



**Agencia
Nacional Digital**



Reporte de vulnerabilidades a terceros

Superintendencia de Transporte

Entregables de la fase orientados al fortalecimiento
institucional de la ciberseguridad

ABRIL 2026

Documento técnico para entrega institucional



**Agencia
Nacional Digital**



CONTROL DE CAMBIOS DEL DOCUMENTO

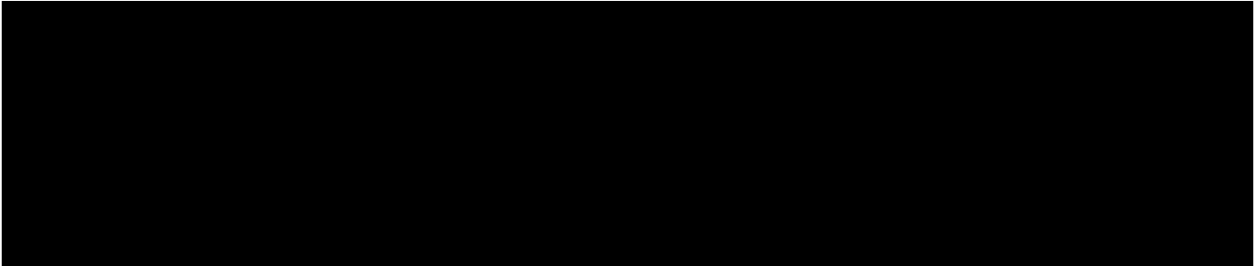
REVISIÓN No.	FECHA	DESCRIPCIÓN	AUTOR DEL CAMBIO
1	09/04/2026	Creación del documento	Virgilio Salgado



Agencia Nacional Digital



Contenido

1.Introducción.....	4
2. Marco teórico.....	5
3. Marco legal	6
4. Metodología	7
5. Sección de vulnerabilidades	9
	
6. Conclusión	22



**Agencia
Nacional Digital**



1.Introducción

En el marco de las actividades de fortalecimiento de la seguridad digital y de la gestión integral del riesgo cibernético de la Superintendencia de Transporte, desarrollamos un ejercicio técnico de evaluación orientado a identificar debilidades de seguridad presentes en plataformas, servicios, componentes o superficies tecnológicas operadas por terceros, pero que mantienen relación funcional, de integración, procesamiento de información o exposición indirecta frente a la Entidad. Este tipo de revisión resulta fundamental, debido a que la postura de ciberseguridad institucional no depende únicamente de los controles implementados sobre la infraestructura propia, sino también del nivel de protección existente en aquellos proveedores, plataformas externas, servicios contratados o soluciones interconectadas que soportan procesos misionales, administrativos o de atención al ciudadano.

La gestión de vulnerabilidades en terceros permite reconocer riesgos que, aun cuando se originen fuera del perímetro tecnológico directo de la Entidad, pueden impactar la confidencialidad, integridad, disponibilidad, trazabilidad y resiliencia de la información institucional. En entornos interconectados, una



Agencia Nacional Digital



debilidad técnica en un servicio externo puede convertirse en un punto de afectación para los procesos internos, la continuidad operativa, la protección de datos, la confianza institucional y el cumplimiento normativo. Por ello, consolidamos en este reporte un enfoque de revisión técnica y análisis ejecutivo que nos permita documentar los hallazgos identificados, valorar su criticidad, estimar su impacto y formular recomendaciones orientadas a su tratamiento y mitigación.

Adicionalmente, este informe se concibe como un insumo para la toma de decisiones, el seguimiento de riesgos tecnológicos y el fortalecimiento de los mecanismos de supervisión sobre terceros que interactúan tecnológica o informacionalmente con la Superintendencia de Transporte. Su propósito no es únicamente evidenciar debilidades técnicas, sino también aportar elementos que permitan promover mejores prácticas de seguridad, mayor control sobre la cadena de suministro digital y una visión más integral del riesgo cibernético institucional.

2. Marco teórico

La ciberseguridad institucional moderna exige comprender que el riesgo no se limita a los activos propios de una organización. En la práctica, las entidades públicas y privadas dependen de ecosistemas digitales compuestos por proveedores, desarrolladores, operadores tecnológicos, plataformas externas, servicios en la nube, APIs, portales integrados y múltiples terceros que participan en el tratamiento, tránsito o exposición de información. En ese contexto, la gestión de vulnerabilidades a terceros se convierte en una disciplina esencial para anticipar escenarios de afectación, evaluar la madurez de los controles existentes y reducir la probabilidad de incidentes derivados de relaciones tecnológicas externas.

Desde una perspectiva conceptual, una vulnerabilidad puede entenderse como una debilidad de carácter técnico, lógico, configuracional, procedimental o de diseño que puede ser aprovechada para comprometer un sistema, servicio o activo digital. Estas debilidades pueden manifestarse en errores de configuración, controles de autenticación insuficientes, deficiencias de autorización, exposición innecesaria de servicios, manejo inseguro de sesiones, fallas de cifrado, validación inadecuada de entradas, errores de despliegue, entre otras. La relevancia de identificar este tipo de situaciones radica en que la presencia de una sola debilidad, aun en un componente externo, puede



Agencia Nacional Digital



convertirse en una vía de acceso, alteración, indisponibilidad o fuga de información con efectos sobre la operación institucional.

En el ámbito de referencia internacional, la norma ISO/IEC 27001:2022 establece los requisitos para implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, promoviendo un enfoque basado en riesgos y orientado a preservar la confidencialidad, integridad y disponibilidad de la información. De manera complementaria, el Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC adopta buenas prácticas y lineamientos para que las entidades públicas gestionen adecuadamente el ciclo de vida de la seguridad de la información dentro del marco de la Política de Gobierno Digital. Ambos referentes respaldan la necesidad de evaluar no solo los controles propios, sino también los riesgos asociados a terceros y a los entornos interconectados.

Por su parte, el NIST Cybersecurity Framework 2.0 plantea un modelo de gestión del riesgo cibernético útil para organizaciones de distintos tamaños y sectores, y permite estructurar la identificación, análisis, priorización y tratamiento de riesgos de forma continua. Bajo este enfoque, la evaluación de vulnerabilidades a terceros no debe entenderse como una actividad aislada, sino como parte de un proceso permanente de gobierno, monitoreo, evaluación y mejora de la seguridad institucional.

