta su destino final, con el fin de facilitar su uso, conservación y preservación*[6]", además, el PDG garantiza la articulación del sistema de gestión documental con los demás sistemas de la entidad, minimizando esfuerzos y racionalizando recursos. Sin embargo, para desarrollar el PGD son necesarios algunos requerimientos normativos, económicos, administrativos, tecnológicos y de gestión del cambio (Ver Ilustración 7).

Ilustración 7. Requerimientos para el Desarrollo del PDG

Fuente DANE a partir del AGN 2018

Una vez se cumplen los requerimientos necesarios, se procede a la implementación del PDG, la cual se divide en cuatro fases (como lo establece el decreto 1080 de 2015), las fases de elaboración, ejecución y puesta en marcha establecen un cronograma de ejecución y una matriz de responsabilidades RACI[7], mientras que en las fases de seguimiento y mejora se realizan acciones

6 Disponible en https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/2_Politica_archivistica/Instrumentos_Archivisticos/PGD/PGD_AGN_2018.pdf

7 Disponible en anexo N°1 https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/2_Politica_archivistica/Instrumentos_Archivisticos/PGD/PGD_AGN_2018.pdf

preventivas y correctivas en el PDG, auditorías internas, visitas de seguimiento a las dependencias y la determinación de acciones de mejora. Además, con el fin de cumplir los objetivos del PGD se establecieron algunos programas específicos (Ver Tabla 4**)**.

Tabla 4. Programas Específicos

Programas específicos			
Programa	**Descripción**	**Objetivo general**	**Actividades a ser ejecutadas durante 2018-2022**
Programa de normalización de formas y formularios electrónicos	Realizar el análisis diplomático de los documentos, independientemente de su soporte, delimitando y fijando sus características y atributos, con el propósito de crear las formas, formatos y formularios, denominándolos con nombres propios; permitiendo con ello establecer: tradición documental, autenticidad y tipología de los documentos, para facilitar la identificación, clasificación y descripción de los documentos.	Establecer las acciones que aseguren el uso de los documentos internos y de origen externo de forma unificada, controlada y actualizada, mediante un método sistemático para la elaboración (edición, revisión, aprobación), manejo (distribución, modificación) y control de los documentos, con el fin de prevenir el uso no intencionado de documentos obsoletos en la Entidad, cumpliendo con los lineamientos del Sistema Integrado de Gestión.	• Diagnóstico de la producción interna de formas, formatos de documentos electrónicos. • Actualizar el procedimiento de producción documental para la normalización de formas, formatos de documentos electrónicos. • Aplicación del procedimiento de producción documental.

Programa de documentos vitales o esenciales	Identificación, evaluación, selección, protección, preservación y recuperación de los documentos del AGN con el fin de i) asegurar el funcionamiento de la entidad, ii) permitir la continuidad del trabajo institucional en caso de emergencia, iii) evidenciar las obligaciones legales y financieras, y iv) la defensa y restitución de derechos y deberes de personas y entidades cuya documentación haga parte del fondo documental administrativo del AGN.	Desarrollar acciones encaminadas a garantizar la custodia y preservación de los documentos vitales o esenciales del AGN con el fin de evitar la pérdida, adulteración, sustracción y falsificación de los mismos y asegurar un plan de contingencia frente a la información que contiene dicha documentación.	• Elaborar matriz de identificación y clasificación de documentos vitales de conformidad con la TRD del AGN y el inventario documental de los documentos vitales del AGN. • Actualizar la matriz de identificación y clasificación de documentos vitales, incluyendo el análisis de los inventarios de registros de activos de información e índice de información clasificada.
Programa de gestión de documentos electrónicos	Este programa está orientado al diseño, la implementación y el seguimiento de estrategias para gestionar el ciclo de vida de los documentos en el entorno electrónico junto con los procesos de gestión documental.	Determinar los proyectos a realizar para la gestión de documentos electrónicos en el AGN, para el cumplimiento normativo.	• Aplicar los instrumentos para el levantamiento de información y análisis del estado actual y perspectiva del funcionamiento del sistema de gestión de documento electrónico de archivo – SGDEA del AGN. • Identificar y realizar un informe del análisis de la producción documental y los registros susceptibles a automatizar teniendo en cuenta los procesos de la entidad, el nivel de complejidad tecnológico (alta, media, baja) • Elaborar el modelo de requisitos para la gestión de documentos electrónicos del AGN.

			• Actualizar la tabla de control y acceso del AGN • Determinar los proyectos a realizar para la gestión de documentos electrónicos en el AGN.
Programa de reprografía	El programa específico de reprografía comprende desde la evaluación de la necesidad del servicio, pasando por la formulación de estrategias y requerimientos para la aplicación de las técnicas reprográficas, captura de metadatos, realizar el seguimiento y control del producto en el marco de la producción documental del fondo administrativo del AGN.	Determinar los proyectos para la implementación del programa de reprografía en el AGN.	• Aplicar los instrumentos para el levantamiento de información y análisis del estado actual y perspectiva de la estrategia de reprografía en el AGN. • Identificar y realizar un informe del análisis de la estrategia de reprografía que evalué el estado de los equipos de microfilmación, la definición de la técnica de reproducción a utilizar para documentos de conservación total, así como los requisitos técnicos necesarios para la implementación. • Determinar los proyectos a realizar en la ejecución del programa de reprografía del AGN.
Programa de archivos descentralizados	Dado el alcance del programa de archivos descentralizados, el Archivo General de la Nación no requiere desarrollarlo, ya que la Entidad cuenta con depósitos con las características técnicas requeridas para el almacenamiento y custodia, así mismo se autoabastece en la prestación de servicios para la organización, administración, preservación y conservación de sus documentos de archivo.		

Programa de documentos especiales	El programa documentos especiales está orientado a la gestión los documentos de archivo que por sus características no convencionales requieren tratamiento diferente, los cuales son: cartográficos, fotográficos, planos, sonoros y audiovisuales. Adicionalmente, establece las actividades técnicas para clasificar, ordenar, describir, conservar, declarar, difundir y consultar, con el fin de facilitar el acceso a la información contenida en los mismos.	Determinar los proyectos a realizar para la gestión de documentos especiales en el AGN, para el cumplimiento normativo.	• Aplicar los instrumentos para el levantamiento de información y análisis para la identificación de documentos especiales tales como: Cartográficos, fotográficos, planos, sonoros y audiovisuales en el AGN. • Actualizar los instrumentos archivísticos producto de la identificación de los documentos especiales • Determinar los proyectos para garantizar la gestión de documentos especiales en el AGN
Programa plan institucional de capacitación	El Plan Institucional de Capacitación contempla los siguientes aspectos en materia de gestión documental de la Entidad: • Programa de Inducción y Reinducción que incluya las temáticas: i) sensibilización sobre el valor patrimonial de los documentos físicos y electrónicos y la preservación a largo plazo, ii) explicación de políticas, procesos y procedimientos de la gestión documental y iii) comprensión y conocimiento de las funciones archivísticas y sus beneficios. • Entrenamiento y capacitación: los servidores públicos cuya vinculación sea de carrera administrativa, de libre nombramiento y remoción.		
Programa de auditoría y control	Verificar y evaluar la conformidad de las actividades señaladas en el Programa de Gestión Documental del Archivo General de la Nación con la normatividad archivística existente.	Evaluar el grado de cumplimiento en cada una de las actividades señaladas en la implementación del Programa de gestión Documental – PGD del Archivo General de la Nación – AGN, en el Grupo de Gestión Documental y a la totalidad de las dependencias del AGN.	

Fuente DANE a partir del AGN 2018

Sistema de Gestión de Documentos Electrónicos de Archivo –SGDEA

Los avances en las tecnologías de la información y las telecomunicaciones requieren de nuevas prácticas y formas de gestionar los documentos que permitan el acceso, consulta, transparencia,

optimización y disponibilidad de la información, para ello es fundamental el establecimiento de políticas claras sobre la producción, distribución, consulta, retención, almacenamiento, preservación y disposición final de los documentos, pues independientemente de la forma de estos, la concepción es "electrónica" y debe ser gestionada por al menos un componente tecnológico.

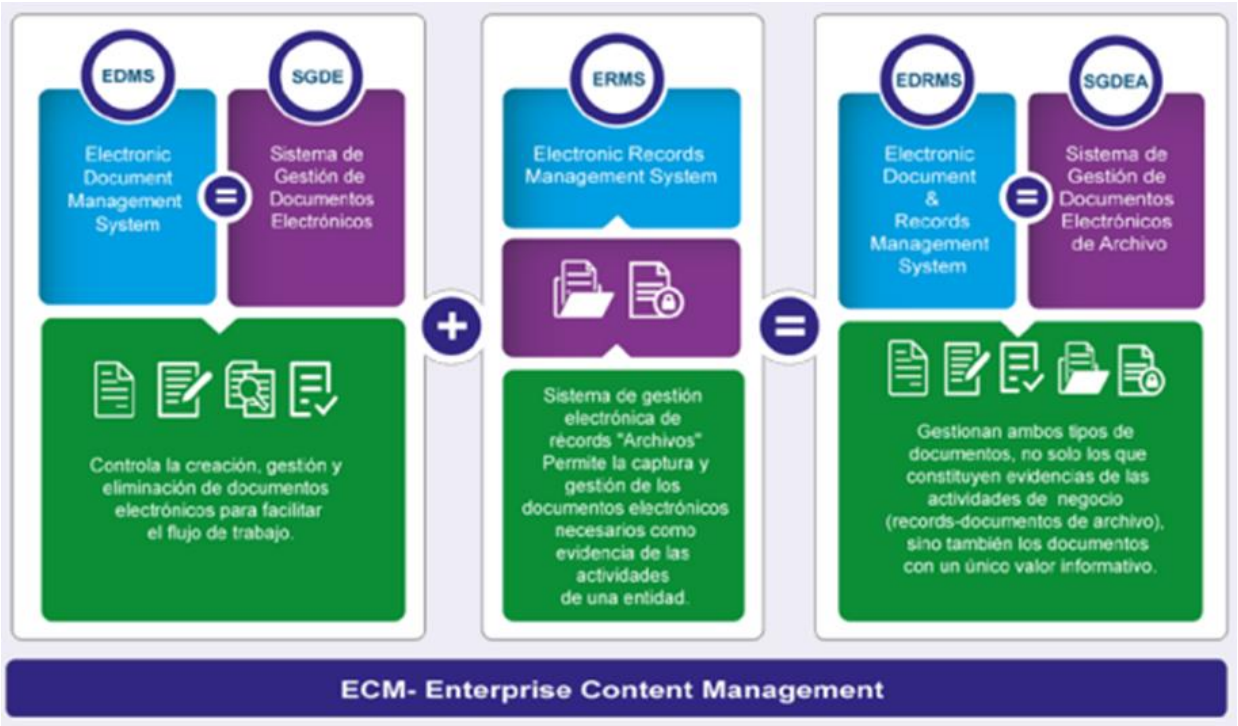
Aunque hoy en día, producto de las actuaciones administrativas las entidades generan diferentes documentos, los cuales normalmente se imprimen para crear expedientes físicos, los aplicativos usados comúnmente son transaccionales y no están diseñados como gestores documentales que permitan parametrizar las tablas de retención y administrar los documentos y expedientes, pues "*independientemente de la forma de creación, ingreso o captura de los documentos, estos deben gestionarse a través de un gestor documental que permita la conformación del expediente, con todas sus características y componentes de archivo y que refleje la totalidad de los documentos que hacen parte de un mismo trámite*", para ello es necesario el documento técnico *Guía para la gestión de documentos y expedientes electrónicos*[8].

Existen diferentes sistemas de información asociados al control y gestión de documentos, entre ellos están: i) el Sistema Electrónico de Gestión de Documentos – EDMS (SGDE en Colombia) el cual es un sistema de software que controla y organiza los documentos en toda la organización, independientemente de que se hayan declarado como documentos electrónicos de archivo o no, este sistema maneja documentos que hacen parte de archivos de gestión que pueden cambiar como resultado del trabajo diario, ii) el Sistema de Gestión de Documentos y Registros Electrónicos – ERMS por su parte no permite modificar documentos una vez que se declaran como documentos de archivo por lo que el documento podrá consultarse, pero no editarse ni borrarse, iii) el EDRMS (SGDEA en Colombia) es el resultado de unificar los sistemas EDMS y ERMS, este sistema ha incorporado otras funcionalidades y tecnologías informáticas permitiendo gestionar tanto los documentos de archivos, como documentos con un único valor informativo (Ver

Ilustración 8).

Ilustración 8. Sistemas Gestión de Documentos

8 Disponible en http://observatoriotic.archivogeneral.gov.co/project/guia-expedientes-electronicos/



Fuente Archivo General de la Nación 2017[9]

El documento Guía de Implementación de un SGDEA,[10] publicado por el Archivo General de la Nación, tiene como propósito establecer una estructura conceptual y una ruta de implementación del SGDEA en una organización, este documento toma como referencia los lineamientos y mejores prácticas nacionales e internacionales para establecer los requisitos funcionales y no funcionales del SGDEA, las Normas Técnicas Colombianas – NTC 15489-1 y NTC 15489- 2 para sustentar las políticas, procedimientos y prácticas de gestión documental que definirán el modelo contemplado en las NTC 30301, NTC 30302. La implementación del SGDEA consta de cinco fases (Ver

Tabla 5):

Tabla 5. Fases de implementación del SGDEA

Fase	Actividades

9 Disponible en https://www.archivogeneral.gov.co/caja_de_herramientas/docs/2.%20planeacion/DOCUMENTOS%20TECNICOS/IMPLEMENTACION%20DEL%20SGDEA.pdf
10 Disponible en https://www.archivogeneral.gov.co/caja_de_herramientas/docs/2.%20planeacion/DOCUMENTOS%20TECNICOS/IMPLEMENTACION%20DEL%20SGDEA.pdf

Fase de planeación	Definición del alcance: determinar actividades orientadas a establecer las etapas de desarrollo del proyecto de implementación del SGDEA, describiendo la definición y el control de lo que se va a hacer.
	Establecimiento de objetivos del SGDEA: Formulación de los objetivos a corto, mediano y largo plazo que la entidad (deben ser específicos, medibles, alcanzables y con tiempos definidos).
	Analizar estándares normativos nacionales, internacionales y/o de la organización (leyes, decretos y políticas existentes) en materia de gestión de documentos en materia de gestión de documentos, seguridad de la información, interoperabilidad, gestión de la calidad, gestión ambiental, entre otros.
	Identificar y establecer roles y responsabilidades tanto de la Dirección como responsabilidades operacionales y técnicas enfocadas a un cargo específico, teniendo en cuenta que el personal que realizará estas actividades sea competente para llevarlas a cabo.
	Elaborar un plan de trabajo el cual desglose el proyecto definiendo fases o etapas de implementación entregables, tiempos y responsables en cada una de ellas, con el fin de garantizar que se cumplan los objetivos planteados.
	Planificar la gestión de riesgos, identificando y analizando cada riesgo asociado a la implementación del SGDEA, así mismo definir las estrategias de monitoreo y control, con el fin de evaluar la probabilidad de ocurrencia, su impacto y la estrategia de mitigación.
Fase de análisis	El análisis organizacional consiste en identificar la estructura organizativa de la entidad, sus relaciones y la definición de funciones y responsabilidades.
	El análisis técnico / tecnológico abarca todas las actividades orientadas a identificar los aspectos técnicos y tecnológicos de la entidad, permitiendo determinar si la infraestructura actual soporta la implementación del SGDEA, en el caso contrario la entidad deberá definir las acciones y aspectos requeridos para garantizar la ejecución y puesta en marcha del proyecto. Esta fase comprende la planeación, adquisición y el diseño de la arquitectura necesaria, la verificación del ciclo de vida de los componentes de hardware y software existente como las aplicaciones, servidores, estaciones de trabajo, centros de datos, canales de comunicación, los soportes, formatos y la gestión de las herramientas que apoyaran la implementación del SGDEA.
	En el análisis documental se determina determinar el estado actual de cada uno de los procesos de la gestión documental, incluyendo la identificación de los documentos, su estructura y formatos, así como la verificación del nivel de aplicación de los instrumentos archivísticos. Las actividades a realizar son: • Diagnóstico de la gestión documental. • Identificación de documentos vitales y/o esenciales. • Normalización de formas, formatos y formularios. • Definición del esquema de metadatos.

	• Alineación con los instrumentos archivísticos (PINAR, PGD, CCD, TRD, inventarios documentales, las Tablas de Control de Acceso a los Documentos, el modelo de requisitos para la gestión de documentos electrónicos, los bancos terminológicos de series, subseries y tipos documentales, los mapas de procesos, flujos documentales y la descripción de las funciones de las unidades administrativas de la entidad.
Fase de diseño	Diseñar una estrategia de implementación que permita el cumplimiento de los objetivos planteados y contemple el desglose de actividades detalladas que permitan la implementación progresiva de las diferentes fases alineadas a una solución integral.
	Analizar alternativas por medio del planteamiento de estrategias para el diseño de un sistema de gestión documental electrónica que esté acorde con las necesidades de la entidad (análisis de las soluciones existentes en el mercado, adaptación del software existente o desarrollo a la medida, desglose de las etapas para la adquisición o adaptación de una herramienta tecnológica, estimación de tiempo, sostenibilidad financiera y organizacional, definición de metas de desempeño e interoperabilidad).
Fase de implementación	Una vez se tiene claridad sobre qué procesos o procedimientos se van a automatizar dentro del SGDEA, y se han identificado las necesidades que se pretenden cubrir, se inicia la fase de implementación. Para la fase de implementación se sugiere que cada organización cuente con dos ambientes para su instalación y despliegue (uno de pruebas y uno de producción), a fin de realizar las pruebas pertinentes antes de poner el sistema en marcha Es recomendable hacer la implementación progresiva, garantizando escalabilidad, continuidad e interoperabilidad con lo implementado anteriormente).
Fase de evaluación monitoreo y control	En esta fase se definen las acciones que contribuyen a realizar seguimiento y monitoreo sobre las actividades de cada una de las fases del proyecto, y su avance según su planificación. Esta fase es de vital importancia porque permite identificar y gestionar los riesgos, enumerar y evaluar los hitos importantes del proyecto SGDEA y documentar los cambios o ajustes que hayan surtido durante su implementación. Dentro de las actividades de seguimiento al proyecto SGDEA y a la solución tecnológica están: • Gestión de calidad del proyecto y de las herramientas tecnológicas por medio de indicadores que permitan demostrar el cumplimiento del avance del proyecto con los mismos. • Gestión del cambio por medio de la disposición de estrategias para preparar, entrenar y capacitar en el uso de herramientas digitales y para los cambios que estas conllevan. • Definir estrategias de mejora como actividades, responsables y objetivos que contribuyan a controlar los cambios posteriores a los procesos de implementación del SGDEA, con el fin de verificar que el SGDEA satisface las necesidades por la cuales fue iniciado.

Fuente DANE a partir de AGN 2017

Finalmente, para lograr unificar el SGDEA en la entidad, pueden necesitarse servicios de interoperabilidad, en el cual los documentos creados en los diferentes aplicativos conformen el expediente electrónico, facilitando así su tratamiento, conservación y acceso, para ello debe tenerse

en cuenta el documento técnico "*Modelo de requisitos para la implementación de un sistema de gestión de documentos electrónicos de archivo -SGEDA*[11] ".

1.3.4 Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia

Política de gobierno Digital[12]

Colombia se ha encontrado en una constante evolución del gobierno electrónico y se ha resaltado la importancia de las Tecnologías de la Información y las Comunicaciones para con esto poder mejorar la gestión de las funciones de las entidades públicas. En este camino de transformación y constante fortalecimiento no solo se toman en cuenta los proceso que ya existen, sino que abre las posibilidades a modificar la manera en que el estado a través de las entidades se relaciona con el ciudadano. El gobierno digital se ha ubicado en el centro denominado como "motor" para la transformación digital del Estado. Lo cual permite que las entidades del estado sean más eficientes para con esto poder atender las necesidades de los ciudadanos.

Dentro de esta política de Gobierno Digital, el ministerio de las Tecnologías de la Información y las Comunicaciones expide el 15 de febrero de 2022 el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la política, así mismo se dictan los lineamientos generales para su implementación.

Con la intención de dar un contexto de la política de gobierno digital se desatacan a continuación los componentes y habilitadores transversales para posteriormente poder ahondar un poco más en las guías y buenas prácticas que se han estipulado en el Plan Nacional de Infraestructura de datos. Dentro de los elementos que forman los pilares para la implementación de la política del Gobierno Digital se ubican los componentes y tres habilitadores transversales, estos terminan definiendo los lineamientos para tener un desarrollo de servicios digitales de confianza y calidad, como procesos digitales seguros y eficientes, contar con información de calidad, promoviendo la implementación de la tecnología para empoderar al ciudadano y a los territorios.

Componentes:

11 Disponible en https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/ModeloDeRequisitosSistemaDeGestionElectronicos.pdf

12 Disponible en https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

1. TIC para la sociedad: fortalecer la sociedad y su relación con el Estado en el entorno digital, de manera que este sea confiable, permita la apertura y el aprovechamiento de los datos públicos.
2. TIC para el estado: fortalecer las competencias de T.I. (tecnologías de la Información) de los servidores públicos, como parte fundamental de la capacidad institucional.

Habilitadores transversales:

1. **Seguridad y Privacidad:** Busca las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de las entidades del Estado, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado.

Modelo de seguridad y privacidad de la información[13]

Este componente se desarrolla, a través de lineamientos en materia de seguridad y privacidad de la información, así como de gestión de riesgos de seguridad digital, lo cuales soportan las acciones establecidas por cada entidad para proteger los activos de información, preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos. Es un elemento que apoya a las entidades de manera transversal.

Estrategias:

Se generan como apoyo para que el Gobierno Nacional logre fortalecer las capacidades de las entidades públicas para enfrentar las amenazas del entorno digital, contribuyendo en la creación de una cultura de gestión de riesgos que afiance la confianza en el uso del entorno digital. Es por esto que se considera fundamental robustecer el liderazgo del Gobierno nacional y construir una nueva visión tomando como referentes las mejores prácticas internacionales para abordar los riesgos de seguridad digital.

- ✓ ***CSIRT gobierno****: Equipo de Respuestas a Incidentes de Seguridad digital para las Entidades del Gobierno*

[13] Disponible en https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/

- ✓ ***MGRSD**: El Modelo de Gestión de Riesgos de Seguridad Digital, es un conjunto de lineamientos y buenas prácticas en la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad digital.*
- ✓ ***MSPI**: imparte lineamientos a las entidades públicas para la adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información.*

Iniciativas:

Facilitan las actividades de acompañamiento, apropiación, adopción e implementación de buenas prácticas, con el fin de fortalecer competencias y capacidades en la gestión de la seguridad y privacidad de la información.
Buenas prácticas: Espacio dedicado como repositorio de consejos y buenas prácticas para que las entidades tengan una guía de cómo cumplir con normativa específica o necesidades adicionales dentro de la implementación de la seguridad y privacidad de la información.

2. **Arquitectura:** Busca que las entidades públicas apliquen en su gestión, un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI, aplicando los lineamientos, estándares y mejores prácticas contenidos en el marco de Referencia de Arquitectura empresarial del estado.

Documentos relacionados.

Modelo de Gestión y Gobierno TI[14], este documento describe la estructura del Modelo de Gestión y Gobierno TI – MGGTI, los dominios y lineamientos, las guías que componen el modelo, las evidencias que se deben generar y los procesos que permiten gestionar TI de forma adecuada. Este documento está dirigido a los líderes estratégicos de TI, a los profesionales de las áreas de TI y a los profesionales encargados de la implementación de la política de gobierno digital en las entidades públicas.
Documentos Maestro de Arquitectura Empresarial[15], donde está dirigido a los líderes estratégicos de TI y a los profesionales encargados de la implementación de la política de gobierno digital en las entidades públicas.

Modelo de Gestión de Proyectos de TI[16] , donde Este documento describe la estructura del Modelo de Gestión de Proyectos TI – MGPTI, los dominios y lineamientos, las guías que componen el modelo, las evidencias que se deben generar y los procesos que permiten gestionar TI de forma adecuada.

[14] Disponible en https://www.mintic.gov.co/arquitecturati/630/articles-144767_recurso_pdf.pdf
[15] Disponible en https://www.mintic.gov.co/arquitecturati/630/articles-144764_recurso_pdf.pdf
[16] Disponible en https://www.mintic.gov.co/arquitecturati/630/articles-144766_recurso_pdf.pdf

Este documento está dirigido a los líderes estratégicos de TI, a los profesionales de las áreas de TI, a los gerentes de proyectos internos y externos de la entidad, a los profesionales del área de planeación, a la oficina de gestión de proyectos – PMO y a los profesionales encargados de la implementación de la política de gobierno digital en las entidades públicas.

Plan Nacional de Infraestructura de Datos[17]

A través de la **Resolución 460 de 2022**[18], el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC expidió el Plan Nacional de Infraestructura de Datos – PNID y su Hoja de Ruta, con el fin de impulsar la transformación digital del Estado y el desarrollo de una economía basada en los datos. La iniciativa desarrollará diferentes mecanismos en los que se promoverán modelos de intercambio de datos *(Data trust), datos comunes (Data commons),* mercado de datos *(Data Marketplace)* y portales de datos. La estructuración de este Plan Nacional fue liderada por el Gobierno Nacional en cabeza del Ministerio TIC, el Departamento Nacional de Planeación y el Departamento Administrativo de la Presidencia de la República, asimismo, involucró la participación del sector privado, la academia y la sociedad civil.
Dentro de sus documentos hoja de ruta se resalta tener claro el ciclo de vida del dato, ya que este funciona de base para estipular el Plan Nacional de Infraestructura de datos. Dentro de este ciclo se ubica la creación del dato, el procesamiento, almacenamiento, transferencia, análisis, preservación y reutilización del dato. En la Tabla 6 se puede ahondar en cada una de estas fases del ciclo de vida del dato.

Tabla 6. Ciclo de vida del Dato

Fase, ciclo de vida	Descripción
Crear y obtener	Los datos pueden provenir de diferentes fuentes, estructuradas, no estructuradas o fuentes secundarias como las redes sociales; asimismo también son diversos los formatos en que pueden venir (Ej. Pdf, jpg, docx, xml, txt, json, csv, png, entre muchos otros). Los datos suelen ser creados por las organizaciones, usualmente de las siguientes formas: Reutilización Creación Procesamiento Almacenamiento Intercambio Uso y análisis de datos Archivo y preservación 5 · Adquisición de datos: adquisición de datos ya existentes que se han producido fuera de la organización.

[17]Disponible en https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/198952:MinTIC-expide-el-Plan-Nacional-de-Infraestructura-de-Datos-que-impulsara-la-transformacion-digital-del-Estado
[18] Disponible en https://www.mintic.gov.co/portal/715/articles-198952_resolucion_00460_2022.pdf

	▪ Entrada de datos: entrada manual de nuevos datos por parte del personal dentro de la organización. ▪ Captura de datos: captura de datos generados por dispositivos utilizados en varios procesos de la organización. El modelado y diseño de datos es de suma importancia en esta fase, pues determina que información es la que se determina utilizar.
Procesar	La etapa de procesamiento incluye las siguientes tareas: ▪ Limpieza de datos: en la que un conjunto de datos se limpia y se transforma de su forma sin procesar a algo más accesible y utilizable. Esto también se conoce corrección de datos. ▪ Compresión de datos: en la que los datos se transforman en un formato que se puede almacenar de manera más eficiente. ▪ Cifrado de datos: en el que los datos se traducen a otra forma de código para protegerlos de problemas de privacidad. ▪ Calidad de los datos: en los procesos de obtención y procesamiento de datos, donde principalmente se aplican las políticas y controles, establecidas en el diseño, con el propósito de determinar cuáles datos son utilizables.
Almacenar	El almacenamiento y operaciones incluyen el diseño, la implementación y el soporte de los datos almacenados para maximizar su valor, utilizando tanto formatos como repositorios que busquen el equilibrio entre disponibilidad y coste de almacenamiento, según los distintos escenarios de consulta, por ejemplo, diferenciando datos de alta demanda o disponibilidad de otros que no se consultan frecuentemente. Comúnmente el almacenamiento se realiza mediante la creación de bases de datos o conjuntos de datos. Estos conjuntos de datos pueden almacenarse en la nube, en servidores on premise o utilizando otras formas de almacenamiento físico como discos duros magnéticos o de estado sólido, memorias o cintas magnéticas, entre otros.
Transferir y compartir	A medida que las organizaciones requieren de datos de fuentes secundarias, generados por otros actores del ecosistema de datos, útiles para la toma de decisiones, la planificación, la optimización de operaciones, entre otros, existe una mayor presión para compartir también datos generados. Los datos compartidos pueden ayudar a mejorar las decisiones, ya que las organizaciones pueden obtener una vista más completa de los impactos que sus decisiones han tenido con base en las contribuciones de nuevos conjuntos de datos de una variedad más amplia de fuentes, tanto internas como externas. Esta capacidad de compartición de datos debe estar soportada en una capa de interoperabilidad y haciendo uso de un estándar de lenguaje común de intercambio.

Analizar y usar	Durante la fase de uso del ciclo de vida de los datos, los datos se utilizan para respaldar las actividades de la organización. Los datos se pueden ver, procesar, modificar y guardar. Se debe mantener un registro de auditoría para todos los datos críticos, con el propósito de garantizar que todas las modificaciones que se realicen a los datos sean completamente rastreables y auditables. Los datos también pueden estar disponibles para exponer a otros actores del ecosistema de datos que se encuentren fuera de la organización. El análisis de datos se refiere a procesos que intentan obtener información significativa a partir de datos sin procesar. Los analistas y científicos de datos utilizan diferentes herramientas y estrategias para realizar estos análisis. Algunos de los métodos más utilizados incluyen modelado estadístico, algoritmos, inteligencia artificial, minería de datos y aprendizaje automático.
Archivar y preservar	El archivado de datos hace referencia a la copia de datos en un entorno donde se almacenan en caso de que se necesiten nuevamente en un ambiente de producción, así mismo también incluye la eliminación de estos datos de todos los entornos de producción activos. Un archivo de datos es simplemente un lugar donde se almacenan los datos, pero donde no se realiza mantenimiento o uso general. Si es necesario, los datos se pueden restaurar a un entorno en el que se puedan utilizar. Dado que el volumen de datos archivados crece inevitablemente, si bien es posible que desee guardar todos los datos de manera indefinida, los costos de almacenamiento pueden incentivan la destrucción de los datos que ya no se requieren. Por otro lado, es posible que se disponga de datos de uso limitado a una ventana de tiempo o a hasta /durante la ocurrencia de un suceso. La destrucción o depuración de datos es la eliminación de cada copia de un elemento de datos de una organización.
Reutilizar	Reutilizar significa usar datos que originalmente fueron recopilados para otro fin o propósito. La reutilización de datos también se puede llamar análisis secundario.

Fuente: Tomado de Anexo 1.2 “Ciclo de vida del dato” del Plan Nacional de infraestructura de datos

Guías, instrumentos y lineamientos[19]

ArCo es la metodología que busca optimizar y mejorar la eficiencia de la oferta institucional de los instrumentos de política pública que brindan las entidades del orden nacional en materia de competitividad, productividad, emprendimiento, ciencia, tecnología e innovación en Colombia. En el

[19] Disponible en https://www.mintic.gov.co/portal/715/articles-198952_anexo_1_3_guias_instrumentos_lineamientos.pdf

marco de esta metodología se presentan a continuación las guías, lineamientos e instrumentos con los que cuenta el país para apoyar la implementación del PNID en sus distintos componentes.

Tabla 7. Guías para la implementación del Plan Nacional de la Infraestructura de datos

Nombre del instrumento, guía, lineamientos	Descripción	Relación con la infraestructura de datos
PETI	El Plan Estratégico de las Tecnologías de la Información y Comunicaciones es el artefacto que utilizan las Entidades para expresar la Estrategia de TI. Incluye una visión, unos principios, unos indicadores, un mapa de ruta, un plan de comunicación y una descripción de todos los demás aspectos (financieros, operativos, de manejo de riesgos, etc.) necesarios para la puesta en marcha y gestión del plan estratégico.	Las iniciativas y proyectos relacionados con la implementación de la infraestructura de datos del Estado colombiano deben estar contempladas en la planeación estratégica de TI de las entidades, en ese sentido, es necesario que con base en los casos de uso identificados para el aprovechamiento y explotación de los datos con los que se cuenta, se establezcan en el PETI los proyectos que permitan explotar, consumir, exponer, compartir información.
Marco de Referencia de Arquitectura Empresarial	El Marco de Referencia Arquitectura Empresarial – MRAE es el instrumento principal para apoyar a las instituciones en la adopción de la práctica de Arquitectura Empresarial, la gestión de proyectos de TI, y la gestión y gobierno de TI.	Siendo la información un aspecto transversal de toda entidad, el MRAE se articula con el Plan Nacional de Infraestructura de Datos, principalmente en el Dominio de arquitectura de Información: "Los lineamientos de este dominio permiten definir: el diseño de los servicios de información, la gestión del ciclo de vida del dato, al análisis de información y el desarrollo de capacidades para el uso estratégico de la misma".
	El Modelo de Seguridad y Privacidad de la Información –	Este instrumento está muy ligado al componente de Seguridad y

Modelo de seguridad y protección de información (MSPI)	MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la adecuada ejecución de la Política de Gobierno Digital.	privacidad de los datos de la Infraestructura de datos, en la medida en que permite la adopción de buenas prácticas y estándares para garantizar la seguridad de los datos.
Marco de transformación digital	En cumplimiento del artículo 147 de la Ley 1955 del 2019 – Plan Nacional de Desarrollo, que dispone que las entidades estatales del orden nacional deben incorporar en sus planes de acción el componente de transformación digital, se adopta el Marco de Transformación Digital, cuyo propósito es posibilitar la habilitación de capacidades a las entidades públicas para apalancar su transformación digital y el uso de tecnologías emergentes, a través, de la reinvención o modificación de los procesos, productos o servicios, para asegurar la generación del valor de lo público.	El marco de transformación digital permite a las entidades el desarrollo de planes de transformación digital en las dimensiones de personas, procesos y tecnología, bajo la cual, las entidades públicas pueden definir iniciativas que desarrollen la infraestructura y el uso de datos para la toma de decisiones.
	Es un instrumento estandarizado que tiene por objetivo fomentar la explotación de datos en las entidades públicas y fortalecer la cultura basada en datos, al considerarlos como un activo estratégico para impulsar la transformación digital y mejorar la toma de decisiones en el	A través de este modelo, las entidades públicas pueden medir el desarrollo de sus capacidades para aprovechar los datos, gobernarlos y gestionar su ciclo de vida.

