

Nota Julio 2024: Esta versión se encuentra en proceso de publicación oficial con el director general del DNP. Por lo tanto, pueden presentarse cambios en el contenido. Agradecemos no publicar hasta tanto sea el documento final.

Retos y recomendaciones de interoperabilidad de la información en materia de control a la deforestación y defensa de los recursos naturales por parte del Sector Defensa



Retos y recomendaciones de interoperabilidad de la información en materia de control a la deforestación y defensa de los recursos naturales por parte del Sector Defensa

Bogotá D.C
2023

Derechos reservados ©
Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC) para la Región Andina y el Cono Sur

Las opiniones expresadas en el presente documento no comprometen ni vinculan a ninguna de las instituciones que hacen parte del proyecto, y sus contenidos son puntos de vista expresados por sus autores/as que no tienen otro fin que servir a manera de recomendaciones, por lo cual no se entiende que sean vinculantes.

Las denominaciones empleadas en este documento y la forma en que aparecen presentados los datos no implican, de parte de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) opiniones de las acciones internas del Estado colombiano.

La información sobre recursos y enlaces a sitios de internet contenidos en el documento se consigna para facilitar la consulta y es exacta al tiempo de la elaboración. Las Naciones Unidas no asumen ninguna responsabilidad por la exactitud de dicha información en el futuro ni por el contenido de sitios web externos. Además, la inclusión de referencias, vínculos o enlaces a otros documentos o sitios web no tiene la intención de asignar importancia a esos autores o sitios, y la información contenida en ellos, no tiene por objeto respaldar, recomendar o favorecer a las opiniones expresadas, o productos comerciales o servicios ofrecidos en estos sitios externos, o las organizaciones que patrocinan los sitios, por nombre comercial, marca comercial, fabricación, o de similar naturaleza.

Los puntos de vista y opiniones expresados en este documento no representan ni reflejan necesariamente las de las Naciones Unidas o de la UNODC, y no serán utilizados con fines publicitarios o de patrocinio de personas o productos.

Este documento fue elaborado en el marco del Proyecto *“Fortalecimiento del Estado de Derecho Ambiental”* apoyado por la Embajada Británica en Colombia e implementado por la Oficina de Naciones Unidas contra la Droga y el Delito – UNODC – Colombia (2023).

Retos y recomendaciones de interoperabilidad de la información en materia de control a la deforestación y defensa de los recursos naturales por parte del Sector Defensa

Oficina de las Naciones Unidas contra la Droga y el Delito para la Región Andina y el Cono Sur (UNODC)

Candice Welsch, Representante Regional de UNODC

Olivier Inizan, Representante Regional Adjunto de UNODC

Diego Ricardo Quintero Martínez, Coordinador del Área de Crimen Organizado

Joel Salek, Coordinador (a.i) del Programa de Prevención y Justicia Ambiental

Elaborado por:

Programa de Prevención y Justicia Ambiental – Área de Crimen Organizado

Lizet Arcos Mendez

Líder en Políticas Públicas en Deforestación

Manuel David López Villadiego

Profesional Esp. En Monitoreo y Seguimiento de Proy. Ambientales

Subdirección de Seguridad y Defensa del Departamento Nacional de Planeación

Sidney Cruz Pinilla

Asesora

Equipo de apoyo UNODC

Adriana Quintana, Líder en Deforestación

Catherine Duarte, Profesional SIG

2023

Bogotá D.C. – Colombia

Contenido

1. Introducción	5
2. Metodología	6
3. Información en las instituciones del sector defensa	6
3.1. Ministerio de Defensa Nacional	6
3.2. Comando General	8
3.3. Ejército Nacional	10
3.4. Fuerza Aérea	10
3.5. Policía Nacional	11
3.6. Defensa Civil	12
4. Barreras para interoperabilidad en el Sector Defensa	13
4.1. Dominio Político - Legal	13
4.2. Dominio Organizacional	15
4.3. Dominio Técnico	18
4.4. Dominio Semántico	19
5. Recomendaciones para la interoperabilidad en el Sector Defensa	19
5.1. Recomendaciones para fortalecer las capacidades institucionales instaladas de las entidades del sector defensa	20
5.2. Recomendaciones para superar las barreras de la interoperabilidad de información del sector Defensa y Seguridad	22
6. Bibliografía	26

1. Introducción

El presente documento hace parte de los productos desarrollados en el marco del Proyecto “Fortalecimiento del Estado de derecho ambiental” (Pilar II de TEFOS) apoyado por el Reino Unido y facilitado por la Oficina de Naciones Unidas Contra la Droga y el Delito. Proyecto que busca desarrollar acciones para abordar los motores de la deforestación, los delitos ambientales en Colombia y la defensa del medio ambiente. Su elaboración se llevó a cabo con la participación permanente de la Subdirección de Seguridad y Defensa del Departamento Nacional de Planeación, y en consulta permanente de las instituciones que hacen parte del sector Defensa y Seguridad: Ministerio de Defensa, Ejército Nacional, Fuerza Aérea, Policía Nacional y Defensa Civil.

Las instituciones del sector Defensa y Seguridad destacan que producen información útil y relevante e identifican que la información generada tendrá mayor relevancia al forjar dinámicas de intercambio de información con otros actores, puesto que les permitirá reconocer las dinámicas del sector (particularmente para el control a la deforestación y la defensa del ambiente) por tanto, ser más eficientes en la planeación estratégica y operacional, reducir costos, tiempos y optimizar los aportes del recurso humano disponible.

Por lo anterior, las recomendaciones sugeridas en el presente documento se constituyen en un aporte para superar las barreras y/o retos existentes en las instituciones para la interoperabilidad. Siendo un aporte para dinamizar el intercambio de información (general y con base en la evidencia) para la toma de decisiones en el ejercicio de las funciones misionales de las entidades.