3. Marco legal

El presente reporte se fundamenta en el marco jurídico y normativo aplicable a la seguridad de la información, la protección de datos personales, la transparencia pública y la gestión digital del Estado colombiano. En primer lugar, la **Ley 1581 de 2012** establece el régimen general de protección de datos personales en Colombia, lo cual resulta especialmente relevante cuando los terceros evaluados almacenan, transmiten, consultan o procesan información asociada a ciudadanos, funcionarios, contratistas o bases de datos institucionales. En consecuencia, cualquier debilidad identificada en activos tecnológicos de terceros puede tener incidencia directa sobre los principios de seguridad, confidencialidad y circulación restringida de la información personal. De igual manera, la **Ley 1273 de 2009** incorporó al ordenamiento penal colombiano la protección de la información y de los datos, tipificando conductas relacionadas con accesos no autorizados, obstaculización del funcionamiento de sistemas, interceptación de datos y demás afectaciones contra activos



Agencia Nacional Digital



informáticos. Este marco normativo resalta la necesidad de documentar de forma adecuada las vulnerabilidades y los riesgos detectados, dado que una exposición técnica no tratada oportunamente puede facilitar conductas contrarias al ordenamiento jurídico y afectar tanto a la Entidad como a los terceros involucrados.

Adicionalmente, la **Ley 1712 de 2014**, en materia de transparencia y acceso a la información pública, impone deberes de gestión adecuada de la información y de protección frente a accesos indebidos cuando existan límites legales o datos con tratamiento especial. Esto implica que la seguridad de los sistemas vinculados a la administración pública no solo es una exigencia técnica, sino también una condición necesaria para garantizar un acceso responsable, controlado y conforme a la ley.

En el ámbito sectorial TIC, el **Decreto 1078 de 2015** compila la regulación del sector de Tecnologías de la Información y las Comunicaciones, mientras que el **Decreto 620 de 2020** estableció lineamientos generales de la Política de Gobierno Digital y del uso y operación de servicios ciudadanos digitales. Estos instrumentos refuerzan la necesidad de que las entidades públicas adopten controles, lineamientos y mecanismos de gobernanza que también consideren la interacción con terceros, las integraciones tecnológicas y la seguridad de los servicios digitales puestos a disposición de usuarios internos y externos.

Finalmente, como marco orientador de buenas prácticas para entidades públicas, el **Modelo de Seguridad y Privacidad de la Información (MSPI)** de MinTIC establece lineamientos para la implementación y adopción de prácticas de seguridad y privacidad de la información, apoyando el ciclo de planeación, implementación, evaluación y mejora continua. En consecuencia, este reporte se alinea tanto con las obligaciones legales aplicables como con las buenas prácticas técnicas y de gestión que exigen una supervisión constante de los riesgos cibernéticos asociados a terceros.

4. Metodología

La metodología aplicada para la construcción del presente reporte fue desarrollada con base en lineamientos reconocidos internacionalmente para la evaluación de seguridad, priorización de riesgos y documentación técnica de hallazgos. En particular, se tomó como referencia el **NIST Cybersecurity Framework 2.0**, el cual permite estructurar la gestión del riesgo cibernético mediante un enfoque continuo de gobierno, identificación, protección,



Agencia Nacional Digital



detección, respuesta y recuperación. Bajo esta lógica, la evaluación de terceros se abordó no solo como un ejercicio de revisión técnica puntual, sino como una actividad orientada a identificar exposiciones relevantes para la postura de seguridad de la Superintendencia de Transporte, valorar su impacto potencial y aportar criterios de tratamiento.

Asimismo, se consideraron los lineamientos del **NIST SP 800-115**, documento que orienta la planeación y ejecución de pruebas técnicas de seguridad, el análisis de hallazgos y la formulación de estrategias de mitigación. Este referente resulta especialmente útil para dar orden al proceso de evaluación, ya que propone una aproximación disciplinada para la identificación de superficies de exposición, la revisión técnica de controles y la consolidación de evidencia suficiente para soportar observaciones de seguridad de manera formal y verificable.

En el componente aplicado a aplicaciones web, portales, APIs o servicios expuestos, se adoptaron criterios del **OWASP Web Security Testing Guide (WSTG)**, el cual organiza el análisis de seguridad en dominios como recolección de información, gestión de configuración y despliegue, gestión de identidades, autenticación, autorización, manejo de sesiones, validación de entradas, manejo de errores, criptografía, lógica de negocio, cliente y APIs. De forma complementaria, se tomó como referencia el **OWASP Top 10**, cuya edición vigente es la de 2025, como documento de sensibilización y priorización sobre los riesgos más críticos de seguridad en aplicaciones web.

Bajo estos marcos, enfocamos la evaluación en identificar debilidades técnicas que pudieran derivar en accesos no autorizados, exposición indebida de información, escalamiento de privilegios, afectación a la disponibilidad de servicios, fuga de datos, configuraciones inseguras o fallas de lógica con impacto sobre activos tecnológicos administrados por terceros o conectados con la operación institucional. Orientamos la valoración de los hallazgos a determinar el nivel de riesgo, la criticidad del activo comprometido, el posible alcance del impacto y la necesidad de tratamiento, manteniendo un criterio técnico, ético y controlado durante todo el proceso de revisión.

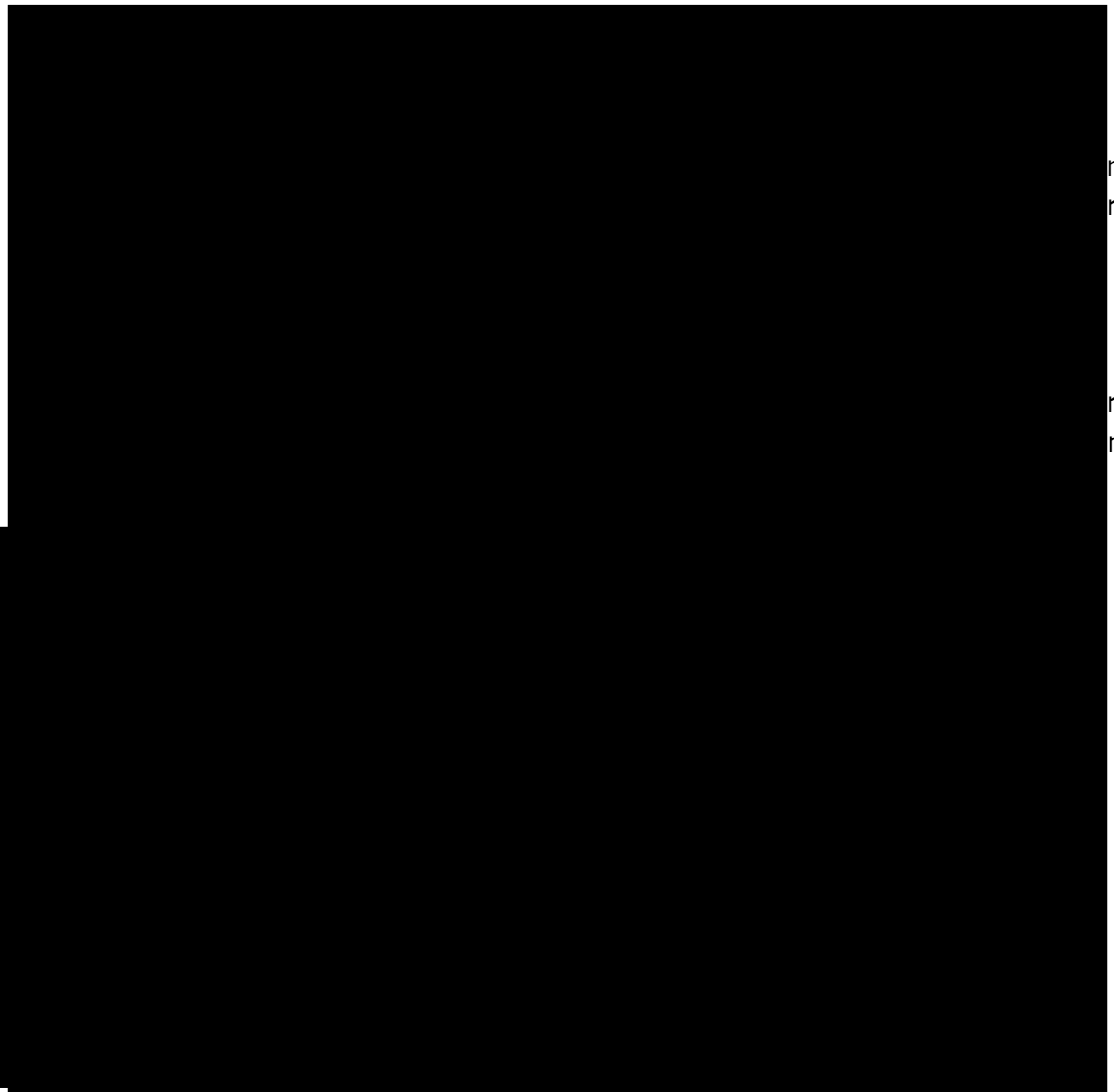
Finalmente, la documentación de resultados fue estructurada con enfoque gerencial y técnico, buscando que cada hallazgo pudiera ser entendido tanto desde su dimensión operativa como desde su implicación para la seguridad institucional, la continuidad del servicio, el cumplimiento normativo y la relación con terceros. De esta manera, la metodología no solo permitió identificar vulnerabilidades, sino también convertir los resultados obtenidos en