Modelo de explotación de datos	sector público. Este modelo está articulado con la Política de Gobierno digital liderada por el Ministerio de las Tecnologías de la Información y las Comunicaciones, por lo que está dirigido a entidades públicas del orden nacional y territorial.	
Marco de interoperabilidad	Este Marco define el conjunto de principios, recomendaciones y directrices que orientan los esfuerzos políticos, legales, organizacionales, semánticos y técnicos de las entidades, con el fin de facilitar el intercambio seguro y eficiente de información entre las entidades del Estado.	Como parte de una constante evolución para el buen uso de las tecnologías, se han identificado diferentes escenarios para intercambiar información entre entidades del Estado. El marco de interoperabilidad establece unas actividades mínimas que deben realizar las entidades para garantizar en todos los ámbitos la interoperabilidad en beneficio de la relación entre ciudadanos y el Gobierno.
Lenguaje común de intercambio de datos	Este Lenguaje Común de Intercambio de Información brinda un significado y una estructura unificada sobre los datos, facilitando el entendimiento del negocio y el intercambio de información de la entidad. Es esencial entender la información o datos que comparten dos o más entidades en un proceso de intercambio, para lo cual se debe hacer uso del estándar nacional definido y administrado por el Ministerio de Tecnologías de la Información y las Comunicaciones. El estándar de lenguaje común fue diseñado para entender y facilitar el intercambio de información entre las entidades públicas con	Con el estándar de lenguaje común se garantiza que los datos que se encuentren disponibles en el Plan Nacional de Infraestructura de Datos cumplan con los principios de Calidad de los datos, la reutilización y la estandarización para el uso adecuado de los datos y metadatos, acorde a lo definido en el Marco de Interoperabilidad para Gobierno Digital. Respecto a la calidad de los datos, se debe mantener como una característica que se define en los acuerdos realizados entre las entidades para publicar o intercambiar información en un entorno que facilite la reutilización de servicios con datos estandarizados para

	el propósito de mejorar los servicios digitales dirigidos a los ciudadanos y empresas. El uso del estándar brinda un significado y una estructura unificada sobre los datos, facilitando el entendimiento del negocio y el intercambio de información de la entidad. Así mismo, este Lenguaje Común de Intercambio de información puede ser utilizado por las entidades del Estado para obtener la información de los ciudadanos, a través de formularios, o para entregar datos o información estructurada.	ayudar a reducir costos y esfuerzos a las entidades y ciudadanos. Además de reutilizar estos servicios, es claro que también se logra reutilizar y compartir conocimiento, experiencias y cooperar en el desarrollo de soluciones conjuntas durante el proceso de estandarización y la implementación de servicios de intercambio. El estándar, a su vez, ofrece un diccionario para las entidades, amplio y mejorado, el cual permite la consulta y disponibilidad de los metadatos con la correspondiente semántica y sintaxis.
Guía para el uso y aprovechamiento de Datos	Este documento proporciona orientaciones y buenas prácticas para el desarrollo de estrategias de apertura y re uso de datos abiertos, que estén orientadas a la generación de valor en lo económico, social, político, cultural, ambiental, y en general, en los distintos ámbitos de la sociedad.	A través de esta Guía, las entidades públicas pueden implementar las orientaciones y buenas prácticas para el desarrollo de estrategias de apertura y re uso de sus conjuntos de datos abiertos.
Guía de gobierno de datos	La Guía de Gobierno de datos apoya la implementación de los lineamientos asociados al registro y seguimiento de componentes de información, al establecimiento de los mecanismos de actualización, la creación y mantenimiento del repositorio unificado de estructuración de los componentes de información, la clasificación de componentes de información para el intercambio y consolidación de estos a nivel	La guía de Gobierno de datos ayuda a organizar la forma en que se conciben y comunican conceptos complicados o ambiguos. El uso de un marco formal puede ayudar a todos los interesados, desde directivos a personal de IT, de gestión de datos y otras disciplinas, a articularse para lograr una claridad de pensamiento y propósito. El uso de un marco formal de trabajo puede ayudar a la gerencia y al personal en

	sectorial; para presentar los Componentes que pueden ser aplicados por las entidades para el buen Gobierno del Dato, desde la perspectiva del dominio de Información del Marco de Referencia de Arquitectura Empresarial.	general a tomar buenas decisiones. Puede ayudarles a llegar a un acuerdo acerca de la forma de "decidir cómo se debe decidir". De esta forma se pueden crear reglas de forma más eficiente, garantizando que las normas se siguen, y haciendo frente a las ambigüedades, los problemas y los incumplimientos.

Fuente: Tomado de Anexo 1.3 "Guías, instrumentos y lineamientos de Plan Nacional de infraestructura de datos.

1.3.5 Ministerio de Educación Nacional

El Ministerio de Educación Nacional – MEN, desarrolló el Programa de Gestión Documental – PGD 2019-2024[20], enmarcado en el cumplimiento de la ley 594 de 2000 (Ley general de archivo), Ley 1712 de 2014 (Ley de transparencia y acceso a la información), y el Decreto 1080 de 2015. El PGD es un programa que fortalece la construcción de la cultura de gestión del documento electrónico con política cero papel y fácil acceso a la información para usuarios internos y externos, preservando siempre las buenas prácticas.

El PGD se vincula al Sistema Integrado de Gestión a través de la ejecución y seguimiento del Sistema de Desarrollo Administrativo, acorde al Decreto 2482 de 2012, el cual contempla la Política de Eficiencia Administrativa que tiene cómo pilar el logro de los objetivos del Estado, por medio de la implementación de temas relacionados con "cero papel", racionalización de trámites, modernización institucional, gestión de tecnologías de información y gestión documental. Cuenta con varios ejes temáticos encaminados a un óptimo manejo de la información:

Producción documental: con este proceso se busca generar documentos físicos, digitales o electrónicos, teniendo en cuenta el principio de racionalidad, la creación y diseño de formas, formularios y documentos, aplicando el contexto normativo, legal, funcional, técnico, archivístico y tecnológico para cumplir con las funciones y procesos de las dependencias del Ministerio.

20 Disponible en https://www.mineducacion.gov.co/1759/articles-362792_galeria_33.pdf

Gestión y trámite de los documentos: cuyo propósito es garantizar la disponibilidad, recuperación, trámite y acceso a la información generada, con el fin de brindar una respuesta oportuna a las solicitudes de los usuarios.

Organización y transferencia documental: busca garantizar desde el SGD la correcta organización e identificación de los documentos de conformidad con la tabla de retención documental para archivos físicos y electrónicos, clasificando, describiendo y ordenando la información en el archivo de gestión.

Transferencia documental: se deben realizar los traslados documentales una vez cumplidos los tiempos de permanencia de conformidad con el ciclo vital del documento, acorde con los tiempos de retención establecidos en los cronogramas, con el fin de generar las condiciones de conservación y evitar la aglomeración de documentos en las oficinas.

Disponibilidad final de los documentos: asegurar la correcta selección, conservación y eliminación análoga, electrónica o digital de los documentos para garantizar la integridad y preservación de la información del Ministerio.

Preservación a largo plazo: el programa busca determinar las acciones a seguir para lograr la adecuada preservación en el tiempo para documentos físicos, electrónicos y digitales para la consulta. Desde el planteamiento, establece la necesidad de:

- Elaborar e implementar el sistema integrado de conservación.
- Definir los lineamientos para la preservación de documentos análogos, digitales y electrónicos.
- Realizar un estudio de necesidades para la adecuación de la infraestructura de datos.
- Establecer la política de seguridad de la información.
- Definir los parámetros para la seguridad de la información en entornos electrónicos.
- Identificar cuáles son los documentos electrónicos de archivo que se producen o generan en el Ministerio.
- Establecer políticas de Backups.

Programa de auditoría y control: tiene como propósito, generar a mediano plazo la cultura de autocontrol en la administración de archivos y la producción documental, aplicando estándares de calidad, identificando procesos, procedimientos, indicadores y mapa de riesgo para la evaluación y el control del Macroproceso de Gestión Documental – MGD, involucra todos los componentes de gestión documental, servidores públicos y herramientas tecnológicas.

El programa de auditoría y control permitirá identificar, controlar, evaluar y modificar las situaciones o circunstancias que afecten negativamente el Macroproceso de Gestión Documental. Los pasos para su implementación se desarrollan de la siguiente manera:

- Establecer contacto con la Oficina de Control Interno para establecer las condiciones de coordinación y apoyo que se debe prestar al Macroproceso de Gestión Documental.
- Solicitar capacitaciones de autocontrol a la Oficina de Control Interno.
- Programar y realizar actividades de autoevaluación del MGD.
- Generar acciones de mejora, producto de la autoevaluación para el MGD.

Actualmente, el Ministerio cuenta con protocolos de seguridad, establecidos en el Manual de Seguridad Informática21. Dicho manual tiene como objetivo, propender que los servicios tecnológicos y de comunicaciones se ofrezcan con calidad, confiabilidad, integralidad y eficiencia, su alcance se extiende a funcionarios, contratistas, personal de apoyo y terceros no vinculados directamente al MEN, pero que presten su servicio y utilicen insumos del Ministerio.

1.3.6 Departamento Nacional de Planeación

El Departamento Nacional de Planeación – DNP desarrolló el Manual y Políticas de Seguridad de la Información[22] en el año 2019, con el objetivo de garantizar que los riesgos asociados a la seguridad de la información sean identificados, valorados, controlados y administrados de una forma estructurada y eficiente, dando cumplimiento a lo establecido en el Marco de la Protección de Datos Personales. El cumplimiento del manual es obligatorio para todos los usuarios, incluyendo terceros que se encuentren vinculados a la entidad.

El Sistema de Gestión de la Seguridad de la Información - SGSI del DNP, es un sistema integrado de políticas, procesos, instructivos, lineamientos, guías, formatos, mapas de riesgos, estructura organizacional, mecanismo de verificación y control, que permiten minimizar los riesgos asociados a la seguridad de la información y atender en forma positiva incidentes de este tipo. Su propósito está soportado en el Proceso de Gestión de la Seguridad de la Información en el componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad. El SGSI protege los activos de información que la entidad identifica a través del lineamiento para la identificación y valoración de activos de información en el Sistema de Seguridad de la Información.

21 Disponible en https://www.mineducacion.gov.co/1759/articles-322548_Manual_de_Seguridad_Informatica_.pdf).
22 Disponible en https://colaboracion.dnp.gov.co/CDT/DNP/SE-M01%20Manual%20y%20Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Información.Pu.pdf

Características básicas de la seguridad de la información

La gestión integral de la información se protege desde la plataforma tecnológica, infraestructura física y recurso humano que la soporta, de acuerdo a la resolución Nº 0442 de 2009 del DNP.

La información debe estar protegida para que sea accedida por usuarios autorizados:

- Públicos: Cualquier información no clasificada se considera como privada. La información pública, era aquella cuya divulgación no afecte a la Entidad en términos de pérdida de imagen y/o económica.
- De uso interno: Información que, sin ser privada ni confidencial, debe mantenerse dentro de la Entidad y no debe estar disponible externamente, excepto para terceros involucrados en el tema. En el caso de terceros, deberán comprometerse a no divulgar dicha información firmando un acuerdo de confidencialidad.
- De uso privado o restringido: Información sensible, interna a áreas o proyectos a los que deben tener acceso restringido, controlado otros grupos, pero no toda la Entidad debido a que se puede poner en riesgo la seguridad e intereses de la Entidad, de sus clientes o asociados y empleados.
- Confidencial o de reserva: Información de alta sensibilidad que debe ser protegida por su relevancia sobre o de reserva, decisiones estratégicas, impacto financiero, oportunidad de negocio, potencial de fraude o requisitos legales.

Todo tipo de información que se maneje en DNP, debe cumplir con las siguientes características:

- Debe estar adecuadamente protegida para asegurar que no sea alterada.
- Los activos de información solo pueden estar disponibles, verificando la identidad de un sujeto o recurso.
- Los activos de información deben tener controles que permitan su revisión.
- Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.
- Los riesgos de seguridad de la información se identifican mediante el AR-L02 Lineamiento para la Gestión Integral de Riesgos disponible en la intranet en la sección Sistema integrado de Gestión, Macroprocesos, Gestión Integral Institucional, Proceso gestión integral de riesgos.

Respaldo de la información – *Backup*

- La información del DNP debe ser respaldada de forma frecuente y debe ser almacenada en lugares apropiados, el respaldo de la información contenida en las estaciones de trabajo es responsabilidad de los usuarios.
- Es responsabilidad de la Oficina de Tecnologías y Sistemas de Información – OTSI el respaldo de forma frecuente de la información para ser recuperada en caso de incidentes de seguridad con los equipos de procesamiento y almacenamiento.
- En caso de que el usuario requiera apoyo en la realización de *backup* o copia de seguridad de la información almacenada en las estaciones de trabajo, debe solicitarlo al centro de servicios.
- Semanalmente, los operadores del centro de cómputo verificarán la ejecución correcta del backup, suministrarán las cintas requeridas para cada copia y controlarán la vida útil de cada cinta o medio.
- La OTSI debe mantener un inventario actualizado de las copias de respaldo.
- La OTSI tiene la responsabilidad de generar las copias de respaldo de la información de los discos de red. La recuperación de la información se garantizará por los últimos 12 meses anteriores a la fecha de solicitud.
- La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el responsable de la información.
- Las conexiones de acceso remoto deben ser registradas en los logs de auditoría.

1.3.7 Organización Internacional de Normalización – ISO

Las normas ISO[23] son estándares internacionales que se agrupan de acuerdo con diferentes actividades y que contribuyen a los Objetivos de Desarrollo Sostenible – ODS, **Error! Reference source not found.**, hasta la fecha han publicado más de 24.350 Normas Internacionales relacionadas con tecnología y fabricación; cada país cuenta con un representante de ISO; existen 807 comités y subcomités técnicos encargados del desarrollo de normas.

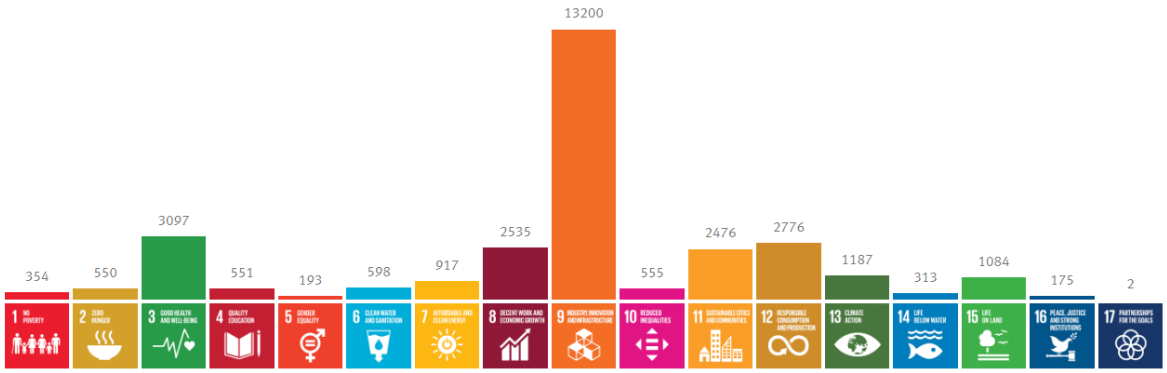
Estos estándares son creados a partir de la experiencia de expertos en distintas áreas, quienes conocen las necesidades de las organizaciones y representan fabricantes, compradores, clientes, asociaciones comerciales, usuarios o reguladores. Como parte de las normas que están publicadas se encuentra:

- Estándares de gestión de calidad: para ayudar a trabajar de manera más eficiente y reducir las fallas del producto.

[23] Disponible en https://www.iso.org/standards.html

- Estándares de gestión ambiental: para ayudar a reducir los impactos ambientales, reducir los desechos y ser más sostenibles.
- Estándares de salud y seguridad: para ayudar a reducir los accidentes en el lugar de trabajo.
- Estándares de gestión de energía: para ayudar a reducir el consumo de energía.
- Normas de seguridad alimentaria: para ayudar a evitar que los alimentos se contaminen.
- Estándares de seguridad de TI: para ayudar a mantener segura la información confidencial.

Ilustración 9. ISO contribuye a todos los objetivos de desarrollo sostenible



Fuente: ISO, 2022

Esta sección se centra en la familia de las ISO relacionadas con los estándares de Seguridad de TI, como se muestra en la Tabla 8.

Tabla 8. ISO sobre Seguridad de TI

ISO	Nombre	Actualización
22301	Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Requisitos	2019
27001	Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos	2013
27002	Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información	2022
27032	Tecnologías de la información — Técnicas de seguridad — Directrices para la ciberseguridad	2012
27701	Técnicas de seguridad. Extensión a ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la privacidad de la información. Requisitos y directrices.	2019

Fuente: Elaboración propia

NORMA ISO 22301:2019[24]: Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Requisitos.

Esta norma presenta los requisitos para implementar, mantener y mejorar un sistema de gestión para proteger, reducir las probabilidades de riesgo, prepararse para responder y recuperarse de los inconvenientes que surjan. Los requisitos descritos son genéricos y se pueden aplicar a todas las organizaciones, sin importar su tamaño o naturaleza; su alcance depende del entorno operativo y la complejidad de la organización.

Se puede implementar en organizaciones que mantienen o quieren mejorar el Sistema de gestión de la continuidad del negocio – SGCN; garantizar la política de continuidad del negocio; y la capacidad para adoptar mecanismos para entregar los productos y servicios. Se debe hacer una planificación para implementar el SGCN, que abarque la gestión de registros y oportunidades; consecución de objetivos, objetivos de continuidad del negocio; y cambios en el SGCN, como se presenta en la Ilustración 10.

Ilustración 10. Planificación SGCN

Fuente: DANE a partir de ISO 22301

Norma 27001:2013[25] Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos.

Esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información – SGSI dentro del contexto

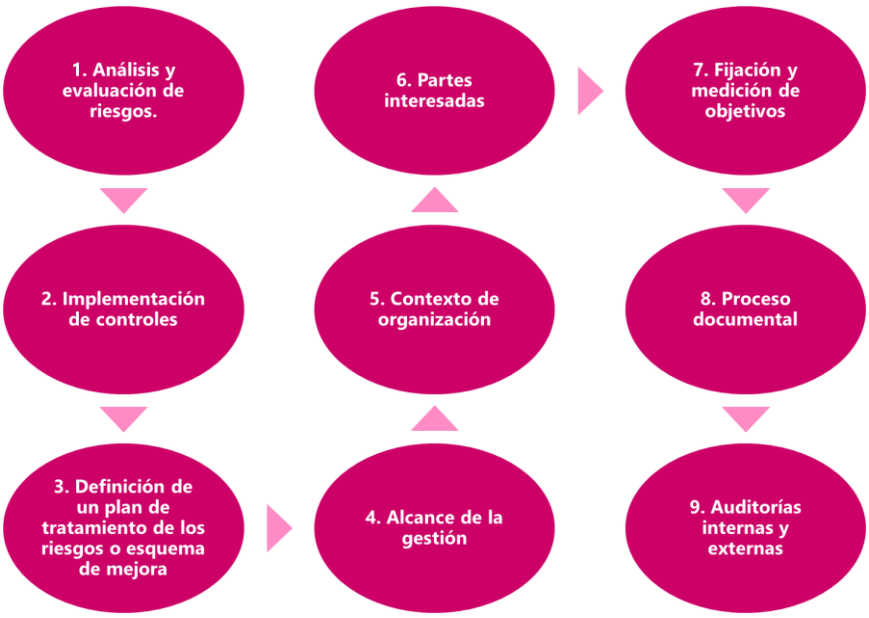
[24] Disponible en https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-22301-Guia-de-implantacion.pdf
[25] Disponible en https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

de la organización. Además, incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización.

Tiene relación con la Norma 22301:2019, en aspectos de seguridad de la empresa, sin embargo, la 27001 no cuenta con tiempos de recuperación, los cuales son cruciales para evaluar los planes de contingencia.

El propósito de un SGSI es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática y estructurada. Para dar cumplimiento a este propósito establece nueve fases para elaborar un SGSI, presentadas en la Ilustración 11.

Ilustración 11. Fases de un SGSI basado en la norma ISO 27001



Fuente: DANE a partir de ISO 27001

- ***Fase 1. Análisis y evaluación de riesgos.***

Se inicia realizando una identificación y análisis de las principales amenazas, y a partir de estas establecer una evaluación y planificación de riesgos. Las amenazas se definen como "evento que puede afectar los activos de información", causados por recurso humano, eventos naturales o fallas técnicas.

Para llevar a cabo un proceso de identificación se debe (1) identificar todos los activos de información que tienen algún valor para la organización; (2) asociar las amenazas relevantes con los activos; (3) determinar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas; y (4) identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

- ***Fase 2. Implementación de controles***

La norma establece 113 puntos de control que se dividen en políticas de seguridad de la información, organización de la seguridad de la información, seguridad de los recursos humanos, gestión de activos, controles de acceso, criptografía – cifrado y gestión de claves, seguridad física y ambiental, seguridad operacional, seguridad de las comunicaciones, adquisición, desarrollo y mantenimiento del sistema, gestión de incidentes de seguridad de la información, y cumplimiento.

- ***Fase 3. Definición de un plan de tratamiento de los riesgos o esquema de mejora***

En esta fase se define el plan de tratamiento o esquema de mejora, teniendo en cuenta las distintas consecuencias potenciales de los riesgos para evaluarlos con objetividad. Existen tres formas de afrontar el riesgo; eliminarlo, mitigarlo o trasladarlo.

Se debe eliminar si es un riesgo muy crítico y pone en peligro la continuidad de la organización. Se mitiga si no es posible eliminarlo en su totalidad, porque se requiere de él o no se considera lo suficientemente crítico y se debe establecer medidas preventivas o correctivas para que no ocurra un impacto. Se traslada cuando se contrata algún seguro que compense las consecuencias económicas de una pérdida o deterioro de la información.

- ***Fase 4. Alcance de la gestión***

Desde la planeación se debe definir el alcance para implementar un SGSI en la organización, teniendo en cuenta su tamaño, número de empleados, número de clientes, volumen de activos físicos y lógicos, cantidad de sedes y elementos adicionales para dar contexto a la organización. Recomiendan incluir este sistema en las áreas donde se genera el cumplimiento de la misión institucional.

- ***Fase 5. Contexto de organización***

Se realiza un contexto de la organización para determinar problemas internos y externos, se revisan sus debilidades, amenazas, fortalezas y oportunidades que afectarían la implementación.

- ***Fase 6. Partes interesadas***

Se debe involucrar a todas las partes interesadas para comprender las necesidades y expectativas. Por ejemplo, proveedores de servicios de información y de equipamientos de Tecnologías de la Información – TIC; clientes, respetando la gestión de datos de protección personal; fuerzas de seguridad de cada estado y autoridades jurídicas para tratar los aspectos legales; la sociedad en general.

- ***Fase 7. Fijación y medición de objetivos***

Fijar objetivos para la gestión de riesgos que sean medibles, puede que no sean cuantificables; se deben comunicar a toda la organización para involucrarlos en el proceso; y deben contar con unos indicadores que permitan realizar un seguimiento al cumplimiento de las actividades.

- ***Fase 8. Proceso documental***

Esta norma establece de manera estricta la gestión de documentación y exige que se realicen procedimientos documentados para gestionar toda la información interna y externa, con el fin de ser consultada.

- ***Fase 9. Auditorías internas y externas***

Para garantizar el correcto funcionamiento de un SGSI basado en la norma ISO 27001, es necesario llevar a cabo auditorías internas periódicamente, con el fin de comprobar que el sistema se encuentra en un estado idóneo.

Norma 27002:2022[26] Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información.

Proporciona un conjunto de referencias de controles genéricos de seguridad de la información, incluida una guía de implementación y está diseñado para utilizarlo en organizaciones que implementan el SGSI, consideren implementar controles de seguridad de la información basados en las mejores prácticas, y quieran desarrollar directrices en materia de gestión de seguridad de la información de la organización.

Es un estándar útil para los responsables de diseñar, implantar o mantener el SGSI de cualquier organización, independientemente de su sector y tamaño. Los puntos principales de esta norma son:

- Proporciona una base común para desarrollar las normas de seguridad dentro de las organizaciones.

[26] Disponible en https://www.escuelaeuropeaexcelencia.com/2022/03/iso-270022022-principales-cambios-en-la-nueva-guia-de-controles-de-seguridad-de-la-informacion/

- Provee de prácticas eficaces para la implantación del SGSI haciendo uso de las nuevas tecnologías, evitando ataques informáticos.
- Proteger adecuadamente a las empresas.
- Maximizar el retorno de las inversiones y oportunidades de negocio.
- Es flexible y autónomo, lo que garantiza su adaptación a cualquier tecnología o sistema que ya esté siendo utilizado por la empresa.

Esta norma tiene una actualización en marzo de 2022 y presenta algunos ajustes de los controles[27] con respecto a su versión del 2013, se reduce el número de controles de 114 a 93, presentando una fusión en algunos controles y la inclusión de temas que no se tenían en cuenta; como por ejemplo, la inteligencia sobre amenazas, la vigilancia de la seguridad física, la eliminación de información, las actividades de seguimiento, la gestión de la configuración, el filtro web, la codificación segura, la seguridad de la información para el uso de servicios en la nube, la preparación de las TIC para la continuidad de la actividad, la prevención de la fuga de datos y el enmascaramiento de datos.

Adicionalmente, en esta versión se presentan 4 secciones adicionales; los controles organizaciones, los controles de personas, los controles físicos y los controles tecnológicos. En términos de definir atributos en ciberseguridad se pretende identificar, proteger, detectar, responder y recuperar la información; en capacidad operativa, revisar la gestión de activos, seguridad de recursos humanos, gobernanza, protección de la información, seguridad de aplicaciones, controles de acceso, riesgos, amenazas y vulnerabilidad.

Norma 27032:2012[28] Tecnologías de la información — Técnicas de seguridad — Directrices para la ciberseguridad.

Esta norma es una orientación para mejorar el estado de la ciberseguridad, destacando la seguridad de información, seguridad de la red, seguridad en internet, y protección de la infraestructura de información crítica – CIIP; cubre las prácticas básicas de seguridad para las partes interesadas en el ciberespacio. Además, proporciona una visión general de la ciberseguridad, una explicación de la relación entre la Ciberseguridad y otros tipos de seguridad, una definición de las partes interesadas y una descripción de sus funciones en la ciberseguridad, orientación para abordar problemas comunes de ciberseguridad, y un marco para permitir que las partes interesadas colaboren en la resolución de problemas de ciberseguridad.

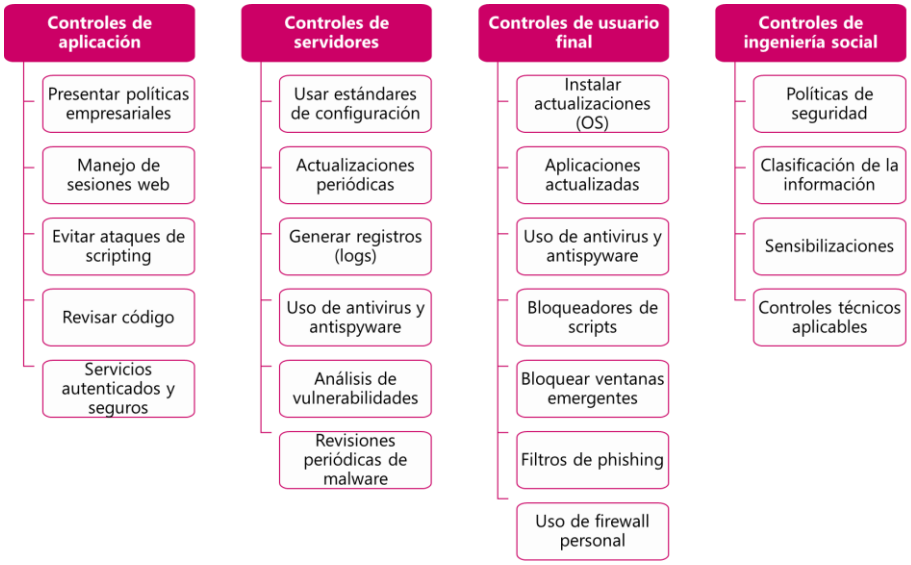
Se proponen tres estrategias[29] para mitigar los riesgos; detección, preparación y respuesta; con un marco para compartir información, gestionar incidentes y coordinar respuestas. Además de

[27] Disponible en https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27002-Mapping-ES.pdf
[28] Disponible en https://www.iso.org/standard/44375.html
[29] Disponible en https://sisteseg.com/blog/wp-content/uploads/2018/12/ISO-27032-v-2.pdf

mantener la confidencialidad, integridad y disponibilidad en la seguridad de la información; en las aplicaciones se considera revisar la seguridad en los procesos, componentes, software, resultados y datos; en la seguridad de la red se revise el diseño, implementación y operación; en la seguridad de internet verificar el servicio de internet seguro, las redes, la disponibilidad del servicio y la fiabilidad de servicios, y la seguridad en la infraestructura revisar el *datacenter*, las condiciones ambientales, el acceso físico y sitios alternos.

En la norma se establecen las metas de la ciberseguridad como proteger el ciberespacio, gestión de crisis, educación, alerta sobre amenazas, coordinación entre entidades, y controles de ciberseguridad que se presentan en la Ilustración 12.

Ilustración 12. Controles de ciberseguridad



Fuente: DANE a partir de ISO 27032

Norma 27701:2019[30] Técnicas de seguridad. Extensión a ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la privacidad de la información. Requisitos y directrices.

Esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de gestión de Privacidad de la Información – SGPI, y es complemento de la norma 27001 y 27002 para la gestión de privacidad dentro del contexto de la organización. Es aplicable a todos los tipos y tamaños de organizaciones, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro, que son controladores de PII y/o procesadores de PII que procesan PII dentro de un SGSI.

[30] Disponible en https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27701-Mini-Implementation-Guide-ES.pdf

1.3.8 Marco COBIT – Objetivos de Control para las Tecnologías de la Información y Relacionadas:

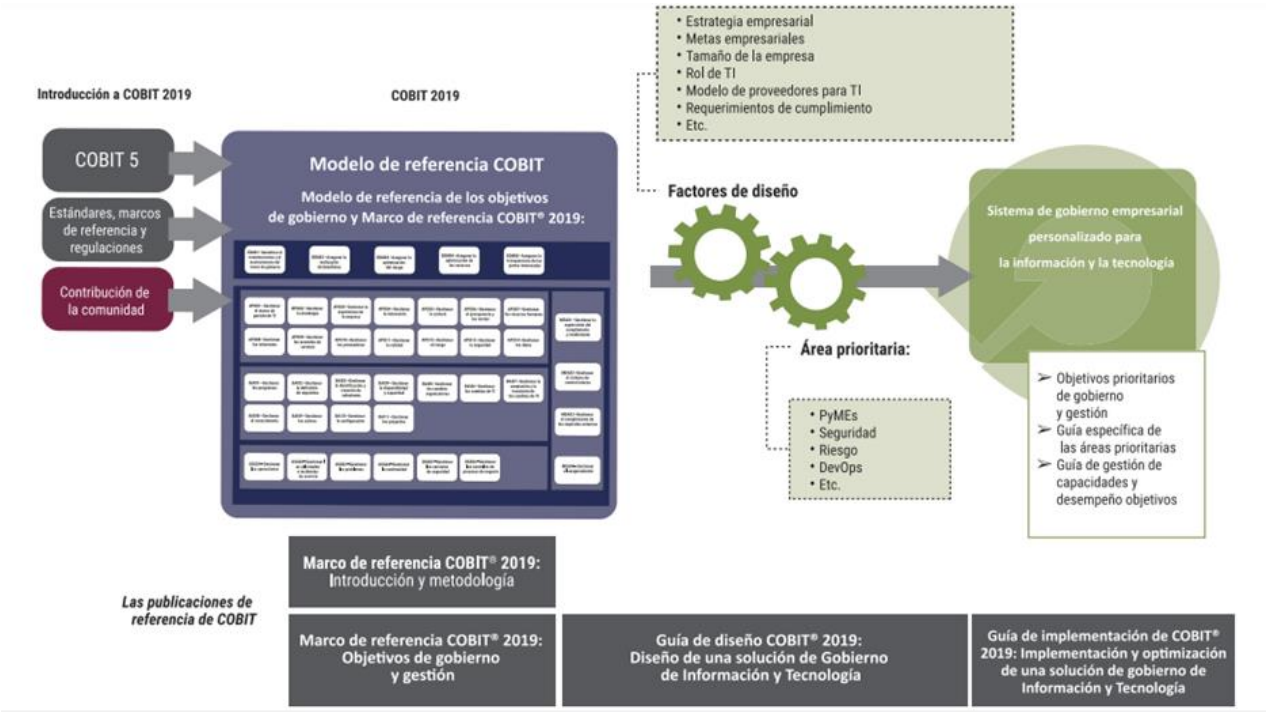
Actualmente, la transformación digital y las tecnologías de la información son vitales en el apoyo, sostenibilidad y crecimiento de las empresas, dado esto, en los últimos treinta años ha surgido un enfoque específico en gobierno de empresa y tecnología de la información – EGIT, y aunque no existe una "ideal forma" de diseñar, implementar y mantener un EGIT dentro de una organización, los miembros de los órganos ejecutivos deben adaptar sus medidas EGIT y aplicación al contexto y necesidades específicas, asegurando con una adaptación exitosa tres resultados:

1. Realización de beneficios por medio de la creación de valor para la empresa a través de tecnologías de la información y la eliminación de activos que no estén creando suficiente valor.
2. Gestión del riesgo, abordando el riesgo asociado con el uso, operación, participación, influencia y adopción de las Tecnologías de la información dentro de una empresa (en otras palabras, la gestión de riesgos se centra en la conservación del valor).
3. Optimización de recursos, pues asegura que se proporcione una infraestructura de TI integrada y económica.

En busca de satisfacer las necesidades de las empresas, ISACA promovió el marco COBIT desde su primera versión en 1996 hasta la más reciente COBIT 2019. Actualmente, están disponibles las siguientes publicaciones: i) Marco de Referencia COBIT 2019: Introducción y metodología[31], el cual presenta los conceptos clave de COBIT 2019 ii) Marco de Referencia COBIT 2019: Objetivos de gobierno y gestión[32], en el cual explica los 40 objetivos principales del gobierno y la gestión, y los procesos y componentes relacionados (esta guía también hace referencia a otros estándares y marcos relacionados), iii) Guía de diseño COBIT 2019: Diseño de una solución de Gobierno de Información y Tecnología[33], el cual investiga los factores de diseño que pueden influir en el gobierno y además incluye un flujo de trabajo para la planificación de un sistema de gobierno personalizado para la empresa, y iv) Guía de implementación de COBIT 2019: Implementación y optimización de una solución de gobierno de Información y Tecnología[34], el cual es la evolución de la guía COBIT 5 y desarrolla una hoja de ruta para la mejora continua del gobierno. La Ilustración 13 muestra como las diferentes publicaciones de COBIT 2019 cubren distintas generalidades.

[31]Disponible en https://pdfcoffee.com/cobit-2019-framework-introduction-and-methodology-res-eng-1118-2-5-pdf-free.html
32 Disponible en https://pdfcoffee.com/cobit-2019-framework-governance-and-management-objectives-res-eng-1118-2-pdf-free.html
33 Disponible en https://pdfcoffee.com/cobit-2019-design-guideresspa0719pdf-3-pdf-free.html
34 Disponible en https://pdfcoffee.com/cobit-2019-implementation-guideresspa0719pdf-5-pdf-free.html

Ilustración 13. Generalidades de COBIT



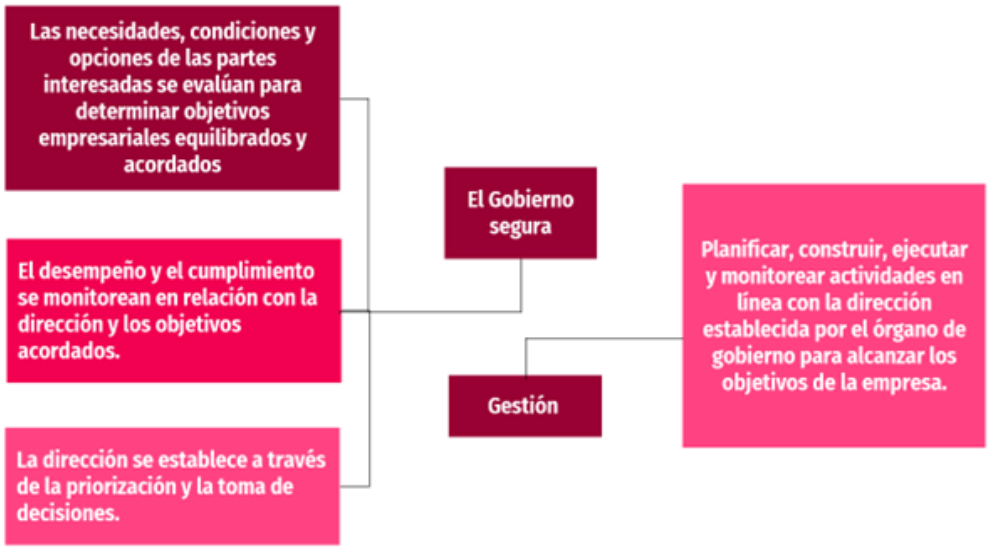
Fuente ISACA, COBIT 2019 – Implementación y optimización de una solución de gobierno de Información y Tecnología

COBIT es un marco que establece lineamientos de buenas prácticas dirigidos al gobierno y gestión de la información y la tecnología empresarial – TI, donde TI se refiere a "*toda la tecnología y procesamiento de la información que la empresa usa para lograr sus objetivos*[35]", además, está alineado con diferentes estándares y marcos relacionados que según ISACA lo consolidan como el paraguas del marco de gobierno de TI. El marco establece una clara distinción entre gobierno y gestión, pues son disciplinas distintas que abarcan diferentes actividades, estructuras organizativas y propósitos (Ver

Ilustración 14).

