

Informe de seguimiento

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

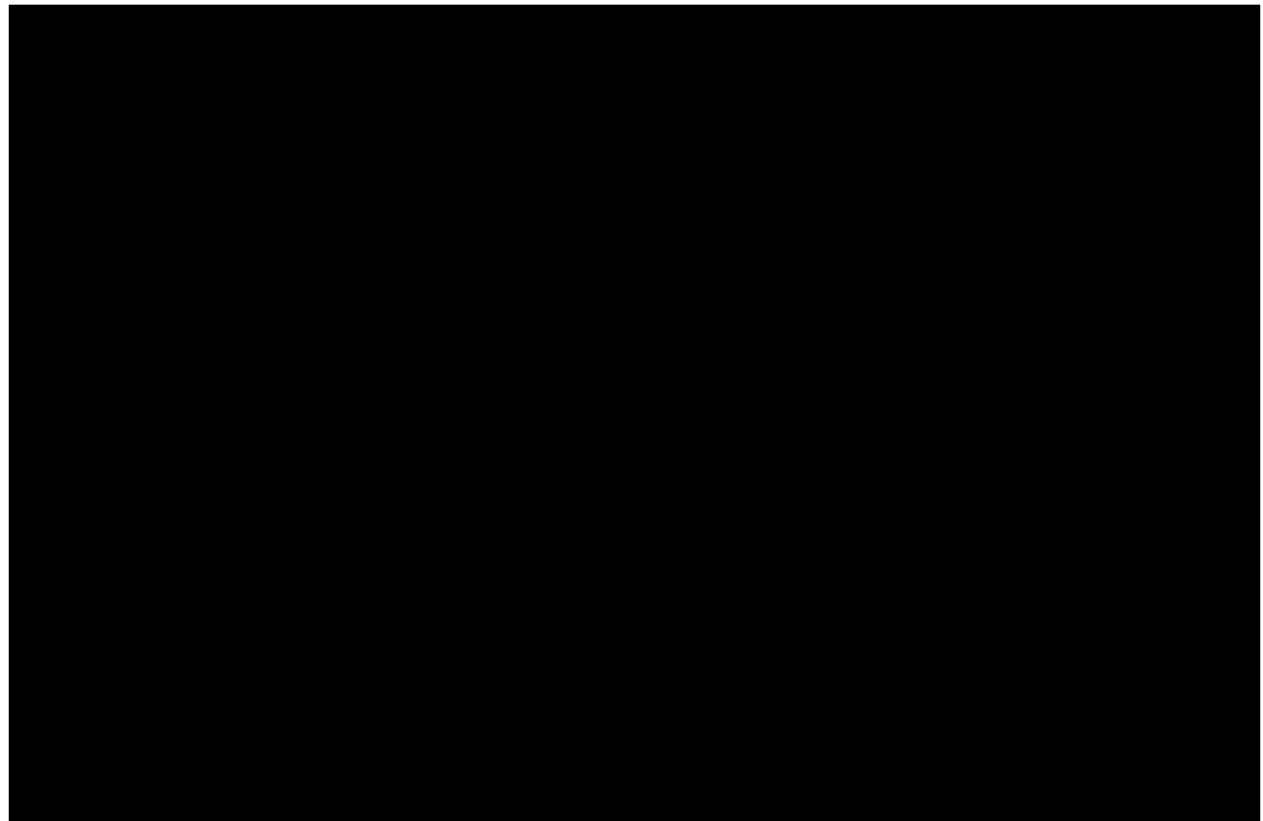


Agencia Nacional Digital



Contenido

1. Introducción.....	4
2. Objetivo General	4
3. Objetivos Específicos.....	5
4. Marco Legal y Normativo	5
5. Metodología de Pentest	6
5.1 Planeación y definición de alcance.....	6
5.2 Recolección de información y reconocimiento	6
5.3 Análisis de vulnerabilidades	7
5.4 Explotación controlada y validación técnica	7
5.5 Análisis de impacto y priorización	7
5.6 Documentación y reporte.....	7
6. Hallazgos	8



7. Conclusión	45
----------------------------	-----------



Agencia Nacional Digital



1. Introducción

El presente **Informe de Auditoría de Ciberseguridad** tiene como finalidad documentar el desarrollo, alcance, resultados y hallazgos obtenidos durante la ejecución de un ejercicio de evaluación de seguridad ofensiva controlada sobre la infraestructura tecnológica de la **Superintendencia de Transporte**, en adelante **Supertransporte**. Este proceso se orienta a la identificación de vulnerabilidades técnicas, debilidades de configuración, deficiencias de control y posibles vectores de ataque que puedan comprometer la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional.

En el marco de esta auditoría, realizamos un **pentest sobre toda la arquitectura tecnológica objeto de evaluación**, incluyendo, según aplique, aplicaciones web, servicios expuestos, componentes de red, servidores, controles de autenticación, gestión de sesiones, mecanismos de autorización, configuraciones de seguridad, superficies de exposición pública e interacciones entre componentes críticos. El propósito del ejercicio no es únicamente detectar fallas existentes, sino también aportar una visión técnica y estratégica que permita fortalecer la postura de seguridad de la entidad, reducir el riesgo de materialización de incidentes y promover la mejora continua en la gestión de la ciberseguridad.

Desarrollamos la auditoría bajo criterios de autorización, control, trazabilidad y confidencialidad, garantizando que todas las actividades ejecutadas correspondan a pruebas técnicas planificadas, delimitadas y debidamente soportadas. Asimismo, los hallazgos identificados serán clasificados de acuerdo con su nivel de criticidad, impacto potencial, facilidad de explotación y exposición de activos, con el fin de priorizar su tratamiento y facilitar la toma de decisiones por parte de las áreas técnicas, administrativas y directivas involucradas.

2. Objetivo General

Realizar una auditoría de ciberseguridad a la arquitectura tecnológica de la Superintendencia de Transporte, mediante la ejecución de pruebas técnicas de penetración controladas, con el fin de identificar vulnerabilidades, evaluar el nivel de exposición de los activos tecnológicos y emitir recomendaciones orientadas al fortalecimiento de la seguridad de la información y la reducción del riesgo institucional.



Agencia Nacional Digital



3. Objetivos Específicos

Evaluar el nivel de seguridad de los activos tecnológicos que hacen parte del alcance definido para la auditoría, identificando debilidades en aplicaciones, infraestructura, configuraciones, controles de acceso y mecanismos de protección implementados.

Detectar vulnerabilidades explotables que puedan ser utilizadas por un atacante para comprometer servicios, sistemas, datos o funcionalidades críticas de la entidad.

Verificar la efectividad de los controles de seguridad existentes frente a amenazas comunes y avanzadas, tales como fallas de autenticación, deficiencias de autorización, exposición de información sensible, errores de configuración y validaciones insuficientes.

Clasificar y documentar los hallazgos encontrados con base en su criticidad, probabilidad de explotación, impacto técnico y riesgo para la operación institucional.

Presentar recomendaciones de mitigación, corrección y fortalecimiento que sirvan como insumo para la toma de decisiones, la priorización de remediaciones y la mejora continua de la postura de ciberseguridad de Supertransporte.

4. Marco Legal y Normativo

La presente auditoría se enmarca en principios técnicos, jurídicos y organizacionales aplicables a la seguridad de la información y a la protección de activos digitales en entidades públicas. En el ámbito nacional, se toma como referencia la **Ley 1273 de 2009**, por medio de la cual se fortalece la protección penal de la información y de los datos, incorporando conductas relacionadas con el acceso abusivo a sistemas informáticos, interceptación de datos, daño informático y uso de software malicioso. De igual forma, se considera la **Ley 1581 de 2012**, que establece el régimen general de protección de datos personales, especialmente relevante en escenarios donde las pruebas pudieran involucrar tratamiento, exposición o validación de controles sobre información personal. También se tiene en cuenta la **Ley 1712 de 2014**, relacionada con la transparencia y el acceso a la información pública, en armonía con la necesidad de preservar la reserva, integridad y disponibilidad de la información institucional. Adicionalmente, se referencia el **Decreto 1078 de 2015**, como Decreto Único Reglamentario del sector TIC, junto con las directrices de Gobierno Digital y seguridad digital aplicables al sector público colombiano.



Agencia Nacional Digital



En el ámbito técnico y metodológico, el ejercicio puede apoyarse en buenas prácticas y marcos reconocidos internacionalmente, tales como **NIST SP 800-115**, que orienta la planificación y ejecución de pruebas técnicas de seguridad; el **OWASP Web Security Testing Guide**, como guía de referencia para pruebas sobre aplicaciones web; el **OWASP Top 10**, como marco de referencia para riesgos frecuentes en aplicaciones; y **PTES**, como estándar para estructurar ejercicios de penetration testing desde la etapa de planeación hasta el reporte final. Estos referentes brindan lineamientos para desarrollar pruebas controladas, generar evidencia técnica suficiente y formular recomendaciones de mitigación priorizadas.

5. Metodología de Pentest

La metodología aplicada para el desarrollo de la auditoría de ciberseguridad se basa en un enfoque técnico, sistemático y controlado, orientado a simular de forma autorizada las acciones que podría ejecutar un atacante real sobre la infraestructura objeto de evaluación. Este enfoque contempla fases sucesivas de planeación, levantamiento de información, identificación de vulnerabilidades, validación técnica de hallazgos, análisis de impacto y elaboración del informe final. La finalidad de la metodología no es afectar la continuidad operativa de la entidad, sino identificar debilidades de forma responsable y con el menor nivel de afectación posible sobre los servicios institucionales.