El documento está dividido en tres acápites, el primero detalla la gestión institucional de las entidades que hacen parte del sector Defensa y Seguridad; en el segundo, son descritos las barreras para la interoperabilidad de la información en los dominios político legal, organizacional, técnico y semántico; por último, las recomendaciones para dinamizar la interoperabilidad de la información en las instituciones que pertenecen al sector Defensa y Seguridad

2. Metodología

La construcción del presente documento tuvo como punto de partida la consulta de información secundaria, de lo cual se destaca los siguientes documentos:

- Marco de interoperabilidad para el gobierno digital del Ministerio de Tecnologías de la información y la comunicación (2019).
- Diagnóstico de la capacidad instalada en los componentes humano, técnico, tecnológico e interoperabilidad de instituciones priorizadas de la Oficina de Naciones Unidas Contra la Droga y el Delito (2022).

Posteriormente, una vez identificadas las categorías claves a indagar (Político Legal, Organizacional, Técnico y Semántico) se llevaron a cabo tres jornadas¹ para profundizar sobre las limitantes que impiden la interoperabilidad de la información e identificar de oportunidades de mejora. Este ejercicio, fue desarrollado con el uso de la técnica de **Ábaco de Regnier** que consiste en la consulta a expertos, quienes para el desarrollo de este producto eran los actores en representación de las instituciones del sector Defensa y Seguridad.

El total de la información recopilada durante las tres jornadas fue sistematizada y analizada a través de las categorías analíticas propuestas, para la identificación de los barreras y retos para la construcción de las recomendaciones propuestas.

3. Información en las instituciones del sector defensa

A continuación son descritos los sistemas de información con los que cuentan cada una las instituciones que hacen parte del sector defensa y seguridad.

3.1. Ministerio de Defensa Nacional

El Ministerio de Defensa Nacional de Colombia (Mindefensa) es la máxima autoridad del país en materia de defensa, seguridad y asuntos militares. Tiene a su cargo la formulación, diseño, desarrollo y ejecución de las políticas de defensa y seguridad nacional²; conduce la Fuerza Pública, la cual está conformada por:

¹ 21 y 28 de noviembre, y 5 de diciembre de 2023.

² Fuente: Art 4. Decreto Número 1512. 11 de agosto de 2000.

- Fuerzas Militares, (Ejército Nacional, Armada Nacional, Fuerza Aérea),
- Policía Nacional.
- Defensa Civil Colombiana (Institución Social y Humanitaria de Rescate y Socorro) por adscripción.

En lo referente al manejo de la información, el Ministerio de Defensa Nacional, en su esfuerzo constante por mejorar la calidad de la información estadística del Sector Defensa y Seguridad, elaboró en marzo de 2013 la Directiva Permanente No. 004 sobre “Lineamientos generales para la gestión de la información estadística del Sector Defensa y Seguridad”, la cual fue modificada por la Directiva 013 de 2022, como consecuencia de la reestructuración del Ministerio en diciembre de 2021, mediante Decreto 1874.

Esta Directiva se creó con el objetivo de emitir lineamientos para la consolidación, estandarización y gestión de la información estadística producida en el Sector, con el fin de armonizar el esfuerzo institucional, implementar mecanismos de intercambio de datos, asignar responsabilidades a las diferentes instancias que intervienen en la producción de la información estadística y de esta manera, garantizar altos niveles de calidad y confiabilidad.

Igualmente, en el marco de esta directiva, se creó el Comité de Gerencia de la Información Estadística del Sector (CGIES), el cual se encarga de establecer la estandarización de los procesos de homologación de conceptos, almacenamiento, recolección, difusión y regulación de las metodologías utilizadas para la producción de información, el cual formalizó su creación mediante la Resolución 5016 de 2022.³

Actualmente, el Observatorio de Derechos Humanos y Defensa Nacional – ODHDN realiza la consolidación de información de delitos y de resultados operacionales de la Fuerza Pública, en este proceso, el Sistema de Información de Seguridad y Defensa (SISyD) se alimenta de la información proveniente del BISIGOI del Comando General de las Fuerzas Militares, el cual reúne la información reportada en los sistemas de información del Ejército Nacional (SICOE), la Armada Nacional (SIGO) y la Fuerza Aérea Colombiana (SIIOC2). Respecto a la información de operatividad de la Policía Nacional, el SISyD toma la información proveniente del SIEDCO y finalmente el SISyD obtiene la información de desmovilizados y sometimiento a la justicia a través del SIGAHD.

³ Metodología para la Consolidación de la Información Estadística del Sector Defensa y Seguridad Nacional

Gráfico 1 - Consolidación de la información estadística del Sector Defensa y Seguridad Nacional



Fuente: Metodología para la Consolidación de la Información Estadística del Sector Defensa y Seguridad Nacional

3.2. Comando General

El Comando General de las Fuerzas Militares – COGFM es la entidad de más alto nivel de planeamiento y dirección estratégica para las instituciones castrenses de Colombia y está conformado por el Ejército Nacional de Colombia, la Armada de Colombia y la Fuerza Aérea Colombiana.

De sus dependencias emanan las directrices y las políticas de mando para los soldados de tierra, mar, aire y río en estricto y cabal cumplimiento de la misión prevista en el artículo 217 de la Constitución Nacional.

El manejo de la información ambiental desde el CGFM se administra a través de varias dependencias, por parte del Ejército Nacional los temas ambientales se centran en dos dependencias: por un lado, lo referente a la parte operacional y por otra parte los temas planeación:

- Departamento Conjunto Ambiental y de Gestión del Riesgo de Desastres, encargado de Asesorar al Comandante General de las Fuerzas Militares y a las Fuerzas en los temas relacionados con gestión ambiental, protección ambiental y gestión del riesgo de desastres en el nivel estratégico estableciendo coordinaciones eficientes con las Fuerzas Militares y las instituciones relacionadas con estos temas a nivel nacional.
- Departamento Conjunto de Amenazas Transnacionales a cargo de los temas operacionales.

Con el propósito de mejorar la gestión ambiental, desde el CGFM se hacen esfuerzos permanentes en la implementación de Sistemas de Información Ambiental, en este sentido y en línea con el plan de guerra (espada de honor – 2012) se identificó la necesidad de mejorar el acceso a la información geográfica con el fin de mejorar la interoperabilidad, iniciativa que se logró hasta el 2022 con la creación del Business Intelligence Sistema de Información Gerencial del Centro Operaciones e Inteligencia del Comando General de las Fuerzas Militares – BISIGOI. Este aplicativo denominado permite consolidar la información de los resultados operacionales producidos por los sistemas del Ejército Nacional (SICOE), la Armada Nacional (SIGO) y la Fuerza Aérea Colombiana (SIIOC2).