Ilustración 14. Propósitos de Gobierno y Gestión

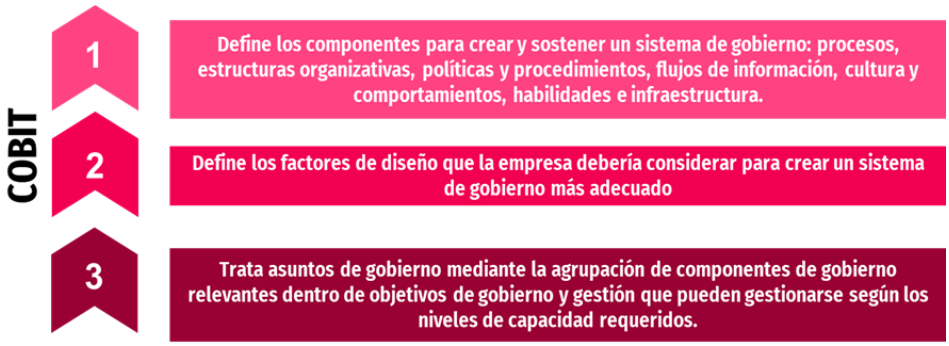
35 Disponible en https://toaz.info/doc-view



Fuente: DANE a partir de ISACA 2019

Aunque COBIT establece lineamientos de buenas prácticas dirigidos al gobierno y gestión de la información y la tecnología empresarial, **no** es ni una descripción completa de todo el entorno de TI de una empresa, ni un marco para organizar los procesos de negocio o gestionar la tecnología, ni ordena decisiones relacionadas con TI, sino que más bien COBIT tiene como objetivo definir todos los componentes que describen que, como y quien debería tomar las decisiones (Ver Ilustración 15).

Ilustración 15. Marco COBIT

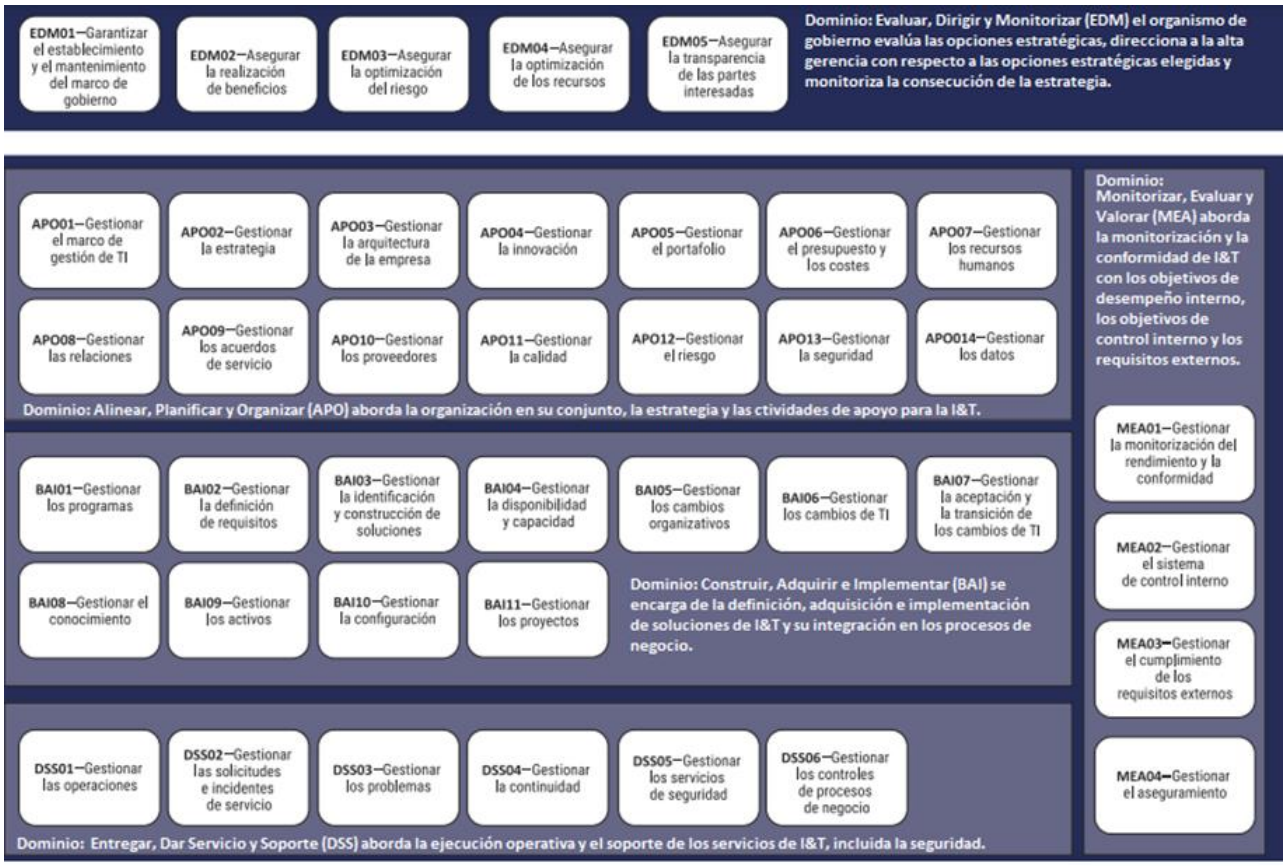


Fuente DANE a partir de ISACA 2019

Ahora bien, para que la información y la tecnología contribuyan a los objetivos de la empresa, es necesario que también se alcancen objetivos de gobierno y gestión, donde cada objetivo de gobierno está relacionado con un proceso de gobierno (fondo azul oscuro Ilustración 16) y cada objetivo de gestión está relacionado con un proceso de gestión (fondo azul claro Ilustración 16). Los

objetivos de gobierno y gestión de COBIT están agrupados en cinco dominios, uno de gobierno (EDM) y cuatro de gestión (APO, BAI, DSS y MEA).

Ilustración 16. Modelo Core de COBIT



Fuente ISACA – Objetivos de gobierno y gestión 2019

Asimismo, las empresas deben establecer, personalizar y sostener un sistema de gobierno creado a partir de una serie de componentes con el fin de cumplir con los objetivos de gestión y gobierno, los componentes pueden ser: genéricos, los cuales se describen en la Ilustración 16 y en principio se aplican a cualquier situación, por lo general suelen requerir una adaptación antes de que se puedan implementar en la práctica; o variantes de los componentes genéricos, los cuales se basan en estos, pero se adaptan para un propósito o contexto específico dentro de un área prioritaria (donde un área prioritaria "*describe un tópico, dominio o asunto de gobierno determinado que puede abordarse como una serie de objetivos de gobierno y gestión y sus componentes*", el marco COBIT permite una cantidad ilimitada de estas áreas lo cual hace que COBIT sea un marco abierto).

Además, COBIT 2019 admite un esquema de capacidad de procesos basado en el modelo de madurez de capacidad CMMI, en el cual dentro de cada objetivo de gobierno y gestión puede

gestionar con distintos niveles de capacidad, los cuales son una medida de lo bien que se ha implementado y ejecutado un proceso, donde el nivel cero representa la falta de cualquier capacidad básica y/o la estrategia incompleta para abordar el propósito de gobierno y gestión; y el nivel cinco representa que el proceso logró su propósito, está bien definido y su rendimiento se mide para mejorar el desempeño y continuar su mejora.

Finalmente, existen factores de diseño que influyen de diversas maneras en la personalización del sistema de gobierno de una empresa, el marco COBIT distingue tres clases de impacto diferentes (Ver Tabla 9).

Tabla 9. Factores de diseño

Factor de diseño	Descripción
Gestión de prioridad/selección del objetivo	El modelo Core COBIT incluye 40 objetivos de gobierno y gestión; cada uno consiste en un proceso y una serie de componentes relacionados. Estos son intrínsecamente equivalentes; no hay ningún orden de prioridad natural entre ellos. Sin embargo, los factores de diseño pueden influir en esta equivalencia y hacer que algunos objetivos de gobierno y gestión sean más importantes que otros, a veces hasta el extremo de que algunos objetivos de gobierno y gestión pasen a ser insignificantes. En la práctica, esta mayor importancia se traduce en el establecimiento de unos niveles de capacidad objetivos más altos para objetivos de gobierno y gestión importantes.
Variación de componentes	Los componentes deben alcanzar los objetivos de gobierno y gestión. Algunos factores de diseño pueden obligar a variaciones específicas de los componentes o pueden influir en la importancia de los componentes.
Necesidad de directrices para áreas prioritarias específicas	Algunos factores de diseño, como el escenario de amenazas, riesgo específico, métodos de desarrollo a cumplir y configuración de la infraestructura, impulsará la necesidad para variar el contenido del modelo Core de COBIT para un contexto determinado.

Fuente DANE a partir de ISACA 2019

1.3.9 Marco COSO[36]

Comité de Organizaciones Patrocinadoras del Treadway – COSO es una organización de carácter voluntario constituida por empresas estadounidenses cuyo objetivo es crear conocimiento frente a tres temas: (*i)* la gestión del riesgo empresarial, *(ii)* el control interno, y *(iii)* la lucha contra el fraude.

[36] Committee of Sponsoring Organizations of the Treadway

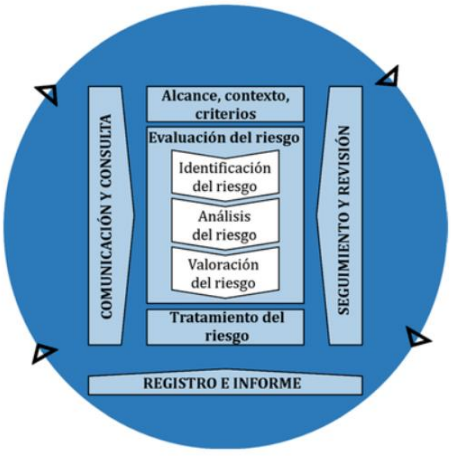
El marco actual para el control interno de los riesgos es llamado COSO ERM 2017[37] que se actualizó para abordar la gestión de riesgos en la era cibernética y satisfacer las demandas de un entorno empresarial en evolución. En la Ilustración 17. Los 20 principios que componen el marco COSO de gestión de riesgos:

Ilustración 17. Los 20 principios que componen el marco COSO de gestión de riesgos

Fuente: COSO. Gestión del Riesgo empresarial Integrando Estrategia y Desempeño.

Los diferentes modelos COSO y las tres líneas de defensa en *Risk Management* son soportados por la norma ISO 31000[38] que proporciona un enfoque común para gestionar cualquier tipo de riesgo y no es específico de una industria o un sector.

Ilustración 18. Proceso de gestión del riesgo



[37] Disponible en COSO Enterprise Risk Management – Integrating with Strategy and Performance
[38] Disponible en https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Fuente: ISO 31000

Frente a la evaluación de riesgos cibernéticos, el COSO publicó una guía sobre *Gestión de riesgos cibernéticos en la era digital*[39] que tiene como fin proporcionar una descripción general sobre la gestión del riesgo cibernético a través de los principios definidos en el Marco de gestión de riesgos empresariales. En particular, la Guía proporciona un contexto de los conceptos fundamentales de las técnicas de gestión de riesgos cibernéticos y no pretende ser una guía para desarrollar e implementar estrategias técnicas.

La Guía describe los 20 principios del marco COSO ERM y señala cómo estos principios pueden abordar la exposición a riesgos cibernéticos. A continuación, se menciona algunos aspectos clave para gestionar la ciberseguridad en las organizaciones en el marco del COSO.

Tabla 10. Aspectos clave para gestionar la ciberseguridad

Componentes de gestión COSO	Descripción
Gobernanza y cultura	Es un componente clave para administrar el riesgo cibernético y debe impulsar la segregación de funciones en las responsabilidades laborales y el acceso al sistema y la ejecución de una estrategia comercial que incorpore múltiples líneas de defensa en toda la organización.
Establecimiento de estrategia y objetivos	La gestión del riesgo cibernético se integra en el plan estratégico de la entidad a través del proceso de establecimiento de la estrategia y los objetivos comerciales. Con una comprensión del contexto empresarial, la organización puede obtener información sobre los factores internos y externos y su efecto sobre el riesgo.
Desempeño	La organización identifica y evalúa los riesgos cibernéticos que pueden afectar el logro de esa estrategia y los objetivos comerciales. Prioriza los riesgos de acuerdo con su severidad. Luego, la organización selecciona las respuestas al riesgo y monitorea el desempeño para el cambio.
Riesgo y monitorización	El componente de revisión y monitorización es clave, ya que la disrupción y la digitalización del mundo cibernético en constante evolución continúan impulsando la necesidad de cambios y mejoras en la gestión del riesgo cibernético.
Información, comunicación y reporte	La gerencia utiliza información relevante de fuentes internas y externas para respaldar la gestión del riesgo cibernético. Juntos forman una base para

[39] Disponible en Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO). (2019). Gestión del riesgo cibernético en la era digital https://incp.org.co/Site/publicaciones/info/archivos/Cyber-risk-in-a-digital-age.pdf

	todos los demás componentes de ERM. La organización aprovecha los sistemas de información para capturar, procesar y administrar datos e información. Mediante el uso de información que se aplica a todos los componentes, la organización informa sobre el riesgo, la cultura y el desempeño.

Fuente: Managing Cyber Risk in a Digital Age.

1.3.10 Agencia de Ciberseguridad de la Unión Europea – ENISA[40]

La ciberseguridad es la piedra angular de la transformación digital y su necesidad es transversal a todos los sectores a todos los sectores, por lo que resulta necesario tenerla en consideración en una amplia serie de iniciativas y entornos políticos. La ciberseguridad no debe limitarse a una comunidad especializada de expertos técnicos en cibernética. La ciberseguridad debe estar integrada en todos los entornos de las políticas de la UE. Es, por tanto, esencial evitar la fragmentación y contar con un enfoque coherente teniendo en cuenta al mismo tiempo las características específicas de cada sector.

La seguridad siempre ha sido central para la protección de la confidencialidad, integridad y disponibilidad de los datos personales. La seguridad no se trata solo de la aplicación de una o más medidas y ninguna medida de seguridad por sí sola puede proporcionar un nivel de protección adecuado para los datos personales. Por el contrario, la seguridad de los datos personales debe seguir un marco de controles minucioso y supervisado continuamente, tanto técnicos como organizativos, adecuados a la naturaleza del procesamiento de datos y los riesgos asociados.
Debido al alcance y los objetivos de ENISA, la seguridad es su principal objetivo operativo en una serie de áreas, incluidos los datos personales.

- Una dimensión es apoyar la adopción de Metodologías de Evaluación de Riesgos y Medidas de Seguridad en una variedad de sectores y diferentes tipos de controladores y procesadores de datos.
- Otra dimensión es estudiar medidas de seguridad específicas que puedan contribuir a la protección de los datos personales, como son los Protocolos y Herramientas Criptográficas, donde ya se ha puesto mucho empeño.

Tabla 11. Herramienta de Marco Nacional de Evaluación de Ciberseguridad – NCAF

[40] Disponible en ENISA 2022 https://www.enisa.europa.eu/

Temas	Descripción
Objetivo	El principal objetivo del NCAF es medir el nivel de madurez de las capacidades de ciberseguridad de los Estados miembros para ayudarlos a realizar una evaluación de su capacidad nacional de ciberseguridad, mejorar la conciencia del nivel de madurez del país, identificar áreas de mejora y desarrollar capacidades de ciberseguridad. Este marco debería ayudar a los Estados miembros, y en particular a los responsables políticos nacionales, a realizar un ejercicio de autoevaluación con el objetivo de mejorar las capacidades nacionales de ciberseguridad.
Beneficios	✓ Llevar a cabo la evaluación de sus capacidades nacionales de ciberseguridad. ✓ Mejorar la conciencia del nivel de madurez del país. ✓ Identificación de áreas de mejora. ✓ Creación de capacidades de ciberseguridad
Lo que se evalúa	**Gobernanza y estándar de ciberseguridad**: este clúster mide la capacidad de los Estados miembros para establecer una gobernanza adecuada, estándares y buenas prácticas en el ámbito de la ciberseguridad. **Fomento de la capacidad y sensibilización**: mide la capacidad del país para desarrollar continuamente capacidades de seguridad cibernética y aumentar el nivel de conocimiento y habilidades dentro de este dominio. **Legal y regulatorio**: mide la capacidad de los Estados miembros para establecer los instrumentos legales y reglamentarios necesarios para abordar y contrarrestar el aumento del delito y los incidentes cibernéticos relacionados, y para proteger la infraestructura de información crítica. **Cooperación**: evaluar la cooperación y el intercambio de información entre diferentes grupos de partes interesadas a nivel nacional e internacional como una herramienta importante para comprender mejor y responder a un entorno de amenazas en constante cambio.
El informe	El informe Marco Nacional de Evaluación de Capacidades, tiene como objetivo proporcionar a los Estados miembros una autoevaluación de su nivel de madurez mediante la evaluación de los objetivos, que ayudaran a mejorar y desarrollar capacidades de ciberseguridad tanto a nivel estratégico como operativo. El público objetivo de este informe son los formuladores de políticas, expertos y funcionarios gubernamentales responsables o involucrados en el diseño, implementación y evaluación de un Marco de Evaluación de Capacidades Nacionales y, en un nivel más amplio, las capacidades de seguridad cibernética.
Enfoque Metodológico	Se basa en cuatro pasos principales:

Temas	Descripción
	1. **Investigación documental**: revisión extensa de la literatura para recopilar las mejores prácticas con respecto al desarrollo de un marco de evaluación de madurez para las estrategias nacionales de seguridad cibernética. El marco de análisis se basa en la metodología Becker para el desarrollo de modelos de madurez que establece un modelo de procedimiento genérico y consolidado para el diseño de modelos de madurez. 2. **Recopilación del punto de vista de expertos y partes interesadas**: ENISA se puso en contacto con su Grupo Nacional de Expertos en Estrategias de Ciberseguridad y los Oficiales Nacionales de Enlace para encontrar a los expertos relevantes en cada Estado miembro. Además, se realizaron entrevistas a algunos expertos. 3. **Análisis de la entrada de inventario**: los datos recopilados a través de la investigación documental y posteriormente se analizaron las entrevistas para identificar las mejores prácticas. 4. **Finalización del modelo**: los expertos en la materia de ENISA revisaron una versión actualizada del marco de autoevaluación de las capacidades nacionales y luego los expertos la validaron a través de un taller realizado en octubre de 2020 antes de la publicación.

Fuente: elaborado a partir de ENISA, Marco de evaluación de capacidades nacionales

ENISA publicó en enero de 2022 un informe titulado "Protección de Datos Ingeniería. De la teoría a la práctica". El alcance general de este informe es dar una mirada más amplia a la ingeniería de protección de datos con el fin de ayudar a los profesionales y organizaciones con la implementación práctica de los aspectos técnicos de la protección de datos desde el diseño y por defecto. En esta dirección, este informe intenta presentar las tecnologías y técnicas (de seguridad) existentes y discutir las posibles fortalezas y la aplicabilidad en relación con el cumplimiento de los principios de protección de datos. Este trabajo se realiza en el contexto de las tareas de ENISA en virtud de la Ley de Ciberseguridad para ayudar a los Estados miembros en aspectos específicos de ciberseguridad de la política y la legislación de la Unión en relación con la protección de datos y la privacidad.

PROTECCIÓN DE DATOS DE INGENIERÍA

La evolución de la tecnología ha traído consigo nuevas técnicas para compartir, procesar y almacenar datos. Esto ha generado nuevos modelos de procesamiento de datos (incluidos los datos personales), pero también ha introducido nuevas amenazas y desafíos. Parte de la evolución de la

privacidad y la protección de datos. Los desafíos asociados con las tecnologías y aplicaciones emergentes incluyen: falta de control y transparencia, posible reutilización de datos, inferencia y reidentificación de datos, creación de perfiles y toma de decisiones automatizada.

La implementación de los Principios de Protección de Datos de GDRP es un desafío, ya que no se puede implementar de manera tradicional e intuitiva, hay que repensar las operaciones de tratamiento, posiblemente con la definición de nuevos actores y responsabilidades y con un papel destacado de la tecnología como elemento de garantía.

En un informe de 2015[41], ENISA exploró el concepto de privacidad por diseño siguiendo un enfoque de ingeniería. Además del análisis del concepto, se presentó ocho estrategias de privacidad por diseño, tanto orientadas a datos como a procesos, destinadas a preservar ciertos objetivos de privacidad. Como un enfoque diferente a la ingeniería de privacidad y protección de datos, se propuso un marco que comprende seis objetivos para identificar y salvaguardar los sistemas de TI que procesan datos personales. Además de la típica tríada de seguridad de "confidencialidad" "integridad" y disponibilidad", también se propusieron tres objetivos adicionales "desvinculación", "transparencia" e "intervenibilidad".

Protección de datos por Diseño: la privacidad por diseño no es solo una lista de principios ni puede reducirse a la implementación de tecnologías específicas. De hecho, es un proceso que involucra varios componentes tecnológicos y organizativos, que implementan principios de privacidad y protección de datos mediante el despliegue adecuado y oportuno de medidas técnicas y organizativas que incluyen también PETS (uso de tecnologías específicas de mejora de la privacidad).

Conexión con Protección de Datos: es uno de los requisitos introducidos en el RGPD y también puede percibirse como parte del enfoque de "protección desde el diseño y por defecto". Además del énfasis puesto por estos principios en la ingeniería de protección de datos, requisitos en las operaciones de procesamiento, tal énfasis también es evidente en el Artículo 35 (7) (d) del RGPD.

Tecnologías de mejora de la privacidad: las tecnologías de mejora de la privacidad cubren una gama más amplia de tecnologías que están diseñadas para respaldar la implementación de los principios de protección de datos a nivel sistémico y fundamental.

Las tecnologías de mejora de la privacidad son "un sistema coherente de medidas TIC que protege la privacidad eliminando o reduciendo los datos personales o evitando el procesamiento innecesario

[41] Disponible en https://www.slideshare.net/richard.claassens/pripare-methodologyhandbookfinalfeb242016

y/o no deseado de los datos personales, todo ello sin perder la funcionalidad del sistema de información".

Con respecto a herramientas y tecnologías específicas, en la Tabla 12 se muestra otra categorización que puede basarse en las características de la tecnología.

Tabla 12. Características de la tecnología en relación con los datos que se procesan

Características	Descripción
Preservación de la verdad	El objetivo de la ingeniería de privacidad es preservar la precisión de los datos mientras se reduce su poder de identificación. Este objetivo se puede lograr, por ejemplo, diluyendo la granularidad de los datos (por ejemplo, desde la fecha de nacimiento hasta la edad). De esta manera, los datos siguen siendo precisos, pero de una "manera minimizada", adecuada para el propósito en cuestión. Además, el cifrado puede considerarse como una técnica de conservación de la verdad, ya que el cifrado aplicado en la dirección inversa restaura completamente los datos originales sin inyectar ninguna incertidumbre en el proceso.
Preservación de la integridad	Los datos se conservan en un formato que "tiene un significado" para el responsable del tratamiento, sin revelar los atributos reales de los interesados.
Tecnología Operable	Se pueden ejecutar operaciones matemáticas y lógicas (por ejemplo, una suma o una comparación) sobre los resultados de sus aplicaciones. Operabilidad no implica necesariamente inteligibilidad, ya que (como se dirá en este informe) existen familias de técnicas de cifrado en las que los resultados (no inteligibles) son directamente operables mediante operaciones correctamente ejecutables en el dominio cifrado.

Fuente: a parir de ENISA

ANONIMIZACIÓN Y SEUDONIMIZACIÓN

La anonimización y la seudonimización son dos técnicas muy conocidas que se utilizan ampliamente para implementar en la práctica principios de protección de datos como la minimización de datos. La seudonimización también se menciona explícitamente en el RGPD como técnica que puede respaldar la protección de datos desde el diseño (Art. 25 RGPD) y la seguridad del procesamiento de datos personales (Art. 32 RGPD).

Se considera en el RGPD, que la información anónima se refiere a información que no se relaciona con una persona física identificada o identificable y, por lo tanto, los datos anónimos no se

consideran datos personales. Por el contrario, los datos seudonimizados, que se pueden (re)atribuir a una persona física con el uso de información adicional, son datos personales y se les aplican los principios de protección de datos del RGPD. Un error común es considerar que los datos seudonimizados son equivalentes a los datos anonimizados.

- **Anonimización**: la anonimización de datos es un problema de optimización entre dos parámetros en conflicto: la utilidad de los datos y la protección contra la reidentificación. De hecho, la anonimización de los datos se logra alterando los datos, ya sea haciendo ruido o generalizando. Proporcionar una fuerte protección de reidentificación generalmente requiere alterar fuertemente el conjunto de datos y, por lo tanto, afectar negativamente su utilidad. Por lo tanto, la anonimización de datos implica encontrar la mejor compensación entre estos dos parámetros; y esta compensación a menudo depende de la aplicación y el contexto (es decir, cómo se distribuye y utiliza el conjunto de datos).
- **K-Anonimato**: el modelo de anonimato k se introdujo a principios de la década de 2000 y se basa en la idea de que, al combinar conjuntos de datos con atributos similares, se puede oscurecer la información de identificación sobre cualquiera de las personas que contribuyen a esos datos. Se considera que un conjunto de datos brinda protección de anonimato k si la información para cada sujeto de datos contenida en el conjunto de datos no se puede distinguir de al menos k-1 sujetos de datos cuya información también aparece en el conjunto de datos. El concepto clave es abordar el riesgo de reidentificación de datos anónimos a través de la vinculación con otros conjuntos de datos disponibles.
- **Privacidad Diferencial**: los algoritmos de privacidad diferencial pueden garantizar que después de analizar un conjunto de datos de varias personas, el resultado del análisis no se verá afectado y seguirá siendo el mismo, incluso si los datos de cualquier individuo no se incluyeron en el conjunto de datos. En otras palabras, la privacidad diferencial permite estudiar tendencias estadísticas más amplias en el conjunto de datos, pero protege los datos sobre las personas que participan en el conjunto de datos.

CÁLCULOS DE ENMASCARAMIENTO DE DATOS Y PRESERVACIÓN DE LA PRIVACIDAD

El enmascaramiento es un término amplio que se refiere a funciones que, cuando se aplican a los datos, ocultan su verdadero valor. Los ejemplos más destacados son el cifrado y el *hashing,* pero como el término es bastante amplio, también cubre técnicas adicionales, algunas de las cuales se analizarán en esta sección.

La principal utilidad del enmascaramiento con respecto a los principios de protección de datos es la integridad y la confidencialidad (seguridad) y, según la técnica o el contexto de la operación de procesamiento, también puede incluir responsabilidad y limitación del propósito.

Tabla 13. Cálculos de enmascaramiento de datos y preservación de la privacidad

Características	Descripción
Cifrado Homomórfico	Es un elemento básico para muchas tecnologías que mejoran la privacidad, como la computación segura de múltiples partes, la agregación de datos privados, la seudonimización o el aprendizaje automático federado, por nombrar algunas. El cifrado homomórfico permite realizar cálculos sobre datos cifrados, sin tener que descifrarlos primero. El caso de uso típico para el cifrado homomórfico es cuando un sujeto de datos quiere subcontratar el procesamiento de sus datos personales sin revelar los datos personales en texto sin formato. Es evidente que tales funcionalidades se adaptan muy bien cuando el procesamiento lo realiza un tercero, como un proveedor de servicios en la nube.
Cálculo multipartes seguro	El concepto de computación multiparte segura se refiere a una familia de protocolos criptográficos que se introdujeron en 1986 e intenta resolver problemas de confianza mutua entre un conjunto de partes donde ninguna parte individual puede ver los datos de las otras partes.
Entornos de ejecución de confianza	El cifrado es una herramienta poderosa para proteger datos; sin embargo, se vuelve inutilizable si el dispositivo que se usa para almacenar, cifrar o descifrar los datos se ve comprometido.
Recuperación de la información privada	La recuperación de información privada es una técnica criptográfica que permite a un usuario recuperar una entrada en una base de datos sin revelar al custodio de los datos (p. ej., el propietario o administrador de la base de datos) qué elemento se ha consultado. Es por eso que puede ser utilizado como una técnica de minimización de datos por parte de los controladores de datos. Supongamos que una empresa quiere proporcionar acceso a una base de datos a sus clientes. Hay dos modelos principales de recuperación de información privada. El primer modelo es computacional. Recuperación de información privada y solo hay un servidor que almacena la base de datos. Se considera que este modelo proporciona un mejor nivel de protección, pero tiene limitaciones con respecto a las conexiones que se pueden establecer con el servidor y la base de datos. En el segundo modelo, *Información Teórica Recuperación de Información Privada,* la base de datos se almacena en varios servidores controlados por diferentes propietarios. Este modelo permite una mejor complejidad de comunicación, pero se supone que los servidores no se confabulan ni intercambian información.
Datos Sintéticos	Los datos sintéticos son datos elaborados en una forma en que se asemejan de manera realista a los datos reales, pero en realidad no se refieren a ningún identificado o identificable específico.

Fuente: construcción a parir de ENISA

Desde la perspectiva de la ingeniería de protección de datos, los canales de comunicación deben ir más allá de la provisión de seguridad como su funcionalidad principal e incorporar características

adicionales que mejoren la privacidad, como quién puede tener acceso al contenido de la comunicación, incluidos los proveedores, la ubicación y el acceso al cifrado. Claves, ubicación y tipo del proveedor, información del usuario divulgada, etc. Hacia esta dirección, se analizan a continuación dos tecnologías, a saber, el cifrado de extremo a extremo y el enrutamiento de proxy.

- **Cifrado de extremo a extremo:** es un método para cifrar datos y mantenerlos cifrados en todo momento entre dos o más partes que se comunican. Solo las partes involucradas en la comunicación tienen acceso a las claves de descifrado. La implementación del cifrado de extremo a extremo es claramente una característica fundamental para las aplicaciones de mensajería segura y ha cobrado mucha fuerza en los últimos años, donde una serie de servicios *Over-The-Top* – OTT ampliamente utilizados, como las aplicaciones de mensajería, afirman implementar el cifrado de extremo a extremo.

- **Enrutamiento de cebolla y proxy:** otro aspecto son los metadatos de la comunicación (datos que describen otros datos e incluyen información sobre quién, qué, dónde, cuándo, etc.) que, según la revisión de la Directiva sobre privacidad electrónica y la Propuesta de Reglamento sobre privacidad electrónica "pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas, lo que implica altos riesgos para sus derechos y libertades".

ALMACENAMIENTO PARA PRESERVAR LA PRIVACIDAD

El almacenamiento que preserva la privacidad tiene dos objetivos: proteger la confidencialidad de los datos personales en reposo e informar a los controladores de datos en caso de que se produzca una infracción. El cifrado es la principal técnica utilizada para proteger la confidencialidad de los datos del acceso no autorizado. Dependiendo de las limitaciones de los controladores de datos, se puede aplicar en tres niveles diferentes: (i) nivel de almacenamiento, (ii) nivel de base de datos y (iii) cifrado a nivel de aplicación.

CONTROL DE ACCESO, AUTORIZACIÓN Y AUTENTICACIÓN PARA MEJORAR LA PRIVACIDAD

La autenticación, la autorización y el control de acceso tienen como objetivo evitar que se produzcan actividades no autorizadas y/o no deseadas mediante la implementación de controles y restricciones sobre lo que pueden hacer los usuarios, a qué recursos pueden acceder y qué funciones pueden realizar con los datos, incluida la visualización y modificación no autorizadas. O copiar. La autenticación confirma la identidad de un usuario que solicita acceder a los datos, mientras que la

autorización determina qué acciones puede realizar un usuario autenticado. El control de acceso se refiere a una técnica que garantiza que solo los usuarios autenticados puedan acceder a la información a la que tienen derecho. Estos tres elementos están estrechamente relacionados y la omisión de uno solo de ellos puede debilitar el nivel de protección de los datos, ya que los usuarios autorizados pueden acceder a ellos o los usuarios autorizados pueden realizar acciones no autorizadas.

1. **Credenciales basadas en atributos que mejora la privacidad**: permiten la autenticación de una entidad mediante la autenticación selectiva de diferentes atributos sin revelar información adicional que normalmente se usa y que muy bien podría incluir datos personales.
2. **Prueba de conocimiento cero**: son primitivas que se pueden utilizar para hacer cumplir los principios de confidencialidad y minimización de datos del RGDP. La idea central de una prueba de conocimiento cero es permitir que un usuario (un sujeto de datos) demuestre a un servidor (controlador de datos) que conoce una información secreta sin revelar nada sobre este secreto.

El RGPD no solo exige transparencia en el procesamiento de datos, sino que también es necesaria para que las personas entiendan por qué se recopilan sus datos personales y cómo se procesan, por ejemplo, si se transfieren a otras partes.

Tabla 14. Herramientas de transparencia, intervención y control del usuario

Herramientas	Descripción
Políticas de Privacidad	En el mundo en línea, un instrumento muy conocido para proporcionar información a los usuarios es la política de privacidad (a veces también llamada; declaración de protección de datos, política de datos, aviso de privacidad o similar.
Iconos de privacidad	También se puede lograr una mejor comprensibilidad si la información se transmite no solo mediante un texto que requiere habilidades de lectura y esfuerzo, sino también mediante símbolos gráficos (iconos). Los iconos son un método bien conocido para apoyar, a veces sustituir, información textual. Los íconos de privacidad pueden convertirse en un muy buen enfoque para respaldar, o incluso sustituir, información textual en procesamiento de datos personales.
Paneles de Privacidad	El objetivo de los paneles de control de privacidad es brindar a los interesados una descripción general de cómo un controlador de datos procesa sus datos personales. En contraste con la información proporcionada en las políticas de privacidad que a menudo proporcionan descripciones bastante abstractas de las operaciones de procesamiento, los

Herramientas	Descripción
	paneles de control de privacidad se pueden usar para mostrar los elementos de datos personales reales a los que puede acceder el controlador. Esto facilita una mejor comprensión por parte del interesado de cuáles de sus datos personales se están procesando. A menudo, también se muestra cuándo ya quién se divulgan los datos personales, por ejemplo, si los datos personales se transfieren a otras organizaciones o si (y posiblemente con qué propósito) una persona ha accedido a elementos de datos personales específicos. Los interesados también pueden verificar si sus datos personales, tal como se muestran a través del panel de privacidad, están desactualizados, son incorrectos, incompletos o excesivos, o si la divulgación a otros es plausible o bastante inesperada.

Fuente: a parir de ENISA

Reglamento General de Protección de Datos (RGPD) [42]

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, el nuevo Reglamento General de Protección de Datos ('RGPD') de la Unión Europea ('UE'), regula el procesamiento por parte de un individuo, una empresa o una organización de datos personales datos relativos a personas físicas en la UE.

No se aplica al tratamiento de datos personales de personas fallecidas o de personas jurídicas. Las normas no se aplican a los datos procesados por un individuo por razones puramente personales o para actividades realizadas en el hogar, siempre que no esté relacionado con una actividad profesional o comercial. Cuando un individuo utiliza datos personales fuera de la esfera personal, por ejemplo, para actividades socioculturales o financieras, entonces se debe respetar la ley de protección de datos.

¿Cuáles son los principales aspectos del Reglamento General de Protección de Datos (RGDP) que una administración pública debe conocer? [43]

Una administración pública está sujeta a las reglas del RGPD cuando procesa datos personales relacionados con un individuo. Es responsabilidad de las administraciones nacionales apoyar a la administración regional y local en la preparación para la aplicación del RGPD.

[42] Disponible en https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

[43] Disponible en https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_en

La mayoría de los datos personales en poder de las administraciones públicas se procesan generalmente con base en una obligación legal o en la medida en que sea necesario para realizar tareas realizadas en interés público o en el ejercicio de la autoridad oficial que le ha sido conferida.

Al procesar datos personales, una administración pública debe respetar principios clave, tales como:

- procesamiento justo y legal;
- limitación del propósito;
- minimización de datos y retención de datos.

En el caso de procesamiento sobre la base de la ley, esta ley ya debería garantizar que se observen estos principios (por ejemplo, los tipos de datos, el período de almacenamiento y las salvaguardias apropiadas). Antes del procesamiento de datos personales, las personas deben ser informadas sobre el procesamiento, como sus propósitos, los tipos de datos recopilados, los destinatarios y sus derechos de protección de datos.

Una administración pública está obligada a nombrar un delegado de Protección de Datos, sin embargo, se puede designar un único delegado de protección de datos para varios organismos públicos y, por lo tanto, compartirse entre ellos o subcontratar este trabajo a un DPD externo.

También debe asegurarse de que se han implementado las medidas técnicas y organizativas apropiadas para proteger los datos personales. Si partes del procesamiento se subcontratan a una organización externa (el llamado 'procesador'), debe haber un contrato u otro acto legal que garantice que el procesador brinda garantías suficientes para implementar las medidas técnicas y organizativas apropiadas que cumplen con los estándares del RGPD.