5.1 Planeación y definición de alcance

En esta fase se establece el alcance de la auditoría, los activos a evaluar, las restricciones operativas, las ventanas de ejecución, los responsables institucionales, los criterios de severidad, los mecanismos de contacto y escalamiento, así como las autorizaciones requeridas para la realización de las pruebas. También se identifican las dependencias tecnológicas críticas y se delimitan claramente los objetivos del ejercicio.

5.2 Recolección de información y reconocimiento

Corresponde a la identificación de activos, servicios, tecnologías, versiones, puntos de exposición, superficies de ataque y relaciones entre componentes. Esta fase incluye reconocimiento pasivo y activo, siempre dentro del alcance

autorizado, con el propósito de construir una visión técnica inicial de la arquitectura evaluada.

5.3 Análisis de vulnerabilidades

En esta etapa se realiza la identificación de debilidades técnicas, errores de configuración, fallas de autenticación, problemas de autorización, exposición de información sensible, validaciones insuficientes, servicios inseguros, controles ausentes o mal implementados y otros hallazgos relevantes. El análisis podrá apoyarse en herramientas especializadas y en validaciones manuales por parte del equipo auditor.

5.4 Explotación controlada y validación técnica

Una vez identificadas las posibles vulnerabilidades, se procede a validar técnicamente aquellas que resulten pertinentes, siempre bajo un enfoque controlado y autorizado. La explotación se ejecuta únicamente con fines de comprobación, evitando afectar la disponibilidad de los servicios o alterar indebidamente la información institucional. El objetivo de esta fase es confirmar la existencia real de la vulnerabilidad, determinar su explotabilidad y medir su impacto potencial.

5.5 Análisis de impacto y priorización

Los hallazgos confirmados son analizados considerando el nivel de exposición del activo, la facilidad de explotación, el impacto sobre la confidencialidad, integridad y disponibilidad, el alcance del compromiso potencial y el riesgo institucional asociado. Con base en ello, se asigna una criticidad que permita priorizar las acciones de remediación.

5.6 Documentación y reporte

Finalmente, se consolidan los hallazgos en el presente informe, incluyendo descripción técnica, evidencia, impacto, criticidad y recomendaciones de mitigación. El informe busca servir como insumo técnico y de gestión para que Supertransporte adopte medidas correctivas, preventivas y de fortalecimiento continuo de su postura de ciberseguridad.

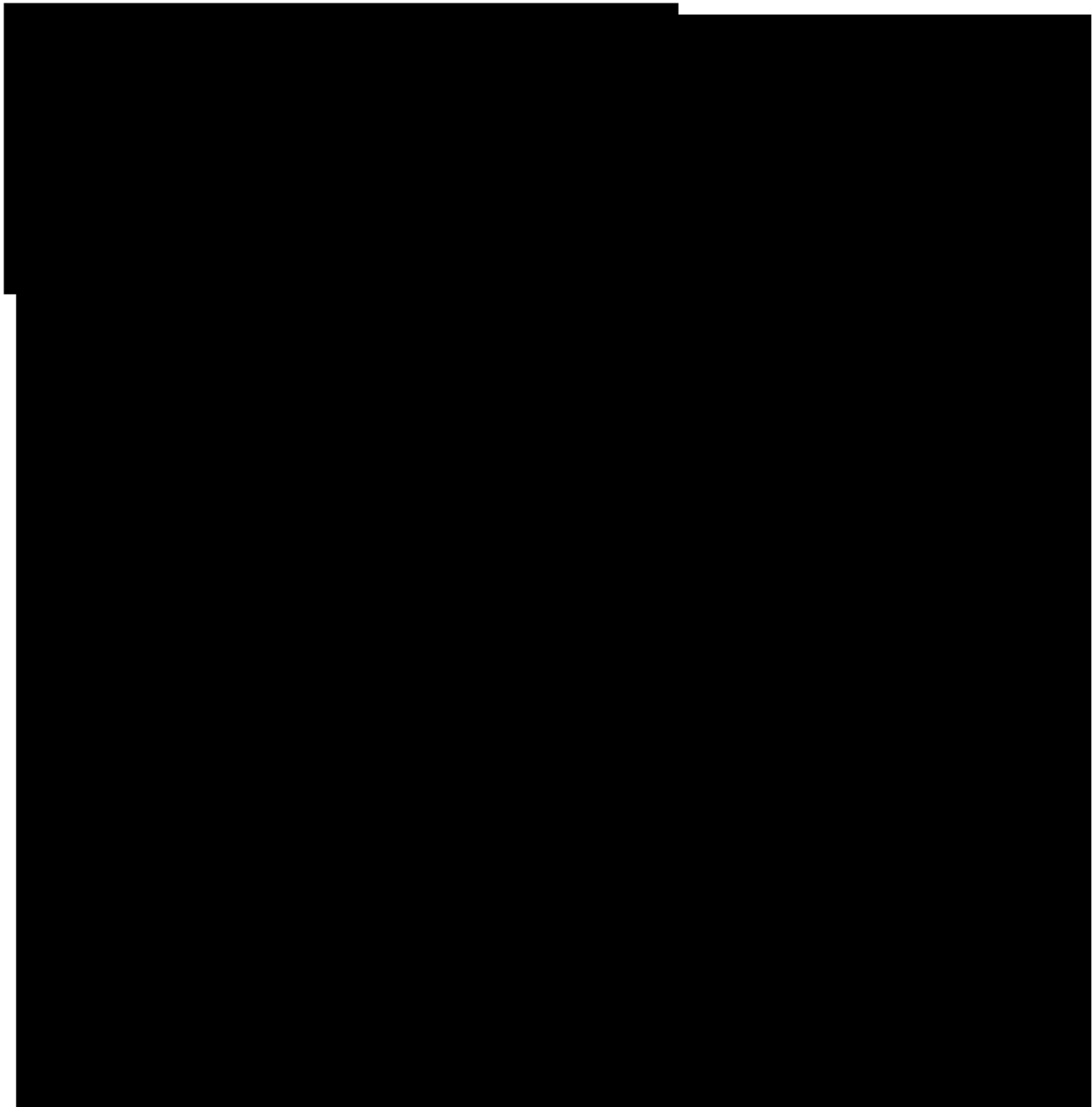


Agencia
Nacional Digital



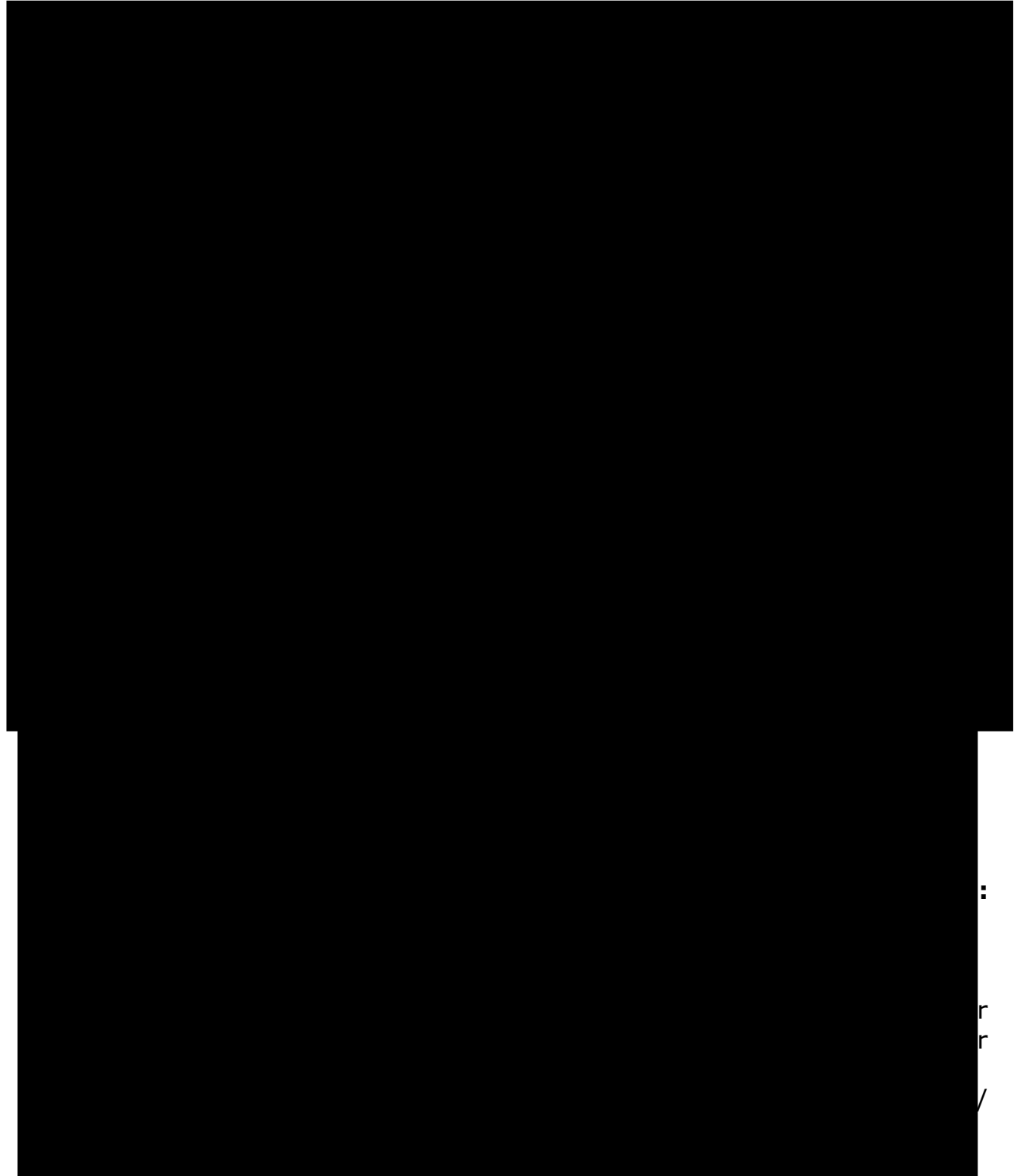
6. Hallazgos

En el marco de la metodología definida para la presente auditoría, las actividades de evaluación técnica fueron ejecutadas desde la red interna institucional, haciendo uso de credenciales autorizadas y suministradas para la correcta realización de las pruebas de seguridad contempladas dentro del