Agencia
Nacional Digital

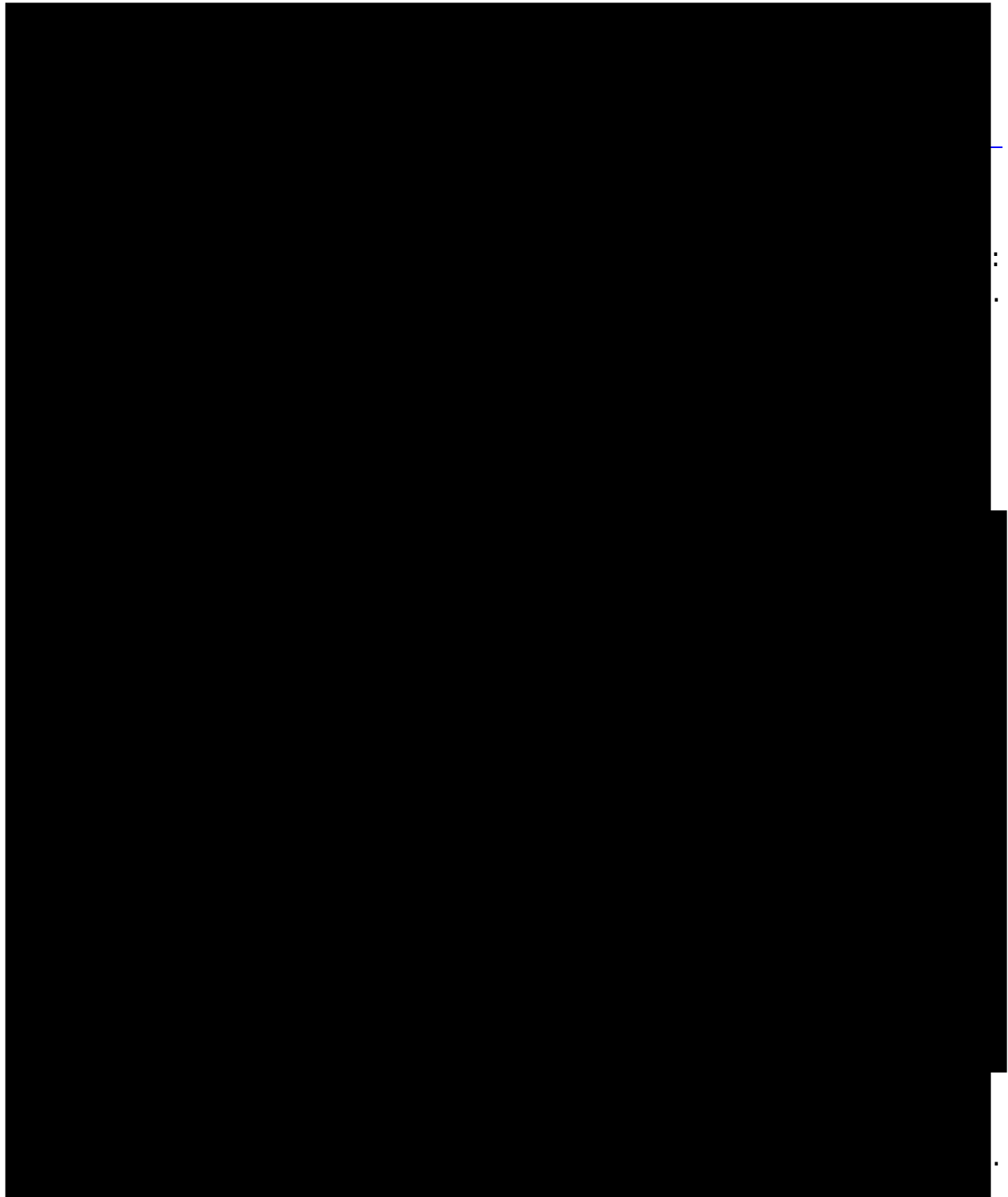


5. Sección de vulnerabilidades



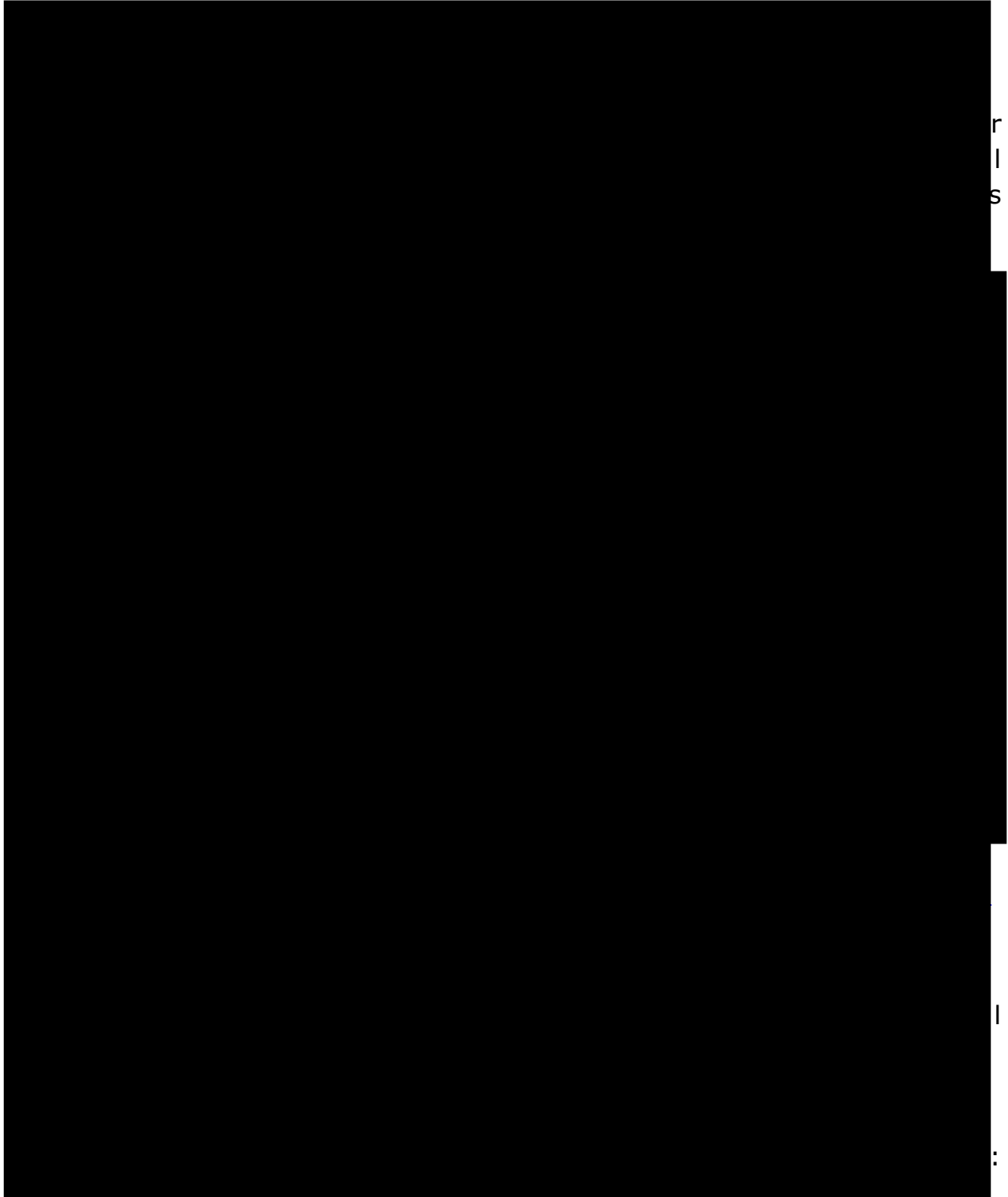