El Comando General de las Fuerzas Militares, a través del BISIGOI, extrae la información mediante procesos de cargue programados que consultan los datos autorizados y expuestos de las Fuerzas hacia Comando General. Durante este proceso el sistema realiza una validación registro a registro con el fin de mantener la homologación de los datos y controlar la creación de variables con la debida autorización del CGIES. Finalmente, una vez se realiza cada registro, los procesos almacenan los datos en un único sistema para ser utilizado como fuente de información operacional oficial de las Fuerzas Militares.

El personal encargado del BISIGOI, el Sistema de Información donde se consolidan los resultados de las operaciones de las Fuerzas Militares, diariamente, hace revisiones de la información consolidada con el fin de garantizar que no se tenga ningún problema de duplicidad o de incongruencia en la información.⁴

Gráfico 2 - Proceso de Consolidación de información del Comando General de las Fuerzas Militares (COGFM)



Fuente: Metodología para la Consolidación de la Información Estadística del Sector Defensa y Seguridad Nacional

⁴ Metodología para la Consolidación de la Información Estadística del Sector Defensa y Seguridad Nacional

3.3. Ejército Nacional

El Ejército Nacional de Colombia es la fuerza militar terrestre legítima que opera en todo el territorio nacional, tiene a cargo el desarrollo de operaciones militares orientadas a la defensa de la soberanía, la independencia y la integridad territorial y a la protección de la población civil y los recursos privados y estatales para contribuir a generar un ambiente de paz, seguridad y desarrollo, que garantice el orden constitucional de la Nación.

Para el manejo estadístico de su información, el Ejército Nacional cuenta con un Sistema de Información de Comando Ejército – SICOE, el cual es un aplicativo Web, que puede ser utilizado de forma remota desde cualquier equipo conectado a la red del Ejército Nacional, favoreciendo su uso en todas las Brigadas, Divisiones y en la Jefatura de Operaciones.

En cada Brigada y División se asignan usuarios con permisos de acceso que admitan el cargue de información operacional, la cantidad de usuarios puede variar en cada unidad, pero se requiere como mínimo el nombramiento de dos usuarios en cada Brigada y División, idealmente pertenecientes a la sección de operaciones y/o de la sección de comunicaciones de la unidad. Estos usuarios están debidamente capacitados y como medida de seguridad y control se les asigna una clave individual, con el fin de poder conocer en todo momento qué cambios se realizan en el sistema y el autor de estos.

El SICOE está permanentemente conectado al BISIGOI del Comando General de las Fuerzas Militares, por lo cual, cualquier evento que se cargue por alguna unidad del Ejército puede ser visualizado de inmediato en el BISIGOI facilitando la interoperabilidad de los sistemas.

3.4. Fuerza Aérea

La Fuerza Aeroespacial Colombiana – FAC es una de las tres instituciones de las Fuerzas Militares de Colombia, encargada de ejercer y mantener el dominio del espacio aéreo para defender la soberanía, integridad territorial y el orden constitucional.

El manejo de la información generada desde la FAC se lleva a cabo a través del Sistema Integrado de Información Operacional e Inteligencia de Comando y Control (SIIOC2), herramienta que se implementa desde el año 2005, y que ha evolucionado técnicamente en la mejora en las plantilla y módulos para una mayor precisión en la información alojada y generada por este aplicativo. En él, se registra el resumen de cada operación realizada por la institución, facilitando permite la búsqueda de registros históricos de algunas variables a partir de 2007 y otras a partir de 2019 de una manera práctica y sencilla, así como la seguridad de esta.

Los registros administrativos brindan una especificación detallada como: unidad que efectuó la operación, horas voladas por aeronave, pasajeros y carga transportada, entidad apoyada, hora inicio y término de la operación, material de guerra empleado y novedades ocurridas en el cumplimiento de la operación, número de requerimientos cumplidos y llegados, número de operaciones en recuperación de personal y cantidad de pacientes o personal trasladado (enfermo o herido); número de operaciones de extinción de incendios, número de descargas y cantidad en galones de agua o retardante lanzado, entre otros resultados operacionales.

La FAC cuenta con un Centro de Comando y Control – CCOFA, desde donde se controlan la totalidad de las operaciones aéreas, en línea con el principio de control centralizado y ejecución descentralizada, que contribuye en la planeación, dirección, coordinación y el control de las operaciones desde la perspectiva aérea. El desarrollo de las operaciones aérea está basado en requerimientos operativos de entidades civiles, gubernamentales, militares, policiales e internos de la FAC, que son recibidos por el Comando de Operaciones Aéreas y Espaciales – COAES y las unidades aéreas. Dichos requerimientos son ingresados al aplicativo SIIOC2 para el planeamiento, ejecución y desarrollo de las operaciones aéreas, lo cual apoya el proceso misional de la FAC y la contribución a los fines del Estado.⁵

3.5. Policía Nacional

La Policía Nacional de Colombia es un cuerpo armado de naturaleza civil, a cargo de la seguridad pública de la República de Colombia. La institución a través del Sistema de Información Estadístico Delincuencial, Contravencional y Operativo – SIEDCO, dispone de información de delitos y resultados operacionales realizados por la entidad en el territorio nacional e internacional. Este sistema está integrado por la base de datos SIEDCO la cual contiene variables estandarizadas y la herramienta de inteligencia de negocios SIEDCO PLUS, la cual permite la extracción, transformación y presentación de la información alineada con indicadores delictivos y operativos.

El flujo de datos hacia el sistema de información se realiza de forma sistemática y permanente los 365 días del año, a partir de varias fuentes de información, quienes a su vez establecen mecanismos de validación, que aunados a los procesos de verificación y validación de los datos permiten dar consistencia y calidad a los mismos.