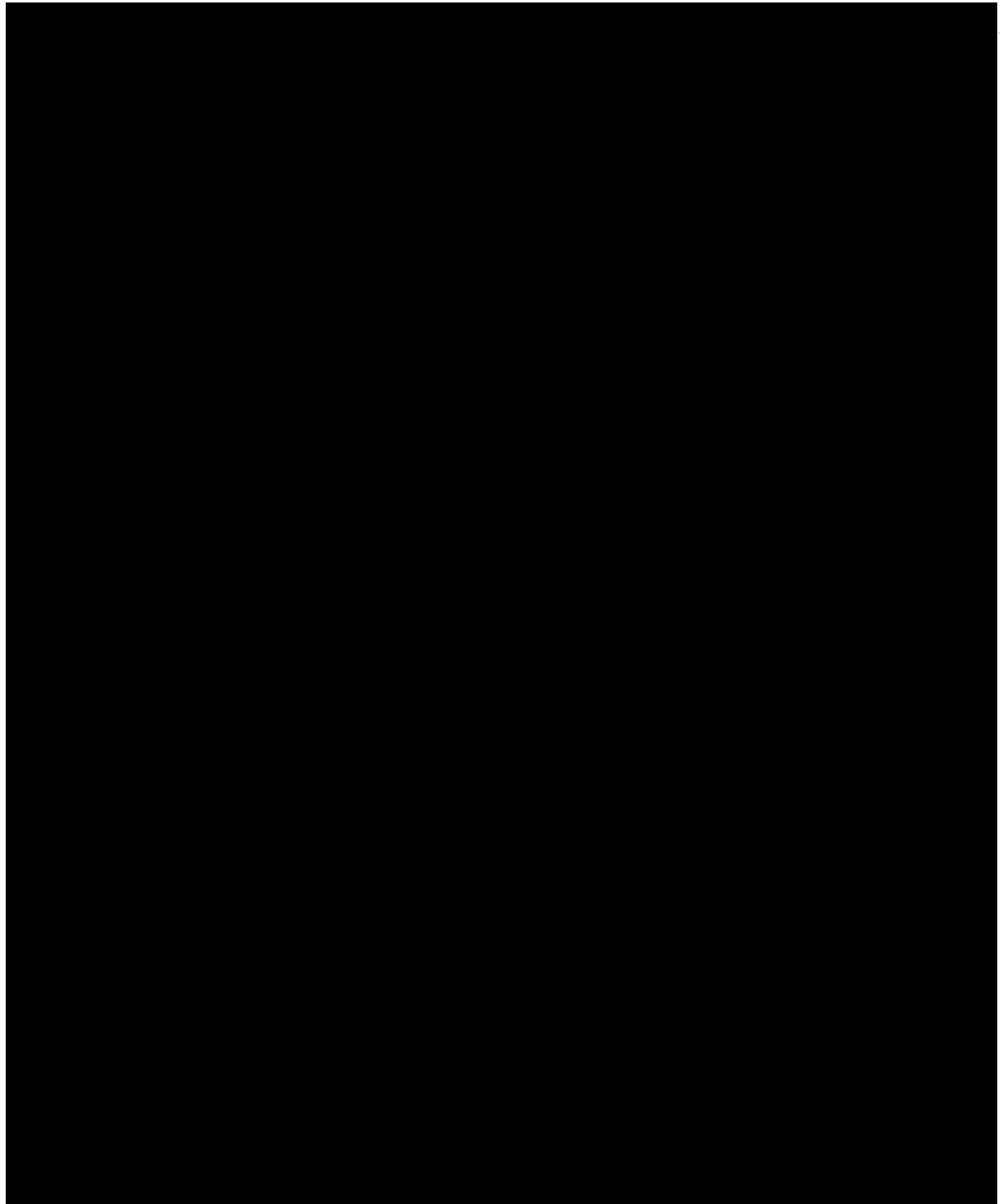


Agencia Nacional Digital



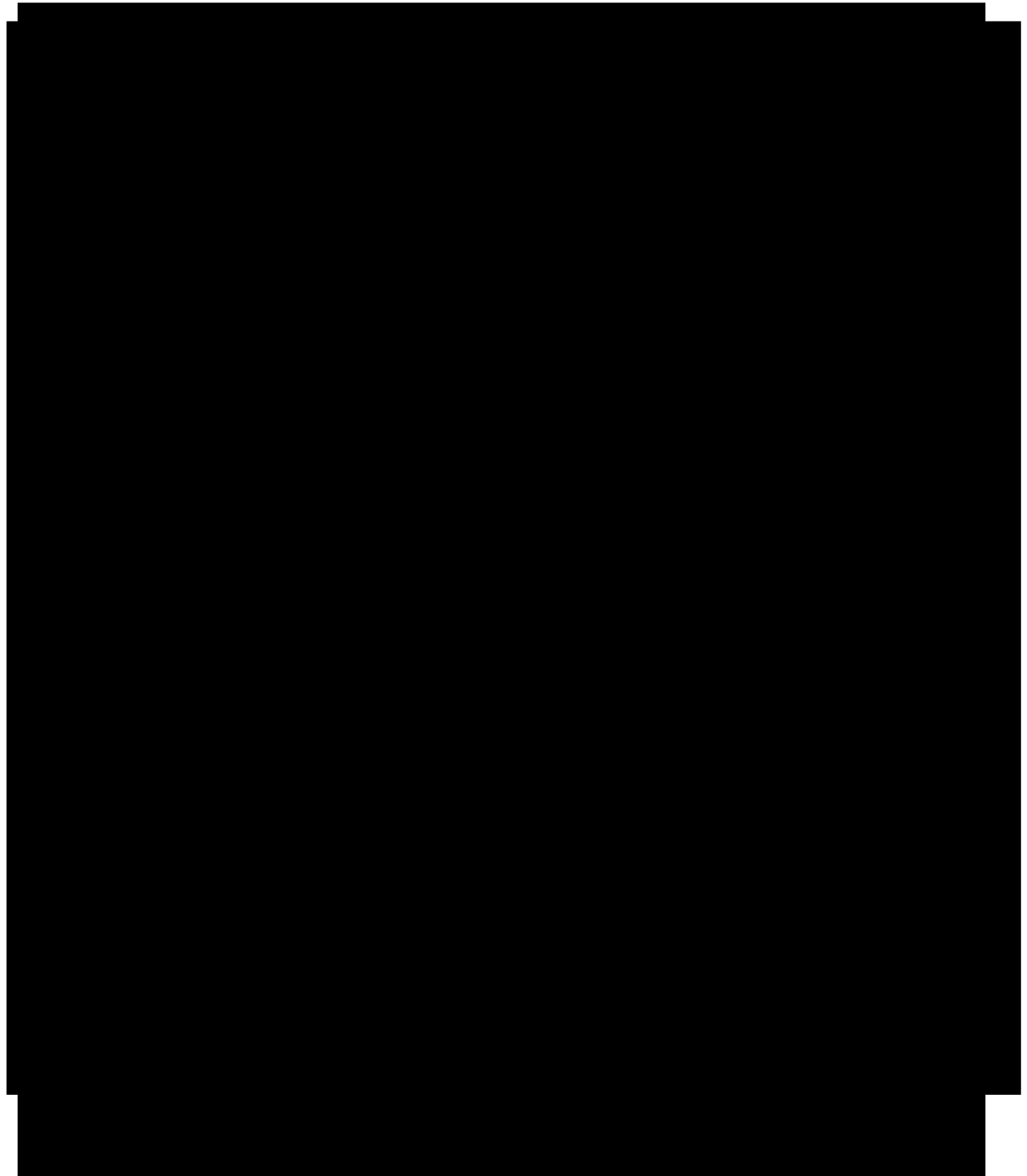


Agencia Nacional Digital





Agencia
Nacional Digital