Agencia Nacional Digital





Agencia
Nacional Digital



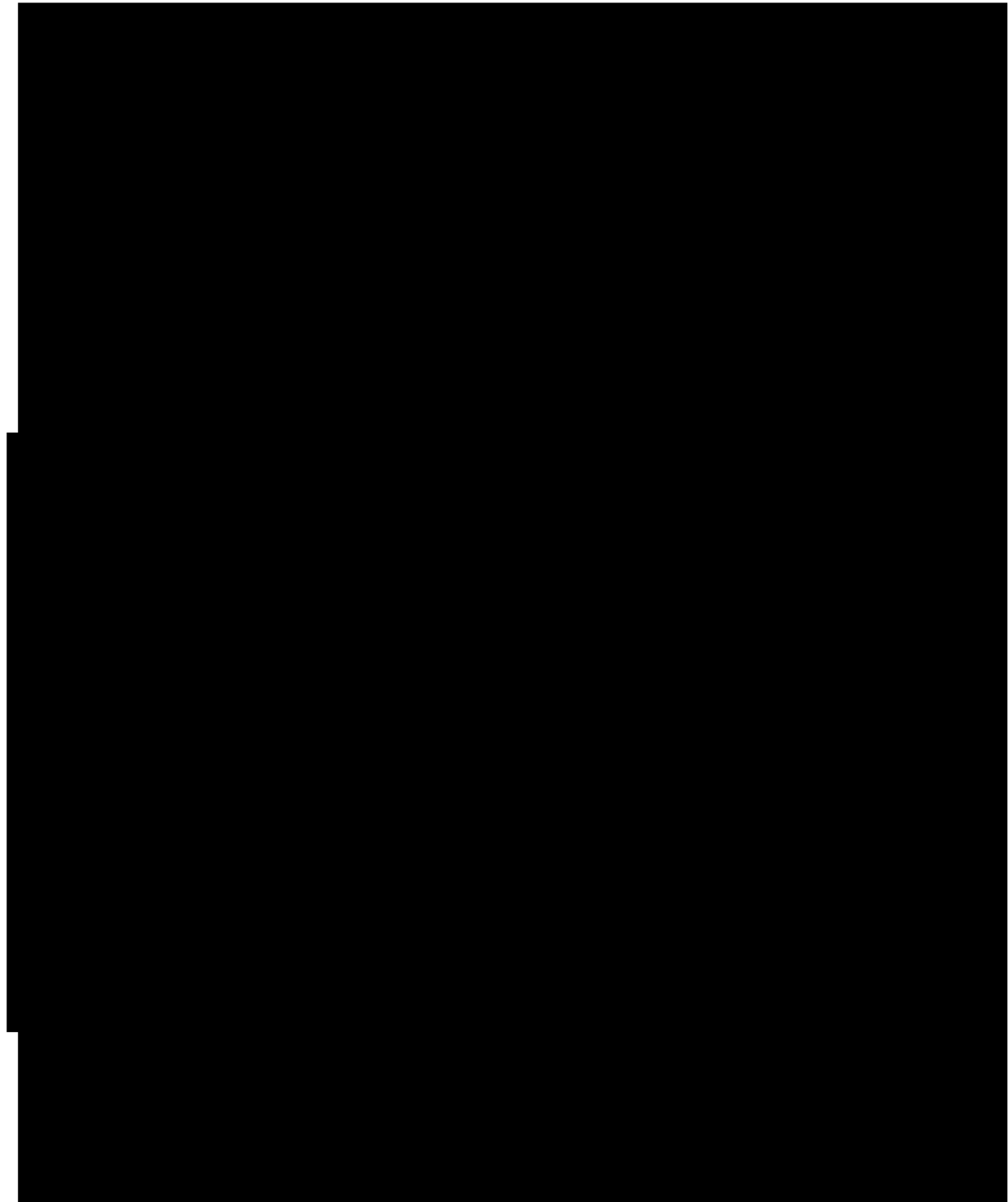


Agencia Nacional Digital