En los casos en que los datos personales en posesión se divulguen accidental o ilegalmente a destinatarios no autorizados o no estén disponibles temporalmente o se alteren, la violación debe notificarse a la Autoridad de Protección de Datos – APD sin demora indebida y, a más tardar, dentro de las 72 horas posteriores a haber tenido conocimiento del incumplimiento. La administración pública también puede necesitar informar a las personas sobre la infracción.

Tabla 15. Reglamento General de Protección de Datos – RGDP[44]

Temas	Descripción
Objetivos del reglamento	• El reglamento general de protección de datos (GDPR) protege a las personas cuando sus datos están siendo procesados por el sector privado y la mayor parte del sector

[44] Unión Europea, EUR-Lex. Disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A310401_2

Temas	Descripción
	público. El procesamiento de datos por parte de las autoridades competentes con fines de aplicación de la ley está sujeto a la directiva de aplicación de la ley de protección de datos. • Permite a las personas controlar mejor sus datos personales. También moderniza y unifica las reglas, lo que permite a las empresas reducir los trámites burocráticos y beneficiarse de una mayor confianza de los consumidores. • Establece un sistema de autoridades de control completamente independientes a cargo de monitorear y hacer cumplir. • Es parte de la reforma de protección de datos de la Unión Europea (UE) junto con la directiva de aplicación de la ley de protección de datos y el Reglamento (UE) 2018/1725 sobre la protección de las personas físicas con respecto al procesamiento de datos personales por parte de las instituciones y organismos de la UE, oficinas y agencias.
Derechos de las personas	El RGPD fortalece los derechos existentes, proporciona nuevos derechos y brinda a las personas más control sobre sus datos personales. Incluye lo siguiente: • **Acceso más fácil a los datos propios de un individuo**. Esto incluye brindar más información sobre cómo se procesan esos datos y garantizar que esa información esté disponible de manera clara y comprensible. • **Un nuevo derecho a la portabilidad de datos**. Esto facilita la transmisión de datos personales entre proveedores de servicios. • **Un derecho de supresión más claro (derecho al olvido)**. Cuando una persona ya no desea que se procesen sus datos y no hay una razón legítima para conservarlos, los datos se eliminarán. • **El derecho a saber cuándo sus datos personales han sido violados**. Las empresas y organizaciones deben notificarlo a la autoridad de control de protección de datos pertinente y, en caso de violaciones graves de datos, también a las personas afectadas.
Reglas para empresas	• **Un único conjunto de normas para toda la UE**. Una ley única de protección de datos para toda la UE aumenta la seguridad jurídica y reduce la carga administrativa. • **Un delegado de protección de datos**. Las autoridades públicas y las empresas que procesan datos a gran escala o cuya actividad principal es el procesamiento de categorías especiales de datos, como los datos relacionados con la salud, deben designar a una persona responsable de la protección de datos. • **Ventanilla única**. Las empresas solo tienen que tratar con una sola autoridad de control (en el Estado miembro de la UE en el que tienen su establecimiento principal); las autoridades de control pertinentes cooperan en el marco del Consejo Europeo de Protección de Datos para casos transfronterizos.

Temas	Descripción
	• **Normas de la UE para empresas no pertenecientes a la UE**. Las empresas con sede fuera de la UE deben aplicar las mismas reglas al ofrecer servicios o bienes, o al monitorear el comportamiento de las personas dentro de la UE. • **Reglas favorables a la innovación**. Una garantía de que las garantías de protección de datos se integran en los productos y servicios desde la etapa más temprana de desarrollo (protección de datos desde el diseño y por defecto). • **Técnicas amigables con la privacidad**. Se recomienda, por ejemplo, la seudonimización (cuando los campos de identificación dentro de un registro de datos se reemplazan por uno o más identificadores artificiales) y el cifrado (cuando los datos se codifican de tal manera que solo las partes autorizadas pueden leerlos), para limitar la intrusión. De procesamiento. • **Eliminación de notificaciones**. El RGPD eliminó la mayoría de las obligaciones de notificación y los costos asociados con estas. Uno de sus objetivos es eliminar los obstáculos que afectan a la libre circulación de datos personales dentro de la UE. Esto facilitará la expansión de las empresas en el mercado único digital. • **Evaluaciones de impacto de la protección de datos**. Las organizaciones deberán realizar evaluaciones de impacto cuando el procesamiento de datos pueda dar como resultado un alto riesgo para los derechos y libertades de las personas. • **Mantenimiento de registros**. Las pequeñas y medianas empresas no están obligadas a mantener registros de las actividades de procesamiento, a menos que el procesamiento sea regular o pueda ocasionar un riesgo para los derechos y libertades de la persona cuyos datos se procesan, o incluye categorías sensibles de datos. • **Una caja de herramientas moderna para transferencias internacionales de datos**. El RGPD ofrece varios instrumentos para transferir datos fuera de la UE, incluidas las decisiones de adecuación adoptadas por la Comisión Europea cuando el país no perteneciente a la UE ofrece un nivel adecuado de protección, cláusulas contractuales preaprobadas (estándar), normas corporativas vinculantes, códigos de conducta y Certificación. Esto facilita una mejor comprensión por parte del interesado de cuáles de sus datos personales se están procesando. A menudo, también se muestra cuándo ya quién se divulgan los datos personales, por ejemplo, si los datos personales se transfieren a otras organizaciones o si (y posiblemente con qué propósito) una persona ha accedido a elementos de datos personales específicos. Los interesados también pueden verificar si sus datos personales, tal como se muestran a través del panel de privacidad, están desactualizados, son incorrectos, incompletos o excesivos, o si la divulgación a otros es plausible o bastante inesperada.

Fuente: Unión Europea, Reglamento General de Protección de Datos

1.3.11 CIS

Los controles desarrollados por el centro de seguridad en internet - CIS son un conjunto prescriptivo y prioritario de mejores prácticas en seguridad cibernética y acciones defensivas que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance, y apoyar el cumplimiento en una era de múltiples marcos. Estas mejores prácticas procesables para la defensa cibernética son formuladas por un grupo de expertos en tecnología de la información utilizando la información obtenida de ataques reales y sus defensas efectivas. Los controles de CIS proporcionan una orientación específica y una vía clara para que las organizaciones alcancen las metas y los objetivos descritos por múltiples marcos jurídicos, reglamentarios y normativos.

Esta implementación de los controles de seguridad desarrollados por CIS, pueden aportar en el fortalecimiento del programa que se tenga de seguridad de la información, identificar un conjunto de mejores técnicas para asegurar la seguridad, fortalecer la gestión de riesgos para la seguridad informática. CIS realiza la publicación del documento *Controles de seguridad y privacidad para organizaciones y sistemas de información federales*[45], donde se establecen un conjunto de medidas enfocadas a los sistemas de información del sector público. Es importante resaltar que este documento trae un mapeo de puntos en común relacionados desde el marco de seguridad de CIS y el Marco del Instituto Nacional de Estándares y Tecnología denominado – NIST.

Desde la perspectiva de CIS[46], existen 18 controles de seguridad, los cuales incluyen 3 categorías de sub-controles, que aumentan en complejidad según la madurez de las defensas cibernéticas de la organización.

- IG1 incluye los controles de seguridad de nivel básico que toda organización de nivel empresarial debe tener implementada. Piense en esto como el estándar mínimo, diseñado para ayudar a las empresas con experiencia limitada en ciberseguridad a frustrar ataques generales no dirigidos.

- IG2 está diseñado para ayudar a las organizaciones que administran múltiples departamentos de TI, con diversos grados de riesgo, a hacer frente a una mayor complejidad operativa.

[45] Disponible en https://www.cisecurity.org/insights/white-papers/controls-and-sub-controls-mappings-to-nist-special-publication-800-53-r4
[46] Disponible en https://raxis.com/blog/cis-vs-nist

- IG3 está dirigido a organizaciones que emplean expertos en seguridad de TI y está diseñado para ayudarlos a proteger datos confidenciales y disminuir el impacto de los ataques cibernéticos.

A diferencia de CIS, el marco NIST[47] está diseñado como una herramienta de análisis de brechas basada en el estado operativo objetivo de la organización. Incluye un conjunto básico de cinco funciones de seguridad cibernética que presentan estándares y pautas de la industria para todos los niveles de una organización. Estos se desglosan de la siguiente manera:

- Identificar: Desarrollar una comprensión organizacional para gestionar el riesgo de ciberseguridad para sistemas, personas, activos, datos y capacidades.

- Proteger: desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios.

- Detectar: Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.

- Responder: Desarrollar e implementar actividades apropiadas para actuar con respecto a un incidente de ciberseguridad detectado.

- Recuperar: Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restaurar cualquier capacidad o servicio que se vio afectado debido a un incidente de seguridad cibernética.

Dentro de cada función hay categorías que son grupos de resultados de ciberseguridad estrechamente vinculados a las necesidades y actividades. Un ejemplo sería "Protección de Datos". Dentro de cada categoría hay subcategorías que identifican resultados específicos o estados operativos. Para el ejemplo anterior, las subcategorías incluyen: "los datos están protegidos en reposo" y "los datos están protegidos en tránsito".

Controles de seguridad y privacidad para organizaciones y sistemas de información federales.

i) Inventario y Control de Activos de Hardware: administre activamente (inventario, seguimiento y corrección) todos los dispositivos de hardware en la red para que solo los

[47] Disponible en Ibídem

dispositivos autorizados tengan acceso, y los dispositivos no autorizados y no administrados se encuentren y eviten que obtengan acceso.

ii) Inventario y Control de Activos de Software: administrar activamente (inventariar, rastrear y corregir) todo el software en la red para que solo el software autorizado se instale y pueda ejecutar, y que el software no autorizado y no administrado se encuentre y evite su instalación o ejecución.

iii) Gestión continua de vulnerabilidades: adquiera, evalúe y tome medidas continuamente sobre nueva información para identificar vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.

iv) Uso controlado de privilegios administrativos: los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el uso, asignación y configuración de privilegios administrativos en computadoras, redes y aplicaciones.

v) Configuración segura de hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores: establezca, implemente y administre activamente (rastree, informe sobre, corrija) la configuración de seguridad de dispositivos móviles, computadoras portátiles, servidores y estaciones de trabajo mediante un riguroso proceso de administración de configuración y control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.

vi) Mantenimiento, Monitoreo y Análisis de Logs de Auditoría: recopile, administre y analice registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

vii) Protecciones de correo electrónico y navegador web: minimice la superficie de ataque y las oportunidades para que los atacantes manipulen el comportamiento humano a través de su interacción con los navegadores web y los sistemas de correo electrónico.

viii) Defensas contra software malicioso: controle la instalación, propagación y ejecución de código malicioso en múltiples puntos de la empresa, mientras optimiza el uso de la automatización para permitir una actualización rápida de la defensa, la recopilación de datos y la acción correctiva.

ix) Limitación y Control de Puertos de Red, Protocolos y Servicios: administre (rastree/controle/corrija) el uso operativo continuo de puertos, protocolos y servicios en dispositivos en red para minimizar las ventanas de vulnerabilidad disponibles para los atacantes.

x) Capacidades de recuperación de datos: los procesos y herramientas utilizados para respaldar adecuadamente la información crítica con una metodología comprobada para la recuperación oportuna de la misma.

xi) Configuración segura para dispositivos de red, como cortafuegos, enrutadores y conmutadores: establezca, implemente y administre activamente (rastree, informe sobre, corrija) la configuración de seguridad de los dispositivos de infraestructura de red

mediante un riguroso proceso de administración de configuración y control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.

xii) Defensa de límites: detectar/prevenir/corregir el flujo de información que transfiere redes de diferentes niveles de confianza con un enfoque en los datos que dañan la seguridad.

xiii) Protección de Datos: los procesos y herramientas utilizados para evitar la exfiltración de datos, mitigar los efectos de los datos exfiltrados y garantizar la privacidad e integridad de la información confidencial.

xiv) Acceso controlado basado en la necesidad de saber: los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el acceso seguro a activos críticos (por ejemplo, información, recursos, sistemas) de acuerdo con la determinación formal de qué personas, computadoras y aplicaciones tienen la necesidad y el derecho de acceder a estos activos críticos. Sobre la base de una clasificación aprobada.

xv) Control de acceso inalámbrico: los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el uso de seguridad de redes de área local inalámbricas (WLAN), puntos de acceso y sistemas de clientes inalámbricos.

xvi) Seguimiento y control de cuentas: administre activamente el ciclo de vida de las cuentas del sistema y de la aplicación (su creación, uso, inactividad, eliminación) para minimizar las oportunidades de que los atacantes las aprovechen.

xvii) Implementar un programa de capacitación y concientización sobre seguridad: para todos los roles funcionales en la organización (priorizando aquellos de misión crítica para el negocio y su seguridad), identifique los conocimientos, habilidades y capacidades específicos necesarios para respaldar la defensa de la empresa; desarrollar y ejecutar un plan integrado para evaluar, identificar brechas y remediar a través de políticas, planificación organizacional, capacitación y programas de concientización.

xviii) Seguridad del software de aplicación: administre el ciclo de vida de seguridad de todo el software desarrollado y adquirido internamente para prevenir, detectar y corregir las debilidades de seguridad.

xix) Respuesta y gestión de incidentes: proteja la información de la organización, así como su reputación, desarrollando e implementando una infraestructura de respuesta a incidentes (p. ej., planes, roles definidos, capacitación, comunicaciones, supervisión de la administración) para descubrir rápidamente un ataque y luego contener el daño de manera efectiva, erradicando la presencia del atacante. Y restauración de la integridad de la red y los sistemas.

xx) Pruebas de penetración y ejercicios del equipo rojo: pruebe la fuerza general de la defensa de una organización (la tecnología, los procesos y las personas) simulando los objetivos y las acciones de un atacante.

1.4 Conclusiones

El Programa de Gestión Documental - PGD desarrollado por AGN (actualmente usado por el DANE) tiene la finalidad de garantizar la integridad, disponibilidad, fiabilidad y usabilidad de los documentos. Este programa ha sido adaptado por entidades públicas como es el caso del Ministerio de Educación Nacional - MEN, el cual vincula su PDG al Sistema Integrado de Gestión - SIG[48], por medio del Sistema de Desarrollo Administrativo, como lo establece el Decreto 2482 de 2012, además, dado que las normas aplicadas para el cumplimiento de la función archivística y la gestión documental para las entidades del orden nacional son expedidas por el AGN, este es uno de los organismos de inspección y vigilancia de la gestión documental en Colombia[49].

El PDG plantea la necesidad de digitalizar y producir digitalmente los documentos en la entidad por medio un Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA, para ello el AGN desarrolló el documento Guía de Implementación de un SGDEA[50] el cual tiene como propósito establecer una estructura conceptual y una ruta de implementación del SGDEA en una organización, este documento toma como referencia los lineamientos y mejores prácticas nacionales e internacionales para establecer los requisitos funcionales y no funcionales del SGDEA, las Normas Técnicas Colombianas – NTC 15489-1 y NTC 15489- 2 para sustentar las políticas, procedimientos y prácticas de gestión documental que definirán el modelo contemplado en las NTC 30301, NTC 30302.

Asimismo, el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC desarrolló la política de gobierno digital en Colombia, la cual expidió:

- El Plan Nacional de Infraestructura de datos - PNID y su hoja de ruta, con el fin de impulsar la transformación digital del Estado y el desarrollo de una economía basada en los datos, en los documentos de hoja de ruta se resalta la importancia del Ciclo de vida del Dato (creación del dato, el procesamiento, almacenamiento, transferencia, análisis, preservación y reutilización del dato), pues este funciona de base para estipular el PNID.
  En el marco de la metodología ArCo (la cual optimiza y mejora la eficiencia de la oferta institucional de los instrumentos de política pública) se presentan las siguientes guías para apoyar la implementación del PNID y sus distintos componentes: i) PETI, ii) Marco de referencia de arquitectura empresarial, iii) Modelo de seguridad y protección de información,

[48] Disponible https://www.mineducacion.gov.co/portal/Ministerio/Informacion-Institucional/135295:Sistema-Integrado-de-Gestion-SIG
[49] Disponible en https://www.mineducacion.gov.co/1759/articles-362792_galeria_33.pdf
50 Disponible en https://www.archivogeneral.gov.co/caja_de_herramientas/docs/2.%20planeacion/DOCUMENTOS%20TECNICOS/IMPLEMENTACION%20DEL%20SGDEA.pdf

iv) Marco de transformación digital, v) Modelo de explotación de datos, vi) Marco de interoperabilidad, vii) Lenguaje común de intercambio de datos, viii) Guia para el uso y aprovechamiento de datos y ix) Guia de gobierno de datos.

- La política del gobierno digital, la cual cuenta con componentes (TIC para la sociedad y TIC para el estado) y habilitadores transversales que conforman los pilares de su implementación, entre los habilitadores se tienen:
    a. Seguridad y privacidad, el cual busca que las entidades públicas incorporen la seguridad de la información en todos sus activos con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado.
    b. Arquitectura, el cual busca que las entidades públicas apliquen en su gestión, un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI, aplicando los lineamientos, estándares y mejores prácticas contenidos en el marco de Referencia de Arquitectura empresarial del estado.

Además, se resalta la importancia de los estándares internacionales como las normas ISO relacionadas con los modelos de Seguridad de TI, que cuentan con requisitos genéricos aplicables a todas las organizaciones (sin importar su tamaño o naturaleza), las más relevantes para un Sistema de Gestión son las ISO 22301 y 27001, mientras que para la seguridad de la información son las ISO 27002, 27032 y 31000.

Igualmente múltiples entidades privadas han desarrollado lineamientos de buenas prácticas dirigidos al gobierno y gestión de la información y la tecnología empresarial, como es el caso de la Asociación de Auditoría y Control de Sistemas de Información – ISACA quien desarrolló el marco COBIT para este fin, sin embargo, ISACA resalta que COBIT **no** es ni una descripción completa de todo el entorno de TI de una empresa, ni un marco para organizar los procesos de negocio o gestionar la tecnología, ni ordena decisiones relacionadas con TI, sino que más bien COBIT tiene como objetivo definir todos los componentes que describen que, como y quien debería tomar las decisiones. Actualmente, están disponibles las siguientes publicaciones de este marco: i) Marco de Referencia COBIT 2019: Introducción y metodología[51], el cual presenta los conceptos clave de COBIT 2019 ii) Marco de Referencia COBIT 2019: Objetivos de gobierno y gestión[52], en el cual explica los 40 objetivos principales del gobierno y la gestión, y los procesos y componentes relacionados (esta guía

51Disponible en https://pdfcoffee.com/cobit-2019-framework-introduction-and-methodology-res-eng-1118-2-5-pdf-free.html
52 Disponible en https://pdfcoffee.com/cobit-2019-framework-governance-and-management-objectives-res-eng-1118-2-pdf-free.html

también hace referencia a otros estándares y marcos relacionados), iii) Guía de diseño COBIT 2019: Diseño de una solución de Gobierno de Información y Tecnología[53], el cual investiga los factores de diseño que pueden influir en el gobierno y además incluye un flujo de trabajo para la planificación de un sistema de gobierno personalizado para la empresa, y iv) Guía de implementación de COBIT 2019: Implementación y optimización de una solución de gobierno de Información y Tecnología[54], el cual es la evolución de la guía COBIT 5 y desarrolla una hoja de ruta para la mejora continua del gobierno.

En esta línea, las entidades públicas nacionales también disponen de manuales que les permiten gestionarla la seguridad, entre ellos: i) el MEN cuenta con el Manual de Seguridad Informática, el cual establece protocolos de seguridad con el objetivo de que los servicios tecnológicos y de comunicaciones se ofrezcan con calidad, confiabilidad, integralidad y eficiencia, ii) el DNP desarrolló el Manual y Políticas de Seguridad de la Información, con el objetivo de garantizar que los riesgos asociados a la seguridad de la información sean identificados, valorados, controlados y administrados de una forma estructurada y eficiente, como lo establece el Marco de protección de datos personales, asimismo, el DNP cuenta con el Sistema de Gestión de la Seguridad de la Información – SGSI el cual está conformado por de políticas, procesos, instructivos, lineamientos, guías, formatos, mapas de riesgos, estructura organizacional y mecanismos de verificación y control, que permiten minimizar los riesgos asociados a la seguridad de la información y atender en forma positiva incidentes de este tipo, este sistema protege los activos de información que la entidad identifica a través del lineamiento para la identificación y valoración de activos de información en el Sistema de Seguridad de la Información.

Por otra parte, en relación con la Ciberseguridad, a nivel internacional se han desarrollado guías para ayudar a realizar ejercicios de autoevaluación de capacidades de ciberseguridad, como es el caso de la Agencia de Ciberseguridad de la Unión Europea – ENISA quien desarrolló el documento Herramienta de Marco Nacional de Evaluación de Ciberseguridad – NCAF, cuyo objetivo es medir el nivel de madurez de las capacidades de ciberseguridad de los estados miembros, con el fin de ayudar a mejorar la conciencia del nivel de madurez del país, identificar áreas de mejora y desarrollar capacidades de ciberseguridad. Adicionalmente, en enero del 2022 publicó un informe titulado "Protección de Datos Ingeniería. De la teoría a la práctica", en el que se presentan las tecnologías y técnicas (de seguridad) existentes y discuten sus posibles fortalezas y la aplicabilidad en relación con el cumplimiento de los principios de protección de datos.

53 Disponible en https://pdfcoffee.com/cobit-2019-design-guideresspa0719pdf-3-pdf-free.html
54 Disponible en https://pdfcoffee.com/cobit-2019-implementation-guideresspa0719pdf-5-pdf-free.html

Finalmente, las organizaciones de carácter voluntario también han elaborado marcos sobre este tema, entre ellos está la guía sobre *Gestión de riesgos cibernéticos en la era digital*[55] que tiene como fin proporcionar una descripción general sobre la gestión del riesgo cibernético a través de los principios definidos en el Marco de gestión de riesgos empresariales (no pretende ser una guía para desarrollar e implementar estrategias técnicas), además, COSO desarrolló el marco para el control interno de riesgos en la era cibernética, el cual proporciona un enfoque común para gestionar cualquier tipo de riesgo y no es específico de una industria o un sector.

1.5 Recomendaciones para el DANE

El DANE debe continuar en su robustecimiento de los métodos y mecanismos tecnológicos para asegurar una adecuada gestión documental, de la información, de la seguridad de esta y su almacenamiento. La Entidad ha hecho y está recorriendo un camino de aprendizaje continuo desde la gestión de riesgos, como base de cada uno de los anteriores marcos de referencia expuestos, como también de la implementación y mantenimiento de las políticas de Gobierno Digital, Seguridad Digital y las asociadas a la Seguridad y Privacidad de la Información.

Respecto a los métodos, el DANE debe continuar con el fortalecimiento de su gobernanza de datos y de la gestión documental, al igual con la especialización de cada uno de los procesos asociados y tecnologías que las apalancan. Esto para asegurar la madurez y mantenimiento de estas dos capacidades críticas para la operación de la Entidad, para asegurar su acervo documental (Legal, administrativa, técnica, entre otros) e información histórica estadística.

De igual forma, la necesidad creciente en renovar las capacidades tecnológicas permitirá al DANE dar una mirada más estratégica en la concepción, adopción, uso u apropiación de tecnologías que faciliten el desarrollo de las operaciones estadísticas, censales y administrativas, en pro de la efectividad frente a la ciudadanía y demás grupos de valor de la Entidad. Los anteriores marcos de referencia no ven la tecnología como un componente de soporte sino como un componente estratégico que apalanca el desarrollo de los modelos.

Es importante entender que todos los modelos anteriormente expuestos, si bien requieren de unos componentes tecnológicos lo suficientemente robustos para asegurar el cumplimiento de requisitos de seguridad y privacidad de la información, la concientización del buen uso de la información y de las herramientas destinadas para tal fin, incluyendo factores físicos como el puesto de trabajo, son

[55] Disponible en Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO). (2019). Gestión del riesgo cibernético en la era digital. https://incp.org.co/Site/publicaciones/info/archivos/Cyber-risk-in-a-digital-age.pdf

críticos e implican la participación activa de todos los servidores públicos y de todos los niveles organizacionales.

Finalmente, es necesario comprender que, si bien las mejores prácticas tienen puntos en común y algunos "Deber ser", es necesario que se identifiquen cuáles de las prácticas, adicionales a las de obligatorio cumplimiento normativo, deben ser adoptadas de manera práctica, asegurando su correcta implementación, ejecución y mantenimiento, sin sobrecargar el Sistema Integrado de Gestión Institucional - SIGI y operación normal del DANE. Esto se logra con el entendimiento, articulación y unificación de los sistemas de gestión de riesgo y la homologación de requisitos e instrumentos de cada modelo.

2. Buenas prácticas de las Instituciones Públicas para garantizar la propiedad intelectual sobre la divulgación de productos de investigación.

2 Buenas prácticas de las Instituciones Públicas para garantizar la propiedad intelectual sobre la divulgación de productos de investigación, desarrollo e innovación

2.1 Resumen

La Propiedad Intelectual – PI otorga el derecho a goce y disposición sobre las obras producidas por su creador derivadas del intelecto humano en el ámbito industrial, científico, literario y artístico, esta rama del derecho cubre los derechos de autor y conexos; los cuales contemplan las obras literarias, artísticas, musicales, software, entre otros. Mientras que la propiedad industrial se aplica sobre invenciones, diseños industriales o signos distintivos; según el artículo 671 del Código Civil de Colombia sobre la propiedad intelectual "*Las producciones del talento o del ingenio son una propiedad de sus autores*[56]".

Como se mencionó anteriormente, los derechos de autor protegen el ingenio y talento humano en los dominios literarios y artísticos, en cualquiera que sea su modo de expresión o estilo, en Colombia, este reconocimiento se hace por medio de la Ley 23 de 1982[57], la Decisión Andina 351 de 1993, la adhesión de Colombia al Convenio de Berna para la protección de las obras literarias y artísticas por medio de la Ley 33 de 1987, y el Tratado de la OMPI sobre derecho de autor en la Ley 565 de 2000, que establecen para los autores de obras literarias y artísticas la propiedad sobre estas de orden moral y patrimonial[58].

Actualmente, en el DANE se están presentando nuevas situaciones de producción intelectual derivadas del plan de acción de cada equipo, como es el caso del Grupo Interno de Trabajo de Prospectiva y Análisis de Datos - GIT PAD, que al igual que otros grupos de la entidad se encuentra enfocado en el desarrollo de actividades de investigación, y uno de los objetivos esperados de este GIT es que se elaboren documentos científicos de divulgación en revistas especializadas, así como la producción de otro tipo de material científico.

[56] Disponible en http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil_pr020.html#:~:text=ARTICULO%20671.,se%20regir%C3%A1%20por%20leyes%20especiales.

[57] Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=3431#:~:text=Esta%20Ley%20protege%20exclusivamente%20la,obras%20literarias%2C%20cient%C3%ADficas%20y%20art%C3%ADsticas.p

[58] Disponible en http://www.cecolda.org.co/index.php/derecho-de-autor/normas-y-jurisprudencia/direccion-nacional-de-derecho-de-autor/98-circular-nro-7-el-servidor-publico-como-titular-de-derecho-de-autor

Las actividades realizadas por el GIT PAD iniciaron como una exploración general y con metas agregadas abordando temas relacionados con estadísticas experimentales o mejoras de procesos y procedimientos al interior del DANE, los cuales se realizaron bajo tres líneas: machine learning, visualización y aprovechamiento de fuentes alternativas. A partir del trabajo conjunto con las áreas involucradas han ganado un mayor nivel de robustez, generando productos concretos como metodologías, tableros de control y artículos académicos, y en algunos casos se ha alcanzado el nivel de publicación científica; no obstante, dado que estas dinámicas son nuevas para el grupo y se desconoce como garantizar la propiedad intelectual en estos productos derivados de la investigación, desarrollo e innovación, el GIT PAD plantea la necesidad de contar con una revisión de referentes, donde se identifiquen las buenas prácticas realizadas en las instituciones públicas sobre la propiedad intelectual y los derechos de autor, donde se aborden en específico de los siguientes temas:

- Propiedad intelectual de los productos de investigación.
- Derechos de paternidad y reconocimiento de los productos de investigación.
- Reconocimiento de los derechos morales a los autores de investigación.
- Alcances de los derechos patrimoniales, uso y abuso de estos derechos.
- Control a la práctica del free rider o polizón en la investigación pública.
- Consideraciones éticas.
- Control a la divulgación y usufructo en espacios externos por los investigadores una vez se desvinculan de la entidad (e inclusive durante su vinculación).

Los referentes de interés en la investigación son las entidades públicas que presentan situaciones similares, pues dado que la temática está atada a la normativa interna de cada país se planteó acotar el reporte a una revisión nacional, haciendo énfasis en la Ley 23 de 1982 y relacionadas. Lo anterior, con el fin de iniciar una agenda de trabajo clara que permita abordar y definir buenas prácticas y principios sobre la propiedad intelectual y los derechos de autor desde el punto de vista de la producción estadística.

2.2 Síntesis de hallazgos

A continuación, en la **Error! Reference source not found.**8 se presenta una breve descripción de los principales hallazgos de la revisión de referentes nacionales sobre buenas prácticas para garantizar la propiedad intelectual sobre la divulgación de productos de investigación, desarrollo e innovación.

Tabla 16. Principales hallazgos sobre buenas prácticas para garantizar la propiedad intelectual sobre la divulgación de productos de investigación, desarrollo e innovación.

Referente	¿Cómo las entidades públicas en el país (Colombia) garantizan la propiedad intelectual y los derechos de autor sobre la divulgación de productos de investigación, desarrollo e innovación?
Ministerio de Ciencia, Tecnología e Innovación	El Ministerio de Ciencia, Tecnología e Innovación desarrolló el Programa Colombia Científica, el cual tiene como objetivo contribuir a mejorar la calidad de las Instituciones de Educación Superior por medio del fortalecimiento de la capacidad investigativa de estas, en el marco de este programa se ha detectado la necesidad de generar una guía orientadora en relación con el uso y asignación de la propiedad intelectual, para tal fin desarrolló la *Guía de Propiedad Intelectual* en el que expone los casos generales de titularidad de los derechos de propiedad intelectual de acuerdo con el tipo de creación y algunos casos especiales para los que en ausencia de la voluntad expresa de las partes, la ley es quien determina la titularidad de la materia protegida, dentro de estos casos se encuentran los derechos patrimoniales de obras realizadas por funcionarios públicos en virtud de sus obligaciones constitucionales o legales, los cuales le pertenecen a la entidad para la cual este preste sus servicios, como lo dicta el artículo 91 de la Ley 23 de 1982. Asimismo, el Centro Colombiano del Derecho de Autor reconoce esta ley y destaca que las obras cuya autoría pertenezca a servidores públicos en las condiciones establecidas tendrán por autor a la persona natural que las creó y esta conservará los derechos morales más no patrimoniales de su obra, no obstante, los servidores públicos que realicen obras susceptibles a propiedad intelectual, pero que no sean realizadas en función de la actividad propia de su cargo, se consideran de propiedad moral y patrimonial del servidor, y, por lo tanto, las obras tendrán toda la protección legal que el régimen jurídico le aporte en esta materia.

Referente	¿Cómo las entidades públicas en el país (Colombia) garantizan la propiedad intelectual y los derechos de autor sobre la divulgación de productos de investigación, desarrollo e innovación?
Ministerio de Educación Nacional	El Ministerio de Educación Nacional, desarrolló la Guía de Política de Protección Sobre la Propiedad Intelectual: eje derechos de autor, que tiene por objetivo proteger los derechos de autor y conexos como una dimensión de propiedad intelectual en relación con obras artísticas, literarias y científicas, que sean originales, inéditas o resultantes del trabajo desarrollado por servidores, contratistas, o terceros vinculados al Ministerio por relación contractual. En este contexto, los derechos de autor sobre las obras creadas por empleados o servidores públicos en el ejercicio de sus funciones son cedidos a la entidad desde el momento de su creación. En el caso de los procesos de contratación o adquisición, desarrollo de proyectos o convenios de investigación, cooperación u otros acuerdos con contratistas, consultores, proveedores, investigadores, etc. Se deben definir previo a la contratación o convenio los activos de propiedad intelectual producto del objeto contractual.
Departamento Nacional de Planeación	El DNP publicó el CONPES 4062 sobre la Política Nacional de Propiedad Intelectual, en el cual se plantea un plan de acción que involucra a varias entidades públicas para que presenten estrategias, documentos, mapeos, caracterizaciones y guías; con el fin de fomentar, utilizar y divulgar la importancia, beneficios y aportes de la propiedad intelectual en los diferentes sectores del país, se establece un horizonte de 10 años para su ejecución (2022 – 2031).
Dirección Nacional de Derechos de Autor	La Dirección Nacional de Derechos de Autor publicó el *Manual de derechos de autor* en donde detalla aspectos conceptuales y legales sobre propiedad intelectual y derechos de autor. El Manual se sustentan en la Ley 23 de 1992 y de manera particular destaca que, las obras creadas por servidores públicos pueden asociarse a 2 situaciones: (i) que la obra sea creada en cumplimiento de las obligaciones constitucionales y legales que le competen, o (ii) que sea creada por fuera del cumplimiento de tales obligaciones. De acuerdo con cada caso, es generada la titularidad de los derechos de autor.
Agencia Nacional de Contratación Pública	La Agencia Nacional de Contratación Pública dispone de la Guía de Propiedad Intelectual en la Contratación Pública, la cual permite identificar a las autoridades que velan por la garantía y protección de los derechos de autor y propiedad intelectual, de igual manera, expone los diferentes mecanismos y herramientas internacionales a los que Colombia se encuentra vinculado para la defensa de derechos de autor sobre productos de investigación desarrollo e innovación. Y, a la vez, esta expone puntualmente las normativas vigentes sobre la cesión y tratamiento de los derechos

Referente	¿Cómo las entidades públicas en el país (Colombia) garantizan la propiedad intelectual y los derechos de autor sobre la divulgación de productos de investigación, desarrollo e innovación?
	patrimoniales y morales, y, la manera en que estos son vinculados en los contratos laborales, de prestación de servicios, por producto y de aprendizaje.
Ministerio de Defensa	El Ministerio de Defensa Nacional de Colombia posee la Política de propiedad intelectual y transferencia de tecnología, en la cual se establecen los lineamientos generales que deben seguir las instituciones como las Fuerzas Militares, Policía Nacional y diversas entidades adscritas al Ministerio. Dentro de la Política se destaca la Guía de Propiedad Intelectual y Transferencia de Tecnología, la cual destaca secciones para propiedad intelectual y propiedad industrial. El Ministerio, desde el año 2019, pertenece a la Comisión Intersectorial de Propiedad Intelectual.
Instituto Colombiano Agropecuario	El ICA cuenta con Política de derecho de Autor y autorización de uso sobre los contenidos, en la página web se menciona sobre la existencia de la ventanilla única y los portales transversales y aplicativos informáticos, por medio de los cuales el ICA divulga los temas y actividades propias de su misión, visión, objetivos y funciones. Para usar los contenidos de los sitios web, portales y aplicativos informáticos debe tener autorización expedida por ICA, la autorización incluye: a) Cesión parcial o total de derechos sobre los contenidos b) Derecho de utilización c) Derecho de alteración, explotación, reproducción, distribución o comunicación de los contenidos.

Fuente: DANE a partir de las revisiones de referentes.

2.3 Revisión de referentes

En esta sección se presentan, de forma sintetizada, la revisión de los siete referentes en nacionales en el marco de las instituciones públicas, de los cuales seis pertenecen a la rama ejecutiva y uno posee la estructura jurídica de una Unidad Administrativa Especial adscrita el Ministerio del Interior (Dirección Nacional del Derecho de Autor).

2.3.1 Instituto Colombiano Agropecuario – ICA

El Instituto Colombiano Agropecuario – ICA, es un Establecimiento Público del Orden Nacional con personería jurídica, autonomía administrativa y patrimonio independiente, perteneciente al Sistema Nacional de Ciencia y Tecnología, adscrito al Ministerio de Agricultura y Desarrollo Rural.

El ICA cuenta con Política de derecho de Autor y autorización de uso sobre los contenidos, en la página web se menciona la existencia de la ventanilla única y los portales transversales y aplicativos informáticos, por medio de los cuales el ICA divulga los temas y actividades propias de su misión, visión, objetivos y funciones. Para usar los contenidos de los sitios web, portales y aplicativos informáticos debe tener autorización expedida por ICA, la autorización incluye:

a) Cesión parcial o total de derechos sobre los contenidos
b) Derecho de utilización
c) Derecho de alteración, explotación, reproducción, distribución o comunicación de los contenidos.