⁵ Metodología para la Consolidación de la Información Estadística del Sector Defensa y Seguridad Nacional

Así mismo, y con el propósito de verificar la calidad de los datos y la información disponible en el sistema, la Policía Nacional y la Fiscalía General de la Nación, realizan periódicamente cruces de la información contenida en las bases de datos SIEDCO (Policía Nacional) y el Sistema Penal Oral Acusatorio – SPOA (Fiscalía General de la Nación). Lo anterior, se lleva a cabo con el fin de unificar conceptos sobre el delito de hurto y homicidio, en las variables de caracterización y modalidades, que sirvan de orientación a los analistas de la Fiscalía General de la Nación y funcionarios de policía judicial de la Policía Nacional de Colombia, encargados del ingreso de las noticias criminales e información administrativa sobre el hecho punible en las bases de datos.

La captura de la información delictiva, operativa y otras conductas, se realiza a partir de la información contenida en registros administrativos, la cual es consignada en formularios dispuestos en la web desplegados desde el SIEDCO y la obtenida a partir de la intercomunicación con otros sistemas de información, esto con el fin de disponer de una base de datos robusta que se nutre de 4 fuentes:

- Boletín Informativo Policial
- Web service para el intercambio de las noticias criminales entre SPOA y SIEDCO
- Sistema de Denuncias y Contravenciones (SIDENCO)
- Sistema Nacional de Denuncia Virtual ¡A Denunciar!⁶

3.6. Defensa Civil

La Defensa Civil Colombiana es un establecimiento público, descentralizado, del orden nacional, con autonomía administrativa adscrito al Ministerio de Defensa Nacional. Tiene a cargo el desarrollo de procesos en gestión del riesgo de desastres, acción social, gestión ambiental y programas de educación dirigidos al voluntariado y a la comunidad, para contribuir a la seguridad humana y responder a compromisos de orden internacional.

Para la gestión de la información y los datos generados desde la entidad, la Defensa Civil cuenta con el Sistema de Información Misional – SIM como herramienta para recopilar, procesar, almacenar y distribuir datos relevantes para el cumplimiento de la misión de la entidad de forma eficiente y efectiva. Asimismo, ha implementado de manera efectiva el software ArcGIS en el marco de su programa de reforestación “Bosque Naranja”, el cual se beneficia de la capacidad de ArcGIS para la georreferenciación, permitiendo la generación y conservación de información cartográfica detallada sobre las áreas impactadas por el proyecto. Este enfoque basado en la tecnología contribuye

⁶ Policía Nacional, “Documento Guía del SIEDCO”.

significativamente a la planificación estratégica y sostenibilidad a largo plazo del programa de reforestación.

4. Barreras para interoperabilidad en el Sector Defensa

A continuación, son descritas las barreras cualitativas identificadas por las instituciones del sector Defensa y Seguridad que participaron de las consultas llevadas a cabo en las jornadas de trabajo, elementos que son enunciados según los cuatro dominios definidos por el Ministerio de la información y la comunicación - MINTIC, para tener una aproximación holística de las interacciones en las instituciones que facilitaran la interoperabilidad de la información.

4.1. Dominio Político - Legal

Este dominio corresponde a la disposición de políticas y normas que permiten el intercambio de información, a través del establecimiento de instrumentos legales que facilitan la prestación de servicios de intercambio de información; la responsabilidad legal para la provisión de los servicios de intercambio de información de cada una de las partes involucradas; y, la garantía del manejo adecuado de la información confidencial y protección de datos personales. (Mintic, 2019. Pg. 33).

4.1.1. Normatividad para el intercambio de información

El Ministerio de Defensa y Seguridad con la Directiva permanente del 03 del 2022 fijó los lineamientos para la gestión de la información estadística del sector Defensa y Seguridad⁷. No obstante, aunque existe el citado lineamiento no han obtenido los resultados esperados frente a la información que esperan recopilar como sector. Esta situación ha sido justificada por la falta de una directriz institucional de alto rango que ordene su cumplimiento, a su vez por la falta de capacidades técnicas, operativas y de infraestructura que son necesarias para la generación de información por parte de todas las instituciones.

⁷ Para el intercambio de datos a través de sistemas de información interoperable, asignar responsabilidades, armonizar esfuerzos institucionales para generar información estadística del sector que sea confiable, de calidad y basada en definiciones, conceptos y estándares nacionales e internacionales

También se visibilizó que, algunas de las instituciones del sector carecen de la definición de normatividad institucional interna que se materialice en procesos o procedimientos y que caractericen la información según el tipo de información: pública, confidencial, super confidencial o reservada; las condiciones de entrega según actor: internos (otras dependencias) y externos (entidades del sector defensa u otros sectores y ciudadanía; los medios de entrega; datos abiertos o por solicitud; la periodicidad de producción de la información, responsables y la definición de los controles de seguridad identificados (acceso y consulta) para minimizar los riesgos mencionados que han sido identificados (perdida, alteración, fuga de información, entre otros).

En particular, la reserva de la información es calificado como un aspecto muy importante para las instituciones del sector Defensa y Seguridad, para la generación de procesos de interoperabilidad en el sector, lo argumentaron con:

- Se han presentado situaciones de mal uso de la información, situación que pone en riesgo los resultados operacionales.
- No se puede poner a disposición los resultados operacionales del público en general, siempre se debe hacer un trabajo de procesamiento de datos, en particular para entregar respuestas de derechos de petición.
- No se ha definido claramente la clasificación de la información (lo que debe estar reservado o no). Aunque la ley de inteligencia define claramente que información es reservada y cual no.

Las instituciones mencionaron que, los mecanismos usados para el intercambio de información (datos o imágenes) son gestionados a través de convenios o acuerdos de entendimiento, lo cual limita (en algunos casos) el tipo de información, la periodicidad y regularidad, puesto que, el acceso a la información queda supeditada a los términos pactados en el acuerdo de intercambio.

Como buena práctica para la consulta y el intercambio regular de la información, la Dirección de Carabineros y Protección Ambiental referenció los convenios con el Ministerio de Ambiente y Desarrollo Sostenible, IDEAM y Fiscalía General de la Nación, en donde en algunos asuntos tienen acceso para la consulta de información permanentemente. Por su parte, la Defensa Civil manifestó que el lineamiento técnico - normativo para la institución se deriva de la Política Ambiental del Sector Defensa, y el reciente aprobado plan de Plan Integral de Gestión del Cambio Climático del Sector Defensa, enfatizaron que, por ahora no llevan a cabo procesos de interoperabilidad de información con otras entidades.