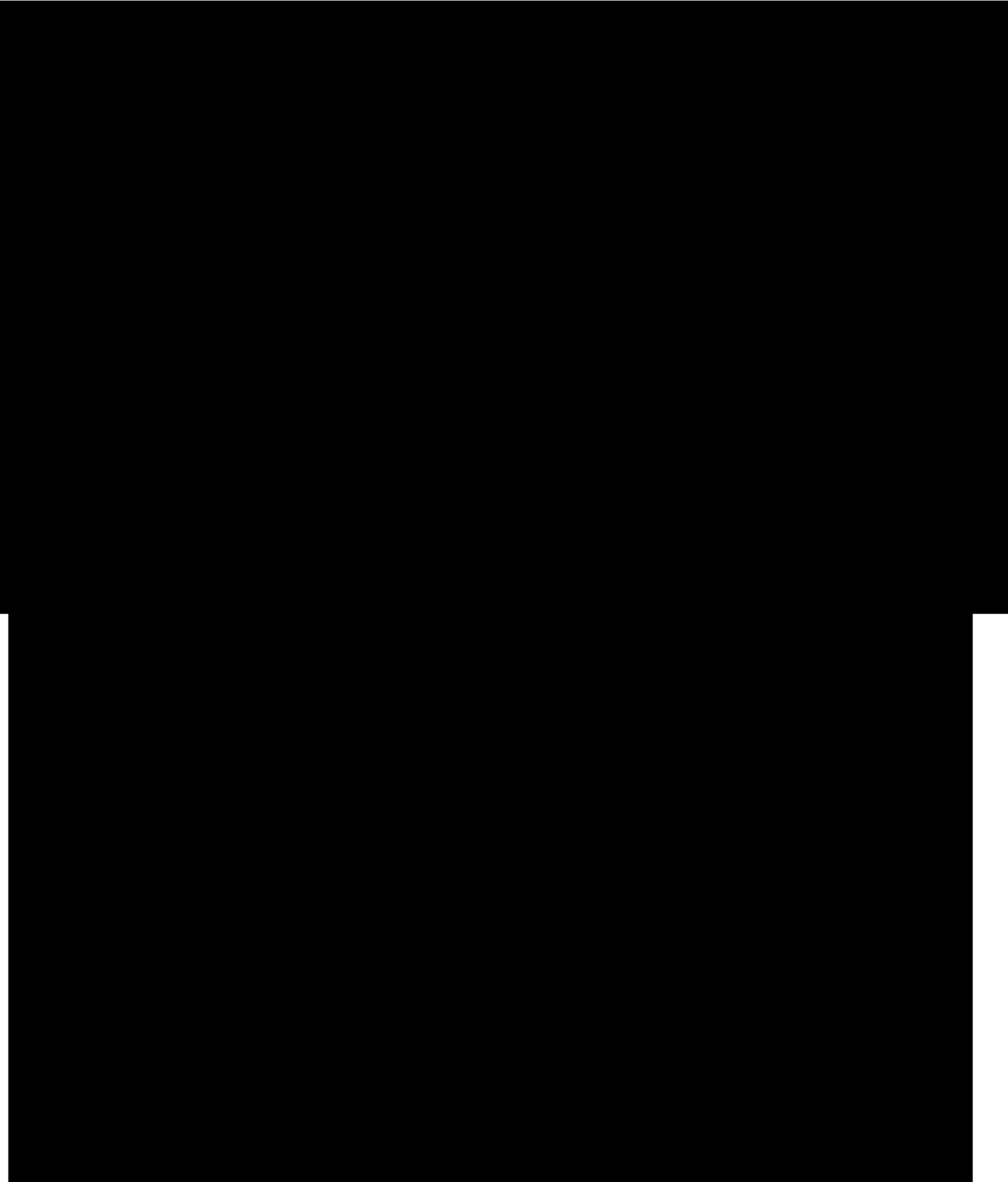


Agencia
Nacional Digital



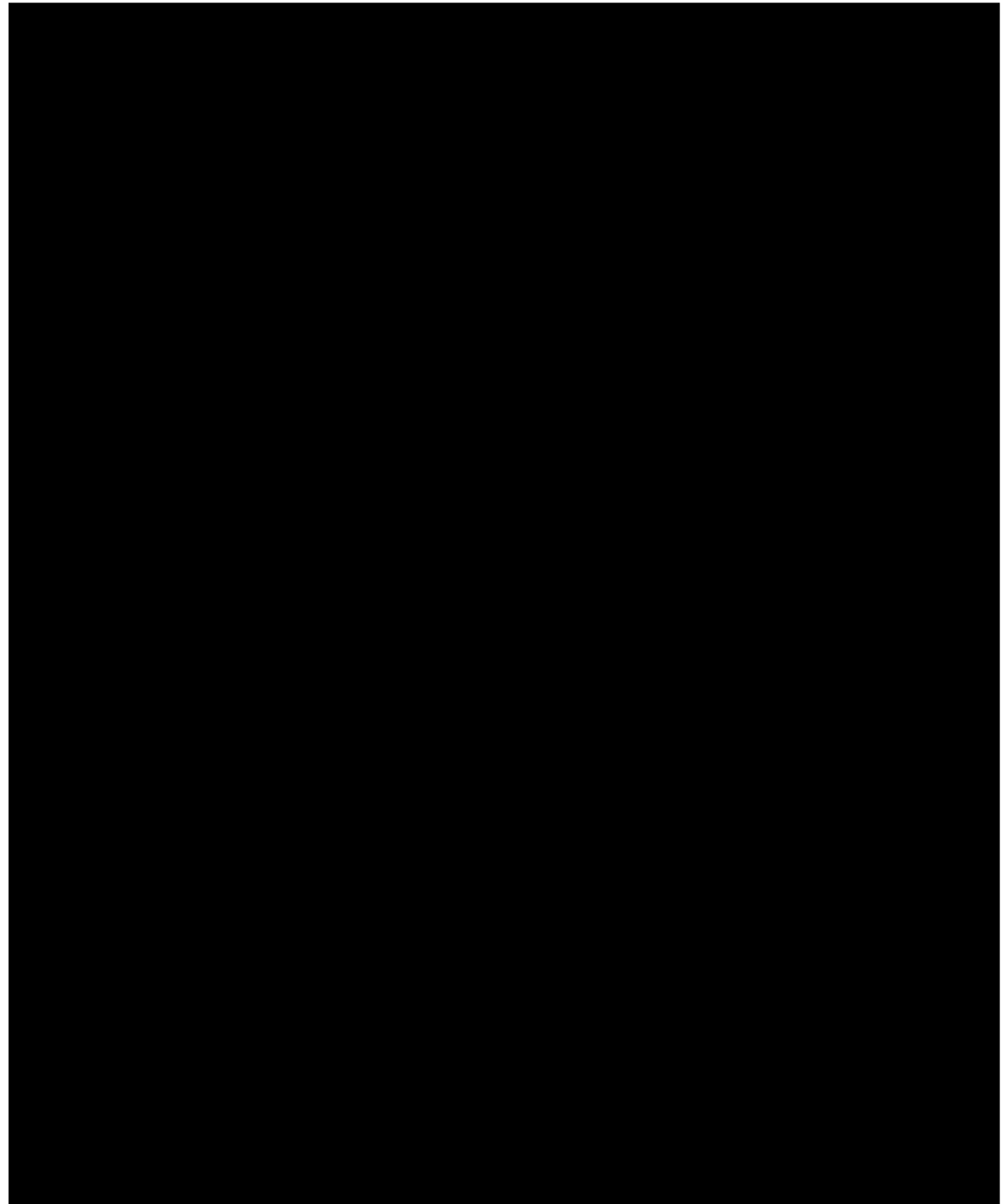


Agencia
Nacional Digital



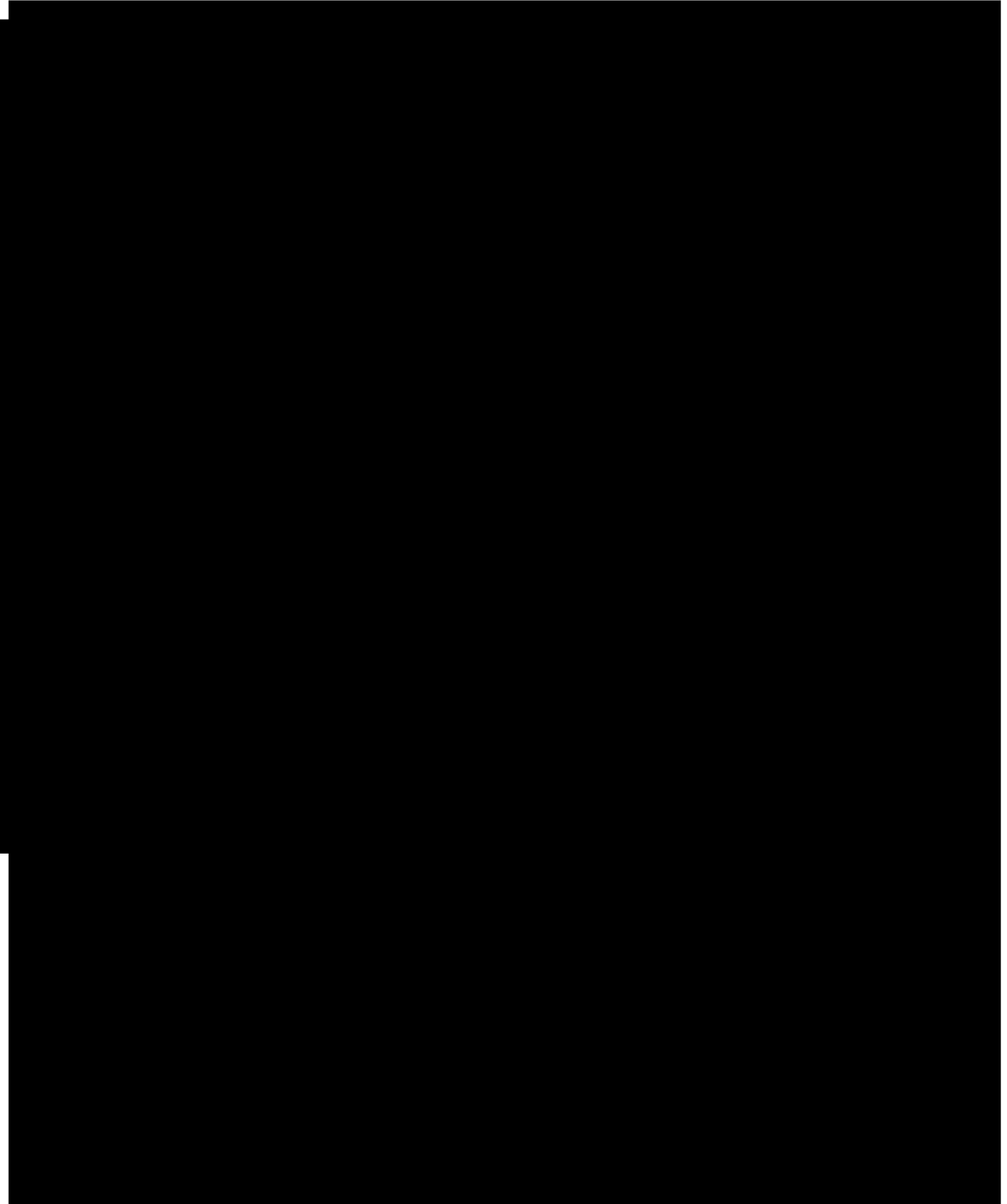


Agencia