Materiales suministrados al ICA

- Todo el contenido está protegido por las normas sobre Derechos de Autor y por todas las normas nacionales e internacionales que le sean aplicables. Exceptuando lo expresamente estipulado en estos Términos de Uso.
- Queda prohibido todo acto de copia, reproducción, modificación, creación de trabajos derivados, venta o distribución, exhibición de los contenidos, de ninguna manera o por ningún medio, incluyendo, más no limitado; a medios electrónicos, mecánicos, de fotocopiado, de grabación o de cualquier otra índole sin previa autorización del ICA, ya que dicha información, registro y derecho personal son exclusivamente propiedad del ICA.
- El funcionamiento de este sitio y la información que contiene se rigen por las leyes de la República de Colombia. El ICA no se asume ninguna responsabilidad sobre la disponibilidad del sitio y su información por cualquier persona que tenga acceso a los mismos desde fuera del territorio y la jurisdicción de la República de Colombia.
- Los materiales suministrados incluyen cualquier marca y logotipo que aparezcan en los sitios web, estas son marcas comerciales registradas. Las marcas comerciales son los nombres de compañías y productos reales mencionados en los sitios web, pueden ser marcas comerciales de sus respectivos propietarios.
- El ICA no reclama la propiedad de los materiales que el usuario suministre al realizar comentarios, sugerencias, anuncios, publicaciones, sin embargo, al anunciar, publicar, subir, escribir, el usuario está otorgando permiso al ICA para publicar y eliminar la información que ha proporcionado.

Política de datos abiertos

Se podrá hacer uso, transformación, distribución, redistribución, reutilización, compilación, extracción, copia, difusión, modificación y/o adaptación de los datos y de la información publicados en formato de datos abiertos en este sitio web, en todo caso debe citarse la fuente de los datos objeto del uso, rehúso y/o transformación, la entidad productora de los datos publicados no será responsable de la utilización que de sus datos hagan las personas que transformen y/o usen dichos datos, ni tampoco de los daños sufridos o pérdidas económicas que, de forma directa o indirecta, produzcan o puedan producir perjuicios económicos, materiales o sobre datos y aplicaciones, provocados por el uso y/o transformación de los datos. Esta licencia de uso se rige por la legislación colombiana, independientemente del entorno jurídico del usuario, cualquier disputa que llegue a surgir en la interpretación de estos términos se resolverá bajo el amparo de la Ley colombiana.

En el día Mundial de la Propiedad Intelectual, el ICA[59] reitera el compromiso de seguir trabajando para la protección de plantas nacionales como incentivo para el desarrollo de nuevas variedades vegetales. A través de los Derechos de Obtentor de variedad vegetales, que son una forma de propiedad intelectual, como lo son también los derechos de autor, las marcas y los dibujos y diseños industriales, el Instituto otorga un derecho exclusivo a quien desarrolla y termina una nueva variedad para su explotación.

Producto del trabajo realizado por el ICA desde la apertura del registro nacional de variedades vegetales en Colombia, el número de solicitudes ha venido en constante crecimiento, constituyendo cifras importantes y generando confianza nacional e internacional.

2.3.2 Ministerio de Ciencia, Tecnología e Innovación

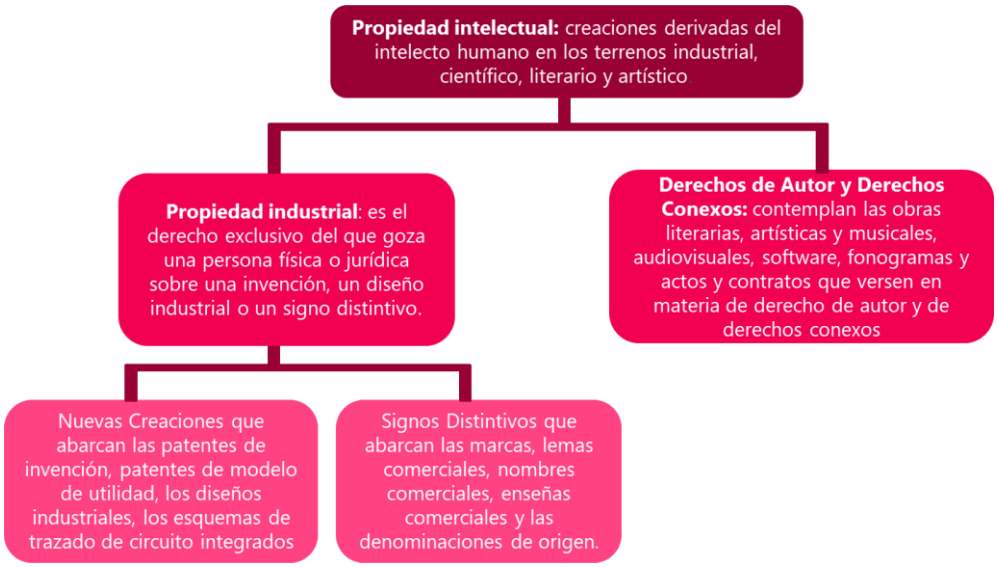
El Programa Colombia Científica[60] tiene como objetivo contribuir a mejorar la calidad de las Instituciones de Educación Superior - IES por medio del fortalecimiento de la capacidad investigativa de las instituciones nacionales. Este programa está compuesto por dos partes (las cuales buscan incentivar la creación de conocimiento y la transferencia tecnológica):

1. El pasaporte a la ciencia, dirigido a la formación de alto nivel.
2. El ecosistema científico, el cual es una red de actores nacionales e internacionales (miembros de la alianza) que se articulan alrededor de retos y áreas comunes, con el fin de producir y

[59] Disponible en ICA, noticias abril 2022 disponible en https://www.ica.gov.co/noticias/ica-compromiso-proteger-nuevas-especies-vegetales
60 Disponible en https://reconstrucciondeltejidosocial.com/

usar conocimiento en función del desarrollo social y productivo del país, donde cada alianza debe desarrollar programas de investigación, tecnológicos o de innovación que incentiven la generación y traspaso de conocimiento y tecnologías, lo que permite (entre otros resultados) proteger las diferentes modalidades de propiedad intelectual - PI de los posibles resultados (Ver Ilustración 19).

Ilustración 19. Modalidades de propiedad intelectual



DANE a partir de Minciencias 2017

En el marco del Programa Colombia Científica, promocionar y proteger la propiedad intelectual es una herramienta vital, pues puede tener impactos significativos sobre la educación superior del país, dado esto, el ecosistema científico ha detectado la necesidad de generar una guía orientadora en relación con el uso y asignación de la propiedad intelectual, pues es una herramienta vital para los procesos de gestión tecnológica y de innovación, y su adecuada gestión permite aumentar la capacidad innovadora y las ventajas competitivas del mercado, para tal fin Minciencias desarrolló la *Guía de Propiedad Intelectual*[61] en el marco del Programa Colombia Científica.

Al interior de las alianzas es muy probable que varias personas intervengan en la ideación, desarrollo y consolidación de productos, procedimientos o servicios que sean susceptibles a ser protegidos por PI, la anterior guía recomienda que previo a realizar la asignación de los derechos de PI generados en el desarrollo de los resultados de una alianza debe advertirse de los alcances que podría tener entre miembros de la alianza la PI, así como las reglas internas para el uso de PI de terceros.

61 Disponible en https://minciencias.gov.co/sites/default/files/upload/convocatoria/anexo8-guia-propiedad-intelectual.pdf

Posteriormente, se realiza la asignación de la titularidad de los derechos de PI de los resultados obtenidos con el fin de dar seguridad y confianza a los diferentes actores de la alianza que intervienen en el desarrollo de dichos resultados (su asignación debe realizarse por los miembros de la alianza), estableciendo así reglas claras de uso de la PI durante el desarrollo del proyecto y la posterior titularidad de los resultados (evitando así posibles controversias), pues en la medida en que estas condiciones son claras, se pueden establecer mecanismos idóneos para potencializar el valor de las invenciones al darles valor económico y transferir sus conocimientos. Minciencias recomienda el establecimiento de acuerdos expresos sobre titularidad y cesión de los derechos de propiedad intelectual, por lo que es vital identificar los aspectos objetivos (objeto y título de protección) como los elementos subjetivos (autores y titulares) asociados a la creación intelectual (Ver Tabla 17).

Tabla 17. Titularidad de los derechos de la propiedad intelectual de acuerdo con el tipo de creación

Tipo de creación	Descripción	Titularidad de los derechos de la propiedad intelectual
Creaciones ocasionales	Aquellas realizadas por una persona natural que no se encuentra en cumplimiento de un contrato laboral o de prestación de servicios, ni en el marco de un ejercicio planificado de creación conjunta. En este caso, el creador independiente que expresa su ingenio en su taller o laboratorio personal, sin utilizar medios o recursos suministrados por un empleador o contratante.	El creador es el titular de los derechos patrimoniales; sin embargo, debe prestar atención al principio del primer solicitante, en aquellos supuestos en que el registro sea constitutivo del derecho de PI.
Creaciones en el ámbito laboral o de servicio	Las creaciones en cumplimiento de un contrato (escrito) de prestación de servicios o de trabajo en donde la creación obedece a una obligación que surge de un acuerdo con obligaciones determinadas, de un manual de funciones de cargo, o son realizadas utilizando recursos del empleador o contratante.	La titularidad de los derechos patrimoniales es cedida al empleador por la presunción legal de cesión o por tratarse de una obra por encargo. Lo anterior, en tanto, las creaciones o invenciones sean realizadas por el trabajador o contratista en el marco de las obligaciones contratadas y/o cuando se elaboran con conocimientos o recursos del empleador o contratante.

Creaciones en conjunto (dirigidas, deliberadas)	Aquellas realizadas por dos o más personas naturales o cuando la titularidad la comparten dos o más personas jurídicas que unen esfuerzos para desarrollar una creación. En este ámbito pueden surgir creaciones como resultado de un plan detallado de I+D, como consecuencia de una relación laboral o de servicios o de manera espontánea u ocasional.	La titularidad se define en virtud de la autonomía de la voluntad. Ante ausencia de esta definición se entiende que existe co-titularidad. Ahora bien, si la creación conjunta surge como resultado del cumplimiento de un contrato laboral o de servicios, le serán aplicables las reglas expuestas para este tipo de creaciones.

Fuente DANE a partir de Minciencias 2016[62]

Asimismo, aunque en términos generales las políticas de los miembros de las alianzas con respecto a la propiedad intelectual determinan cuando se desarrolla un "invento" y la propiedad y derechos derivados de este, existen ciertos casos especiales para los que se han implantado presunciones de ley en las cuales en ausencia de la voluntad expresa de las partes, la ley es quien determina la titularidad de la materia protegida, entre ellas:

- ✓ Los derechos patrimoniales y/o de propiedad industrial de las obras creadas por el cumplimiento de un contrato de prestación de servicios o de trabajo serán transferidos al empleador (para ello se requiere que el contrato sea escrito).
- ✓ El productor de obras audiovisuales se presume como titular de los derechos patrimoniales (salvo pacto contrario).
- ✓ Los derechos patrimoniales de obras realizadas por funcionarios públicos en virtud de sus obligaciones constitucionales o legales serán de la entidad para la cual este preste sus servicios (esta es una presunción iuris tantum o de derecho, es decir, no admite prueba en contrario).

Sobre esta última presunción, de acuerdo con el artículo 91 de la Ley 23 de 1982:

> *"Los derechos de autor sobre las obras creadas por empleados o funcionarios públicos, en cumplimiento de las obligaciones constitucionales y legales de su cargo, serán de propiedad de la entidad pública correspondiente.*
> *Se exceptúan de esta disposición las lecciones o conferencias de los profesores.*

62 Disponible en https://minciencias.gov.co/sites/default/files/ckeditor_files/guia-pi-beneficios-tributarios-2016.pdf

Los derechos morales serán ejercidos por los autores, en cuanto su ejercicio no sea incompatible con los derechos y obligaciones de las entidades públicas afectadas[63]*."*

Por otra parte, el Centro Colombiano del Derecho de Autor, además de esta ley, reconoce la Decisión Andina 351 de 1993, la adhesión al convenio de Berna para la protección de obras literarias y artísticas (Ley 33 de 1987) y al tratado de la OMPI sobre derechos de autor (Ley 565 de 2000) que actúan sobre los atributos de orden moral y patrimonial que les corresponden a los autores de obras literarias o artísticas (Ver Ilustración 20).

Ilustración 20. Derechos morales y Patrimoniales

Fuente DANE a partir de CECOLDA 2002

El artículo 91 de la Ley 23 de 1982 señala que las obras cuya autoría pertenezca a servidores públicos en las condiciones establecidas tendrán por autor a la persona natural que las creó y esta conservará los derechos morales de su obra, pero la entidad estatal será la titular de los derechos patrimoniales, dándole la potestad de explotar libremente las obras y autorizar su uso por parte de terceros. Además, se resalta que las obras cuya titularidad patrimonial pertenezca al estado no son de dominio público, sino que, por el contrario, son bienes inmateriales que pertenecen al patrimonio del Estado (bajo la categoría de bienes fiscales), por lo que el uso de estos debe contar con la autorización previa y expresa de la entidad estatal.

No obstante, los servidores públicos que realicen obras susceptibles a propiedad intelectual, pero que no sean realizadas en función de la actividad propia de su cargo, se consideran de propiedad moral y patrimonial del servidor, y, por lo tanto, las obras tendrán toda la protección legal que el régimen jurídico le aporte en esta materia.

[63] Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=3431#:~:text=ART%C3%8DCULO%2091.,o%20conferencias%20de%20los%20profesores.

Finalmente, con respecto a la capacidad del servidor público para negociar como autor de una obra realizada por fuera de sus funciones legales y constitucionales con las entidades públicas, es necesario aclarar la vigencia del artículo 1 de la ley 44 de 1993, en relación con el artículo 8 de la Ley 80 de 1993 (ya que esta última norma inhabilita a los servidores públicos para contratar con las entidades estatales, sin embargo, no menciona expresamente este caso):

> "*Artículo 1 de la ley 44 de 1993: los empleados y funcionarios públicos que sean autores de obras protegidas por el Derecho de Autor podrán disponer contractualmente de ellas con cualquiera entidad de derecho público*".

La anterior ley introduce una posibilidad específica para que los servidores públicos autores de obras puedan celebrar contratos sobre ellas con entidades públicas, por lo que en este sentido los servidores públicos creadores de obras literarias o artísticas que no estén dentro del marco de las obligaciones constitucionales o legales de su cargo pueden conservar la titularidad de la propiedad patrimonial sobre sus creaciones[64].

2.3.3 Ministerio de Educación Nacional

El Ministerio de Educación Nacional - MEN, desarrolló la Guía de política de protección sobre la propiedad intelectual: eje derechos de autor[65], cuyo objetivo es proteger los derechos de autor y conexos como una dimensión de la propiedad intelectual en relación con todas las obras de tipo artístico, literario y científico, que sean originales, inéditas o derivadas del desarrollo, adquisición, gestión, utilización y protección de propiedad intelectual generada, adquirida o utilizada por el MEN, con creación de sus servidores, contratistas o terceros vinculados por medio de relación contractual. Mediante la guía, el Ministerio establece los criterios aplicables a los derechos de autor y conexos en relación con los bienes que pertenecen o se adquieran en la entidad.

En el marco normativo, el derecho de autor tiene la dimensión moral y patrimonial que constituye un derecho exclusivo, por lo tanto, otorga derechos de disposición sobre los derechos de autor a un tercero. En este contexto, las obras creadas por los servidores públicos en el ejercicio de sus funciones son cedidos desde el momento de la creación de la obra, fundamentado en el artículo 91 de la ley 23 de 1982. A continuación, en la Tabla 18, se relaciona la normatividad aplicable en temática de derechos de autor de entidades públicas en el país.

64 Disponible en http://www.cecolda.org.co/index.php/derecho-de-autor/normas-y-jurisprudencia/direccion-nacional-de-derecho-de-autor/98-circular-nro-7-el-servidor-publico-como-titular-de-derecho-de-autor
65 Disponible en https://www.mineducacion.gov.co/1780/articles-336187_recurso_3.pdf

Tabla 18. Normatividad aplicable en el escenario de derechos de autor en las entidades públicas en Colombia

Normatividad	Descripción	Enlace
Ley 23 de 1982	Esta Ley protege exclusivamente la forma literaria, plástica o sonora, como las ideas del autor son descritas, explicadas, ilustradas o incorporadas en las obras literarias, científicas y artísticas.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=3431
Ley 1915 de 2018	Es un instrumento a partir del cual Colombia implementa algunas de las disposiciones del Tratado de Libre Comercio (en adelante TLC), celebrado entre Colombia y Estados Unidos, en materia de derecho de autor y derechos conexos en el entorno digital.	https://revistas.uexternado.edu.co/index.php/propin/article/view/6072
Ley 1834 de 2017	Tiene como objeto desarrollar, fomentar, incentivar y proteger las industrias creativas. Estas son entendidas como aquellas industrias que generan valor en razón de sus bienes y servicios, los cuales se fundamentan en la propiedad intelectual.	https://economianaranja.gov.co/ley-naranja/
Ley 1680 de 2013	Ley que busca garantizar la autonomía y la independencia de las personas ciegas y con baja visión en el ejercicio de sus derechos a la información, las comunicaciones y el conocimiento, las obras literarias, científicas, artísticas, audiovisuales, producidas en cualquier formato, medio o procedimiento, podrán ser reproducidas, distribuidas, comunicadas, traducidas, adaptadas, arregladas o transformadas en braille y en los demás modos, medios y formatos de comunicación accesibles que elijan las personas ciegas y con baja visión, sin autorización de sus autores ni pago de los Derechos de Autor, siempre y cuando la reproducción, distribución, comunicación, traducción, adaptación, transformación o el arreglo, sean hechos sin fines de lucro y cumpliendo la obligación de mencionar el nombre del autor y el título de las obras así utilizadas.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=55611

Fuente DANE, basado en la Guía de política de protección sobre la propiedad intelectual.

Directrices para el registro de Derechos de Autor en el Ministerio de Educación Nacional

Una vez creada una obra en el MEN, en cabeza del autor o los autores, se tienen dos tipos de derechos, los derechos morales y los derechos patrimoniales.

- Derechos morales de autor: Protección de la propiedad intelectual sobre las obras protegidas por los derechos de autor, estos derechos son definidos como el vínculo moral y espiritual entre el autor y su obra, y tienen carácter inalienable e irrenunciable. Están conformados por el derecho de paternidad, no deformación, conservación inédita o anónima, modificación y retiro.
- Derechos patrimoniales de autor: Protección de la propiedad intelectual sobre las obras protegidas por los derechos de autor, se denominan derechos patrimoniales porque hacen parte del patrimonio del autor, pues tienen la facultad de beneficiarse y disponer de su obra. En este sentido, se heredan, pueden hacer parte de la sociedad conyugal, son embargables, transigibles y no renunciables; se dividen en dos tipos, i) los derechos patrimoniales exclusivos, que al ejercerlos implica una autorización previa y ii) los de mera remuneración, donde no se requiere autorización, sino pago.

Para los procesos de contratación o adquisición, desarrollo de proyectos o convenios de investigación, cooperación u otros acuerdos con contratistas, consultores, proveedores, investigadores, universidades, organismos internacionales o personas de naturaleza pública o privada, se deben tener en cuenta los siguientes aspectos:

- Definir desde el proceso de contratación, convenios o acuerdos y aspectos de titularidad de propiedad intelectual.
- Definir los activos de propiedad intelectual producto del objeto contractual y los modos previstos en la ley para que surjan derechos sobre estos, de acuerdo con su categoría.
- Adoptar la decisión de reservarse la titularidad de la propiedad intelectual, el derecho de registrar la propiedad intelectual a nombre propio o el licenciamiento de derechos que se desarrolle o adquiera durante la ejecución.

Tabla 19. Principios a tener en cuenta en la propiedad intelectual en el MEN

Principio	Descripción
Buena Fe	El Ministerio de Educación Nacional declara que respeta la producción intelectual de sus servidores, directivos, contratistas y terceros, y que presume que la producción de cada uno de ellos es original y no infringe derechos de propiedad intelectual.

Respeto por las normas vigentes	El Ministerio de Educación Nacional declara que está sometida a las normas vigentes en materia de propiedad intelectual, particularmente, a lo dispuesto en la Ley 23 de 1982, la Decisión 391 de 1993 de la Comunidad Andina de Naciones, los tratados internacionales en materia de derechos de autor, la Decisión 486 de 2000 en materia de propiedad industrial, y las demás normas que los modifican o adicionan.
Conservación del patrimonio del Ministerio de Educación Nacional	El Ministerio de Educación Nacional declara que, las obras, nuevas creaciones y signos distintivos sobre los que ostente los derechos de propiedad intelectual se incorporarán a su patrimonio y, por tanto, se promoverán todas las acciones legales y administrativas necesarias para su conservación.
Difusión y capacitación	El Ministerio de Educación Nacional se compromete a la generación de planes y programas dirigidos a sus directivos, servidores, contratistas y terceros tendientes a promover la cultura del respeto de la propiedad intelectual y la difusión de los derechos y deberes que les asisten.

Fuente DANE, basado en la Guía de política de protección sobre la propiedad intelectual.

Finalmente, las obras que sean objeto de creación, tipo obra literaria y artística, tales como las descritas en el artículo 2 de la Ley 23 de 1982 y artículo 1 del Decreto 1360 de 1989, que se han desarrollado en el Ministerio de Educación Nacional, se deben registrar ante las autoridades competentes como Dirección Nacional de Derechos de Autor para efectos probatorios de su existencia y titularidad.

Las obras creadas en el Ministerio de Educación Nacional que tengan disposición para otra entidad del Estado Colombiano o para un tercero, deberán disponer de su respectiva licencia, sea o no de carácter gratuito; potestad que quedará radicada de forma exclusiva en la entidad.
En el mismo sentido, las obras que sean de uso exclusivo o no, por parte del Ministerio que se encuentren sometidas a licencia para su uso, deberán tramitar la respectiva licencia y realizar el pago que legitima la explotación de los derechos intelectuales de terceros, el derecho de autor *(copyright)*, o ante la sociedad de Gestión Colectiva legítimamente constituida en el país y que ostente la explotación de los derechos patrimoniales de autor. La obtención de licencias y realización de pagos se hará conforme a la periodicidad señalada por la ley y a lo establecido por las respectivas entidades involucradas.

2.3.4 Departamento Nacional de Planeación

La Dirección Nacional de Planeación presentó en noviembre de 2021 el CONPES 4062: Política Nacional de Propiedad Intelectual[66], realizando un diagnóstico; que presentó la desarticulación que existe entre la oferta pública que contribuye a la investigación y creación, que genera ineficiencia para la generación de Propiedad Intelectual – PI; el desconocimiento de los derechos de PI, las normas que regulan los procesos y sus los beneficios, para fomentar el uso de la PI.

Adicionalmente, el CONPES 4062 tiene el objetivo de "Consolidad la generación y gestión de la Propiedad Intelectual y su aprovechamiento como herramientas para incentivar la creación, innovación, transferencia de conocimiento e incrementar la productividad del país"; a partir de este objetivo establecieron cinco objetivos específicos y 11 líneas de acción para implementar esta política. Para el presente informe, se destacan las siguientes líneas estratégicas:

- Línea 1. Aumentar y articular la inversión para la generación y gestión de activos de PI

Tabla 20. Acciones para aumentar y articular la inversión de activos de PI

Entidad	Acción	Tiempo de ejecución
DNP	Diseñar un fondo de financiamiento de potencial innovación y tecnología susceptible de protección por PI.	2023 – 2028
Superintendencia de Industria y Comercio - SIC	Diseñar e implementar una estrategia dirigida a fortalecer la oferta de servicios y la cobertura de los programas de fomento de la propiedad industrial.	2022 – 2024
SIC con apoyo del Ministerio de Comercio, Industria y Turismo, a través de iNNpulsa y la Dirección de inversión extranjera directa y servicios	Trabajar en el diseño y divulgación de una guía para el sector empresarial en materia de licenciamiento de la propiedad industrial, transferencia de tecnología y el uso de la información tecnológica que contienen los documentos de patentes.	2023 – 2025
Ministerio de Comercio, Industria y Turismo, Ministerio	Diseñar e implementar una estrategia que contribuya a la comercialización de derechos de propiedad intelectual, con	2022 – 2025

[66] Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%c3%b3micos/4062.pdf

Entidad	Acción	Tiempo de ejecución
de Cultura, el Ministerio de Ciencia, Tecnología e Innovación, la DNDA y la SIC	especial énfasis en los actores de la cadena de valores de las Industrias creativas.	
Ministerio De Ciencia, Tecnología e Innovación y SIC	Incrementar el uso de mecanismos para promover la explotación, comercialización y transferencia de tecnologías.	2022 - 2024
DAyC, la DNDA y el Ministerio de Cultura	Diseñar e implementar una estrategia para ampliar el alcance y la cobertura de programas de fomento de gestión y aprovechamiento de los derechos de autor y conexos.	2023 - 2026
La Agencia Nacional de Contratación Pública - Colombia Compra Eficiente, la SIC y la DNDA	Desarrollar y socializar una guía de buenas prácticas dirigida a entidades públicas, para orientar y precisar el alcance de su capacidad institucional en la negociación de los derechos de propiedad intelectual.	2022 y 2023
Ministerio de Defensa	Estructurar y socializar un inventario de los derechos de propiedad intelectual obtenidos a partir de los avances de investigación y desarrollo que se hayan causado desde la fuerza pública y/o empresas del Grupo Social y Empresarial para la Defensa - GSED.	2022 y 2024
DNP y Departamento administrativo de la presidencia de la república	Realizar un mapeo periódico y generar recomendaciones sobre los instrumentos de las entidades de orden nacional relacionadas con propiedad intelectual, derivadas de la aplicación de la metodología de articulación para la competitividad.	2022 - 2031

Fuente: DANE basado en el CONPES 4062

- Línea 11: generación de información en el sistema de PI para la toma de decisiones basada en evidencia.

Tabla 21. Acciones encaminadas a mejorar los sistemas de información para la PI

Entidad	Acción	Tiempo de ejecución
El DANE, la SIC, la DNDA y el ICA	Generar una caracterización de las actividades económicas que realizan los registros de propiedad intelectual según la muestra de la EDIT.	2022 - 2026

Entidad	Acción	Tiempo de ejecución
SIC	Crear y publicar un reporte que contenga la información consolidada, agregada y actualizada sobre las inscripciones de los derechos de propiedad intelectual que reposan en el Registro Público de la Propiedad Intelectual.	2022 y 2023
Ministerio de Ambiente y Desarrollo Sostenible	Diseñar e implementar una estrategia para la organización del modelo de datos del sector ambiente, a través del Sistema de Información Ambiental de Colombia - SIAC, que permite identificar los formatos como fuente de datos y uso, para orientar la gestión ambiental y periodicidad de la actualización.	2022 y 2026
Ministerio de Ambiente y Desarrollo Sostenible, el Instituto Humboldt y el Ministerio de Ciencia, Tecnología e Innovación	Actualizar el Sistema de Información sobre biodiversidad de Colombia - SiB para permitir la inclusión de información genética.	2022 y 2031
Ministerio de Ambiente y Desarrollo Sostenible, Corporación Colombiana de Investigación Agropecuario y el Instituto Humboldt	Diseñar e implementar una estrategia para el desarrollo de activos de propiedad intelectual a partir de la bioprospección de especímenes depositados en colecciones biológicas, para aquellos en los que sea posible.	2022 y 2026
DNP	Estructurar y socializar un inventario de propiedad intelectual cuya titularidad esté en las entidades del gobierno nacional, con el objetivo de fomentar la explotación de los bienes intangibles generados por el estado.	2024 y 2027

Fuente: DANE basado en el CONPES 4062

Finalmente, como parte de las recomendaciones, se solicita al Departamento Administrativo Nacional de Estadística, generar una caracterización de las actividades económicas que realizan registros de propiedad intelectual, según la muestra de la Encuesta de Desarrollo e Innovación Tecnológica.

También, se solicita al DNP, elaborar un estudio para identificar las fortalezas y debilidades del Sistema Nacional de Propiedad Intelectual; implementar instrumentos de planeación estratégica para realizar seguimiento a la comisión intersectorial de propiedad intelectual; diseñar y socializar

una estrategia de formación y capacitación sobre la valoración y comercialización de activos intangibles relacionados con la propiedad intelectual; realizar un mapeo periódico y generar recomendaciones sobre los instrumentos de las entidades de orden nacional relacionados con la propiedad intelectual, y diseñar un fondo de financiación de potencial innovación y tecnológica susceptible de protección por propiedad intelectual.

2.3.5 Dirección Nacional de Derechos de Autor

La Dirección Nacional de Derecho de Autor es un organismo del Estado Colombiano adscrito al Ministerio del Interior que se encarga del diseño, dirección, administración y ejecución de las políticas en materia de derecho de autor y derechos conexos. Dentro de los documentos publicados en su página web se encuentra el Manual de derecho de autor[67], que detalla aspectos conceptuales sobre propiedad intelectual y derechos de autor.

En particular, el Manual de derechos de autor indica que:

> "La expresión "propiedad intelectual" se utiliza en términos amplios para hacer referencia a todas las creaciones del ingenio humano, y se define como la disciplina jurídica que tiene por objeto la protección de bienes inmateriales, de naturaleza intelectual y de contenido creativo, así como de sus actividades conexas. . ." (Vega, 2010, p. 9)

De igual forma, menciona que:

> "El Derecho de Autor es una especie dentro de la institución de la propiedad intelectual, en virtud de la cual se otorga protección a las creaciones expresadas a través de los géneros literario o artístico, tiene por objeto las creaciones o manifestaciones del espíritu expresadas de manera que puedan ser percibidas, y nace con la obra sin que para ello se requiera formalidad alguna."
>
> "La propiedad Industrial es la otra rama en que se ha dividido tradicionalmente la propiedad intelectual, y se ocupa de la protección a las invenciones, modelos de utilidad, dibujos y

[67] Disponible en Vega Jaramillo, Alfredo. (2010). Manual de derechos de autor. Dirección Nacional de Derechos de Autor. Disponible en http://derechodeautor.gov.co:8080/documents/10181/331998/Cartilla+derecho+de+autor+%28Alfredo+Vega%29.pdf/e99b0ea4-5c06-4529-ae7a-152616083d40

> modelos industriales, marcas de fábrica, lemas y denominaciones comerciales, circuitos integrados, y en algunas clasificaciones se incluye la represión a la competencia desleal, si bien no se trata en este caso del reconocimiento de derechos exclusivos, sino de la sanción a los actos contrarios a los usos honrados en materia industrial y comercial." (p. 9)

El Manual también se refiere a aspectos relacionados con el autor de obras creadas bajo relación laboral. Frente a esto indica que:

> "En la obra realizada bajo relación laboral . . . la creación como acto personal libre y la forma de expresión como elemento propio del autor se atribuyen al autor asalariado y no al patrono. Ello es así, pues si el empleador fuera el creador de la obra, no contrataría al autor. Establecido lo anterior, procede considerar la titularidad de los derechos sobre la obra creada bajo relación laboral, u obra de autor asalariado." (p. 25)

Sobre las obras colectivas realizadas bajo relación laboral, el Manual es específico en mencionar que, según el artículo 92 de la ley 23 de 1982, el titular de los derechos sobre las obras colectivas creadas dentro de un contrato laboral o de arrendamiento de servicios, es el editor o persona jurídica o natural por cuya cuenta y riesgo se realizan. Es más, la relación laboral no le confiere los derechos morales al empleador, pues estos derechos son intransferibles. En este sentido, es recomendable que en el caso de relaciones laborales en cuyo desarrollo se incluya la obligación de crear obras, que en el respectivo contrato laboral se deje constancia sobre la cesión de los derechos patrimoniales al empleador (p. 26).

Por otro lado, en el numeral 9.2.2.1 del Manual se profundiza sobre el contrato de prestación de servicios y elaboración de obra. En este numeral se señala que este es un contrato está sujeto al artículo 183 de la Ley 23 de 1982, se lleva a cabo para realizar una obra sobre un tema específico. Por medio de este contrato se crea un bien intelectual y la titularidad de los derechos patrimoniales son del contratista. Sin embargo, se puede convenir que el derecho patrimonial del autor no se desplace completamente al contratante, sino que la titularidad, en todo o en parte, sea conservada por el autor.

Del mismo modo, el Manual en su numeral 9.4.1 sobre obras creadas por servidores públicos destaca que, en este caso, se presentan dos situaciones: (i) que la obra sea creada en cumplimiento de las obligaciones constitucionales y legales que le competen, o (ii) que sea creada por fuera del cumplimiento de tales obligaciones. Para el primer caso, el artículo 91 de la Ley 23 de 1992 dispone que la titularidad de los derechos radica en la cabeza de la entidad pública, y el servidor público conservará los derechos morales, con el compromiso de no ejercerlos de una manera incompatible con los derechos y obligaciones de la entidad pública. Mientras que, para el segundo caso, el servidor

público está legalmente habilitado para contratar con el Estado a transmisión de los derechos patrimoniales sobre su creación, y podrá hacerlo estableciendo las condiciones contractuales que considere convenientes.

2.3.6 Agencia Nacional de Contratación Pública

Durante el año 2021 la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, publicó la Guía de Propiedad Intelectual en la Contratación Pública, esta expone diferentes lineamentos, buenas prácticas, derechos asociados y obligaciones contractuales vinculadas al tratamiento, uso y manejo de activos de propiedad intelectual. De igual modo, la guía presenta un marco teórico y práctico sobre la propiedad intelectual en el marco de la gestión pública y la contratación estatal, así como un conjunto de pautas, orientaciones básicas y consideraciones sobre la titularidad de derechos. [68].

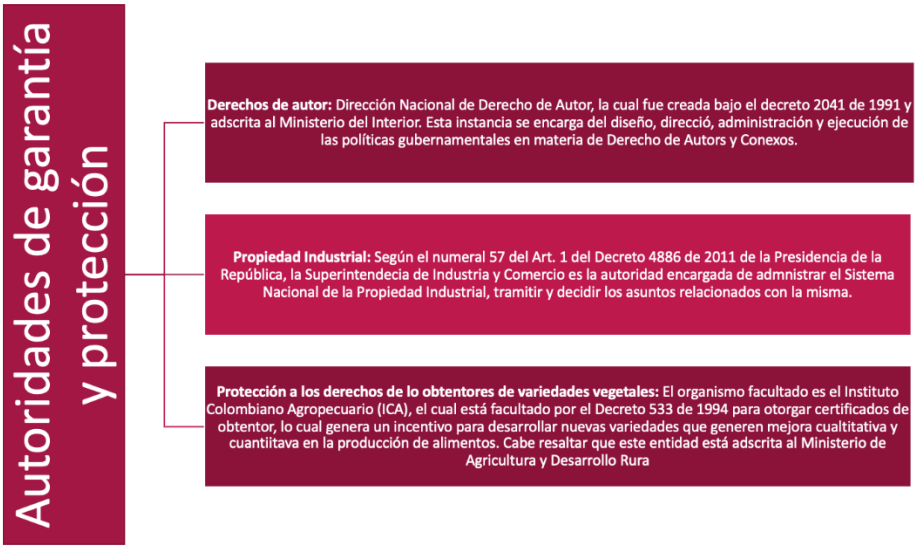
La Agencia Nacional de Contratación Pública elaboró esta guía en concordancia con sus facultades de elaborar, actualizar y difundir herramientas que faciliten la contratación pública, a partir de instrumentos que promueva la eficiencia, transparencia y competitividad. Asimismo, la Guía de Propiedad Intelectual en la Contratación Pública es un documento desarrollado en el marco de la Política Nacional de Propiedad Intelectual, su objetivo es servir como herramienta a funcionarios, contratistas y colaboradores de las entidades públicas en aquellos procesos relacionados con la gestión de activos de propiedad intelectual, sobre todo, en los escenarios enlazados a la contratación pública. Finalmente, esta guía hace la salvedad sobre la naturaleza del documento, el cual no ocasiona un carácter vinculante y aclara que cada una de las consideraciones contenida se hacen sin prejuicio a las competencias de otras autoridades.

Durante el desarrollo de la guía se presentan algunos antecedentes que sirvieron para la realización de la misma, uno de los más transcendentes es la Circular Conjunta 004 de 2006 de la Procuraduría General de la Nación, mediante la cual se impartió un conjunto de lineamientos para el cumplimiento de los derechos de autor y conexos[69], los cuales permitieron sensibilizar a los funcionarios de las entidades públicas sobre la importancia de la identificación y oportuna gestión de los activos de propiedad intelectual, a la vez que permitió generar recomendaciones para evitar el incumplimiento de los derechos de terceros. Hoy día, más de quince años después, la circular sigue vigente y es una de las estrategias que permiten garantizar los derechos de autor sobre la divulgación de productos de investigación, desarrollo e innovación.