4.2. Dominio Organizacional

Este dominio para la interoperabilidad hace referencia al modo en que las instituciones contribuyen a través de procesos de intercambio de información la consecución de metas de comunes. Para lograrlo, las instituciones deben previamente tener identificado y definido como se llevan a cabo las actividades de integración, adaptación, definición de procesos, trámites o servicios a nivel interno que facilitaran la interoperabilidad de la información dentro de la entidad. Así como, la generación de competencias y la habilitación de los medios de colaboración interna con otras entidades.

4.2.1. Liderazgo en el marco de la interoperabilidad

En las instituciones del Sector Defensa y Seguridad no existen un liderazgo por parte de alguna de las entidades que guíe los procesos de gestión del conocimiento del sector para el abordaje de temáticas ambientales. Por tal motivo, se observan esfuerzos aislados dentro de las entidades para la consecución de resultados institucionales. Lo anterior se ve reflejado en situaciones tales como:

- Las instituciones han identificado que sus dependencias (direcciones, áreas, grupos de trabajo) es mínima la articulación para la atención de casos de delitos ambientales. Esta barrera, eventualmente fue superada por directriz desde el Comando General.
- El desconocimiento de los procesos para la atención de casos que son gestionados en las distintas dependencias tiene como resultado esfuerzos aislados (adquisición de software, compra de imágenes, entre otros), lo que puede generar reprocesos frente a compra de imágenes y duplicidad de compras.
- Existen capacidades especializadas en los equipos de trabajo que son desaprovechados al no conocerse la gestión que realizan, los perfiles del personal con el que se cuenta y los resultados obtenidos.

La falta de articulación interinstitucional permanente en el sector Defensa es destacada y justificada en la necesidad de conocer la información y gestión que adelantan las otras entidades, y, cómo cada una ellas pueden aportar a la resolución de casos. Ejemplo de ello es la intervención para la explotación ilícita de yacimientos mineros, en donde manifestaron han obtenido resultados importantes como sector.

Este espacio interinstitucional se caracteriza por: confluyen todas las instituciones del sector, comparten información permanentemente, hay un

liderazgo visible desde el Ministerio de Defensa. Lo cual no ocurre con el abordaje de otros delitos ambientales dada la ausencia de liderazgo o direccionamiento estratégico del sector.

Enfatizaron que, la información compartida en espacios interinstitucionales les ha permitido reconocer que las manifestaciones del multi-crimen que varían y responden de manera diferente según el contexto y región donde es abordado.

4.2.2. Cultura organizacional

Con la identificación de los limitantes para la interoperabilidad de la información se evidenció que son mínimos los procesos que promueven la generación de una cultura organizacional que se consolide en pautas para el intercambio de información a través de capacitaciones al recurso humano, comunicaciones internas, campañas a todos los involucrados en el proceso de producción de datos e información en las entidades que hacen parte del sector.

En algunos casos, el recurso humano que maneja la información que es susceptible de interoperabilidad señalaron que, aunque se llevan a cabo capacitaciones regulares éstas no son suficientes; puesto que existen temas en los que se requiere una la apropiación técnica especializada (ingenieros catastrales, ambientales y forestales, profesionales SIG, entre otros) para el abordaje de algunos asuntos ambientales. Particularmente, la Policía Nacional manifestó que tienen vacíos de conocimientos especializados cuando están adelantando procesos de investigación e inteligencia, estos vacíos han generado que la carga probatoria del proceso no tenga la robustez necesaria ante el juez.

Contar con capacidad técnica especializada, es un elemento clave, en referencia de la Fuerza Aérea, mencionaron que han fortalecido sus procesos de análisis ambiental con la vinculación de profesionales en sus plantas de personal (topógrafos, geodestas, ingenieros), quienes se encargan de producir información especializada a partir de conocimientos técnicos (parámetros de una información geográfica y metadatos, entre otros) lo que les ha permitido la generación de datos con precisión técnica y en el marco de procesos rutinarios. Asimismo, Defensa Civil referenció que cuentan con un ingeniero geógrafo especialista sistemas de información geográfica, encargado del análisis de la cartografía en mantenimiento, conservación y análisis de los datos.

En cuanto a la apropiación temática ambiental se identificó que existe un reconocimiento diferenciado de las problemáticas ambientales, particularmente con el abordaje de la deforestación, algunas instituciones analizaban la problemática de la deforestación a partir de factores dinamizadores y determinadores (motores de deforestación), mientras que, otros de los actores

institucionales lo abordaban a partir de las situaciones referenciadas en el marco del cumplimiento de sus funciones de prevención y control.

Por último, se identificó que existe en las instituciones del sector **resistencia al cambio**, particularmente se observa en que las entidades tienen resistencia a entregar información para la consolidación de resultados integrados como sector. Al respecto, describieron situaciones como “*existen celos o egos*” entre las dependencias y entre las instituciones a la hora de visibilizar resultados.

Lo anterior, visibiliza que no existen procedimientos guía que orienten la difusión de la información en las instituciones y que establezcan pautas de comunicación en donde sean claramente visibilizados los resultados obtenidos con aportes de terceros (otras instituciones).

4.2.3. Adecuación de procesos

La gestión por procesos en las instituciones permite trazar la ruta para la obtener resultados en cumplimiento de las funciones misionales, en particular para este caso, relacionados con temas ambientales. Con la definición de los procedimientos internos para el manejo de información ambiental, las entidades definen clara y abiertamente, cuáles son los resultados a alcanzar como entidad o sector en la atención de casos de importancia ambiental.

Los procesos al interior de las instituciones, que incluyen la gestión de datos e información deben estar documentados, para garantizar que exista un flujo permanente de información (calidad y datos relevantes). A pesar de ello, Observatorio de Derechos Humanos y de Defensa Nacional⁸ encargado de gestionar la información estadística del sector, referenció que la información que se requiere en el marco de la Directiva permanente del 03 del 2022 no cuenta con calidad, frecuencia y suficiencia requerida para el procesamiento y producción permanente de información.