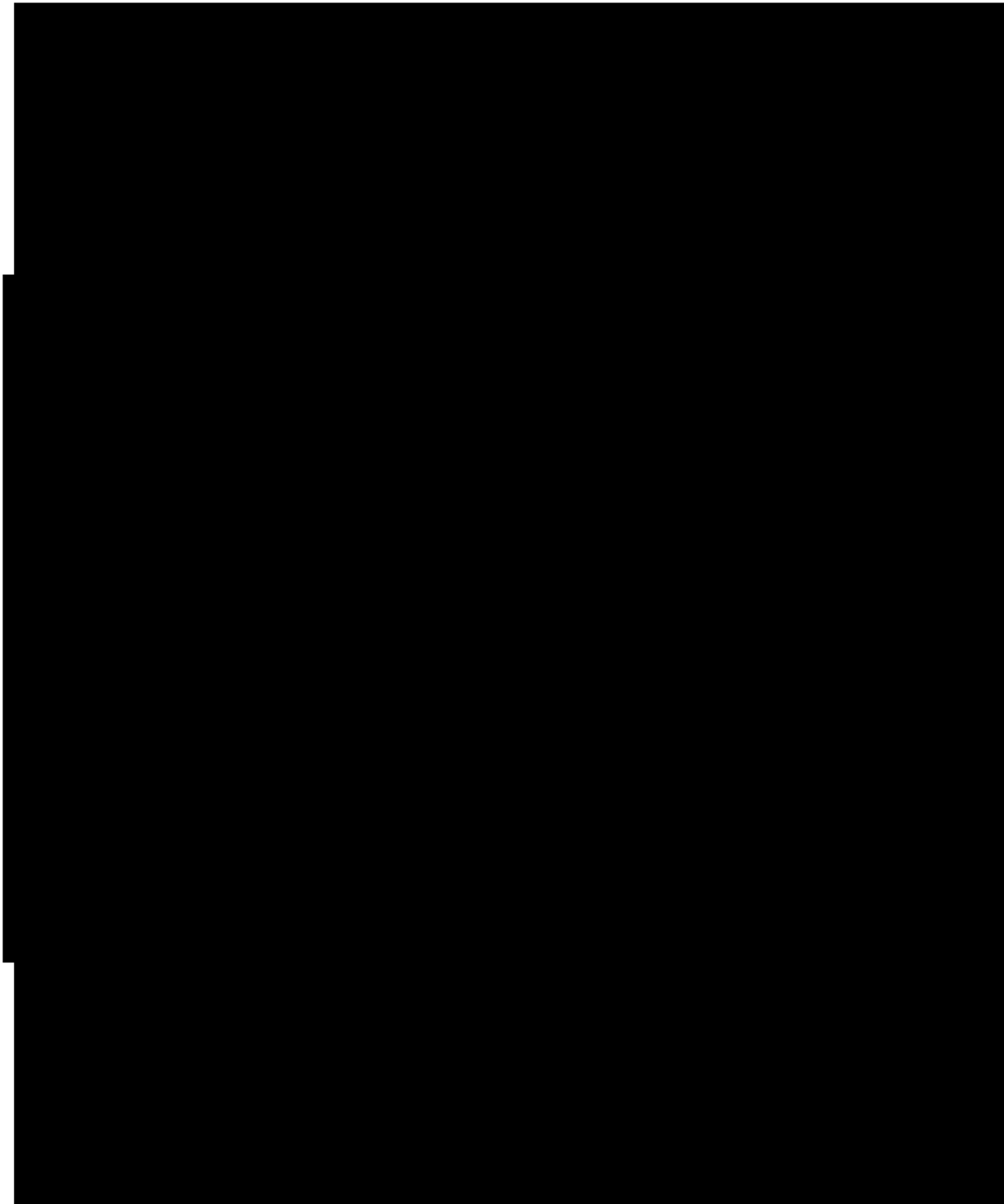


Agencia Nacional Digital



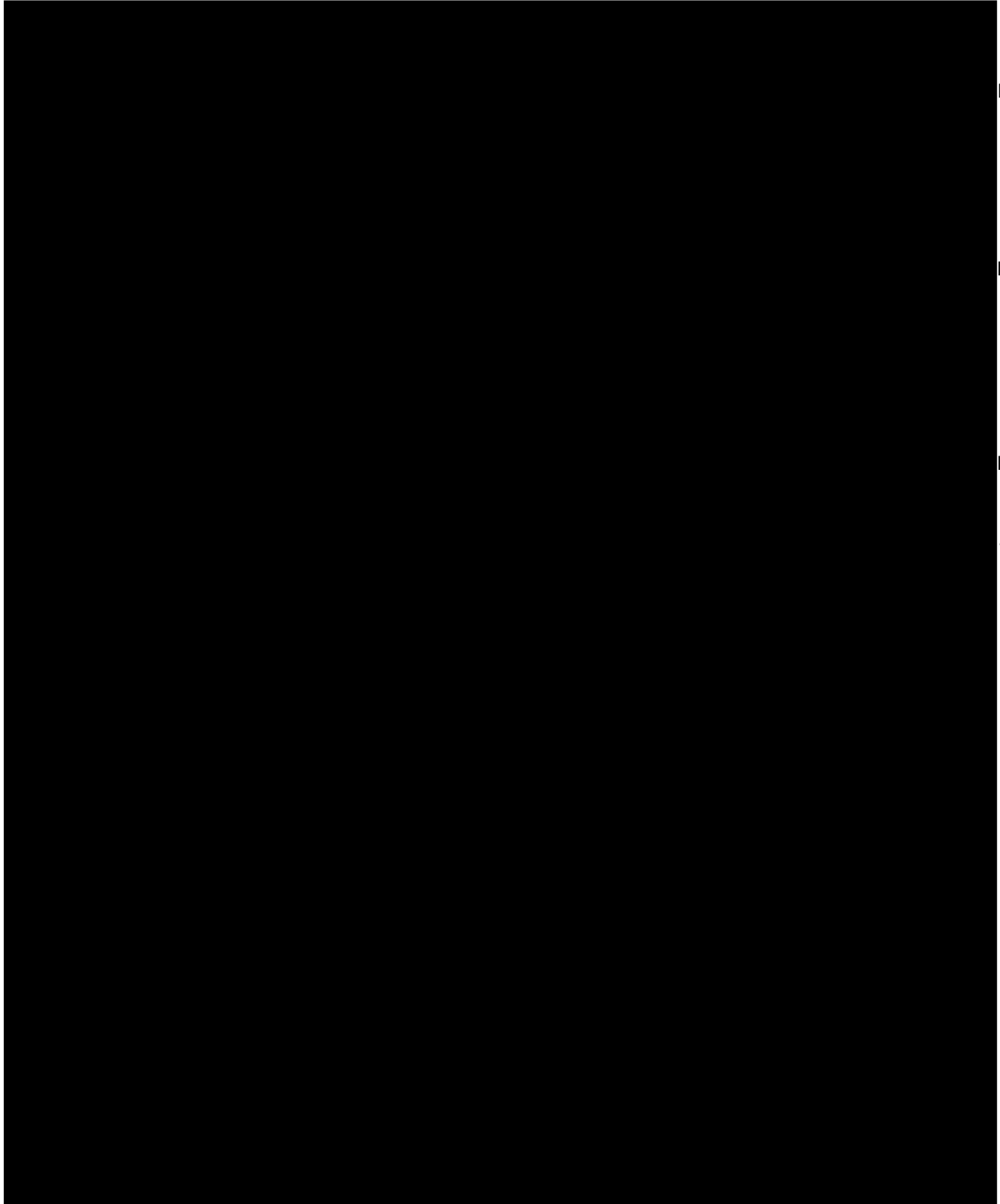


Agencia Nacional Digital