Nacional Digital





Agencia
Nacional Digital





Agencia
Nacional Digital





Agencia
Nacional Digital



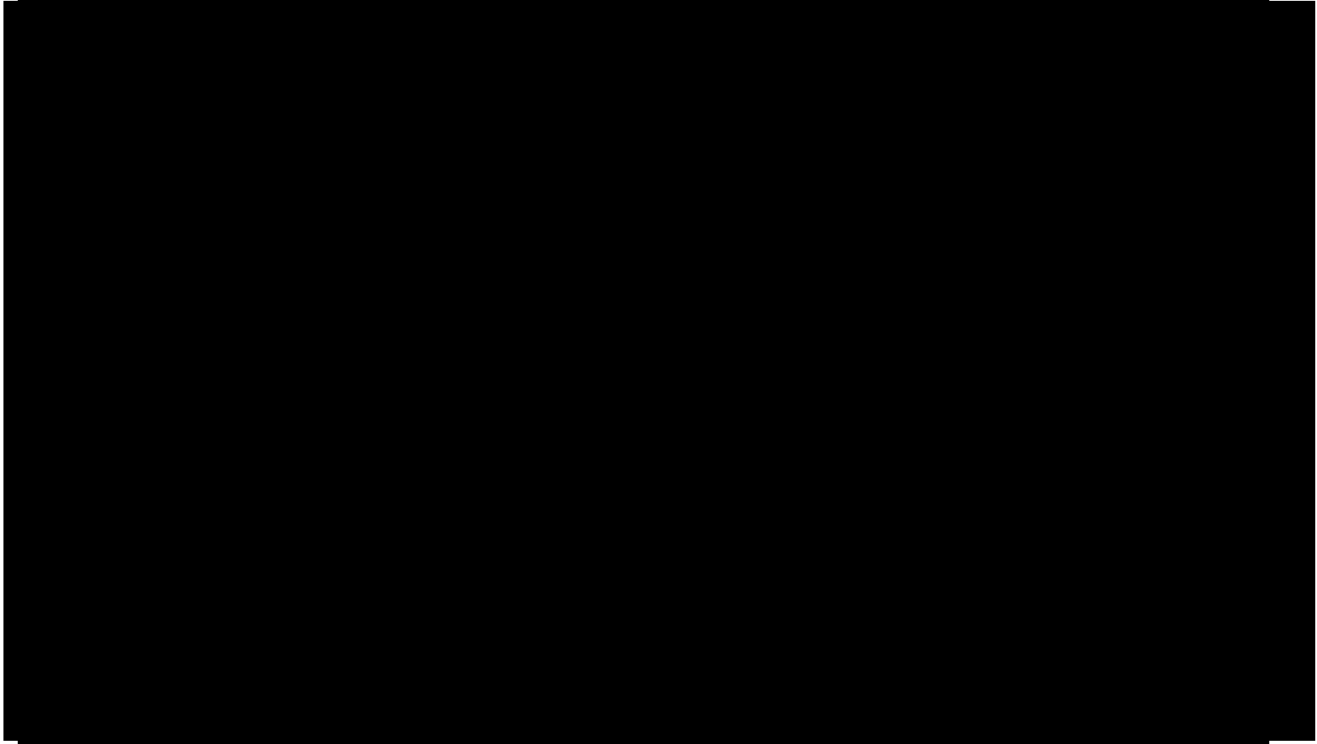
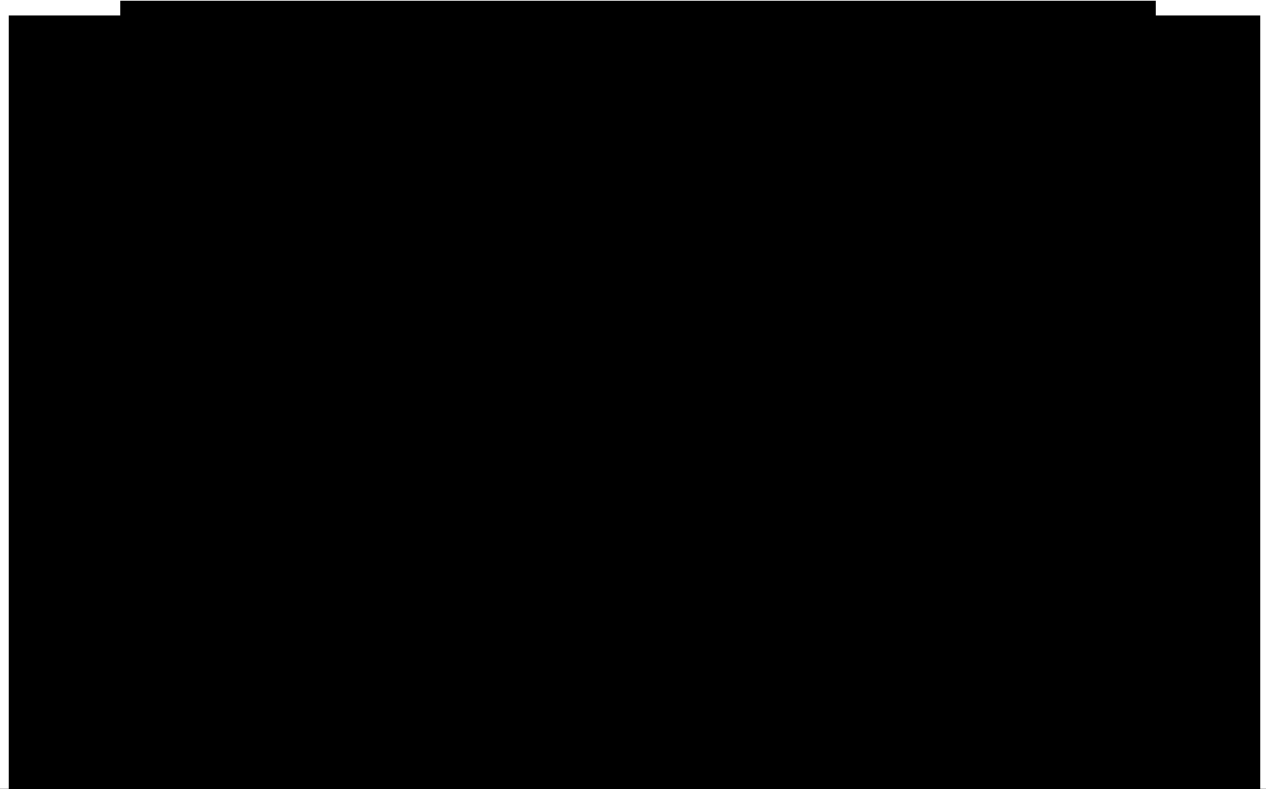