[68] Disponible en https://www.colombiacompra.gov.co/sites/cce_public/files/cce_documents/cce-eicp-gi-15_guia_de_propiedad_intelectual_en_la_contratacion_publica-ancp-cce.pdf
[69] Disponible en https://www.procuraduria.gov.co/portal/media/file/modulo_calidad//599_circularconjunta004-06.pdf

El marco normativo que la guía presenta se basa en tres referentes, en primer lugar, el artículo 61 de la Constitución Política de Colombia, el cual establece que el Estado protegerá la propiedad intelectual. En segundo lugar, la Declaración Universidad de Derechos, la cual en su artículo 27.2 dicta que *"Toda persona tiene derecho a la protección de intereses morales y materiales que le correspondan por producciones científicas, literarias o artísticas de que sea autora"*[70]. Y, finalmente, toma como sustento, la adhesión de Colombia a múltiples instrumentos internacionales sobre Derechos de Autor, Propiedad Industrial y Protección de los derechos del obtentor de Variedades Vegetales, los cuales han sido incorporados al derecho nacional. La Agencia Nacional de Contratación Pública - ANCP también hace mención sobre las autoridades que velan por la protección y garantía de los derechos de autor, propiedad industrial y protección da los derechos de los obtentores de variedades vegetales. Ver Ilustración 21.

Ilustración 21. Autoridades que velan por la protección y garantía de los derechos de autor



Fuente: Elaborado por el DANE con información de la ANCP

En cuanto a la titularidad de Derechos Patrimoniales sobre los productos creados por empleados o funcionarios públicos, la guía menciona que es sumamente importante distinguir entre un producto creado por un empleado público en cumplimiento de las funciones de su cargo y un producto generado por el funcionario como parte de una actividad no vinculada a sus funciones. En el caso de la primera situación, los derechos patrimoniales son de la Entidad Estatal a la cual está vinculada

[70] Disponible en: https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf

el empleado, esto gracias al artículo 91 de la ley 23 de 1982[71], el cual otorga derecho exclusivo y excluyente a la Entidad sobre la obra. Con respecto a la segunda situación, los derechos patrimoniales son del autor, no hay transferencia alguna a la entidad a la cual se encuentra vinculado.

En el caso de los productos producidos por individuos que gozan de un contrato por prestación de servicios o de un contrato de trabajo por el producto, aplica el artículo 20 de la Ley 23 de 1982, el cual dispone la transferencia de los derechos a quien encargo la obra o quien sirve como contratante, es decir la entidad estatal. Finalmente, en aquellas situaciones en las que un aprendiz o practicante se ve involucrado en la producción de una obra, la Entidad podrá obtener los Derechos Patrimoniales a través de un acuerdo de cesión y no bastará con el contrato de aprendizaje.

Finalmente, la guía permite identificar a las autoridades que velan por la garantía y protección de los derechos de autor y propiedad intelectual, de igual manera, expone los diferentes mecanismos y herramientas internacionales a los que Colombia se encuentra vinculado para la defensa de derechos de autor sobre productos de investigación desarrollo e innovación. Y, a la vez, esta expone puntualmente las normativas vigentes sobre la cesión y tratamiento de los derechos patrimoniales y morales, y, la manera en que estos son vinculados en los contratos laborales, de prestación de servicios, por producto y de aprendizaje.

2.3.7 Ministerio de Defensa

El Ministerio de Defensa Nacional de Colombia posee la Política de propiedad intelectual y transferencia de tecnología[72], en la cual se establecen los lineamientos generales que deben seguir las instituciones como las Fuerzas Militares, Policía Nacional y diversas entidades adscritas al Ministerio. El alcance de esta política es hacia los miembros de la Fuerza Pública, Servidores Públicos del Ministerio y aquellas personas receptoras o transmisoras de tecnología en relación con el ministerio. Se resalta que para la implementación y aplicación de la política se deberán tener en cuenta las recomendaciones y comentarios que se ubican en la Guía de Propiedad Intelectual y Transferencia de Tecnología[73], la cual establece las secciones planteadas en la tabla Ilustración 21.

Tabla 22. Contenido Guía de Propiedad Intelectual y Transferencia de Tecnología

Propiedad Intelectual

[71] Ley 23 de 1982. *"Artículo 91: Los derechos de autor sobre las obras creadas por empleados o funcionarios públicos, en cumplimiento de las obligaciones constitucionales y legales de su cargo, serán de propiedad de la entidad pública correspondiente".*

[72] Disponible en https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/ciencia_y_tech/I%2BD%2Bi/DIRECTIVA%20019%2030%20SEP%202008%20Politica%20de%20Propiedad%20Intelectual.pdf

[73] Disponible en https://sena.edu.co/es-co/formacion/sennova/Propiedad%20Intelectual.pdf

• Principios generales • Titulares y derechos de autor • Tipos de Obra • Cosas que protege el Derecho de Autor • Obras originarias y obras derivadas • Derecho moral y derecho patrimonial • Derecho de transformación • Plazos de protección • Limitaciones y excepciones al Derecho de Autor • Obras de dominio público • Transmisión de los derechos patrimoniales • Autor asalariado • Programas de computador • Software Libre
Derechos conexos
• Artistas intérpretes o ejecutantes • Fonogramas • Grabaciones audiovisuales • Protección de los derechos de los autores, intérpretes o ejecutantes, Productores fonogramas y organismos de radio fusión • Registro de obras • Asociaciones de autores o entidades de gestión • Acuerdos internacionales en materia de Derechos de Autor
Normatividad Colombiana sobre derechos de autor
• Leyes • Decretos • Resoluciones
Propiedad Industrial
• Patentes • Diseños industriales • Marcas • Lema comercial • Acciones legales por infracción de derechos de la propiedad industrial • Competencia desleal en relación con la propiedad industrial • Transferencia de tecnología • Convenios internacionales en relación con la propiedad industrial • Legislación Colombiana relativa a la propiedad industrial • Fuentes de información sobre propiedad intelectual • Caso práctico sobre propiedad intelectual y transferencia de tecnología

En el marco de la política se establecen los principios para la gestión de los activos intangibles del ministerio, donde se ahonda en como los activos intangibles del ministerio son fundamentales para cumplir con los objetivos de Seguridad y Defensa del Estado, de igual manera se nombra la coordinación y estructuración de las actividades relacionadas con la propiedad intelectual y transferencia de tecnología; y por último en esta sección hablan sobre la comercialización de los activos intangibles del ministerio.

Adicionalmente, se explica la gestión y protección de los activos intangibles del ministerio, donde se explica el método de identificación de los Activos Intangibles existentes y nuevos. De igual manera, se describe la información clasificada donde se plantea la clasificación de este tipo de información y el manejo adecuado por el que debe pasar este tipo de información y la exploración de los acuerdos de confidencialidad. La Política también describe la titularidad de la propiedad intelectual del ministerio, contratos sobre propiedad intelectual y de transferencia de tecnología; y por último el seguimiento y la evaluación de los procesos de transferencia de tecnología.

Comisión Intersectorial de Propiedad Intelectual.

El Departamento Nacional de Planeación bajo el decreto Número 1650 de 2020[74] modificó el decreto 1162 de 2010, en el cual se creó el Sistema Administrativo Nacional de Propiedad Intelectual, la cual tiene por objeto la coordinación de las entidades estatales y de los particulares para lograr un nivel adecuado de protección, uso y promoción de los derechos de propiedad intelectual. Adicionalmente, se creó la Comisión Intersectorial de Propiedad Intelectual - CIPI, para la coordinación y orientación superior de las políticas comunes en materia de propiedad intelectual y de su ejecución. En una de las sesiones ordinarias llevadas a cabo en 2019, el Ministerio de Defensa solicitó ser miembro de la CIPI, ya que el ministerio presentaba diferentes avances, los cuales han venido aportando a la innovación del país, registrando 34 patentes, 232 marcas, 7 diseños industriales y 2 esquemas de trazado de circuitos integrados. Finalmente, mediante una decisión unánime se aprobó la inclusión del Ministerio de Defensa como miembro con voz y voto.

Política de propiedad intelectual que incentiva la creación y la innovación

En noviembre de 2021, el Gobierno aprobó el CONPES 4062, de "Política Nacional de Propiedad Intelectual", la cual tiene un plan de acción de 10 años (2022-2031) con la participación de 28 entidades (26 son de la Rama Ejecutiva y 2 de la Rama Judicial). En marzo de 2022, a raíz de conocer los beneficios del CONPES 4062, se llevó a cabo un evento de socialización de la política, donde se

[74] Disponible en https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%201650%20DEL%2014%20DE%20DICIEMBRE%20DE%202020.pdf

establecía un espacio para que ciudadanos, inventores, y diferentes actores del ecosistema de la propiedad intelectual se familiaricen con lo contenido en la política y así mismo, poder analizar los diferentes retos para el futuro de la propiedad Intelectual[75].

2.4 Conclusiones

La revisión de referentes internacionales que se realizó acerca de buenas prácticas para garantizar la propiedad intelectual sobre la divulgación de productos de investigación, desarrollo e innovación permitió llegar a las siguientes conclusiones:

Las entidades públicas han desarrollado múltiples guías para la propiedad intelectual, entre ellas se tienen: i) la Guía de Propiedad Intelectual[76] desarrollada por Minciencias en el marco del Programa Colombia Científica, la cual tiene la finalidad de proporcionar una guía orientadora en relación con el uso y asignación de la propiedad intelectual, ii) la Guía de Propiedad Intelectual en la Contratación Pública desarrollada por la Agencia Nacional de Contratación Pública, la cual presenta un marco teórico y práctico sobre la propiedad intelectual en el marco de la gestión pública y la contratación estatal, así como un conjunto de pautas, orientaciones básicas y consideraciones sobre la titularidad de derechos, iii) la Guía de política de protección sobre la propiedad intelectual: eje de los derechos de autor, elaborada por el MEN, la cual tiene el objetivo de proteger los derechos de autor y conexos como una dimensión de la propiedad intelectual en relación con todas las obras de tipo artístico, literario y científico, que sean originales, inéditas o derivadas del desarrollo, adquisición, gestión, utilización y protección de propiedad intelectual generada, adquirida o utilizada por el MEN y iv) el Manual de derecho de autor[77] desarrollada por la unidad administrativa especial del Ministerio del Interior y de Justicia.

El Centro Colombiano del Derecho de Autor reconoce el artículo 91 de la Ley 23 de 1982, la Decisión Andina 351 de 1993, la adhesión al convenio de Berna para la protección de obras literarias y artísticas (Ley 33 de 1987) y al tratado de la OMPI sobre derechos de autor (Ley 565 de 2000) que actúan sobre los atributos de orden moral y patrimonial que les corresponden a los autores de obras literarias o artísticas.

Para el caso de servidores públicos como titulares de los derechos de autor, el artículo 91 de la Ley 23 de 1982 señala que las obras cuya autoría pertenezca a servidores públicos en las condiciones establecidas tendrán por autor a la persona natural que las creó y esta conservará los derechos

[75] Disponible en https://www.dnp.gov.co/Paginas/Gobierno-socializo-politica-de-Propiedad-Intelectual-que-incentiva-la-creacion-y-la-innovacion.aspx

76 Disponible en https://minciencias.gov.co/sites/default/files/upload/convocatoria/anexo8-guia-propiedad-intelectual.pdf

[77] Disponible en http://derechodeautor.gov.co:8080/documents/10181/331998/Cartilla+derecho+de+autor+%28Alfredo+Vega%29.pdf/e99b0ea4-5c06-4529-ae7a-152616083d40

morales de su obra, con el compromiso de no ejercerlos de manera incompatible con los derechos y obligaciones de la entidad pública; pero la entidad estatal será la titular de los derechos patrimoniales, los cuales serán cedidos desde el momento de creación de la obra, dándole la potestad de explotar libremente las obras y autorizar su uso por parte de terceros.

No obstante, los servidores públicos que realicen obras susceptibles a propiedad intelectual, pero que no sean realizadas en función de la actividad propia de su cargo, se consideran de propiedad moral y patrimonial del servidor, y, por lo tanto, las obras tendrán toda la protección legal que el régimen jurídico le aporte en esta materia.

Asimismo, con respecto a la capacidad del servidor público para negociar como autor de una obra realizada por fuera de sus funciones legales y constitucionales con las entidades públicas, es necesario aclarar la vigencia del artículo 1 de la ley 44 de 1993 en relación con el artículo 8 de la Ley 80 de 1993 (ya que esta última norma inhabilita a los servidores públicos para contratar con las entidades estatales, sin embargo, no menciona expresamente este caso):

> *"Artículo 1 de la ley 44 de 1993: los empleados y funcionarios públicos que sean autores de obras protegidas por el Derecho de Autor podrán disponer contractualmente de ellas con cualquiera entidad de derecho público"*.

La anterior ley introduce una posibilidad específica para que los servidores públicos autores de obras puedan celebrar contratos sobre ellas con entidades públicas, por lo que en este sentido los servidores públicos creadores de obras literarias o artísticas que no estén dentro del marco de las obligaciones constitucionales o legales de su cargo pueden conservar la titularidad de la propiedad patrimonial sobre sus creaciones[78].

2.5 Recomendaciones para el DANE

Minciencias y MEN recomiendan que, para los procesos de contratación o adquisición, desarrollo de proyectos o convenios de investigación, cooperación u otros acuerdos con contratistas, consultores, proveedores, investigadores, universidades, organismos internacionales o personas de naturaleza pública o privada, se deben tener en cuenta los siguientes aspectos:

78 Disponible en http://www.cecolda.org.co/index.php/derecho-de-autor/normas-y-jurisprudencia/direccion-nacional-de-derecho-de-autor/98-circular-nro-7-el-servidor-publico-como-titular-de-derecho-de-autor

- Definir desde el proceso de contratación, convenios o acuerdos y aspectos de titularidad de propiedad intelectual (alcance, uso de terceros, etc.), evitando así posibles controversias.
- Definir los activos de propiedad intelectual producto del objeto contractual y los modos previstos en la ley para que surjan derechos sobre estos, de acuerdo con su categoría.
- Adoptar la decisión de reservarse la titularidad de la propiedad intelectual, el derecho de registrar la propiedad intelectual a nombre propio o el licenciamiento de derechos que se desarrolle o adquiera durante la ejecución.

Asimismo, se sugiere el establecimiento de acuerdos expresos sobre titularidad y cesión de los derechos de propiedad intelectual, los cuales generalmente se estructuran con base a los aspectos objetivos (objeto y título de protección) y elementos subjetivos (autores y titulares) asociados a la creación intelectual, donde:

- Las creaciones ocasionales, es decir, en el caso del creador independiente que expresa su ingenio en su taller o laboratorio personal, sin utilizar medios o recursos suministrados por un empleador o contratante (las cuales no se encuentra en cumplimiento de un contrato laboral o de prestación de servicios), el creador es el titular de los derechos patrimoniales y morales de la obra.

  Las creaciones en el ámbito laboral o de servicio, son aquellas realizadas en cumplimiento de un contrato (escrito) de trabajo o de prestación de servicios, o que son realizadas haciendo uso de los recursos del empleador, en este caso la titularidad de los derechos patrimoniales es cedida al empleador, por la presunción legal de sesión (artículo 20 de la Ley 23 de 1982) o por tratarse de una obra por encargo. Sin embargo, los derechos morales de la obra pertenecerán al autor de esta, pues estos derechos son intransferibles.

  No obstante, según el Manual de derechos de autor, en el caso de las obras elaboradas bajo el cumplimiento de un contrato de prestación de servicios, existe la posibilidad de convenir en esta clase de contratos que el derecho patrimonial del autor no se desplace completamente hacia el contratante, sino que el autor conserve la titularidad de tal derecho, en todo o en parte.

- Las creaciones en conjunto corresponden a aquellas realizadas por dos o más personas naturales o cuando la titularidad la comparten dos o más personas jurídicas, la titularidad se define en virtud de la autonomía de la voluntad, y ante la ausencia de esta definición se entiende que hay co-titularidad, sin embargo, si la creación conjunta surge como resultado del cumplimiento de un contrato laboral o de prestación de servicios, le serán aplicables las reglas para este tipo de creaciones. En este sentido, es recomendable que en el caso de relaciones laborales en cuyo desarrollo se incluya la obligación de crear obras, en el

respectivo contrato laboral se deje constancia sobre la cesión de los derechos patrimoniales al empleador, como lo recomienda el Manual de derechos de Autor.

- En aquellas situaciones en las que un aprendiz o practicante se ve involucrado en la producción de una obra, la Entidad podrá obtener los Derechos Patrimoniales a través de un acuerdo de cesión y no bastará con el contrato de aprendizaje.

El equipo jurídico del DANE debe explorar la amplia normativa y manuales vigentes desarrollados por entidades públicas colombianas como MinTIC, MEN, DNDA y la Agencia Nacional de Contratación Pública, sobre temas relacionados con los derechos de autor y propiedad intelectual, así como validar las cláusulas en los contratos, convenios/acuerdos y manuales de funciones del personal así como de aquellos relacionados con la entidad en la elaboración de productos de investigación, garantizando que sean suficientes para cubrir los diferentes aspectos de propiedad intelectual, en el marco de las buenas prácticas y los derechos legales, morales y técnicos.

Se resalta que la presente revisión solicitada por el GIT PAD es de interés general para todas las áreas del DANE, por lo que es necesario generar una agenda de trabajo clara que permita abordar y definir buenas prácticas y principios sobre la propiedad intelectual y los derechos de autor desde el punto de vista de la producción estadística.

3.

3 Reseña del documento Directrices para la Elaboración de una estrategia de Comunicación.

3.1 Introducción

Las estadísticas son vitales para el desarrollo de políticas que permitan alcanzar los Objetivos de Desarrollo – ODS, para la toma de decisiones y para obligar a los gobiernos a rendir cuentas sobre estas, por esta la razón la comunicación de estadísticas es esencial para que el público conozca la

imparcialidad e independencia de los Institutos Nacionales de Estadística - INE, generando así una mayor aceptación y uso de estas por su parte.

Dado lo anterior, contar con una estrategia de comunicación propone una visión estratégica y una hoja de ruta a largo plazo, lo que puede ayudar a los INE a planificar sus actividades y programas para incentivar la participación de las partes interesadas de forma eficaz y dinámica como para alcanzar sus objetivos.

La OECD desarrolló el documento *Directrices para la Elaboración de una Estrategia de Comunicación*[79] con el objetivo de proporcionar una orientación estratégica y determinar los pasos y recursos prácticos que requieren los INE para construir una estrategia de comunicación integral, por medio de un conglomerado de instrucciones, consejos y recursos, los cuales deben adaptarse a las circunstancias y contexto particular de cada INE. Este documento sirve de complemento a las Directrices para la integración de la Comunicación en las Estrategias Nacionales para el Desarrollo Estadístico – ENDE[80].

3.2 Reseña:

PASO 1. Definir los parámetros, determinando el alcance de la actividad como el proceso que se seguirá a fin de desarrollar una estrategia de comunicación eficaz, al establecer este paso se sentaran las bases poder continuar con la elaboración de la estrategia de comunicación.

3.2.1 Formación del equipo de trabajo

[79] Disponible en https://paris21.org/sites/default/files/2022-06/OECD%20Communications%20Strategy%20Guide%20-%20V8_ES_web.pdf
[80] Disponible en https://www.paris21.org/sites/default/files/p21implementguide-es.pdf

El equipo es el responsable de que el proyecto cumpla su objetivo y su primera tarea es evaluar el estado actual de las comunicaciones en la organización, a partir de esta revisión generar un plan preliminar para aplicar la estrategia. Esta será la hoja de ruta que se ajusta durante el proceso de elaboración de la estrategia. Se debe determinar el coordinador principal, quien dirigirá el proceso; se recomienda que la dependencia de comunicaciones dirija el proceso e involucrar personal transversal de la organización, que cuenten con experiencia, antigüedad y tengan una labor programática.

Para formar el equipo de trabajo se debe (1) considerar el tamaño del equipo de redacción de acuerdo con las dimensiones de la organización, (2) escoger el coordinador principal que dirige el proceso, (3) establecer como se involucran los miembros del equipo, (4) que tiempo se va a dedicar al desarrollo del proceso, y (5) si esta labor va a estar apoyada por el supervisor de cada miembro del equipo y contará como parte de sus horas de trabajo.

3.2.2 Delimitación interna del alcance

Posterior a establecer el equipo de trabajo, se convocan a un taller en el cual se determina el alcance y marco de la estrategia, en este punto se debate sobre por qué se elabora la estrategia, los asuntos más importantes, el objetivo de la estrategia, qué se espera solucionar, a quién se dirige la estrategia, se identifican las oportunidades y esferas que generan problemas de comunicación interna o externa, y como se ha trabajado las estrategias anteriores. Esto da pie para evaluar las estrategias existentes, dado que servirán como punto de referencia durante el análisis y redacción de la estrategia.

Adicionalmente, se establece si la estrategia va a ser publicada, a quien va dirigida, que considera el equipo importante para incorporar en la estrategia y si se trabaja un plan integrado o se dividen según las temáticas (comunicaciones internas, comunicaciones externas, labor de promoción). Esta estrategia se debe armonizarse con la Estrategia Nacional de Desarrollo Estadístico – ENDE y puede organizarse incorporando productos específicos en la ENDE que cuenten con comunicación, evaluaciones de la comunicación en el marco de seguimiento y evaluación.

Durante la delimitación se considera necesario solicitar la opinión de varias personas, con el fin de garantizar entendimiento de los desafíos y oportunidades que tienen las comunicaciones actuales, estos resultados se reflejan e incluyen en el análisis de mercado.

3.2.3 Confección de la hoja de ruta

Como paso final para determinar el alcance de la estrategia, deben definirse los plazos en un calendario (hoja de ruta) para la estrategia de comunicación, con el objetivo de delimitar cada una de las fases de la elaboración de la estrategia, así como las actividades principales en cada una de ellas.

El calendario debe contener el departamento o asociado encargado de la ejecución de cada actividad y el método que se empleará (taller, investigación documental, misión, acto público, etc.). Asimismo, puede hacerse uso de un código de colores que permita señalar el nivel de progreso de las actividades y el proceso de gobernanza (si el personal directivo superior tiene que aprobar el trabajo realizado para pasar a la siguiente fase), finalmente, debe añadirse la hoja de ruta al informe del taller, para obtener así una hoja de ruta estratégica y táctica para la elaboración de la estrategia.

Paso 2. Realizar auditorías, investigaciones y consultas con las partes externas interesadas, profundizando en las impresiones que surjan durante el intercambio inicial de ideas y desarrollando pruebas concretas que las respalden, modifiquen o refuten, para que en el paso 3 ayude al equipo a tomar decisiones estratégicas y tácticas que se reflejarán en la estrategia en diferentes aspectos que contribuirán a justificar lo que se incluye o no, preservando solo aquello que esté directamente relacionado con los objetivos definidos.

3.2.4 Análisis de mercado

Para realizar una buena estrategia es necesario conocer la audiencia a la cual va dirigida, los recursos, canales y mensajes de los que dispone el INE para adaptarse a los intereses y necesidades de esta audiencia, para garantizar el máximo número de destinatarios posible. Al mismo tiempo, se manejarán investigaciones que permitan conocer el entorno en el que se comunican las estadísticas nacionales. Para realizar un análisis de mercado minucioso debe profundizarse en dos esferas:

1) Análisis de competidores y homólogos: aunque solo haya un INE en el país, pueden existir otras entidades que elaboren estadísticas, por lo que es necesario realizar un mapeo de los potenciales competidores por medio de la investigación de sus sitios web, medios sociales,

entre otros, que le permita determinar quién es su audiencia, los problemas que abordan, la comunicación con su audiencia y en qué se diferencia del INE.

2) Investigación y segmentación del público seleccionado: después de analizar el resto de los competidores del país, se debe intentar comprender al máximo el público seleccionado, pues de lo contrario se desaprovecharía tiempo y recursos elaborando comunicaciones demasiado genéricas como para tener repercusión, para ello debe elaborarse: i) una lista de los grupos de población objetivo, ii) las motivaciones principales de cada grupo para participar en las estadísticas y un mensaje que se considere convincente para estos grupos, iii) clasificar la audiencia por grupos meta según el orden de importancia y iv) si es posible realizar entrevistas detalladas con miembros de diferentes grupos a fin de recopilar más datos de interés.

3.2.5 Auditorías

Las auditorías documentales son esenciales para evaluar la calidad de las comunicaciones actuales de la organización y los recursos que esta tiene a su disposición, además, contribuirá a identificar los aspectos que funcionan bien y aquellos en los que se debe hacer hincapié. El personal interno de la organización realizará las siguientes auditorías documentales:

Auditoría de marca

La marca es el conjunto de diseños, símbolos y demás características que distinguen a cada oficina nacional de estadística, tener una, implica que se debe reconocer la autoría de todas las comunicaciones de la oficina, en términos de color, lenguaje, mensaje, estilo y fuente que se utilice, pues todas estas características deben ser coherentes y acordes.

Será necesario revisar los materiales de comunicación existentes de la organización, como cartas, anuncios de prensa, anuncios de contratación, boletines de prensa, programas, agendas, folletos, presentaciones, pancartas, materiales promocionales o informes y revisar si:

- Mantienen todos los documentos el mismo estilo
- Usan las mismas fuentes
- Emplean un lenguaje similar
- Utilizan el logotipo de la entidad de forma coherente
- Además, si una persona ajena a la organización al ver el material por primera vez, identificaría en 5 segundos que el documento pertenece dicha organización. En caso de no ser identificada, se debe platear incluir en la estrategia de comunicación unas directrices de marca que establezcan normas claras sobre la apariencia y el contenido de las comunicaciones de la organización y el tipo de lenguaje que debe emplear.

Auditoría de medios de comunicación

Es el proceso de revisión de la representación de una oficina nacional de estadística concreta (y de las estadísticas nacionales de forma general) en prensa escrita, noticias de televisión, blogs y otros canales de comunicación en masa. Se deberá comprobar en la auditoría dónde y cómo se está representando a la entidad y si existen oportunidades para obtener mayor cobertura mediática.

Auditoría de medios sociales

Se debe hacer una auditoría minuciosa de la presencia en línea de la organización, en este contexto, se puede realizar una auditoría de la comercialización digital con el fin de analizar datos de diferentes fuentes y posteriormente usarlos para orientar la estrategia y la toma de decisiones. Al iniciar con una auditoría del sitio web de la organización, se realiza un análisis profundo del tráfico web, las interacciones, la visibilidad en búsqueda, la experiencia del usuario, etc. Una auditoría detallada ofrecerá un mayor conocimiento sobre cómo y con qué frecuencia se consulta el sitio web y qué medidas tomar para fortalecer ambos parámetros, en este punto se puede utilizar Google Analytics para conocer el rendimiento del sitio web.

Hoja de trabajo de habilidades y capacidades humanas: Tras la auditoría del sitio web, se debe realizar una auditoría de los medios sociales en el marco de la auditoría digital, es necesaria para examinar las plataformas de medios sociales que generan buenos resultados, las que no lo están haciendo y determinar las medidas que se puedan adoptar para mejorar su uso.

La plantilla de la auditoría de medios sociales ayuda a facilitar el proceso, primero se deben listar todos los medios sociales que utiliza la organización, después habrá que añadir i) la información de perfil, nombre y url, ii) la frecuencia de la publicación, iii) las interacciones entre organización y usuario por medio de comentarios, respuestas, etc. iv) el número de clics por publicación, v) el alcance de Facebook o el número de seguidores de Twitter, etc.

Al finalizar el ejercicio, se formularán recomendaciones sobre qué medios sociales conservar y cuáles abandonar, en función de la rentabilidad del tiempo invertido en mantener la plataforma y la identificación para llegar al público seleccionado.

Auditoría de habilidades y capacidades humanas

Se debe examinar las habilidades y los recursos humanos disponibles dentro de la organización que puedan contribuir a la aplicación de la estrategia. El objetivo de esta auditoría es reconocer las fortalezas e identificar las carencias, lo que ayudará a fundamentar la contratación del personal a tiempo completo o parcial, o subcontratar proveedores de servicios locales para determinadas funciones. La primera parte de la auditoría es un intercambio de ideas entre los miembros del equipo de redacción, señalando las carencias de capacidad y los recursos que deben obtenerse con el fin de aprovechar la capacidad existente en la organización.

Hoja de trabajo de habilidades y capacidades humanas: Es posible que esta información se encuentre disponible, ya que suele formar parte de las funciones del departamento de recursos humanos, de ser así, solo se hace necesario extraer hallazgos relevantes para las comunicaciones. El éxito de la estrategia depende de la contratación del personal necesario, la adquisición de habilidades determinadas y la disponibilidad de recursos, plataformas o programas informáticos.

Paso 3. Se realizarán análisis y se tomarán decisiones que determinarán las prioridades de la estrategia. A partir de entonces, el equipo deberá definir qué actividades llevar a cabo, para quién, por qué y de qué manera estas van a contribuir a alcanzar los objetivos a largo plazo. Si la estrategia se desarrolla de forma correcta, se procederá al paso de redacción, donde se documentarán todos los hallazgos y se elaborará con ellos un discurso coherente.
A partir de los resultados obtenidos de la delimitación del alcance de la estrategia, la investigación, las auditorías, las entrevistas y los grupos focales, se sintetizará la esencia de los hallazgos y se comenzará a tomar decisiones estratégicas. Se recomienda que este paso se lleve a cabo en un taller con un día de duración.

3.3.1 Revisión de los materiales existentes

Para inaugurar el primer taller, el equipo de redacción tendrá que examinar los resultados clave de todas las actividades realizadas hasta el momento, es decir:

- Ejercicios de delimitación de alcance de la estrategia
- Investigación y auditorías
- La hoja de ruta de la estrategia
- Estrategia básica.

El equipo de redacción se puede dividir en cuatro grupos, para extraer los principales aportes de cada uno de los resultados de las actividades mencionadas.

3.3.2 Análisis DAFO

El análisis DAFO permite comprender las necesidades estratégicas de la organización, así como sus fortalezas, debilidades, oportunidades o amenazas. Los resultados del DAFO se utilizarán para elaborar el análisis de la situación de la estrategia de comunicación.

Esta actividad se divide de forma equitativa para abordar los 4 elementos del análisis DAFO y se incluye una sesión adicional para concluir sobre cómo aprovechar las oportunidades y fortalezas identificadas, además de disminuir los efectos de las debilidades y amenazas. Se sugiere que esta actividad tenga el siguiente orden: (i) fortalezas, (ii) debilidades, (iii) oportunidades, (iv) amenazas, y él (v) análisis DAFO.

El efecto directo de esta actividad ayudará a fundamentar el análisis de la situación y la sección de riesgos y supuestos de la estrategia final.

3.3.3 Intercambio de ideas sobre los objetivos de la estrategia

La lista de objetivos se elaborará a partir de las valoraciones de los grupos focales internos, las auditorias y las entrevistas con los interesados. Los objetivos de la comunicación deben estar estrechamente ligados a los objetivos institucionales de la oficina nacional de estadística, y han de ser concretos y medibles. También deben estar en consonancia con la ENDE y una vez alcanzados deberán ser remplazados por objetivos nuevos.

Frente a la redacción de los objetivos se sugiere que:

- Sean sencillos, fáciles de recordar y comprensibles
- Emplear una frase por objetivo
- Utilizar la siguiente estructura "acción + detalles + fecha de entrega"
- Comenzar por un verbo

Sobre el marco lógico basado en los resultados se priorizarán los objetivos y se vincularán a los efectos directos e indicadores de desempeño.

3.3.4 Riesgos: Evaluación y respuesta

Dentro del informe de síntesis, en la sección de "Evaluación de los riesgos" se estipula una metodología para la identificación de las posibles amenazas que afectan a la oficina nacional de estadística, la cual se compone de la identificación, definir las consecuencias, definir los agentes que están en riesgo. Paralelamente, se dispone de una hoja de trabajo para la realización de la evaluación de riesgos, donde se evalúan los niveles de probabilidad, las posibles consecuencias y la posibilidad de identificar posibles medidas de control para cada riesgo identificado. Los resultados de esta actividad será el fundamento para el análisis de la sección de riesgos y los supuestos de la estrategia final.

3.3.5 Identificación de canales y mensajes

En la sección de "Identificación de canales y mensajes" se comienza por la actividad que se desarrolla con el objetivo de evaluar los canales de comunicación, tanto internos como externos, y posteriormente plantear unos nuevos canales potenciales que puedan llegar a ser más eficaces dependiendo de las diferentes necesidades de comunicación. Algunos ejemplos de los canales comunes de comunicación interna están: correos electrónicos, reuniones llamadas, entrevista en personas, memorandos, etc. y respecto a los ejemplos de canales externos se encuentran los comunicados de prensa, los sitios web, medios sociales, boletines, etc.

Respecto a los mensajes, se hace énfasis en que es necesario que a la hora de comunicarse se adopten mensajes clave que exprese lo que hace, para quien lo hace y con que propósito lo hace. Estos mensajes deben estar en línea con la imagen que desde la organización se quiere proyectar y así, poder resaltar el valor único de la organización en el panorama general del sistema estadístico nacional. Algunas de las recomendaciones es que sean mensajes claros, concisos, memorables, convincentes, tener voluntad educativa y con una intención de llamado a la acción. Por otro lado, es importante resaltar la importancia de la necesidad de que los mensajes clave lleguen a toda la organización y así, asegurarse de un mensaje coherente mientras existe armonía del mensaje entre todos los miembros de la organización.

3.3.6 Consolidación del análisis de la situación

Para la consolidación del análisis de la situación es fundamental tener presente el proceso de investigación realizado en el pasó 2, así como el enfoque estratégico que se logra concertar a lo largo del paso 3. Durante la consolidación del análisis es necesario tener presente los asuntos más

relevantes que la estrategia de comunicación atenderá, a la vez que, se enmarcan y profundizan cada una de las oportunidades. De igual modo, resulta fundamental mencionar el conjunto de acciones que representan los obstáculos, desafíos y recursos de la estrategia, para que así se pueda realizar un análisis completo sobre la estrategia.

Una vez comprendidos los obstáculos, desafíos y recursos, el análisis debe centrar sus esfuerzos en la hoja de trabajo, de manera tal que se puedan identificar los riesgos y de manera proactiva, proponer posibles soluciones, reconociendo los factores que inciden en estos y las posibles afectaciones que puedan representar para la estrategia. Al finalizar la consolidación de la situación, los talleres y actividades se debe preparar una presentación dirigida al personal directivo que contenga los hallazgos más significativos e invite a los receptores a cuestionar los planteamientos, expresar posibles oportunidades de mejora, lograr un consenso de aprobación, y, finalmente establecer aportes para el siguiente paso, la redacción de la estrategia.

Paso 4. Este paso consiste en la redacción de la estrategia, el cual resulta ser el cúmulo de las investigaciones, entradas de datos y talleres. Resulta sumamente importante, proponer y diseñar un calendario editorial, el cual permita hacer un seguimiento a los avances de la redacción de la estrategia.

3.4.1 Plan de trabajo e implementación

El inicio del 4.º paso se sintetiza en el plan de trabajo e implementación, el cual consiste en un esquema donde se señalen y depositen cada una de las de actividad de comunicación que resultan primordiales para el cumplimiento de cada uno de los objetivos de la estrategia. En primer lugar, se deben tomar los objetivos definidos en el "intercambio de ideas de objetivos de la estrategia", cada uno los objetivos identificados tendrán que ser vinculados con las actividades relativas, sin embargo, debe tenerse en cuenta el nivel de posibilidad de alcance. Posteriormente, se deben describir las actividades y los canales de comunicación relacionados, así como el público al que se dirige, el valor estratégico de la actividad, el costo y los costos de la actividad.

En virtud de complementar el plan de trabajo se deben establecer plazos de cumplimiento, así como las etapas necesarias que debe ir cruzando la estrategia, estos plazos serán depositados en el plan de implementación y servirán para los seguimientos y evaluaciones. A partir de los seguimientos se podrá medir el progreso de la estrategia, el estado y las posibles mejoras. En conclusión, el plan de trabajo debe tener presente las acciones necesarias, enmarcarlas en un plazo que esté articulada a una estrategia y que esté en concordancia con los objetivos establecidos anteriormente.