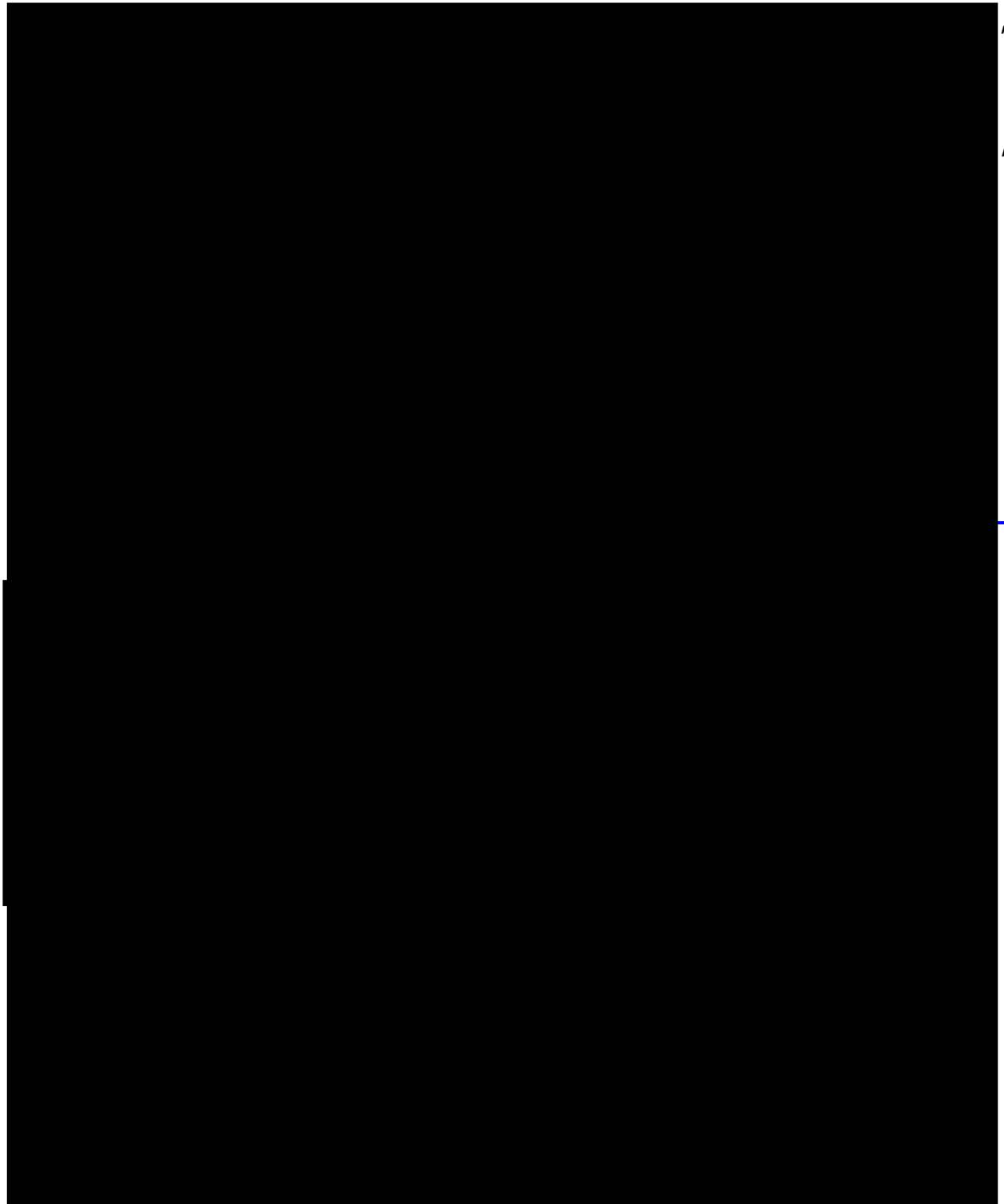


Agencia Nacional Digital



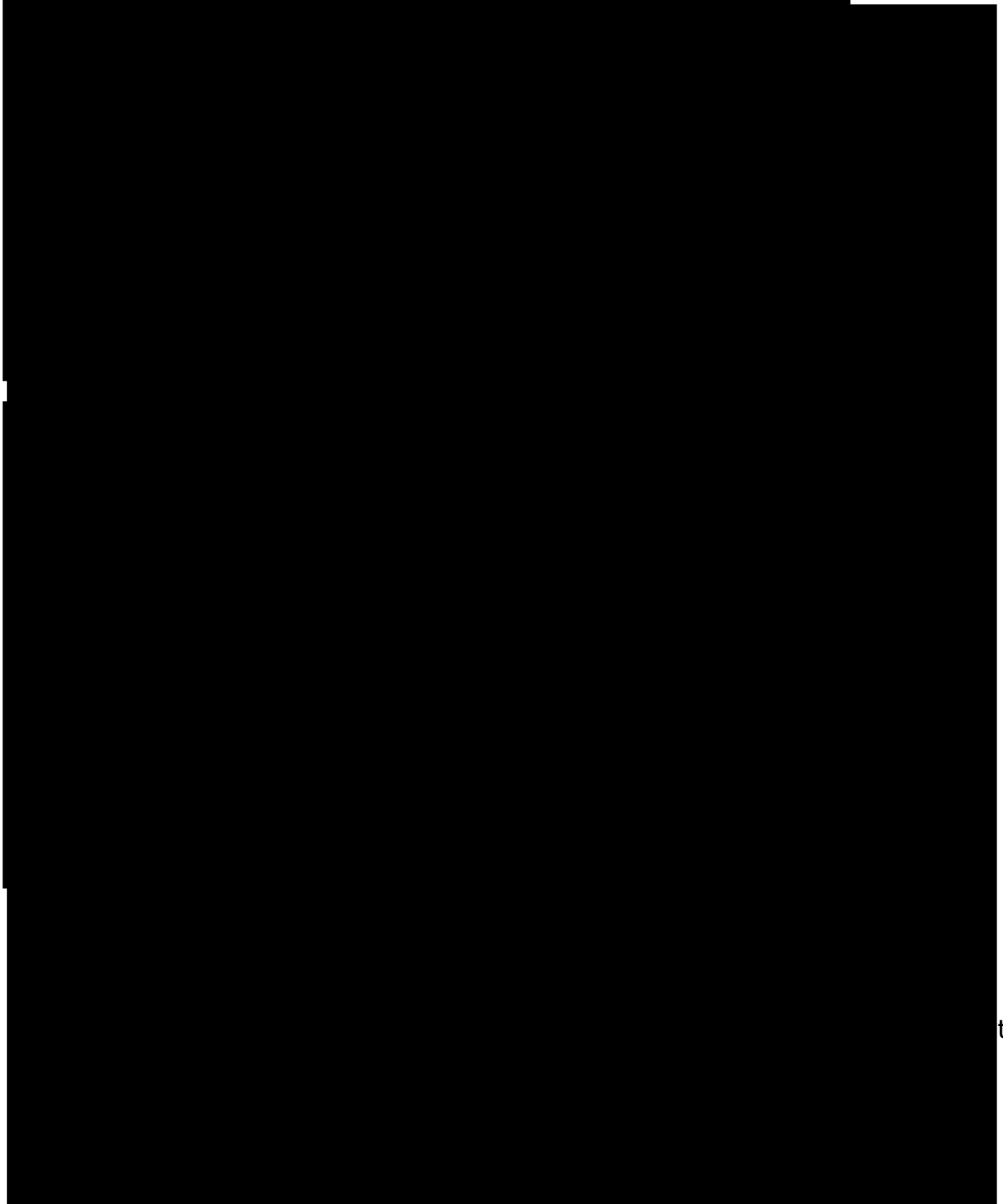


Agencia