Agencia
Nacional Digital





Agencia Nacional Digital



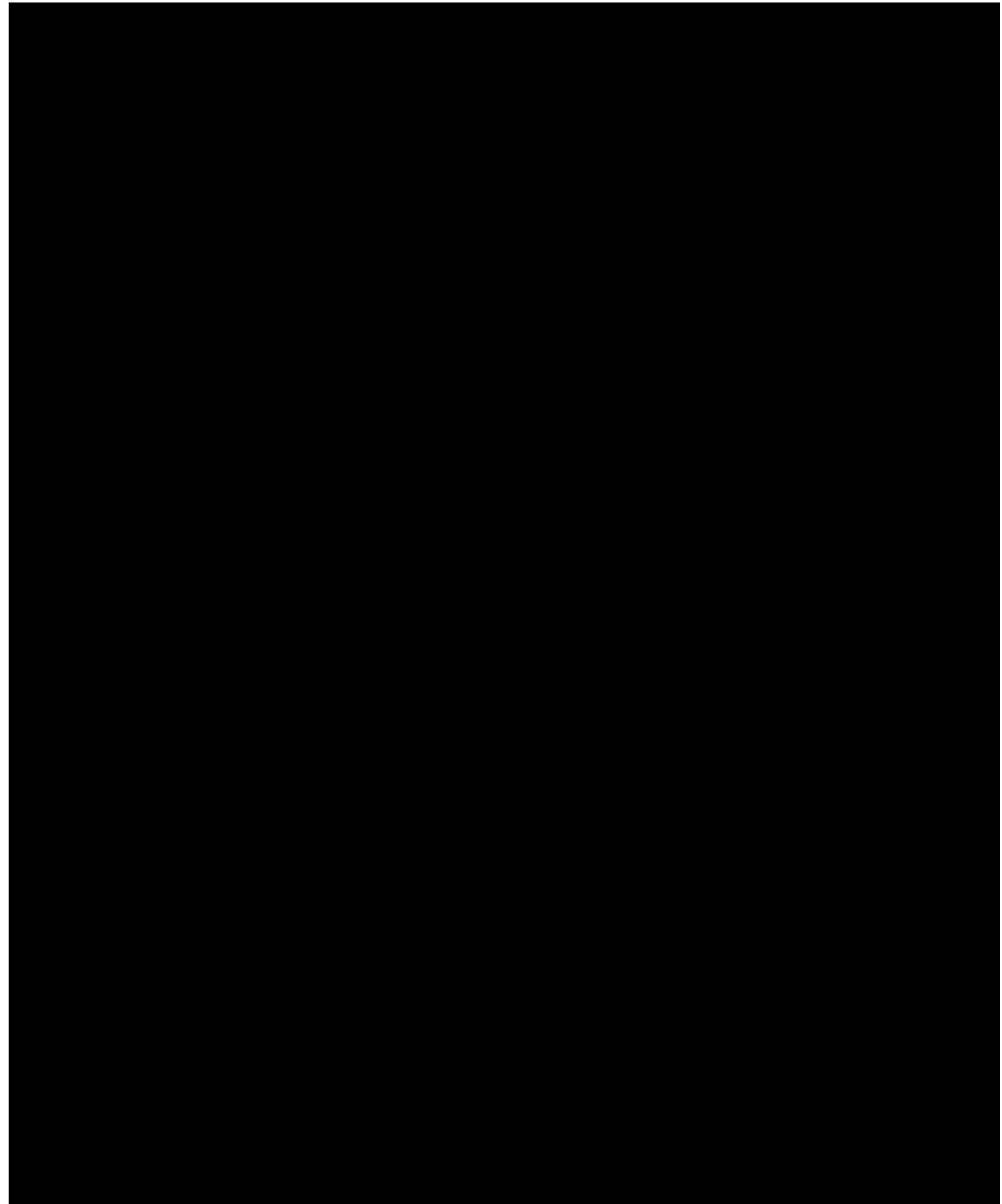


Agencia
Nacional Digital





Agencia
Nacional Digital



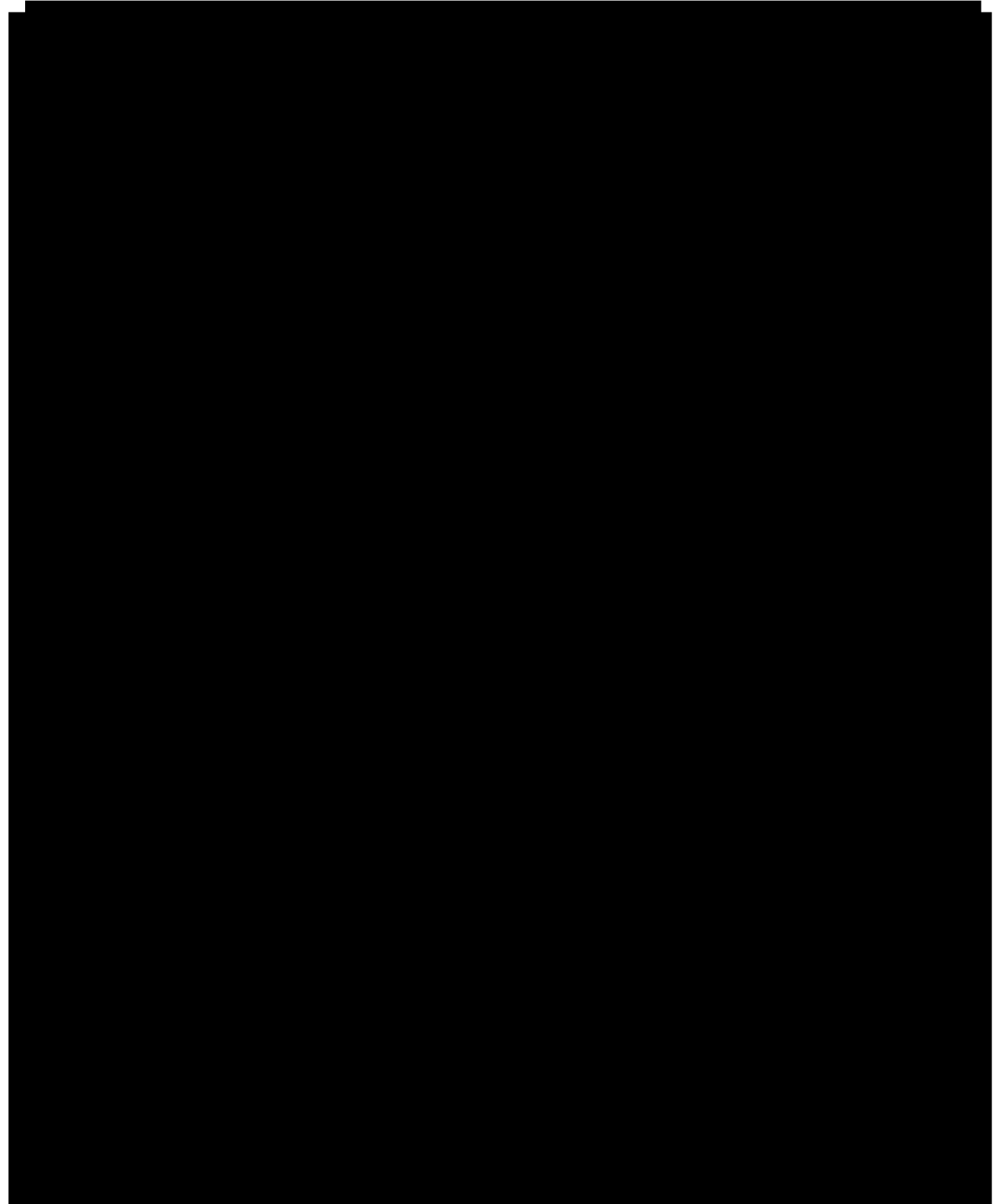


Agencia