3.4.2 Redacción

- La clave para redactar un documento estratégico eficaz es tener siempre en mente al público seleccionado y la esencia del mensaje que se quiere transmitir. El documento debe ser conciso y directo, sin jerga técnica que pueda llevar a confusión.
- Una vez redactado el borrador del documento, un editor se encargará de pulir el estilo y corregir los errores. Asimismo, un diseñador gráfico deberá encargarse de crear una presentación visual atractiva del documento.

Para estructurar la estrategia se debe tener en cuenta las siguientes sugerencias:

1. **Situación actual y antecedentes**. Se basa en la información relevante recogida en la actividad III. VIII de consolidación de la situación.
2. **Objetivos de la estrategia**. Los objetivos deben ser claros y que se distingan unos de otros.
3. **Partes interesadas clave de la estrategia**. Se incluirán los grupos más significativos señalados en la actividad de mapeo de las partes interesadas, y se dividirán en partes interesadas principales y secundarias.
4. **Actividades**. Es el núcleo de la estrategia, describe las actividades definidas en el desarrollo del plan de trabajo asociado a un objetivo y se indicará el público que participa en las actividades y su valor estratégico.
5. **Plan de trabajo de comunicaciones**. Las actividades se deben planificar en un calendario, y se especificarán las fechas de inicio y finalización.
6. **Seguimiento y evaluación del impacto**. Se debe tener una lista de indicadores para hacer seguimiento de las actividades de cada objetivo y evaluarlas.
7. **Riesgos y supuestos**. Se elabora una lista de los factores que pueden repercutir en la implementación y el éxito de la estrategia. Abarca condiciones necesarias para el éxito (supuestos) y también lo que pueda estar fuera del alcance de la organización.
8. **Otros**. Algunas oficinas nacionales de estadística deciden incluir una sección de antecedentes antes de la sección del análisis de la situación, que abarca, entre otros, el mandato, los valores y los objetivos institucionales de la organización.

9. **Anexo**. En esta sección se añadirá cualquier documentación de respaldo que pueda ser relevante para entender la estrategia.

Paso 5. Cuando la estrategia ya tenga forma, solo quedará un par de pasos antes de que se inicie la implementación. En primer lugar, el personal directivo superior deberá aprobar el documento de la estrategia. Después, la estrategia se presentará de forma interna para que todos los miembros del personal conozcan y entiendan las implicaciones en su trabajo.

3.5.1 Entrega de la estrategia al personal directivo superior para su aprobación

Cuando se haya redactado la versión final del documento, deberá recibir la aprobación de los mismos miembros del personal directivo superior que aprobaron los hallazgos al final del paso 3.

3.5.2 Presentación

Cuando se apruebe la estrategia final, se planificará la presentación, por lo que es necesaria la presentación del documento, así como definir sus objetivos principales y elaborar una lista con las oportunidades clave que su presentación puede aportar al éxito de la estrategia.

El formato de la presentación variará en función de cada organización, pero sea cual sea el formato de la presentación de la estrategia, debe asegurarse de que incluya un resumen sencillo de una página que indique: i) Por qué se ha elaborado la estrategia, ii) Cómo ayudará a la oficina nacional de estadística a llevar a cabo su misión, iii) Qué implicaciones tiene para el personal. Y iv) Con quién contactar para recibir más orientaciones.

4. Posición del DANE frente a los temas desarrollados en la 70ª sesión plenaria de la Conferencia de Estadísticos Europeos.

Evento de la 70ª sesión plenaria de la Conferencia de Estadísticos Europeos

Introducción al evento

La Comisión Económica de las Naciones Unidas para Europa – CEPE fue establecida en 1947 por el Consejo Económico y Social de las Naciones Unidas – ECOSOC, la CEPE es una de las cinco comisiones regionales de las Naciones Unidas, cuyo objetivo es fomentar la integración económica de los países pertenecientes a Europa (paneuropeos) por medio del establecimiento de normas, estándares y convenciones, además de mejorar la eficacia de las Naciones Unidas a través de la implementación regional de los resultados de sus conferencias y cumbres mundiales[81].

Anualmente, la entidad lleva a cabo el periodo de sesiones de la Comisión Económica, durante el presente año tuvo lugar el septuagésimo periodo de sesiones plenarias de la Conferencia de Estadísticos Europeos, la cual se realizó los días 20, 21 y 22 de junio en Ginebra Suiza, esta versión dispuso de un total de ocho temas, los cuales fueron desarrollados en formato híbrido permitiendo la presencia física y remota (conexión en línea), contando con la interpretación simultánea en tres idiomas (inglés, francés y ruso)[82].

El presente apartado presenta la posición del DANE frente a las ocho temáticas que se abordaron en las reuniones que contemplo el septuagésimo periodo de sesiones plenarias de la Conferencia de Estadísticos Europeos, de igual forma en cada apartado se presentan los temas clave y en algunos casos las próximas tareas del DANE frente a estos temas (Ver **Error! Reference source not found.**).

Tabla 23 Posición del DANE frente a las temáticas abordadas en el septuagésimo periodo de sesiones plenarias de la Conferencia de Estadísticos Europeos.

Ítem II. 30 aniversario de los Principios Fundamentales de las Estadísticas Oficiales
Posición del DANE Colombia contribuyó al desarrollo de la campaña de comunicación del Principio 5, Fuentes de Estadísticas Oficiales. Al respecto, se implementaron tres campañas principales. • Video sobre la importancia del 5.º principio para el trabajo en el DANE, 8 funcionarios de diferentes niveles gerenciales explican la relevancia del principio mencionado para la producción de estadísticas más granulares y el cumplimiento de las metas de los ODS. Además, se incluyeron

[81] Disponible en https://unece.org/mission
[82] Disponible en https://unece.org/sites/default/files/2022-04/ECE_CES_102-2204000E.pdf

ejemplos sobre cómo integrar fuentes secundarias de información para la producción de estadísticas oficiales.

- Video explicativo "DANE le cuenta": Desarrolló un video animado para usuarios no especializados, allí se explica la diferencia entre fuentes de información primarias y secundarias en las estadísticas oficiales y se muestran varios resultados de la integración de ambos tipos de fuentes.
- Infografías e Instagram: Se consolidaron una serie de imágenes para su distribución a través de Twitter e Instagram, explicando los tipos de fuentes estadísticas y su importancia para el trabajo del DANE. Por medio de la función de encuesta de historias de Instagram se logró interactuar con audiencias más jóvenes.

Además, el DANE participó en la campaña del Reino Unido por el Principio 7 sobre Legislación Estadística, que contó con el director del DANE, Juan Daniel Oviedo, para promover la importancia de contar con un marco normativo actualizado que mejore la producción de estadísticas oficiales.

Temas clave

- Principios Fundamentales de las Estadísticas Oficiales.
- Hacer un balance de cómo las Oficinas Nacionales de Estadística - ONE han estado demostrando e implementando los Principios Fundamentales a lo largo de los años, centrándose en la experiencia práctica de varios países.
- Promover y comunicar la relación entre los Principios Fundamentales de las Estadísticas Oficiales y el valor que representan, dentro de la comunidad estadística y con otras partes interesadas, p. formuladores de políticas, medios de comunicación y el público.
- Aumentar la conciencia de la cooperación internacional en estadísticas oficiales y de la contribución de las ONE al desarrollo global de estadísticas oficiales.

Próximas tareas

- Polonia preparó un vídeo en el que se explica lo que significan los Principios Fundamentales para los estadísticos oficiales y cómo esperan guiarse por los Principios en el futuro. El video se mostrará durante la sesión plenaria de CES y se publicará en el sitio web de UNECE y en los canales de redes sociales. Será un producto colectivo de los países miembros y se invitará a todas las oficinas de estadística a publicarlo en sus propias plataformas.

Ítem III. Valores Fundamentales de las Estadísticas Oficiales

Posición del DANE

Para el desarrollo de la lista de Valores Fundamentales, el DANE contribuyó con:

- La propuesta de resaltar la importancia de entender la producción de estadísticas oficiales como un servicio público, pues desde su experiencia, le permitió enfocarse en la necesidad de promover la igualdad de acceso, la inclusión y el bien público como parte de los principales valores de las estadísticas oficiales, referenciados en el Valor Central.

- Se resalta la importancia de "contrarrestar el uso indebido", se establece en el Marco Ético de Colombia para la producción de estadísticas oficiales.
- Cambio de la referencia que se hace a la privacidad, en el valor V (Respeta la privacidad), respeta la confidencialidad debido a la consulta.
- Productor de la discusión enmarcada en el grupo de trabajo, se encontraron posibles problemas de traducción de la versión en inglés a otros idiomas, por ejemplo polaco, en este contexto Polonia planteó algunos puntos: i) hay un elemento que falta en la lista "verdad", ya que se afirmó que este era el valor final, se deriva del derecho humano fundamental, derecho a la verdad y a ser informado y ii) planteó la importancia de evitar incluir la "privacidad", pues conduciría a la colusión con el FPOS.

Temas clave

- **Valores centrales:** Brindan un marco ético para respaldar la toma de decisiones y las interacciones con los gobiernos, la sociedad y otras partes interesadas, estos valores se comunican con el objetivo de promover la confianza en las estadísticas oficiales y las entidades que las producen.
- **Valor relevante:** Usar un enfoque comprometido, receptivo y centrado en el usuario, basado en la comunicación clara.
- **Valor Imparcial:** La comunidad de estadísticas oficiales en todos los aspectos de trabajo, actuando con justicia e integridad para servir al bien público.
- **Valor Transparente:** Las estadísticas oficiales, los métodos, los procesos, los productos y los informes de calidad se comunican al público a través de los canales apropiados y están abiertos al escrutinio.
- **Valor Profesional e Independiente:** Las estadísticas deben ser creíbles y fidedignas, libres de interferencia externa.
- **Valor Respeta la Confidencialidad:** La comunidad de estadísticas oficiales protege la privacidad, asegurándose de que la recopilación de datos se limite a lo necesario.

Ítem IV. Profunda de la Medición de la Economía Informal No Observada

Posición del DANE

- Colombia ha trabajado en un acuerdo interinstitucional para definir, caracterizar y adoptar políticas públicas en materia de informalidad (CONPES 3956 de 2019), que se basa en la definición de un conjunto de pilares de gradualidad que permiten tipificar este fenómeno en función de sus diferentes características, incluyendo criterios para el registro de trabajadores informales en los sistemas de seguridad social, empresariales y tributarios, entre otros.
- Para el año base de 2015, el DANE desarrolló una medición limpia de la economía no observada, combinando información de diferentes estadísticas y registros administrativos, para reflejar el efecto de la dinámica productiva a nivel de actividad económica y para la economía en su conjunto. Las fuentes de estos cálculos son los datos de ingresos proporcionados por los hogares en la Gran Encuesta Integrada de Hogares - GEIH, el Formulario Integrado de Liquidación de Contribuciones - PILA, la Encuesta de Microempresas - EMICRON, los registros tributarios disponibles, etc.

Colombia ha implementado un enfoque de medición de la economía no observada que adopta el enfoque tabular exhaustivo de Eurostat para lograr una cobertura y representatividad completas de las transacciones y los agregados macroeconómicos, así como el Manual de Economía No Observada de la OCDE para el tratamiento de las actividades económicas, como referencias conceptuales para la medición de estos fenómenos en la base de 2015 de las Cuentas Nacionales. Asimismo, Colombia ha avanzado en la documentación estadística del empleo informal, a partir de la difusión de información relacionada con este fenómeno desde la Gran Encuesta Integrada de Hogares - GEIH y un módulo especializado de esta Operación Estadística, enfocado en profundizar en segunda instancia la caracterización de pequeñas unidades económicas con actividad productiva dentro de los hogares y que se denomina encuesta de microempresas - EMICRON.

- El DANE apoya la propuesta de unificar el marco conceptual y estadístico para medir la informalidad y armonizarla con la economía no observada y acuerda crear un grupo de trabajo para revisar los estándares estadísticos sobre informalidad en vista de la actualización del Sistema de Cuentas Nacionales dentro de la Organización Internacional del Trabajo prevista para 2025.

Temas clave

- La economía informal es un concepto dinámico, consiste en todas las actividades productivas informales realizadas por personas y unidades económicas.
- En países con altas tasas de informalidad, como Colombia, es necesario profundizar las acciones para visibilizar la medición de la economía no observada y reducir el margen de incertidumbre respecto a los niveles y dinámicas de la actividad económica de las pequeñas unidades productivas, a partir del fortalecimiento de las operaciones estadísticas y registros administrativos existentes; integrar todos los elementos disímiles en un marco estadístico que facilite la medición y considerar la información de las Oficinas Nacionales de Impuestos - OTN que es esencial para desarrollar información estadística para el trabajo. Por ello, es importante sensibilizar a las organizaciones no gubernamentales sobre la importancia de establecer asociaciones y acuerdos con las Oficinas Nacionales de Estadística para compartir información.

Ítem IV. Revisión a Profundidad de las medidas subjetivas de pobreza

Posición del DANE

- Respecto a los principios fundamentales, se plantea la pertinencia de la participación activa y reconoce que cualquier revisión debe ser objetiva y técnica, separada de cualquier perspectiva partidista.
- En cuanto a valores fundamentales, Colombia, como servidor público, reconoce que el enfoque colaborativo es importante para mantener las discusiones y le permite interactuar con nuevas perspectivas éticas en la sociedad.
- Resalta la importancia de la apropiación documental en español.

- Colombia se encarga de la producción de datos sintéticos que aseguran la comparabilidad entre usuarios y organismos internacionales, propone ampliar el alcance de SDMX a nivel de producción y de difusión.

Temas clave

- Obligatoriedad en las entidades productoras de estadísticas oficiales en el desarrollo y descripción de Valores Fundamentales.
- Impactos de la informalidad en los resultados de la política.
- Medición de economía informal no observada.
- Características y desafíos de las nuevas fuentes de datos.
- Principios fundamentales, Valores Fundamentales y ética de los datos en el marco de la privacidad y la generación de confianza.

Ítem IV. Revisión sobre la colaboración con proveedores de datos del sector privado

Posición del DANE

- El informe se debe enmarcar sobre lo que se entiende como *nuevas fuentes de datos,* dando relevancia al principio 5 de las estadísticas oficiales.
- Es indispensable revisar el posible conflicto de intereses con el uso comercial y la línea de negocio de los proveedores de datos del sector privado cuando el INE utilice estos datos.
- Es primordial comprender las mejores prácticas y metodologías para lograr esquemas eficientes de intercambio y colaboración.
- El principio de interés público debe guiar los acuerdos de intercambio con proveedores de datos privados para generar valor público.

Temas clave

Cooperación con los proveedores de datos del sector privado; impacto de la crisis de COVID-19 en el uso de datos privados por parte de las estadísticas oficiales.

Próximas tareas

Profundizar sobre ¿Cuáles son las principales características de los equipos dentro de cada INE encargado de la cooperación con los proveedores privados?, ¿Cuál debe ser la composición ideal de estos equipos?, ¿debería crearse una nueva unidad o dependencia dentro del INE?
¿cuáles son los principales incentivos que hacen que esas empresas clave estén más ansiosas por cooperar con las organizaciones internacionales en lugar de con los INE?

Ítem V. Vista geoespacial del Modelo Genérico de Procesos de Negocios Estadísticos (GSBPM)

Posición del DANE

El DANE destaca el trabajo realizado en el desarrollo del modelo GeoGSBPM, que describe las actividades y consideraciones relacionadas con el dominio geoespacial en cada etapa del proceso de producción, desde el diseño, el proceso y la difusión. Gracias a este modelo, es posible describir la producción de estadísticas de forma general y orientada a procesos.

Temas clave:

- El DANE tiene como objetivo fomentar el uso del Marco Geoestadístico Nacional (NGS) y otras fuentes de observación de la tierra de sensores remotos para fortalecer la producción y difusión de estadísticas utilizando las mejores prácticas.
- El NGS es parte de la infraestructura estadística, y sus objetivos son fortalecer el proceso de producción estadística, mejorar la calidad del intercambio, la interoperabilidad, la integralidad y el uso de las estadísticas.
- Colombia ha desarrollado el Manual para el uso del Marco Geoestadístico Nacional V. 2.0, que tiene como objetivo orientar a los responsables del proceso de producción estadística en el uso del NGSM para las fases del proceso estadístico establecidas en los Lineamientos para el Proceso Estadístico

Próximas tareas:

- En medio de los avances realizados por la comunidad geoespacial dentro de las estadísticas oficiales, el DANE se ofrece en respaldar el GeoGSBPM, ya que esto permitirá mejorar la pertinencia y la calidad de la información que producimos, particularmente para la fase de difusión.

El DANE recomienda la incorporación de procesos geoespaciales en el contexto del modelo GSBPM, para la evaluación de la infraestructura tecnológica utilizada para el procesamiento y análisis de datos, con el fin de comprender el papel de las tecnologías geoespaciales en la transformación de la infraestructura tecnológica.

Ítem V. Informe sobre el trabajo del Grupo de Alto Nivel para la Modernización de las Estadísticas Oficiales en 2021

Desde el DANE se ha contribuido a la modernización de la producción de información estadística en el marco del SEN y se destacan actividades como:

- Adaptación y socialización del Modelo GSBPM para las diferentes entidades que forman parte del Sistema Estadístico Nacional y, en particular, dependencias del DANE.
- Consolidación de cursos virtuales sobre la adecuación del Modelo GSBPM y diferentes estándares estadísticos con miras a garantizar los atributos de calidad de la información estadística.
- Generación de lineamientos, recomendaciones y guías para la implementación de las diferentes fases del proceso estadístico de acuerdo con la adaptación del modelo GSBPM.

- Acompañamiento a las entidades del SEN para la implementación de los lineamientos del proceso estadístico.
- Incorporación del modelo GAMSO (Modelo Genérico de Actividades para Organismos Estadísticos) en el diseño del nuevo mapa de procesos del DANE, e implementación de los lineamientos establecidos en el modelo para cada uno de los procesos establecidos.

Temas claves

El DANE acoge con entusiasmo la elaboración de la "Guía práctica de datos sintéticos para INE", que puede ser un elemento para que los INE brinden información de manera abierta y transparente.

- Es clave que las instituciones estadísticas pongan en práctica las políticas relacionadas con los principios de gestión y liderazgo éticos, que permitan un uso adecuado de la información desde el proceso de recolección hasta su disposición, a fin de garantizar que los datos sean utilizados para fines legítimos y tratados. de tal forma que se garantice su seguridad y se garantice la privacidad de los usuarios, tomando medidas para que la confidencialidad, disponibilidad e integridad de los datos no se vean comprometidas.

Próximas tareas:

- El DANE Seguirá de cerca los métodos teóricos presentados para crear datos que puedan garantizar la comparabilidad entre diferentes usuarios en el sector académico y privado y organizaciones internacionales
- En relación con *Blue Skies Thinking Network* – BSTN, el DANE está interesado en participar en esta iniciativa, que ofrece una plataforma de investigación e innovación donde los miembros pueden compartir ideas y que permite la búsqueda de socios para explorar sobre innovaciones en producción estadística.

Para Colombia sería de gran utilidad conocer los avances respecto a dónde y cómo se pueden utilizar los estándares estadísticos SDMX y DDI en el proceso estadístico basado en el modelo GSBPM.

Ítem V. El papel de la gestión de la marca y la reputación, el marketing y la comunicación de crisis para las organizaciones estadísticas.

El papel que ha jugado nuestra marca para asegurar la credibilidad de las estadísticas oficiales en Colombia es fundamental para seguir siendo valiosos para los usuarios de datos. Para una NSO, una marca fuerte se convierte en un facilitador para asegurar el cumplimiento de nuestro mandato, que es desbloquear el valor de los datos para todos. Las estadísticas oficiales, como cualquier otra fuente de información, se validan por la confianza que los usuarios tienen en el productor de estadísticas oficiales. Por más calidad, relevancia y actualidad que tengan las estadísticas oficiales, sin una marca que respalde ese trabajo, es inútil para la toma de decisiones.

Temas claves:

- El problema es precisamente que el significado de nuestra marca no es el mismo para los distintos grupos de interés. Si no confían en nosotros, son reacios a buscar el valor de la información que producimos y, por lo tanto, no podrán desbloquear su valor para su propio beneficio.

Próximas tareas:

- Desde el DANE se sugiere conectar esta guía con la discusión sobre la definición del valor de las estadísticas oficiales, ya que la gestión de marca está estrechamente relacionada con garantizar que nuestras estadísticas se perciban como valiosas.
- El DANE sufrió un ataque informático en 2021. Este documento contiene una gran recomendación para la gestión de crisis. Puede ser interesante analizar cómo se aplicaron estas recomendaciones durante el evento de hackeo del DANE el año pasado. Puede permitir establecer algunos protocolos de comunicación para gestionar las crisis de reputación, ya que son una amenaza para la credibilidad de las estadísticas oficiales.

Ítem VI. Orientación sobre las estadísticas de los niños: atención a los niños expuestos a la violencia, en cuidado alternativo y con discapacidad.

EL DANE cuenta con múltiples operaciones que están alineadas a esta temática.

- Gran Encuesta Integrada de Hogares- GEIH, como fuente de medición de trabajo infantil. Desde 2001 el DANE monitorea los principales indicadores de trabajo infantil cada dos años. Con el objetivo de generar información estadística que permita el seguimiento de los principales indicadores de trabajo infantil, anualmente se publica el módulo con resultados como: Tasa de trabajo infantil, Tasa de trabajo infantil por edad y sexo, Tasa de trabajo infantil extendida, entre otras.
- Encuesta de Calidad de Vida- ECV. Dentro de las preguntas de la ECV orientadas a brindar características relevantes del cuidado de los niños y niñas de 0 a 4 años se incluye el lugar o persona con quien pasan la mayor parte del tiempo durante la semana. Adicionalmente, las preguntas sobre educación se enfocan en la asistencia escolar por grupos de edad a cada nivel educativo y nivel educativo alcanzado.
- Índice de Pobreza Multidimensional, que incluye una dimensión denominada "Condiciones de la Niñez y la Juventud", utilizando como fuente la Encuesta Nacional de Calidad de Vida. Desde 2020, es importante destacar la integración ECV- SIMAT - Formulario C-600 para mejorar la precisión del indicador de ausentismo escolar en esta dimensión.
- Encuesta Pulso Social – EPS. La Encuesta Social Pulse busca producir información relacionada con la confianza del consumidor; bienestar subjetivo; redes de apoyo a los hogares; bienestar de los hogares con niños y adolescentes; y conocimiento y acceso a políticas nacionales y locales para apoyar a los hogares. Tiene preguntas sobre la educación de niños, niñas.
- Encuesta Pulso Migratorio. La cual, su cuarta ronda del Pulso Migratorio publicada el 10 de junio de 2022, incluye un módulo sobre el bienestar de la niñez y la adolescencia.

- Geovisor del embarazo adolescente, tiene como objetivo identificar las unidades espaciales (manzanas) con los mayores niveles de vulnerabilidad a la ocurrencia de embarazos infantil-adolescentes, de esta forma, exponer las áreas donde las niñas y adolescentes tienen más probabilidades de tener hijos facilitará la toma de decisiones por parte de los actores sobre políticas e intervenciones de prevención.
- Informes de Estadística Sociodemográfica Aplicada N.º 2. Determinantes y factores asociados a la Tasa de Mortalidad Infantil.
- Publicación de nacimientos y defunciones, utilizando como fuente el Registro Civil.
- Análisis de la nota estadística de accesibilidad a los centros educativos.
- Nota estadística sobre la situación de las familias con niños, niñas y adolescentes en Colombia en medio de la crisis del covid-19.
- Nota estadística de nacimientos en niñas y adolescentes en Colombia.

Temas clave:

- A pesar de los avances que se están logrando en el contexto colombiano, el DANE reconoce que aún existen tanto desafíos metodológicos como vacíos de información en torno a las estadísticas de niñez y adolescencia y también se reconoce la posibilidad de aprovechar el potencial de los registros administrativos, para encontrar soluciones costo eficientes.
- Algunos de los hallazgos del Grupo de Trabajo evidencian la falta de datos y la incidencia de definiciones y metodologías no estandarizadas tanto en países en desarrollo como desarrollados

Próximas tareas:

Si bien desde el DANE se ha avanzado en la elaboración de ejercicios de interoperabilidad dentro del Sistema Integrado de Violencia Basada en Género de Colombia, aún existen algunos vacíos para los cuales consideramos que la guía brinda excelentes recomendaciones, como es el caso de los esquemas de cuidados alternativos.

Ítem VI. Medición del valor de las estadísticas oficiales.

Posición del DANE:
La perspectiva propia del DANE concibe las estadísticas oficiales como un bien público, por un lado, se debe garantizar el acceso de cada una de las personas y la posibilidad de beneficiarse de ellas. Al contrastar este informe con lo realizado en el DANE, se evidencia que el DANE diseña, implementa y evalúa estrategias que se basen en la puntualidad, relevancia, precisión, comparabilidad y calidad estadística para la medición de valor de las estadísticas y la apropiación de las mismas, de manera tal que estas se enlacen y promuevan los ODS.

Temas Clave:

- La Dirección de Comunicaciones del DANE ha trabajado en un indicador que permita identificar y destacar el nivel de uso de las estadísticas oficiales en escenarios como los planes de desarrollo local y departamental.
- El valor de las estadísticas es un elemento que va atado con la calidad de las mismas, así como con el flujo de información preciso y puntual.

Próximas tareas:

- Al querer establecer una estrategia para realizar una medición al "valor" de las estadísticas oficiales, se debe lograr un consenso, delimitar y precisar el concepto "valor", de manera tal que se pueda ser más explícito al hablar del tema. Adicionalmente, se debe tener presente que "valor" es completamente a "valores".

Ítem VI. Uso de nuevas fuentes de datos para medir la migración internacional.

Posición del DANE:

Con el propósito de avanzar en la implementación y robustecer la Política Integral Migratoria, el DANE propuso y creo el Sistema de Información de Estadísticas de Migración, SIEM. Un sistema articulado, consistente y pertinente con las necesidades de los migrantes en territorio colombiano, cuyo objetivo principal es organizar, consolidar y difundir información estadística relacionada con los procesos de migración, esperando así que las estadísticas sirvan para la generación de normas, procesos técnicos y políticas públicas acertadas.

Temas Clave:

- La transición de los métodos tradicionales para la medición de migración internacional es un proceso que *a priori* se ha venido realizando de manera paulatina y plausible durante los últimos años.
- La integración de información proveniente de registros administrativos, censos y encuestas representa una oportunidad para presentar innovaciones en las mediciones de los diferentes fenómenos de migración.
- Se hace mención sobre la trascendencia de las fuentes de datos tradicionales y los estándares de calidad que estas representan frente a estrategias innovadoras como la inteligencia de datos (*big data)*.

Próximas tareas:

- Si se quiere optar por mecanismo de medición basado en estrategias de *big data* se debe realizar un análisis profundo sobre los niveles de calidad y el posible valor añadido que pueda ofrecer frente a las fuentes tradicionales.

- En noviembre del 2022 se llevará a cabo la Conferencia de *Big Data* en Indonesia, una oportunidad para explorar el uso de esta estrategia en las estadísticas de migración.
- Se debe explorar y estudiar a fondo el modelo DIMIS, un modelo que ofrece nuevos enfoques en las estadísticas de migración.

Ítem VI. Clasificación de Actividades Estadísticas – (CSA) 2.0 y notas explicativas.

Posición del DANE:

El DANE ha adaptado la clasificación de actividades estadísticas para el caso colombiano, esta tiene el propósito de ser aplicada como estándar estadístico para recolección, codificación y análisis de la información estadística en materia de actividades económicas.

Temas Clave:

- La clasificación de actividades estadísticas internacionales, la cual sirve como un esquema de clasificación global.
- Estructuración y organización de eventos estadísticos, materiales de capacitación, referencias o normas.

Próximas tareas:

- La clasificación de las actividades estadísticas propuestas debe incluir información relativa a temas de deportes como infraestructura, recursos humanos, eventos, uso del tiempo libre y actividad física. Asimismo, temas, servicios públicos domiciliarios, la prestación en términos de ingresos, consumos, tarifar, cobertura, vigilancia y control.

Ítem VI. Guía para medir el impacto de la pandemia COVID-19 en mujeres y hombres.

Posición del DANE:

La Encuesta de Pulso Social es una operación estadística aplicada por el DANE, esta permitió medir el impacto de la pandemia de manera diferencial para hombres y mujeres, la EPS inició su recolección en julio de 2020, su propósito es generar indicadores periódicos de percepción sobre el comportamiento de la economía, el bienestar subjetivo y las redes de apoyo y confianza, esperando así obtener una perspectiva general de la sociedad colombiana. En cuanto al enfoque de género, la operación contiene preguntas sobre la percepción de seguridad, la percepción sobre carga en las tareas del hogar y trabajo, salud pública, bienestar de las mujeres, salud sexual, violencia en el hogar, entre otros. Los resultados de la EPS son desagregados por sexo y se realizan ejercicios de comparación entre sexos.

Temas Clave:

- La perspectiva de género es una de las más altas prioridades de política en el desarrollo estadístico y gracias a una fuerte colaboración y coordinación interna se ha podido innovar en ellos, creando nuevas operaciones y fortaleciendo algunas ya existentes.
- El enfoque diferencial ha sido una constante de trabajo en la entidad durante los últimos años, operaciones como la Encuesta de Pulso Social son un reflejo del esfuerzo y la estructuración de este.
- El marco ético del Sistema de Ética Estadística del DANE contiene un eje sobre dignidad, confidencialidad y enfoque diferencial, el cual busca la garantía de un enfoque diferencial en las estadísticas.
- El análisis de los impactos generado por el COVID-19 por sexo permite identificar las disparidades sociales que persisten en la comunidad. A partir de la información estadística producida se pueden implementar políticas, normas y programas que permitan reducir las brechas de género en múltiples ámbitos.

Próximas tareas:

- Este tipo de mediciones deben mantenerse aún fuera del contexto de la pandemia y se debe trabajar en su evolución.

Ítem VI. Manual sobre formas de empleo.

El Manual sobre formas de empleo presenta un marco amplio para clasificar y comprender las formas de empleo que se centra en dos dimensiones principales: las relaciones de trabajo, tal como se definen en la Clasificación Internacional de la Situación en el Empleo de 2018, y las modalidades de trabajo, es decir, la forma en que se coordina el trabajo realizado y compensado. El Manual proporciona definiciones de conceptos clave, principios generales y pautas, así como una lista de indicadores clave recomendados con el objetivo de facilitar los esfuerzos estadísticos nacionales para clasificar, medir y rastrear diversas formas de empleo relevantes para su contexto nacional.

Posición del DANE

- El marco es un referente importante para el DANE, ya que se ha convertido en un referente conceptual que puede ser analizado y adaptado al contexto laboral en Colombia.
- El DANE utiliza actualmente la Clasificación Internacional de Situación en el Empleo (CISE-1993).
- La Encuesta de Población Activa – EPA capta el sistema de protección social en la que se ubica la forma de empleo y algunas características de las personas que se emplean en las formas de empleo.
- El DANE está interesado en introducir preguntas en sus operaciones estadísticas para evaluar la estabilidad y permanencia entre trabajadores independientes y contratistas dependientes.
- Los datos sobre nuevas formas de empleo, particularmente el empleo en plataformas digitales, han sido difíciles de clasificar porque con las nuevas plataformas es difícil definir la categoría correcta. Por ejemplo, Colombia ya tiene algunas empresas Rappi (aplicación de entrega) o Uber que tienen empleados, pero no pagan seguridad social, sin embargo, es importante clasificar como trabajo formal o informal.

Temas clave

Modalidad de trabajo, Relaciones laborales, Clasificación Internacional de la Situación en el Empleo

Próximas tareas

Se debería considerar el desarrollo de una guía práctica sobre los desafíos de recopilación y medición de datos. También sería útil compartir experiencias y buenas prácticas en la medición de formas nuevas y emergentes de empleo entre países.

El mercado laboral está en constante evolución y continuamente surgen nuevas formas de empleo en respuesta a los cambios tecnológicos, legislativos y económicos. Colombia siempre está dispuesta a analizar nuevos conceptos para incorporar en las encuestas. Clasificar las formas de empleo requiere abordar tres desafíos clave:

1. Garantizar que los formularios de un tipo sean más similares entre sí que los formularios de otro tipo. Esto requiere un análisis profundo del mercado laboral en Colombia y pruebas para validar la representatividad de la muestra de estas nuevas formas de trabajo.
2. Colombia está dispuesta a incluir indicadores que sean relevantes a su contexto nacional para monitorear el desempeño, la estabilidad de las relaciones laborales, la población ocupada en riesgo económico y la participación en formas de empleo y formas de trabajo emergentes.
3. El DANE siempre considera implementar las últimas clasificaciones de la OIT. La OIT sugiere agregar una referencia a los conjuntos de preguntas desarrollados por el Grupo de Washington sobre Discapacidades.

Ítem VII. Informe del Grupo de Coordinación Regional sobre Datos y Estadísticas para Europa y Asia Central.

El objetivo del subprograma estadístico de la Comisión Económica de las Naciones Unidas – UNECE, es avanzar en las políticas oficiales a nivel nacional e internacional para la formulación de políticas basadas en evidencia y la evaluación del progreso hacia los ODS.
El objetivo de este documento es de tipo información.

Temas clave

Implementación del Programa Estadístico UNECE 2021
En 2021, la Mesa de la Conferencia revisó en profundidad tres áreas estadísticas con el fin de abordar problemas emergentes:

- Mejorar la coordinación institucional
- Eliminar superposiciones
- Lagunas en las actividades estadísticas realizadas por varias organizaciones internacionales en la región de la UNECE.

Estas revisiones han llevado al desarrollo de recomendaciones prácticas para que los países aborden los desafíos emergentes. Se realizaron las siguientes revisiones:

(i) Nuevas formas de empleo y calidad del empleo: implicaciones para las estadísticas oficiales,
(ii) Medidas subjetivas de pobreza y
(iii) Medición de la economía informal/no observada.

La División de Estadísticas ha facilitado la presentación de informes estadísticos dirigidos por los países de dos formas principales: en primer lugar, UNECE está apoyando a las oficinas nacionales de estadísticas como proveedores y coordinadores nacionales de estadísticas sobre los ODS, proporcionando orientación y una serie de herramientas prácticas para facilitar su implementación.

En segundo lugar, la División de Estadística lleva a cabo un trabajo metodológico y de desarrollo de la capacidad estadística nacional para informar las decisiones de política para el logro de los ODS a través del trabajo sobre estadísticas demográficas, sociales, económicas y ambientales.

En 2021 los grupos de la UNECE prepararon diferentes productos para presentarlos a la sesión plenaria de la Conferencia de Estadísticos Europeos – CES de 2022 para su aprobación. Además, se elaboró una *Guía para medir el impacto de la pandemia de COVID-19 en mujeres y hombres*. Asimismo, prepararon dos publicaciones oficiales de la UNESE: Marco de comunicación estratégica para instituciones estadísticas y aprendizaje automático para estadísticas oficiales.

Finalmente, UNECE finalizó una Evaluación global del Sistema Nacional de Estadística de Kirguistán, así como varios talleres de capacitación en línea y seminarios web para los países de Europa del Este, el Cáucaso y Asia Central.

UNECE está implementando proyectos financiados con fondos externos, un ejemplo es el financiado por el Banco Mundial para "*mejorar la coherencia y la integración de las estadísticas económicas y sociales en apoyo de la implementación del Sistema de cuentas Nacionales de 2008*".

Ítem VII. Informe del grupo de Coordinación Regional sobre Datos y Estadísticas para Europa y Asia Central y Programa Estadístico 2022, 2023 y 2024.

El documento contiene el Programa Estadístico de la UNECE para los años 2022, 2023 y 2024

Posición del DANE
Actualmente, el DANE está teniendo un rol de liderazgo en muchos de los temas definidos como prioritarios para el Programa Estadístico como:

- Copresidente del Grupo Interinstitucional de Expertos sobre Indicadores de los ODS
- Presidente del grupo de Expertos en Indicadores de Hogares de telecomunicaciones de la Unión Internacional de Telecomunicaciones.