Por otro lado, una de las barreras de mayor importancia es la **falta de recursos presupuestales** para la adquisición y desarrollo tecnológico para los procesos de interoperabilidad de la información, así como el desarrollo propio de las actividades misionales, al respecto referenciaron:

- Si no hay recursos no se puede ejecutar actividades preventivas y operativas, las horas de vuelo son muy costosas.
- El mantenimiento de sistemas de información en infraestructura propia o en la nube, pueden ser muy costosos.

⁸ Viceministerio para las políticas de Defensa y Seguridad Nacional del Ministerio de Defensa

- La financiación de control a la deforestación es muy costosa, debido a los lugares lejanos en donde están ubicados, por ejemplo: PNN.

Por último, fue señalado que **existe desconocimiento de la oferta de la información institucional**. En cuanto a qué información se produce y quién lo produce (responsable), puesto que es un elemento clave para avanzar en los procesos de interoperabilidad, debido a que no existen unos canales claros de comunicación.

4.3. Dominio Técnico

Este dominio para la interoperabilidad hace referencia a las aplicaciones e infraestructuras tecnológicas que conectan sistemas de información, mediante los servicios de intercambio de información. Incluye aspectos como especificaciones de interfaz, protocolos de interconexión, servicios de integración de datos, presentación e intercambio de datos y protocolos de comunicación seguros (Mintic, 2019. Pg. 47). En otras palabras, bajo este componente, son observados todos los aspectos tecnológicos que debe tener apropiado las entidades para garantizar los procesos de interoperabilidad funcional y no funcional.

Uno de los aspectos señalados como importante por parte de las instituciones del sector defensa es la **incompatibilidad de los sistemas de información**, argumentado en la necesidad de analizar la información en contexto, por ejemplo, observar un lugar específico en contraste con datos suministrados por el IDEAM o el IGAG.

Aunque, algunas instituciones del sector referenciaron que ya tienen apropiados Sistemas de Información (Biblioteca Nacional, BISIGOI o SIEDCO) para el abordaje ambiental u otros temas, el panorama general es que en la mayoría de los casos no existen infraestructura y desarrollos tecnológicos para la recolección de información, por lo tanto los procesos de análisis son llevados a cabo con el uso herramientas office (Excel), información que es compartida a través de informes de gestión (Word), lo cual genera reprocesos cuando otra institución (receptora) requiere llevar a cabo análisis de la información recopilada. Al respecto referenciaron situaciones como:

- Cuando se pasa la información de Excel a BISIGOI nos puede arrojar unos 1300 datos de error.
- La información que nosotros tenemos (Biblioteca Nacional de la Fuerza) pues es una información muy robusta, la cual no es fácil de enviar, tenemos que hacerlo todo manual, en ocasiones se entrega en discos y etc.

En los escenarios de consulta con expertos la **actualización constante del software** no se considera un tema relevante, no obstante, hubo referencia a que la alta dependencia del uso de tecnología en los procesos representa una vulnerabilidad que debe tenerse en cuenta en las instituciones.

4.4. Dominio Semántico

El dominio semántico debe garantizar que el intercambio de datos, la información y su significado sea exacto para todos los interesados (instituciones, ciudadanía, entre otros) a través de lenguaje común y de consolidación de información estandarizada.

Frente al lenguaje común fue visibilizado la necesidad de establecer los estándares de información para todas las instituciones del sector a través de la **estandarización de formatos y homologación de conceptos**, identificando para cada una: ¿qué información produce?, ¿qué información requiere?, ¿quiénes producen la información relevante para el sector, tanto de otras instituciones como del sector privado?, garantizando a su vez, las condiciones de calidad de los datos que se producen para generar flujos de información permanente.

5. Recomendaciones para la interoperabilidad en el Sector Defensa

Con el siguiente acápite son señaladas las recomendaciones generales que se proponen sean abordadas por el sector Defensa y Seguridad para avanzar en el proceso de interoperabilidad de los sistemas de información. En la primera parte el énfasis de las recomendaciones se sitúa en la capacidad instalada que soporta desde aspectos humanos, técnicos y procedimentales los procesos de interoperabilidad en las entidades; en la segunda, enfatiza en los aspectos básicos para el proceso de interoperabilidad de la información, desde los dominios político legal, organizacional, técnico y semántico.

5.1. Recomendaciones para fortalecer las capacidades institucionales instaladas de las entidades del sector defensa.

Se recomienda llevar a cabo la revisión de las capacidades institucionales en cumplimiento de los lineamientos de las políticas para la gestión y desempeño institucional. Toda vez que, las políticas en mención enfatizan en el conjunto de orientaciones que inducen procesos de modernización en la gestión organizacional y funcional de la Administración Pública para el fortalecimiento de los niveles de gobernabilidad y legitimidad del Estado (Artículo 2.2.22.2.1. Decreto 1499 de 2017). En particular sobre los siguientes aspectos:

En direccionamiento estratégico y planeación institucional

Se sugiere a las instituciones del sector avanzar en caracterizar los grupos de valor⁹ (ciudadanos, instituciones, ONG, academia, privados, entre otros) que requieren información sobre la gestión institucional y resultados en materia ambiental y deforestación. Esto les permitirá clasificar y disponer la información como datos abiertos al público e identificar qué información es confidencial y reservada. A su vez, documentar los procedimientos para la entrega de información (disposición de la información para consulta libre o en respuesta a derechos de petición).

Este proceso se sugiere teniendo en cuenta que, el intercambio de información para las instituciones del sector Defensa tiene limitantes legales, particularmente según lo señalado en la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional¹⁰ (1712 de 2015) donde están establecidas las excepciones: El artículo 18 establece como información exceptuada, el daño de derechos a personas naturales o jurídicas¹¹, mientras que en el artículo 19 hace

⁹ De acuerdo con la definición contemplada en el Manual operativo de Modelo Integrado de Planeación y Gestión, los grupos de valor son personas naturales (ciudadanos), jurídicas (organizaciones públicas o privadas a quienes van dirigidos los bienes y servicios de una entidad) o individuos u organismos específicos receptores de los resultados de la gestión de la entidad.