Nacional Digital



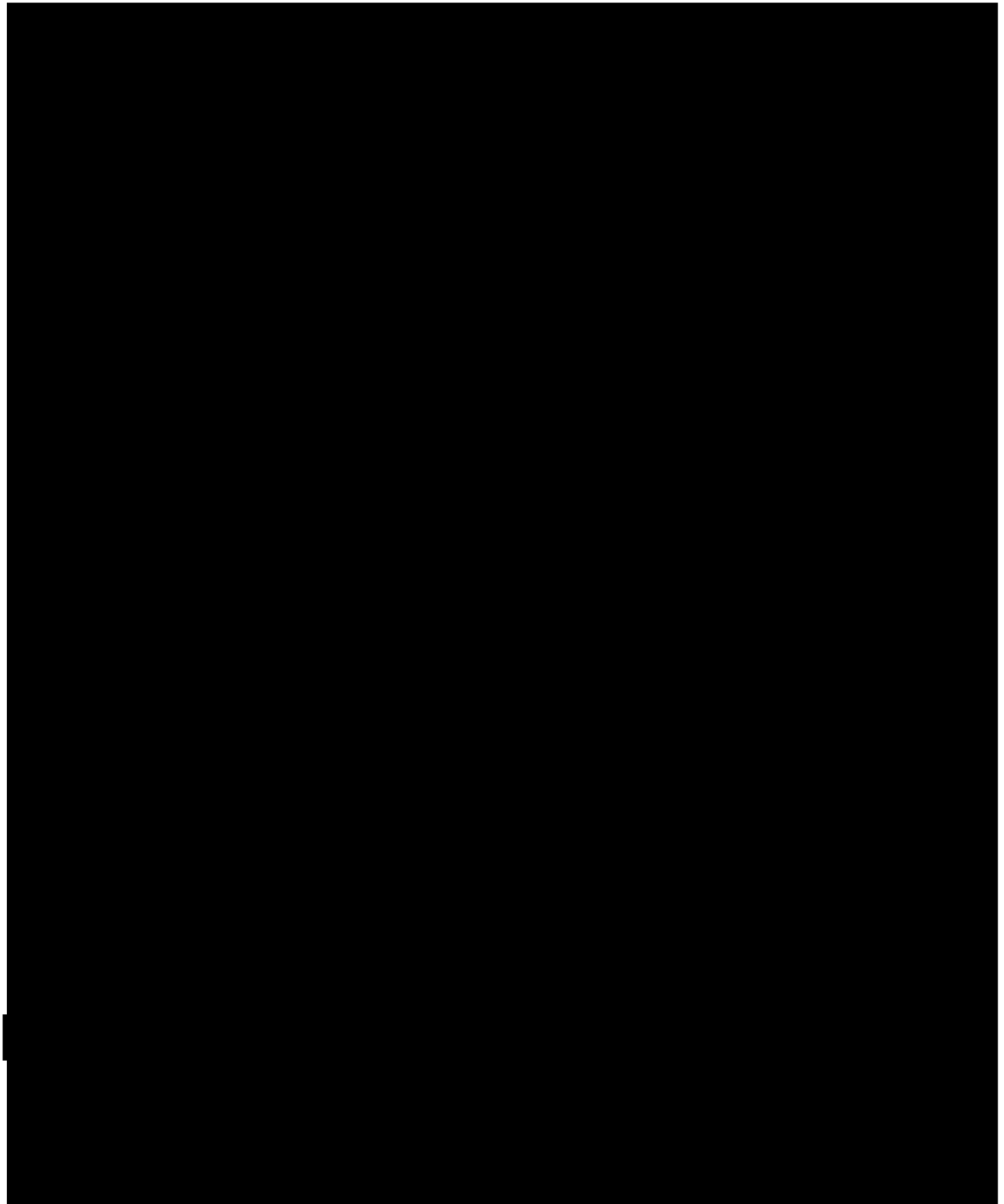


Agencia
Nacional Digital



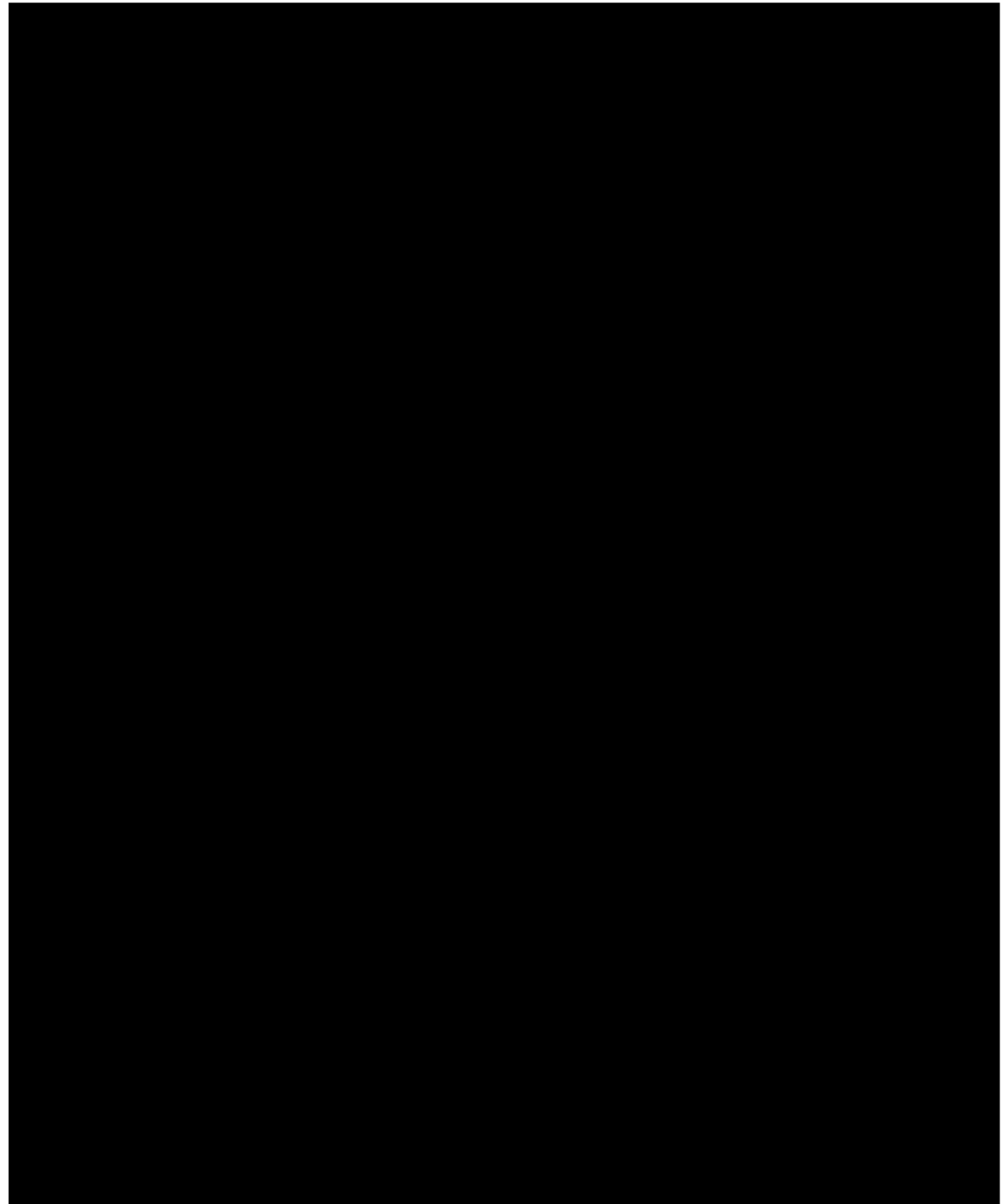


Agencia
Nacional Digital



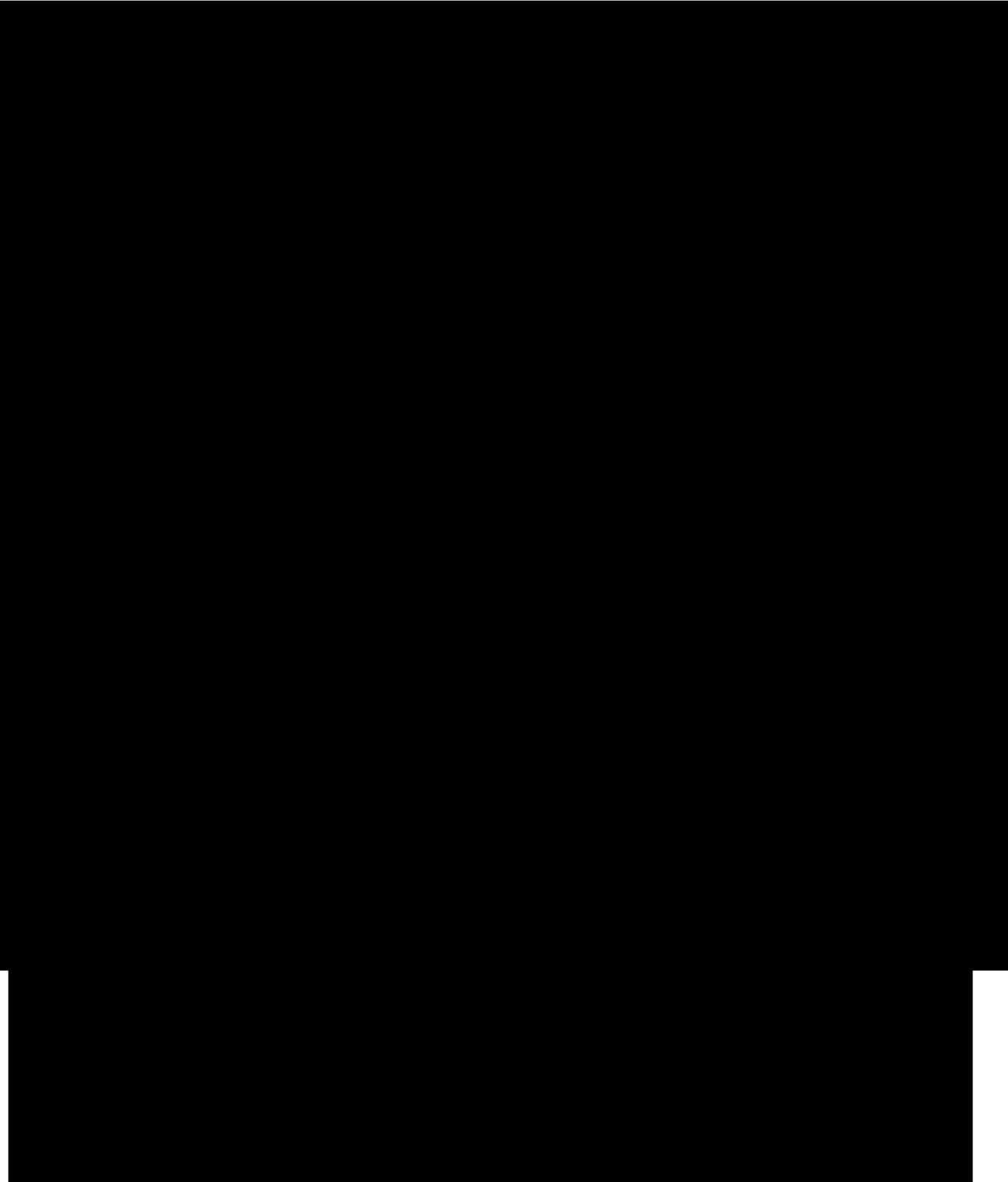


Agencia
Nacional Digital