- Copresidente del Grupo de Trabajo de las Naciones Unidas sobre Administración de Datos
- Miembro del Comité Directivo del Grupo de Expertos en Estadísticas de Refugiados, Desplazados Internos y apatridia – EGRISS

El DANE ha avanzado en múltiples frentes:

- ***Migración****:* se avanzó en el Sistema de Información estadística Migratoria, con el objetivo de articular las entidades del Sistema Estadístico Nacional (SEN), para la identificación, generación e integración de información estadística de calidad para la toma de decisiones y la evaluación del Sistema Integral Colombiano. Política de inmigración.
- ***Pobreza y desigualdad***: el DANE está trabajando en el Programa de las Naciones Unidad para el Desarrollo – PNUD para incluir preguntas en la encuesta del Pulso Social para evaluar las percepciones de los encuestados sobre el tema.
- ***Género*:** el DANE ha avanzado en medir el bienestar subjetivo, para responder a las demandas urgentes de información en el contexto de una pandemia, a través del diseño y difusión de resultados de la encuesta Pulso Social; se han creado nuevas medidas de brechas salariales y de mercado laboral, incluido los ciudadanos no remunerados y el empoderamiento económico de las mujeres. En conjunto con ONU-Mujeres se publicó el "*Iceberg de la violencia de Género en Colombia*" y se publicó una Guía para la Transversalización del Enfoque Diferencial e Interseccional para la Producción Estadística del Sistema Estadístico Nacional.
- ***Modernización de las estadísticas oficiales***: se continúan los esfuerzos para profundizar en la aplicación del concepto de tutela de Datos, tanto a nivel nacional como internacional.
- ***Consejo Asesor del Sistema Estadístico Nacional***: en junio de 2022 se creó este consejo y se han definido múltiples equipos de trabajo que tiene como objetivo profundizar en nuevas tecnologías como Big Data e interoperabilidad, para incorporar el enfoque étnico e interseccional dentro del SEN.
- Se ha liderado la redacción de una nueva Ley de Estadística en el Congreso, que permitirá establecer un nuevo marco legal para la aplicación, producción y difusión de las estadísticas oficiales. El DANE ha codirigido con Polonia el Grupo de Trabajo de las Naciones Unidades sobre la Custodia de Datos.
- Con Argentina, el DANE actualmente co-preside el grupo de trabajo de las Conferencia Estadística de las Américas "Diagnóstico de los alcances del concepto de Custodia de datos en el rol de las Oficinas Nacionales de Estadística de América Latina y el Caribe".
- ***Medio Ambiento y Cambio Climático***: el DANE desarrolló la operación estadística denominada Cuenta Satélite Ambiental, se avanza en la implementación de las Cuentas de Ecosistemas.
- ***Economía Circular***: la formalización del Comité Interno de Economía Circular, el inicio del diseño de la Cuenta Satélite de Economía Circular, el inicio del diseño y construcción de un Sistema de Información de Economía Circular, elaboración y publicación de 4 informes de economía circular, inclusión de preguntas relacionadas con la economía circular.

Temas clave

Liderazgo del DANE como prioritarios para el Programa Estadístico para 2022.

Próximas tareas:

El DANE saluda los esfuerzos realizados por la UNECE presentados en el informe del Grupo de Coordinación Regional Sobre Daos y Estadísticas para Europa y Asia Central y en el Programa Estadístico para 2022.

Ítem VIII. De Vuelta a lo básico: el concepto de administración de datos y sus vínculos con los Principios Fundamentales de las Estadísticas Oficiales – FPOS.

El documento vincula el concepto nuevo y ampliamente utilizado de 'administración de datos' con los Principios fundamentales de las estadísticas oficiales - FPOS. Si bien la comunidad de estadísticas oficiales está reconsiderando su función, los FPOS siguen siendo los principios clave sobre los que operan.

Posición del DANE

Este documento fue redactado conjuntamente por la Oficina de Asuntos Nacionales e Internacionales y Estadísticas de Polonia. El espacio preparado en la agenda para discutir este documento se compartirá, entre otros temas relacionados con la administración de datos.

Temas clave

- Enfoque de administración de Datos.
- Los FPOS se han mantenido como una herramienta increíble para la comunidad estadística porque nuestra interpretación de ellos ha sido capaz de relacionarse con diferentes realidades.
- Con los Principios Fundamentales de las Estadísticas Oficiales – FPOS, cualquier conjunto de buenos principios se caracteriza por su estabilidad en el tiempo, lo que demuestra que siguen siendo relevantes e importantes para una comunidad, independientemente de sus contextos cambiantes.
- Sin embargo, un gran conjunto de principios se caracteriza por seguir siendo relevante porque la realidad se puede abordar a través de sus lentes, más que por la inmutabilidad de los principios mismos. Los FPOS se han mantenido como una herramienta increíble para la comunidad estadística porque nuestra interpretación de ellos ha sido capaz de relacionarse con diferentes realidades.
- El papel como administradores no es solo cumplir con FPOS, sino también fomentar su uso fuera del marco de las estadísticas oficiales. Se ha convertido en nuestro deber ser embajadores de FPOS en medio de la ampliación del ecosistema de datos. Estos principios pueden ser de gran beneficio para todos los productores y usuarios de estadísticas, y no solo para esta comunidad que fue testigo de su nacimiento.

Ítem VIII. Evolución de la gestión de datos en Australia.

Posición del DANE:

El Sistema Estadístico Nacional de Colombia cuenta con cuatro instancias colegiadas: el Consejo Técnico Asesor del Sistema Estadístico Nacional, el Comité de Seguimiento Estadístico, los Comités Estadísticos Sectoriales y el Comité de Custodia de Datos. Este último es el órgano encargado de articular la producción

de información estadísticas y las necesidades de información de la política pública, tecnologías de la información y las comunicaciones, la protección de datos y, la política estadística. De igual manera, este Comité busca promover y gestionar el acceso funcional a los datos en ambientes seguros, responsables y éticamente correctos, asimismo, pretende facilitar la coordinación proactiva para el intercambio de datos y uso con fines estadísticos.

Temas Clave:

- La custodia de datos es un elemento trascendental a la hora de garantizar la protección, calidad y anonimización de las estadísticas. Profundizar en este concepto permite ampliar los actores del ecosistema de datos, así como entornos de colaboración, cultura de uso y reutilización de datos.

Próximas tareas:

- Uno de los aspectos más interesantes del ejercicio realizado en Australia y que se puede replicar en la entidad es el análisis de los diferentes acuerdos de gobernanza de datos y sus particularidades, este podría ser de gran utilidad en el DANE.
- Se debe ser constante en el trabajo sobre el acceso y compresión de los datos, teniendo en cuenta la importancia de las plataformas de datos y cuadramos de mando.
- Es necesario aunar esfuerzos para establecer un marco de trabajo sobre la gestión de datos proveniente de métodos geoespaciales.

Ítem VIII. Marco de gobernanza en apoyo de la calidad de los datos: una perspectiva central.

Posición del DANE

Ha puesto en práctica la perspectiva del "enfoque curador de datos" a través de la definición de lineamientos para producir estadísticas oficiales y el desarrollo de iniciativas para el aseguramiento y promoción de la calidad de los datos administrativos como el esquema de revisión por pares.
Además, considera útil introducir en el debate cómo los acuerdos de gobernanza cambian el alcance de este proceso; con el fin de tener funciones claras dentro del SEN para evitar duplicaciones o incluso posiciones divergentes.

Temas clave

- La administración de datos se extiende más allá del ámbito de las estadísticas oficiales, debido a que varias entidades son responsables y se asocian entre sí, por ello surge la necesidad de contar con un enfoque holístico independiente del componente principal que se esté tratando.
- Se destaca la importancia que, dentro de la Comisión Intersectorial de Gestión de las Finanzas Públicas de Colombia, a través de la cooperación de la Cooperación Económica Suiza (SECO) se esté desarrollando un marco conceptual para la gestión de las Finanzas Públicas y el DANE solicitó que se diferencie en el proyecto de ley, las estadísticas oficiales de otras estadísticas.

Próximas tareas

- Contar con un marco de gobernanza de datos para aliviar los desafíos de la documentación de datos, la calibración y la curación.
- Crear asociaciones formales de estadísticos y foros informales, que compartan las experiencias y difundan las prácticas innovadoras.
- Contar con estadísticas oficiales como información de referencia, con el fin de mantener una realizar una difusión objetiva al público.
- Desarrollar una estrategia de comunicación efectiva de las estadísticas oficiales.

Ítem VIII. Cambios en la cultura organizacional posterior a la pandemia, asegurando un enfoque centrado en el ser humano.

El DANE tiene una encuesta de Ambiente y Desempeño Institucional Nacional y Departamental (EDI). El piloto EDI se implementó entre el 1 y el 18 de diciembre de 2020 a través de una aplicación web proporcionada por el DANE, bajo la cual se obtuvo que los hallazgos más importantes del piloto EDI fueron:

- El 18 % de la plantilla del DANE tuvo dificultad para adaptarse a los cambios provocados por el trabajo en casa.
- El 70 % de los trabajadores afirmó que era capaz de mantener un equilibrio entre la vida laboral y personal.
- El 35,4 % relató dificultades para cumplir con las responsabilidades familiares debido al tiempo que dedican al trabajo.
- La reducción del tiempo de desplazamiento, entre otras razones, permitió a los trabajadores aprovechar mejor su tiempo sin afectar su desempeño laboral.
- El EDI reveló que, en promedio, el 88,1 % de los trabajadores del DANE en ese momento se sentían felices de trabajar en la entidad.

Temas Claves:

- Los resultados EDI para el período 2021 muestran que el 81,4 % de los trabajadores del DANE ha trabajado principalmente a distancia durante los últimos 12 meses. Esta proporción asciende al 92,3 % para el DANE Central, donde se realiza la mayor parte de la fase de procesamiento del ciclo estadístico. El 64 % de los trabajadores del DANE no ha acudido o ha acudido menos de una vez por semana a las instalaciones del DANE en los últimos tres meses previos al proceso de recolección. En cuanto a las posibles barreras para trabajar desde casa, el 76,1 % de los trabajadores no reporta ningún inconveniente al trabajar de forma remota, y solo el 12,8 % reporta haber tenido problemas de acceso a internet.
- Uno de los resultados más interesantes del EDI está relacionados con el bienestar percibido de los trabajadores cuando trabajan desde casa. En comparación con trabajar en la oficina, solo el 11,2 % de los trabajadores está de acuerdo en sentirse más distraído y el 14,4 % más ansioso mientras trabaja de forma remota. En cambio, el 64,2 % de los trabajadores está de acuerdo en ser más productivo cuando trabaja desde casa.

Próximas tareas:

En cuanto a la cantidad de días que los trabajadores quisieran venir a las instalaciones del DANE, se encuentra que solo al 27.2 % del personal le gustaría trabajar cinco días o más en las instalaciones. Al 25,3 % le gustaría trabajar tres días a la semana en la oficina, al 19 % le gustaría trabajar solo dos días y al 12,5 % no le gustaría volver o le gustaría venir ocasionalmente. Estas disparidades en las respuestas son una gran fuente de información, ya que pueden sugerir la necesidad de tener acuerdos de trabajo flexibles según las preferencias de nuestros trabajadores.

Ítem VIII. Estrategia del Comité Regional de Europa - Comité de Expertos de las Naciones Unidas sobre la Gestión Mundial de la Información Geoespacial.

Posición del DANE

El DANE ha llevado a cabo múltiples acciones con el fin de avanzar en la integración de información estadística y geoespacial en diferentes frentes que están plenamente alineados con la estrategia de UN-GGIM: Europa, entre ellas:

- Predicciones del Índice de Pobreza Multidimensional utilizando *machine learning* e imágenes satelitales
- Cálculo del indicador ODS 9.1.1 "Proporción de la población rural que vive a menos de 2 km de una carretera transitable todo el año" utilizando información del Censo Nacional de Población y Vivienda, y aportes cartográficos oficiales del Organismo Catastral – (IGAC).
- Cálculo del indicador 11.3.1 de los ODS. "Relación entre la tasa de consumo de tierras y la tasa de crecimiento de la población" utilizando información de imágenes satelitales y proyecciones de población para calcular las tasas de consumo de tierras y crecimiento de la población. Por este trabajo el DANE recibió el Premio GEO 2021.
- Cálculo del indicador 11.7.1 de los ODS "Proporción media del área urbanizada de las ciudades que es de espacio abierto para uso público, por sexo, edad y personas con discapacidad" utilizando imágenes satelitales, procesos de clasificación y fuentes de acceso abierto como *Open Street Map*, así como la actualización y mantenimiento de marcos estadísticos mediante el uso de imágenes detalladas obtenidas con drones.
- En relación con los temas migratorios, el DANE desarrolló la Encuesta Pulso migratorio con el propósito de complementar la información producida por la entidad que caracteriza a la población migrante de Venezuela, incluyendo a los colombianos retornados, con el propósito de ser útil para diseñar mejores políticas basadas en evidencia y dar a conocer las condiciones de vida de los migrantes a la población en general. Esta encuesta se realizó con el apoyo del Banco Mundial, especialmente del programa "Preguntas Globales sobre Desplazamiento Forzado", y con el apoyo técnico de la Universidad del Rosario. Adicionalmente, el DANE presentó avances en la consolidación del Sistema de Información Estadística Migratoria (SIEM), específicamente del Registro Estadístico Base de Población con marcaje migratorio, la ampliación del geovisor

migratorio internacional y el primer informe estadístico con indicadores migratorios consolidados con las entidades.

Temas clave

- El DANE participa como miembro del Grupo de Trabajo Interinstitucional y de Expertos sobre indicadores de los Objetivos de Desarrollo Sostenible (IAEG-SDGS) de Información Geoespacial, que promueve activamente la adopción de la hoja de ruta geoespacial de los ODS para estadísticas y geoespaciales. La implementación de la hoja de ruta geoespacial de los ODS ha permitido al DANE llevar a cabo un trabajo colaborativo en la explotación del inmenso potencial innovador de la información geoespacial y sus tecnologías asociadas para el cálculo de los ODS, y otras agendas de desarrollo global como el Marco de Sendai para la Reducción del Riesgo de Desastres 2015-2030, la respuesta al COVID-19 y las prioridades nacionales.
- El DANE se ha convertido en un actor relevante para las acciones desarrolladas en el marco de UN-GGIM: Américas, entre las que destaca su rol de coordinación técnica en la implementación del Marco Estadístico y Geoespacial de las Américas (MEGA), en sus diferentes versiones, con el fin de lograr un acuerdo de voluntades entre los diferentes países para hacer disponible información estadística en las principales desagregaciones territoriales.
- Colombia cuenta con el Marco Geoestadístico Nacional MGN con el propósito de promover la integración y difusión de información estadística y geoespacial de acuerdo con los estándares internacionales definidos, garantizando su interoperabilidad a través de la incorporación de los cinco principios definidos en el GSGF. La aplicación del Marco ha promovido la producción y difusión de información estadística de alta calidad, oportuna, fiable y geoespacial. La implementación de los principios del GSGF ha apoyado la respuesta nacional a covid-19 para proporcionar información geoespacial armonizada y estandarizada disponible en el geovisor del índice de vulnerabilidad, la producción de estadísticas experimentales y el cálculo de indicadores de los ODS.

Ítem IX. Colaboración con proveedores de datos privados - organizaciones internacionales.

Posición del DANE

Destaca la importancia de las organizaciones internacionales frente a procesos de colaboración con el sector privado para facilitar el acceso a sus datos. Las organizaciones internacionales actúan como facilitadores reduciendo la percepción del riesgo del sector privado y permite comprender lo qué tienen que ofrecer los INE en las actividades de intercambio y colaboración.

Temas clave

Colaboración con los proveedores de datos del sector privado

Próximas tareas

Generar investigación para profundizar sobre las siguientes preguntas: ¿Se sienten más cómodas las empresas compartiendo sus datos cuando interviene un tercero independiente (organización internacional)? ¿Contribuye la presencia de organizaciones internacionales a la eficiencia en esta materia? ¿Están las organizaciones internacionales proporcionando infraestructura que no está disponible en otros lugares? ¿Cuáles son las características de las empresas que son más propensas a compartir sus datos cuando una organización internacional está involucrada en la negociación?

Ítem IX. Proyecto de Resolución sobre el acceso a los datos en poder del sector privado para fines de estadísticas oficiales.

Posición del DANE

Realiza los siguientes comentarios al Proyecto de resolución de la Conferencia de Estadísticos Europeos sobre el acceso a los datos en poder del sector privado a efectos de las estadísticas oficiales:

- Reconociendo la administración de datos de trabajo en curso en los planos internacional y nacional
- Reconociendo los desafíos asociados con la recopilación de datos primarios de personas, hogares, empresas e instituciones en una sociedad cambiante
- Hacer hincapié en el interés público en la producción de estadísticas oficiales, que se basa en la confianza y la aceptabilidad social del público, lo que respalda la necesidad justificada de cooperar para recopilar datos del sector privado para la producción de estadísticas oficiales
- Afirmamos que las oficinas nacionales de estadística están dedicadas a aportar sus conocimientos especializados para facilitar el acceso a los datos en poder del sector privado para su uso en la producción estadística oficial.
- Asegurar el estricto cumplimiento de las disposiciones legales y los marcos éticos en el acceso a los datos en poder del sector privado a los efectos de las estadísticas oficiales y utilizar dichos datos bajo estricta observancia de los códigos estadísticos y las buenas prácticas;

Temas clave

Acceso a los datos en poder del sector privado para la producción de estadísticas oficiales.

Ítem IX. Proveedores de datos privados.

Posición del DANE

Frente a las experiencias expuestas en Colombia se encuentran las siguientes similitudes:

- Colombia carece de un marco legal sólido para facilitar el acceso a los datos de las partes interesadas privadas, esto se evidencia en las negociaciones con las compañías de telefonía celular que alegan no pertenecer al Sistema Estadístico Nacional.

- La colaboración con los proveedores de datos es más fácil cuando somos capaces de alinear intereses. Obligar a los proveedores de datos a compartir datos no es sostenible ni efectivo para crear asociaciones duraderas.
- Proporcionar cursos de capacitación, soporte para la anonimización, desarrollo de algoritmos y acceso a datos no públicos puede servir como palanca para negociar la transferencia de datos.
- La continuidad del flujo de datos es un problema que debe abordarse, dado que el valor que proporciona el DANE se basa en proyectos, ha sido difícil tener acceso constante a datos privados.

Temas clave

Experiencias y desafíos con el acceso a datos de propiedad privada; Inteligencia de datos/Macrodatos *(Big data)* del sector privado.

Próximas tareas

En cuanto al problema de la estabilidad y continuidad del suministro de datos, es importante conocer cómo ha funcionado la práctica internacional para resolver esta limitación a la hora de buscar fuentes de datos alternativas. Desde un punto de vista técnico, este se considera un punto importante a abordar, ya que, podría ser enriquecedor para la práctica del DANE conocer cuáles fueron las estrategias para lograr la asociación con operadores móviles mencionadas en las experiencias socializadas.

5.

Posición del DANE frente a los temas desarrollados en la 19.ª reunión del Comité de Estadística y Política Estadística – CSSP.

Evento de la 19.ª reunión del Comité de Estadística y Política Estadística – CSSP.

Introducción al evento

La Organización para la Cooperación y el Desarrollo Económico – OECD es una organización internacional, establecida en 1961 como reemplazo de la OECE, tiene el objetivo de diseñar políticas que promuevan la prosperidad, igualdad, oportunidades y bienestar para todos[83]. Dentro de los grupos que conforman la OECD está el Comité de Estadística y Política Estadística – CSSP, el cual tiene el objetivo general de fomentar la formulación de políticas sobre datos de alta calidad comparables internacionalmente, el comité busca lograr este objetivo supervisando la política estadística de la OECD y la amplia gama de datos y estadísticas relevantes para la organización[84].

Anualmente, la organización lleva a cabo sesiones con el fin de establecer un marco para que los gobiernos comparen experiencias de políticas, busquen respuestas a problemas comunes, identifiquen las buenas prácticas y coordinen políticas públicas nacionales e internacionales, durante el presente año tuvo lugar la decimonovena reunión del Comité de Estadística y Política Estadística – CSSP, la cual se realizó los días 22 y 23 de junio en Ginebra Suiza, esta versión dispuso de un total de diez temas, los cuales fueron desarrollados en formato híbrido permitiendo la asistencia física y remota (vía la plataforma Zoom), contando con la interpretación simultánea en dos idiomas (inglés y francés).

El presente apartado presenta la posición del DANE frente a algunas de las diez temáticas que se abordaron en las reuniones que contemplo la decimonovena reunión del Comité de Estadística y Política Estadística, de igual forma en cada apartado se presentan los temas clave y en algunos casos los próximos pasos del DANE frente a estos temas (Ver Tabla 24).

[83] Disponible en https://www.oecd.org/centrodemexico/46440894.pdf
[84] Disponible en https://oecdgroups.oecd.org/Bodies/ShowBodyView.aspx?BodyID=7229&Lang=en

Tabla 24 Posición del DANE frente a las temáticas abordadas en la decimonovena reunión del Comité de Estadística y Política Estadística – CSSP.

CSSP Agenda Ítem I Medición del progreso de los países para alcanzar los objetivos climáticos a largo plazo: progreso del IPAC y desafíos futuros.
Posición del DANE • Se ha avanzado conceptual y metodológicamente en las cuentas de: ii. actividades ambientales y transacciones asociadas iii. activos ambientales iv. flujos de agua, energía y materiales, actualizados a la base 2015 de la Contabilidad Nacional de Colombia • Se formalizó del Comité Interno de Economía Circular, mediante resolución 1598 de 2021. El objeto de este comité es identificar, analizar, verificar y garantizar la calidad de la información estadística producida por las entidades del Sistema Estadístico Nacional (SEN). • Diseño de la Cuenta Satélite de Economía Circular bajo el Modelo Estadístico Genérico de Procesos de Negocio (GSBPM) en el marco del Sistema de Cuentas Nacionales (SCN) y el Sistema de Contabilidad Ambiental y Económica (SCAE). • Diseño y construcción de un Sistema de Información de Economía Circular (SIEC). • Inclusión de preguntas relacionadas con la Economía Circular en los cuestionarios de algunas operaciones estadísticas del DANE. • Producción y publicación de informes de economía circular que incluyen indicadores relacionados con la economía circular derivados de operaciones estadísticas: la Encuesta Nacional de Calidad de Vida, la Encuesta Ambiental Industrial, la Encuesta Anual de Manufactura, la Encuesta Anual de Servicios (módulo ambiental), la Encuesta Nacional Agrícola, el Censo de Construcción y la Cuenta Satélite Ambiental. • Participación en el "I Grupo de Expertos formales sobre una nueva generación de información para una economía circular y eficiente en el uso de los recursos (RECE-XG)", donde se están debatiendo avances en la configuración de una definición de Economía Circular, así como la creación de indicadores relacionados. **Temas clave** • Apropiación de los instrumentos propuestos por la OCDE para continuar con los avances de cero gases de efecto invernadero, con el liderazgo de las Oficinas Nacionales de Estadística. • Capacitar a los actores relevantes (entidades públicas nacionales, la academia y el sector privado) sobre cómo usar y medir con estas metodologías.

- Evitar la duplicación de esfuerzos y crear consenso con el sistema de las Naciones Unidas y las organizaciones económicas internacionales, incluidos el Banco Mundial y el Fondo Monetario Internacional

Próximas tareas

De acuerdo a los compromisos y recomendaciones del CONPES No. 3934 de 2018, cuyo objetivo es promover para 2030 un aumento de la productividad y competitividad económica del país, se deben realizar:
1) generar condiciones que promuevan nuevas oportunidades económicas basadas en la riqueza del capital natural
2) fortalecer los mecanismos e instrumentos para optimizar el uso de los recursos naturales y la energía en la producción y el consumo
3) desarrollar directrices para construir capital humano para el crecimiento verde
4) fortalecer las capacidades en ciencia, tecnología e innovación para el crecimiento verde
5) mejorar la coordinación interinstitucional, la gestión de la información y el financiamiento para la implementación de la Política de Crecimiento Verde a largo plazo.

CSSP. Agenda Ítem II. Distribuciones de Ingresos, Consumos, Ahorros y Riqueza.

Posición del DANE

- Con de la Misión para el Empalme de la Serie Empleo, Pobreza y Desigualdad – Mesep, proporcionó una medición más precisa del ingreso agregado, sin embargo, omitió el ajuste de cuentas nacionales, dado el sesgo que se generó en la distribución de los ingresos; con este cambio se puede comparar con otros países latinoamericanos.
- La aplicación de la Encuesta Continua de Hogares - ECH y su versión posterior, la Gran Encuesta Integrada de Hogares - GEIH, proporcionan información para el cálculo de los indicadores de distribución del ingreso.
- Se aplicaron modelos de imputación para corregir sesgos en la información reportada por la Encuesta de Hogares.
- Los microdatos de la GEIH se vincularon a diferentes registros administrativos para complementar y contrastar la información reportada, revisando los sesgos de algunas fuentes de ingresos y mejorando la medición de las variables de ingreso; esto ha permitido tener una comparación entre el ingreso, la desigualdad y la pobreza monetaria.

Temas clave

- La inclusión de ajustes a las Cuentas Nacionales en la medición del ingreso introdujo sesgos incontrolados en la distribución del ingreso y la composición de la pobreza.
- La metodología utilizada en Colombia para la medición de la pobreza monetaria, la desigualdad y el ingreso es cercana a las metodologías de medición internacionales, puede ser tomada en cuenta para mejorar la comparabilidad a nivel regional.

- Las encuestas retrospectivas pueden enfrentarse a fenómenos de omisión, infradeclaración o sobredeclaración en las preguntas relacionadas con las distintas fuentes de ingresos debido a posibles sesgos derivados del recuerdo humano, por lo que se recomienda aplicar un modelo de imputación.
- En los procesos de enriquecimiento de datos con registros administrativos, se encuentra que este método permite abordar los sesgos de cobertura, de no respuesta y de medición en algunas fuentes de ingreso, y en consecuencia mejorar la precisión y exactitud en la medición de la variable ingreso.

Próximas tareas

- Incluir la dimensión de riqueza, esto proporcionará a los usuarios información coherente sobre las dimensiones clave de la desigualdad económica: ingresos, consumo, ahorro y riqueza.
- Crear un grupo internacional de expertos en colaboración con el Grupo de Expertos del BCE sobre Cuentas Financieras Distributivas (EG, DFA), con el fin de desarrollar metodologías armonizadas y recopilar los resultados de las riquezas.
- Desarrollar técnicas de *nowcasting* para reducir los retrasos existentes entre el informe y el año de referencia de los datos.
- Cada país debe recopilar estos resultados utilizando las fuentes de datos disponibles y de conocimiento especializado sobre la situación de su país.

CSSP. Agenda Ítem V. Encuesta de la OCDE sobre los impulsores de la confianza en las instituciones gubernamentales.

Posición del DANE

- Solicitar los resultados detallados de la encuesta, así como la información metodológica, con el fin de comprender mejor las características técnicas de esta operación estadística.
- Tener la posibilidad de ampliar la información de la experiencia realizada en el INEGI de México, por el método empleado para la recopilación presencial; asi mismo ampliar la recopilación de información en países como Finlandia o Irlanda
- Se espera seguir participando en los espacios de construcción para este tipo de mediciones y de compartir las experiencias respecto a la producción de información relacionada con este tema.

Temas clave

- El estudio presenta los principales factores que contribuyen a explicar las causas de la confianza en las instituciones gubernamentales y aporta pistas para comprender mejor los resultados y los retos que se presentan.
- Teniendo en cuenta las recomendaciones del informe sobre calidad y representatividad de la muestra en línea no probabilística, es importante que en los ejercicios futuros se revise tanto el tamaño de la muestra, su representatividad y el método para llevar a cabo la encuesta; dado que en el documento no se especifica el impacto al obtener una tasa de respuesta "baja" en la recolección

de los datos. Además, es importante considerar si las empresas seleccionadas deben proporcionar un análisis detallado o si se realiza en conjunto con los INE y las empresas o directamente los INE.

Próximas tareas

- Investigación de áreas adicionales de acuerdo a los hallazgos encontrados en la encuesta, desarrollando módulos, agregando preguntas o ampliando los existentes, con el fin de conocer factores específicos en la confianza pública.
- Mejorar la calidad y representatividad de las muestras en línea no probabilísticas, empleando preguntas en las encuestas nacionales para comprar las muestras. Se propone utilizar las preguntas de *Testing Trust Survey*, dado que es una muestra probabilística que permitirá conocer mejor la relevancia de los posibles problemas de precisión.
- Seguir evaluando y mejorando la validez estadística de las medidas de confianza, utilizado pruebas cognitivas y grupos focales de un conjunto de preguntas de la encuesta para ver cómo los encuestados en diferentes contextos interpretan la pregunta

CSSP. Agenda Ítem VI. Integración y aceleración del uso de datos geoespaciales.

Posición del DANE

El DANE ha desarrollado múltiples acciones que se alinean con los cinco flujos de trabajo del Laboratorio Geoespacial de la OECD:
1) Cuenta con una estrategia basada en la visualización digital y la pedagogía para la difusión y comunicación efectiva, utilizando videos, imágenes, infografías, GIF y el Geoportal, con el fin de promover el uso y apropiación de los recursos geoestadísticos disponibles.
2) Ha llevado a cabo operaciones estadísticas que tienen como objetivo obtener información específica y desagregada para la población étnica, al tiempo que se incluye a las comunidades en su cadena de valor estadística con el fin de promover un enfoque de equidad e inclusión, que esté en línea con el uso ético y responsable del mapa geoespacial.
3) Se ha desarrollado un geovisor para la consulta de información del pueblo indígena "Wayúu" el cual brinda información sobre resguardos indígenas para los procesos de difusión y promoción de la cultura estadística.
4) Desde 2015 se ha implementado el uso de imágenes satelitales para calcular los indicadores de los ODS relacionados con el objetivo 11, haciendo uso de la metodología proporcionada por ONU-Hábitat y las recomendaciones del Observatorio Urbano Global. Actualmente, hay tres indicadores calculados: 9.1.1. Proporción de la población rural que vive a menos de 2 km de una carretera para todas las estaciones, 11.3.1 Relación entre la tasa de consumo de tierra y la tasa de crecimiento de la población y 11.7.1 Proporción promedio del área urbanizada de las ciudades que es espacio abierto para uso público, por sexo, edad y personas con discapacidad.

Temas clave

El DANE está interesado en ser parte del trabajo realizado por las diferentes líneas de trabajo, en particular, en las discusiones de *Workstream 2* relacionadas con la presentación de propuestas para un conjunto de estándares éticos y mejores prácticas sobre el uso responsable de los datos geoespaciales y la creación de confianza pública, al mismo tiempo que promueve su uso generalizado.

Próximas tareas

El gobierno de Colombia ha definido la política de Catastro Multipropósito como una de sus principales prioridades. Esto permitirá contar con un inventario (o censo) de casas, lotes, terrenos o bienes inmuebles ubicados en el territorio nacional, en dominio público o privado, independientemente del tipo de propiedad dentro del Modelo de Dominio de Administración de Tierras - LADM. En este marco, se ha integrado la información geoespacial mediante el fortalecimiento de la Infraestructura Colombiana de Datos Espaciales - ICDE y se está trabajando en la construcción de un Observatorio Inmobiliario.

CSSP. Agenda Ítem VII b. Plan de Comunicaciones y difusión CSSP-SDD.

Posición del DANE

En 2021, el DANE lanzó su estrategia de comunicación digital sobre 7 principios de comunicación: 1) equilibrio, ii) economía del lenguaje, iii) información abierta, iv) intercambio de información, v) misión como componente de la cultura estadística, vi) información estadística y vii) consideración de las diferentes realidades. Esta estrategia tiene como fin garantizar que YouTube e Instagram tengan la misma relevancia y frecuencia de actualizaciones que Twitter y Facebook, donde el DANE tiene un mayor número de seguidores. Para ello, creó los siguientes productos:

- Postal Sonora: video con ilustraciones en las que la voz es la protagonista narra datos sobre temas de interés socioeconómico.
- DANE explica: video explicativo para YouTube sobre la metodología y medición de una investigación en particular.

Asimismo, las diferentes herramientas de difusión para la publicación de resultados (visores, contenido de páginas web, informes, resúmenes estadísticos, informes estadísticos sociodemográficos, entre otros.), se utilizan como herramientas socio-pedagógicas para fortalecer el uso, acceso y comprensión de la información estadística. De esta manera, se crea un proyecto transversal de sensibilización como estrategia para acercarse a los principales actores y fuentes de información.

Temas clave

- La personalización del contenido teniendo en cuenta la región es de gran importancia, pues los problemas y necesidades del público varían de acuerdo con la región donde este esté ubicado.
- El contenido debe producirse en el idioma de cada país o región.

CSSP. Agenda Ítem IX. Medición de la salud mental.

Posición del DANE

Identifico la necesidad de medir los cambios en el bienestar de las personas, con la Encuesta de Pulso Social, esta encuesta se empezó a desarrollar en julio de 2020 y es capaz de medir el bienestar subjetivo de la población de manera regular.

La Encuesta Pulso Social cuenta con indicadores sobre aspectos afectivo-emocionales, cognitivo-valorativos, significados o propósito de la vida.

Temas clave

La medición de la salud mental se está convirtiendo en una prioridad para las Oficinas Nacionales de Estadística, ya que las consecuencias de la pandemia en la salud a mediano y largo plazo van a afectar desproporcionadamente las condiciones mentales.

Próximas tareas

Recomienda que los países de la OCDE consideren la posibilidad de incluir las siguientes preguntas específicas en sus futuras encuestas para evaluar las enfermedades mentales, salud mental positiva y el estado general de salud mental.

- Enfermedad mental: La medida *Patient Health Questionnaire - 4 – PHQ - 4* combina dos preguntas de depresión de la escala PHQ-9 más larga y dos preguntas de ansiedad de la herramienta de detección GAD-7. El PHQ-4 cubre tanto la depresión como la ansiedad.
- Salud mental positiva: Utilizar los desarrollos específicos de la OMS para medir la salud mental positiva de manera estandarizada en todos los países.
-

Estado general de salud mental: Incluir preguntas relacionadas con la salud mental y la salud física como dos componentes separados.

CSSP. Agenda Ítem X. Medición del empleo y el trabajo en las plataformas digitales.

Posición del DANE

Desde 2017 el DANE elabora indicadores sobre la implementación de programas de Teletrabajo en las empresas, a través de preguntas insertadas dentro del módulo TIC de las encuestas económicas anuales (Manufactura, Comercio y Servicios).

Temas clave

A raíz de la pandemia, en 2020 se han evidenciado mayores desafíos en la medición de esta información, debido a que las medidas de confinamiento para la población hicieron que las empresas diseñaran nuevas estrategias para que su personal trabajara desde sus hogares conectados a través de internet como medida

temporal, por lo que no se presentan las mismas condiciones y características formales del teletrabajo definidas en la Ley. Teniendo esto en cuenta, y con el objetivo de regular el trabajo en el hogar por su masificación y los riesgos contractuales que implica, en agosto de 2021 se aprobó en Colombia la Ley 2121, que establece el llamado *trabajo remoto*.

La anterior ley incluye aspectos desde la regulación del modelo de conexión y derechos de desconexión hasta la cobertura de temas de seguridad social y el Sistema de Seguridad y Salud en el Trabajo (SGSST), esto ha generado mayores desafíos para la medición estadística de los indicadores de Teletrabajo porque debido al grado de complejidad de las definiciones utilizadas y al diseño probabilístico muestral de las encuestas de hogares, existen enormes retos de comprensión y medición representativa para los hogares y las personas, siendo esta una de las razones por las que en el DANE se están midiendo desde el punto de vista de las empresas, que son las fuentes que pueden tener mayor conocimiento y control de las políticas de teletrabajo o trabajo remoto implementadas para su personal. Sin embargo, la medición que se hace desde las empresas tiene limitaciones, como el hecho de que no tiene en cuenta el efecto del empleo digital en personas independientes o autónomos, o el tamaño de los directorios de las encuestas que solo van a determinados sectores económicos bajo parámetros de inclusión y no a todo el universo productivo.

La preparación del Reporte de esta edición participamos los siguientes funcionarios:

Dahann Valentina Pérez Zárate – dvperezz@dane.gov.co;

Erik Stopwar Arciniegas Rincón – esarciniegasr@dane.gov.co;

Heidy Patricia Forero Muhete – hpforerom@dane.gov.co;

Johana Catherine Ávila Alvarado – jcavilaa@dane.gov.co;

Juliana Catalina Pastás Pastás – jcpastasp@dane.gov.co;

Milena Del Rosario Escobar Morillo – mrescobarm@dane.gov.co;

Mónica Andrea Quiroga Rivera – maquirogar@dane.gov.co;

Revisión de estilo por: Juan Camilo Giraldo Manrique – jcgiraldom@dane.gov.co

Revisión de contenido por: Julieth Alejandra Solano Villa – jasolanov@dane.gov.co

Si tiene dudas comentarios o aportes sobre esta edición, por favor no dude en comunicarse al correo: dvperezz@dane.gov.co