¹⁰ Esta política le permite a la entidad articular acciones para la prevención, detección e investigación de los riesgos de en los procesos de la gestión administrativa y misional de las entidades públicas, así como garantizar el ejercicio del derecho fundamental de acceder a la información pública a los ciudadanos y responderles de buena fe, de manera adecuada, veraz, oportuna y gratuita a sus solicitudes de acceso a la información pública.

¹¹ "La información exceptuada por daño de derechos a personas naturales o jurídicas. Corresponde a toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiese causar un daño a los siguientes derechos de intimidad, vida, salud y seguridad, y los secretos comerciales, industriales y profesionales.

referencia al daño a los intereses públicos¹², además lo estipulado en la Ley de inteligencia y contrainteligencia, Ley 1621 de 2013.

Adecuación de procesos

La gestión por procesos en las instituciones les permite trazar la ruta para la alcanzar los resultados en cumplimiento de las funciones misionales relacionados con la atención delitos ambientales. Con la definición de los procedimientos internos para el manejo de información, las entidades del sector Defensa y Seguridad definen clara y abiertamente, cuáles son los resultados a alcanzar como institución y sector en torno a atención de asuntos ambientales y deforestación.

Siguiendo los lineamientos de la Política de Fortalecimiento Institucional y Simplificación de Procesos¹³ se sugiere identificar los puntos críticos que expliquen por qué la institucionalidad actual no es adecuada para la entrega de productos y servicios para la gestión ambiental y de deforestación. Con esto claro, será posible identificar y resolver las tensiones y actividades necesarias para lograr un fortalecimiento organizacional, o rediseñar lo necesario, particularmente frente a:

- Revisar técnicamente si la arquitectura institucional es la más adecuada, bajo los preceptos de la eficiencia, la productividad y la generación de valor público, en la generación de resultados para atención de delitos ambientales y deforestación.
- Medir el impacto que en materia presupuestal de las instituciones (interna) para la atención eficaz de los asuntos ambientales y deforestación, y para garantizar la asignación de recursos en cada anualidad presupuestal.
- Promover reformas de planta de empleos para garantizar los perfiles requeridos (según necesidades identificadas) en materia ambiental en las áreas funcionales con atención a temas ambientales.

Para la consolidación de la información estadística se recomienda adoptar para todos los procesos que incluyen gestión ambiental y deforestación los lineamientos de la política de información estadística¹⁴:

¹² Información exceptuada por daño a los intereses públicos. Es toda aquella información pública reservada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional: La defensa y seguridad nacional; La seguridad pública; La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso; El debido proceso y la igualdad de las partes en los procesos judiciales; Entre otros”.

¹³ El propósito de esta política es fortalecer las capacidades organizacionales mediante la alineación entre la estrategia institucional y el modelo de operación por procesos, la estructura y la planta de personal, de manera que contribuyan a la generación de mayor valor público en la prestación de bienes y servicios, aumentando la productividad estatal (recuperado en: <https://www.funcionpublica.gov.co/web/mipg/como-opera-mipg>).

¹⁴ Esta política busca que las entidades generen y dispongan la información estadística, así como la de sus registros administrativos, de acuerdo con los lineamientos establecido (recuperado en: <https://www.funcionpublica.gov.co/web/mipg/como-opera-mipg>).

- Realizar autodiagnósticos de los registros administrativos para el fortalecimiento y el aprovechamiento estadístico (caracterización de la información, proceso de producción y calidad, acceso, y uso de la información)
- Establecer acciones para el fortalecimiento de la producción estadística, la administración y la gestión de los registros administrativos.
- Definición de hoja de ruta para fortalecer su producción, accesibilidad y el uso de la información estadística, así como el fortalecimiento de sus registros administrativos en el corto, el mediano y el largo plazo.
- La implementación de los conceptos estandarizados, nomenclaturas y clasificaciones en los registros administrativos e información estadística, de acuerdo con el ámbito de aplicación.
- La documentación de los procedimientos y fichas técnicas de los indicadores, procesos estadísticos y registros administrativos

En cuanto a los procesos para la gestión del conocimiento¹⁵ y capacitación del recurso humano se sugiere:

- Consolidar procesos para la generación de conocimiento e innovación para el abordaje de asuntos ambientales y deforestación en las instituciones a través del aprovechamiento y uso de los sistemas de información existentes y el capital humano disponible.
- Una de las formas de gestionar el conocimiento en las entidades es a través del desarrollo de documentos (infografías, planes, informes, guías, instructivos, herramientas), piezas audiovisuales (presentaciones, videos) que se consoliden en memoria institucional respecto a asuntos ambientales y deforestación. A través de ello la entidad contribuye a la consolidación y comprensión de conocimientos sobre la temática abordada, así mismo deja información disponible para ser consultada, y con ello, generar una solución a la alta rotación de personal que caracteriza a las instituciones del sector Defensa y Seguridad.
- Incluir en los planes de capacitación de la entidad el abordaje de conocimientos temáticas ambientales y deforestación.

5.2. Recomendaciones para superar las barreras de la interoperabilidad de información del sector Defensa y Seguridad

Las instituciones que hacen parte del sector Defensa y Seguridad, para tener mayor precisión técnica y tecnológica debe identificar el modelo de madurez para la interoperabilidad de la información (herramienta diseñada por MINTIC) a

¹⁵ La gestión del conocimiento y la innovación como política de gestión y desempeño tiene como propósito facilitar el aprendizaje y la adaptación de las entidades a los cambios y a la evolución de su entorno, a través de la gestión de un conocimiento colectivo y de vanguardia, que permita generar productos/servicios adecuados a las necesidades de los ciudadanos y, además, propicie su transformación en entidades que a través de su dinámica, faciliten la innovación institucional en el marco de un Estado eficiente y productivo. (recuperado en: <https://www.funcionpublica.gov.co/web/mipg/como-opera-mipg>).

fin de identificar su nivel de avance interno y promover las acciones puntuales para superar las brechas encontradas. Para el desarrollo del ejercicio se sugiere solicitar el acompañamiento del Ministerio de las Tecnologías de la Información y Comunicación, así como la participación de las áreas técnicas (dependencias) y la oficina de sistemas y de planeación, esta última a fin de promover la documentación y consolidación de procesos y procedimientos.