Nacional Digital





Agencia
Nacional Digital



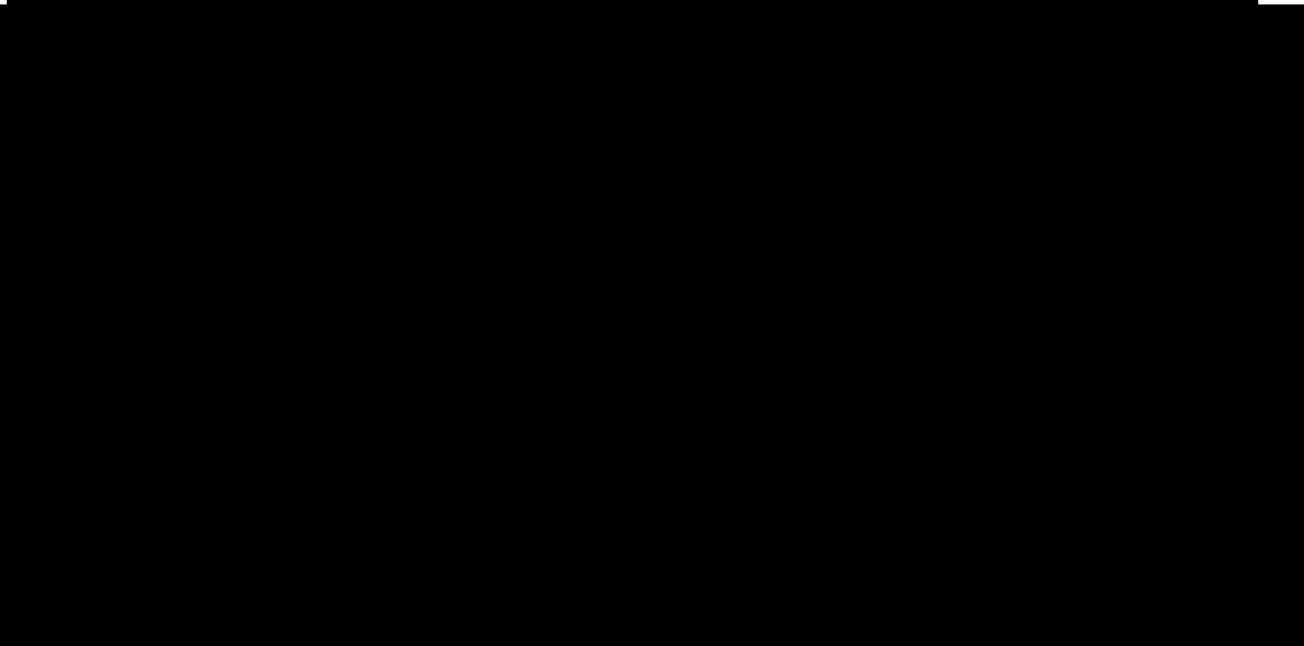
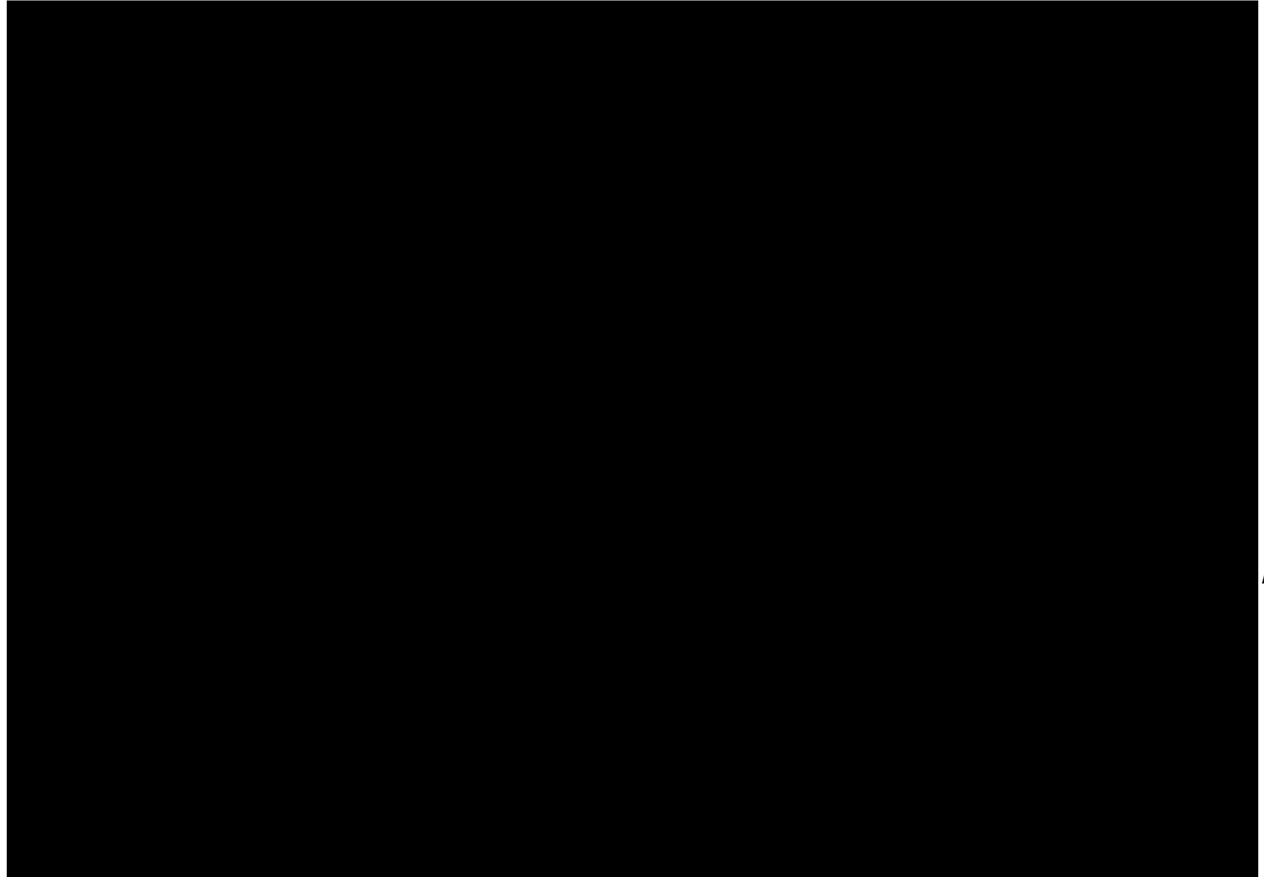