A continuación, son presentados la recopilación de aspectos cualitativos que deben ser observados en conjunto por las instituciones del Sector Defensa y Seguridad para avanzar en el objetivo de generar procesos de interoperabilidad de la información y consolidar un proceso robusto que incluya la superación de expectativas identificadas como barreras y/o retos para la interoperabilidad de la información en el sector.

Dominio organizacional

Las entidades del sector Defensa y Seguridad en atención a los lineamientos de la política de planeación institucional¹⁶, se sugiere llevar a cabo un proceso de Direccionamiento Estratégico y Planeación en donde se promueva el liderazgo desde la Alta Dirección del sector, para la reflexión y la planeación de las entidades frente a los asuntos ambientales y para el control de la deforestación. Particularmente, fue sugerido ampliar la dinámica de trabajo interinstitucional de explotación ilícita de yacimientos mineros (CI3MA) e incluir el intercambio de información sobre los delitos ambientales en general.

A su vez, identificar qué información deber ser interoperable y que deba ser gestionada a través de convenios promovidos desde la alta dirección con actores públicos y privados. Por ejemplo: con empresa Efecty para obtener información sobre movimientos financieros (responsables – montos) o con instituciones académicas para el desarrollo de estudios de inteligencia de negocios. Lo anterior, es considerado como un aporte fundamental para mejorar la gestión y resultados operacionales en materia ambiental y de control a la deforestación.

Se sugiere la construcción conjunta de protocolos (con la participación de todas las entidades del Sector Defensa y Seguridad), en donde se establezca el tipo de información a compartir, sus características (ej. anonimizada), medio de intercambio, periodicidad y responsables institucionales.

¹⁶ El propósito de esta política es permitir que las entidades definan la ruta estratégica y operativa que guiará la gestión de la entidad (particularmente tema ambiental), con miras a satisfacer las necesidades de sus grupos de valor. A través de direccionamiento estratégico, identificación de necesidades para el mejoramiento de desempeño y fortalecimiento institucional, planeación con base en el cumplimiento de obligaciones normativas a mediano y largo plazo; establecimiento de estrategias, objetivo y metas, responsables y distribución presupuestal. Y, la generación de mecanismos de seguimiento y evaluación.

Dominio Político legal

Para garantizar una completa acogida y avances (en paralelo), por parte de todas las entidades del sector, se recomienda que desde los altos directivos del sector Defensa y Seguridad sea emitida una orden dirigida a todas las instituciones del sector, de manera que avancen en las adecuaciones institucionales internas (capacidad instalada) que se requieren en el proceso de interoperabilidad de la información; y garantizar la participación de los escenarios institucionales para consolidar el proceso en conjunto de la interoperabilidad de la información.

Dominio técnico

Se recomienda a las instituciones del Sector Defensa y Seguridad acoger los lineamientos de la política de Gobierno Digital¹⁷ el cual es implementado a través de dos líneas de acción (TIC para el Estado y TIC para la Sociedad) así como de tres habilitadores transversales (Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales). Estos elementos, son fundamentales para garantizar con las condiciones técnicas habilitantes en el inicio de procesos de interoperabilidad de la información descritos en documento marco de interoperabilidad descrito por Mintic.

A su vez, los procesos técnicos (ajustes institucionales) deben ser liderados por las dependencias encargadas de tecnologías de la información y comunicación, oficina de sistemas o quien cumpla sus funciones. Con ello se garantizará el trabajo articulado entre las dependencias para prever situaciones tales como: Incompatibilidad de los sistemas de información, limitaciones de capacidad técnica de los sistemas, mantenimiento del software y su actualización, además de la planificación presupuestaria en sistemas de información para cada vigencia presupuestaria de la institución.

También, se recomienda levantar la caracterización técnica de los sistemas de información que actualmente están operando (BISIGOI, SIEDCO, Biblioteca Nacional, SISyD, entre otros) en las instituciones, así como de los que están en proceso de desarrollo (J3 Diseño plataforma – Contrato DIADF), de manera que sean identificadas las diferencias técnicas y se proyecten soluciones para garantizar el proceso de compatibilidad entre los sistemas de información.

¹⁷ Contribuye a la Transformación Digital del sector público, implica un cambio en los procesos, la cultura y el uso de la tecnología para el mejoramiento de las relaciones externas de las entidades de Gobierno, a través de la prestación de servicios más eficientes. Recuperado en <https://www.funcionpublica.gov.co/web/mipg/como-opera-mipg>

Dominio semántico

Bajo este dominio, las instituciones participantes del Sector Defensa y Seguridad manifestaron la necesidad de proyectar una metodología de consolidación de información estadística para el sector, proceso que se sugiere llevarlo a cabo en consulta a todas las entidades a fin de incorporar las características de información que actualmente producen (datos estadísticos y reconocimiento de registros administrativos).

También, la institución que lideré el proceso de interoperabilidad deberá identificar los procesos de estandarización semántica, a fin de acoger los avances que ya están adelantados. Lo cual se sugiere con base en la información recopilada, para lo cual las instituciones manifestaron que cuentan con los siguientes avances:

- Está en proceso de estandarización semántica de los delitos ambientales.
- Ya existen fichas técnicas para la estandarización del lenguaje en minería

Ejercicio que permitirá identificar los vacíos existentes (falta estandarización de los formatos, hace falta actualización de resultados operacionales y de gestión ambiental) que reconocen las entidades.

6. Bibliografía

Decreto 1499. (11 de septiembre de 2017). Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. Recuperado en <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83433> el 15 de diciembre de 2023.

Ministerio de la Información y la Comunicación (2019). Marco de interoperabilidad para gobierno digital, Recuperado en https://lenguaje.mintic.gov.co/sites/default/files/archivos/marco_de_interoperabilidad_para_gobierno_digital.pdf el 15 de noviembre de 2023.