Agencia
Nacional Digital





Agencia Nacional Digital



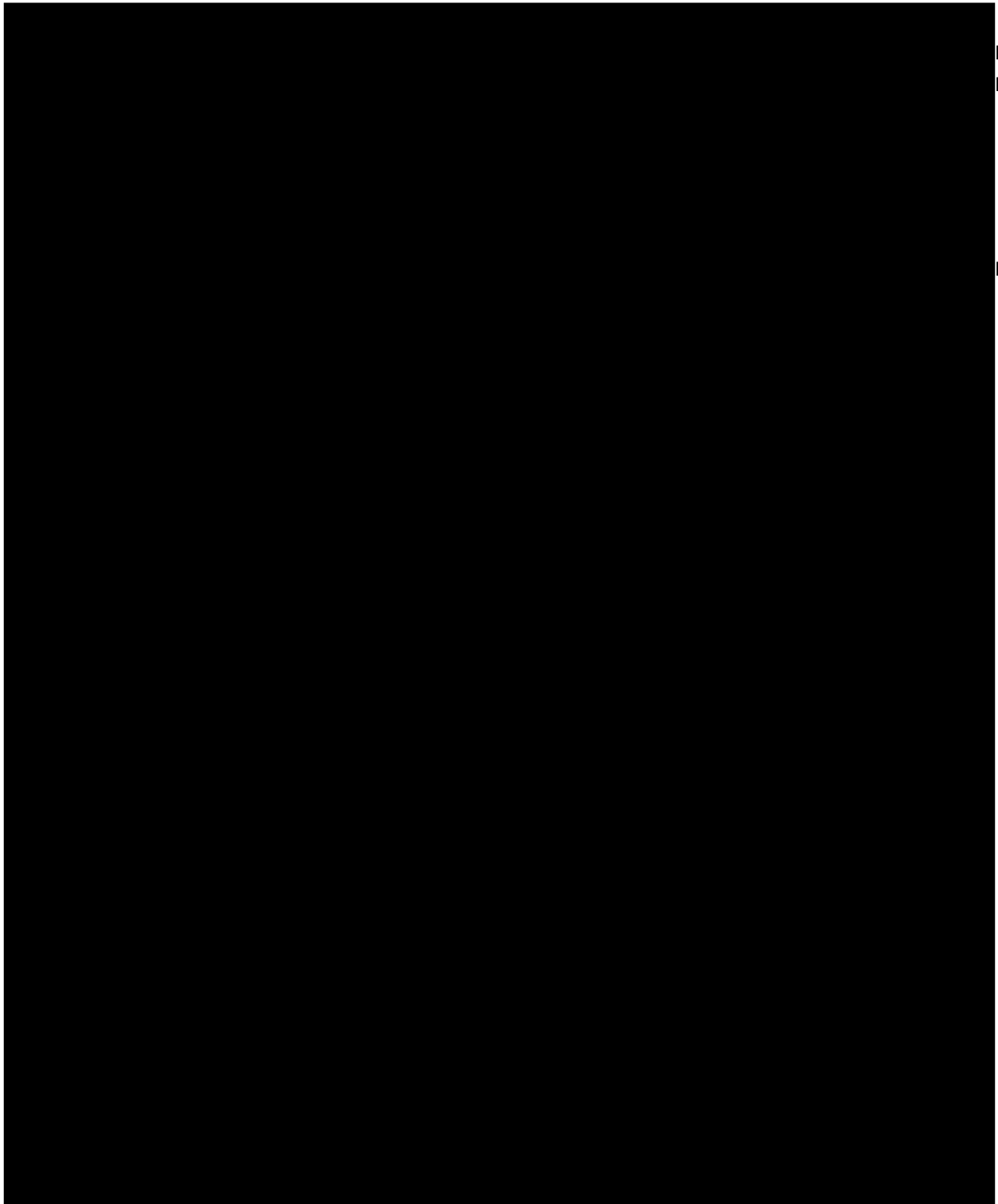


Agencia
Nacional Digital





Agencia Nacional Digital





6. Conclusión

El presente reporte evidencia la importancia de incorporar el análisis de terceros dentro de la estrategia integral de ciberseguridad de la Superintendencia de Transporte. En entornos altamente interconectados, la seguridad institucional no depende exclusivamente de los controles internos, sino también de la madurez técnica, administrativa y operativa de aquellos actores externos que prestan servicios, soportan plataformas, procesan información o mantienen vínculos tecnológicos con la Entidad. En ese sentido, la identificación de vulnerabilidades en terceros constituye un ejercicio clave para anticipar riesgos, fortalecer la supervisión tecnológica y mejorar la capacidad de prevención frente a escenarios que puedan comprometer la operación o la información institucional.

Desde una perspectiva de gestión, los hallazgos que se documenten en este informe deben ser entendidos como oportunidades de mejora y como insumos para la toma de decisiones, el seguimiento de riesgos y la definición de acciones de remediación o control. La aplicación de referentes como OWASP, NIST, ISO/IEC 27001 y los lineamientos del MSPI permite sustentar técnicamente el análisis realizado y asegurar que las observaciones formuladas se encuentren alineadas con buenas prácticas reconocidas en seguridad de la información y gestión del riesgo cibernético.

En conclusión, la evaluación de vulnerabilidades a terceros fortalece la postura de seguridad de la Superintendencia de Transporte al ampliar la visibilidad sobre riesgos externos que podrían impactar la confidencialidad, integridad, disponibilidad y continuidad de los servicios. Por ello, recomendamos mantener este tipo de revisiones como parte de un proceso continuo de control, seguimiento y mejora, promoviendo planes de tratamiento, verificaciones posteriores y una relación más robusta con terceros desde la perspectiva de ciberseguridad y cumplimiento normativo.