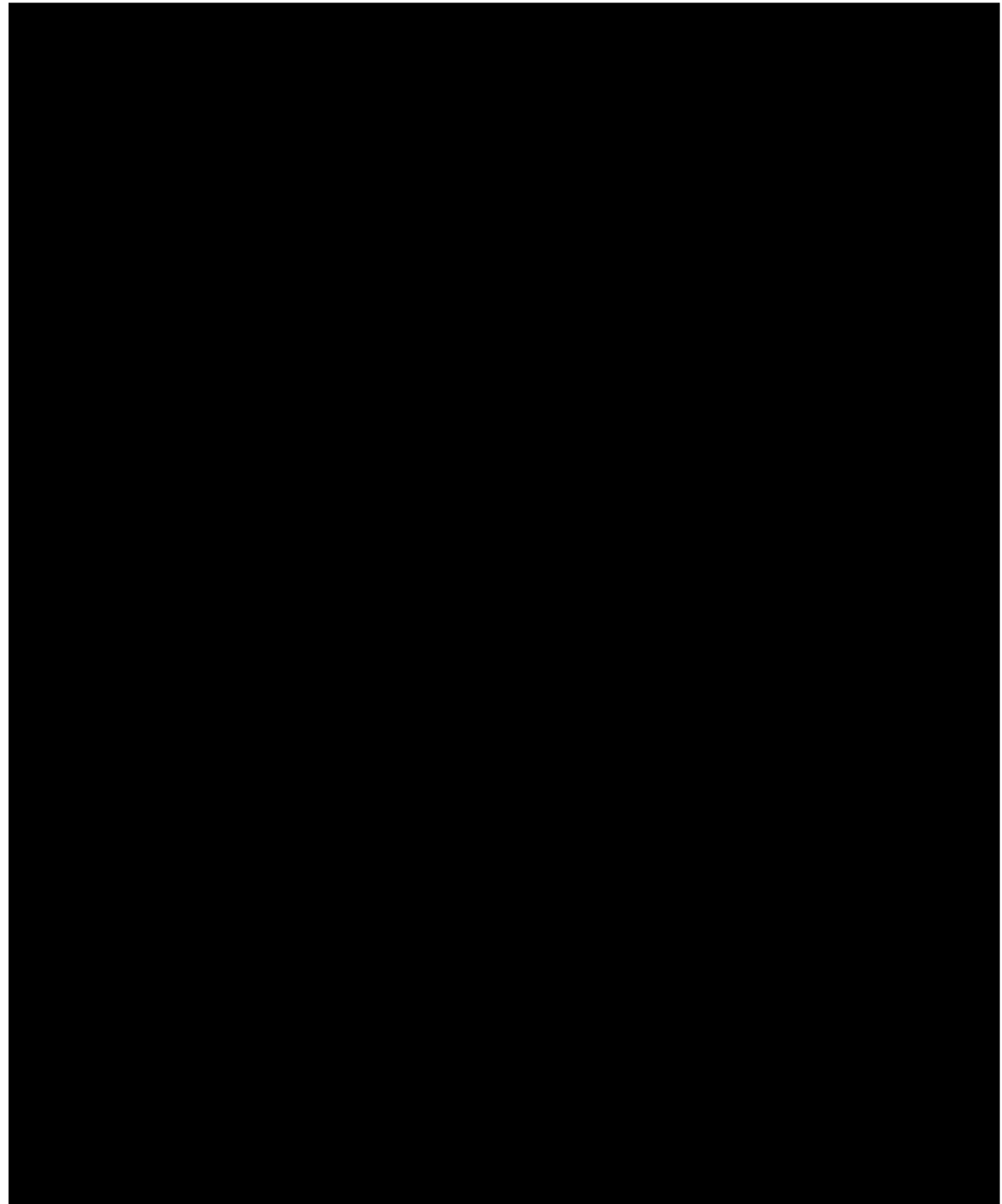


Agencia
Nacional Digital



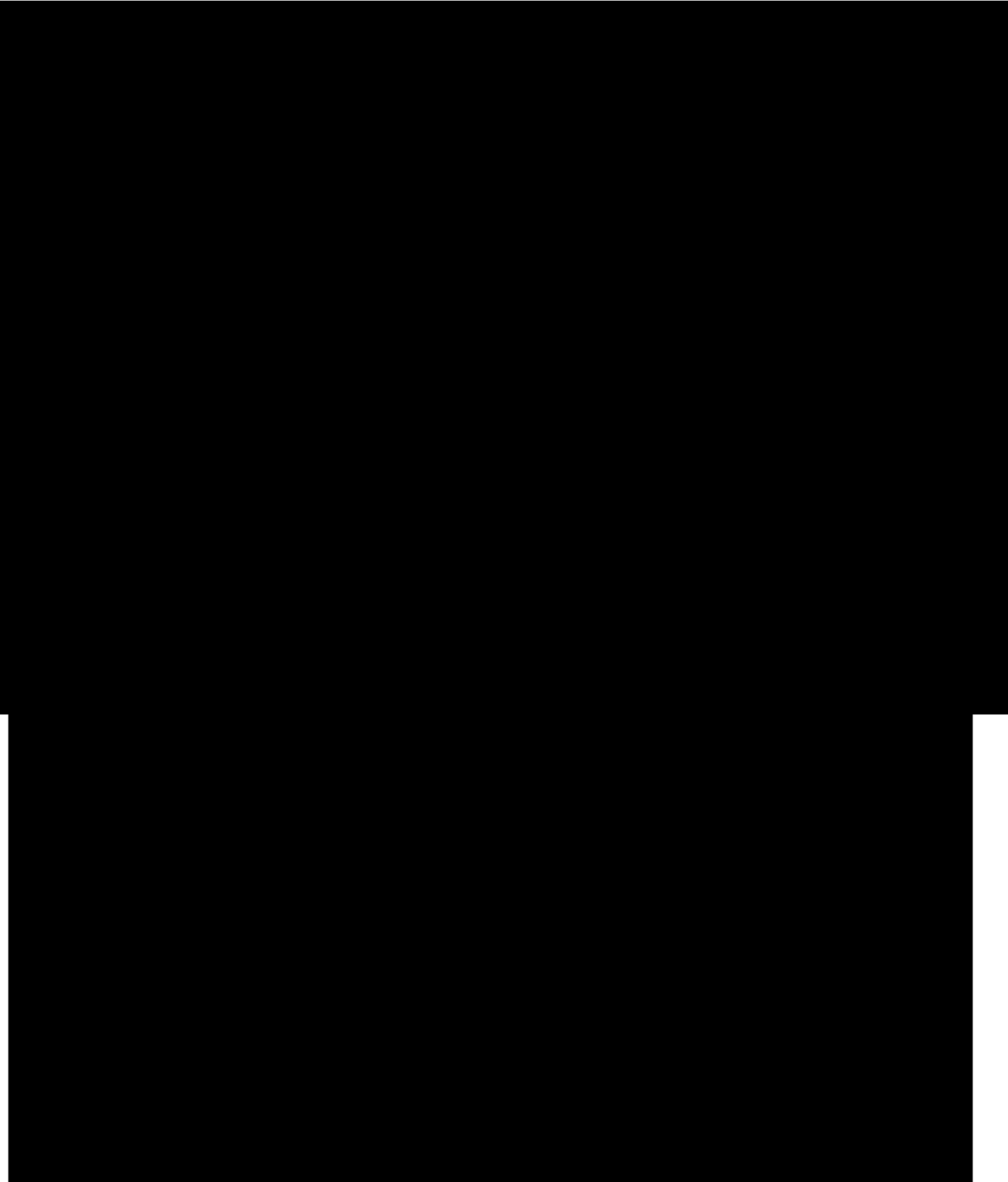


Agencia
Nacional Digital



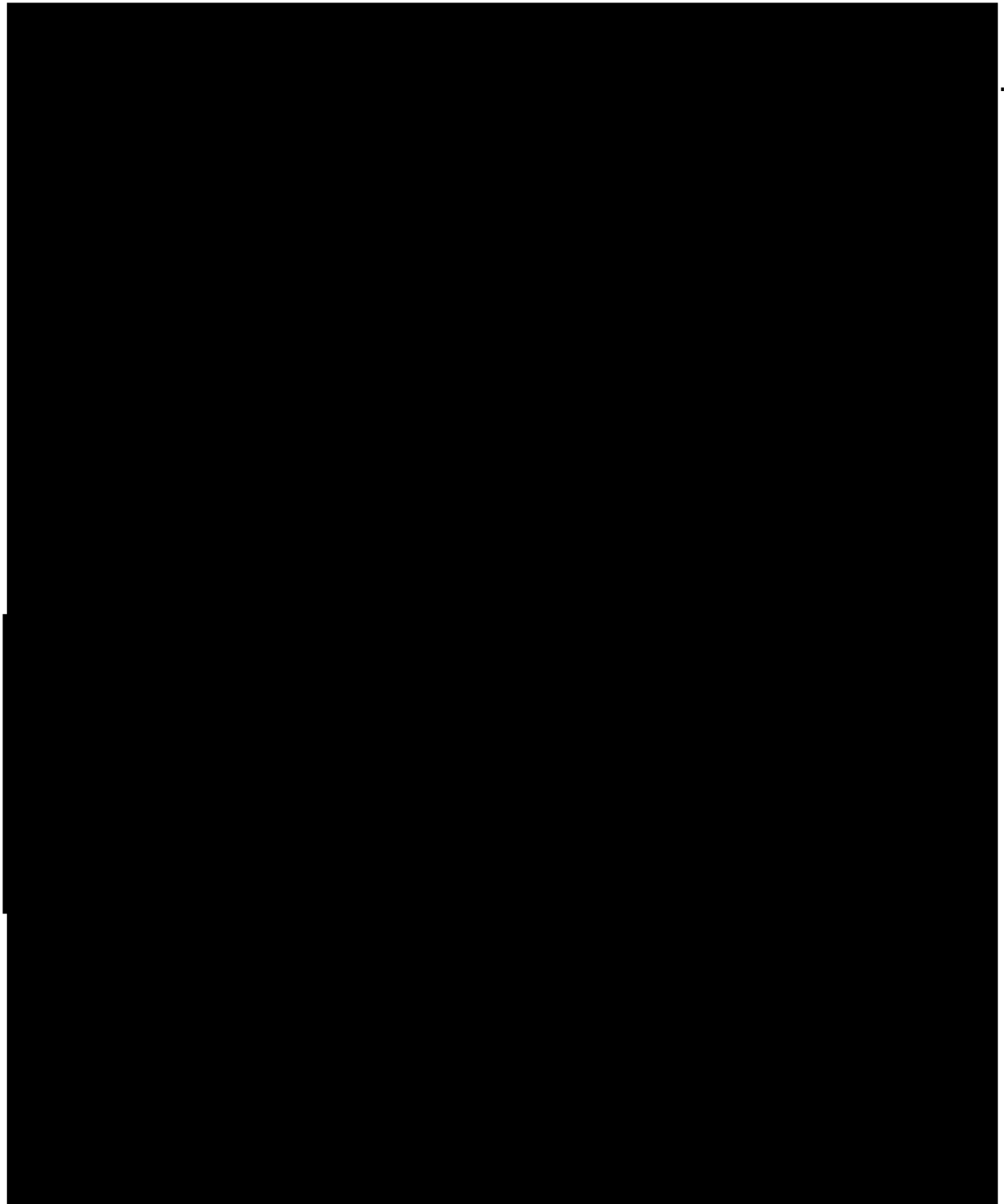


Agencia Nacional Digital



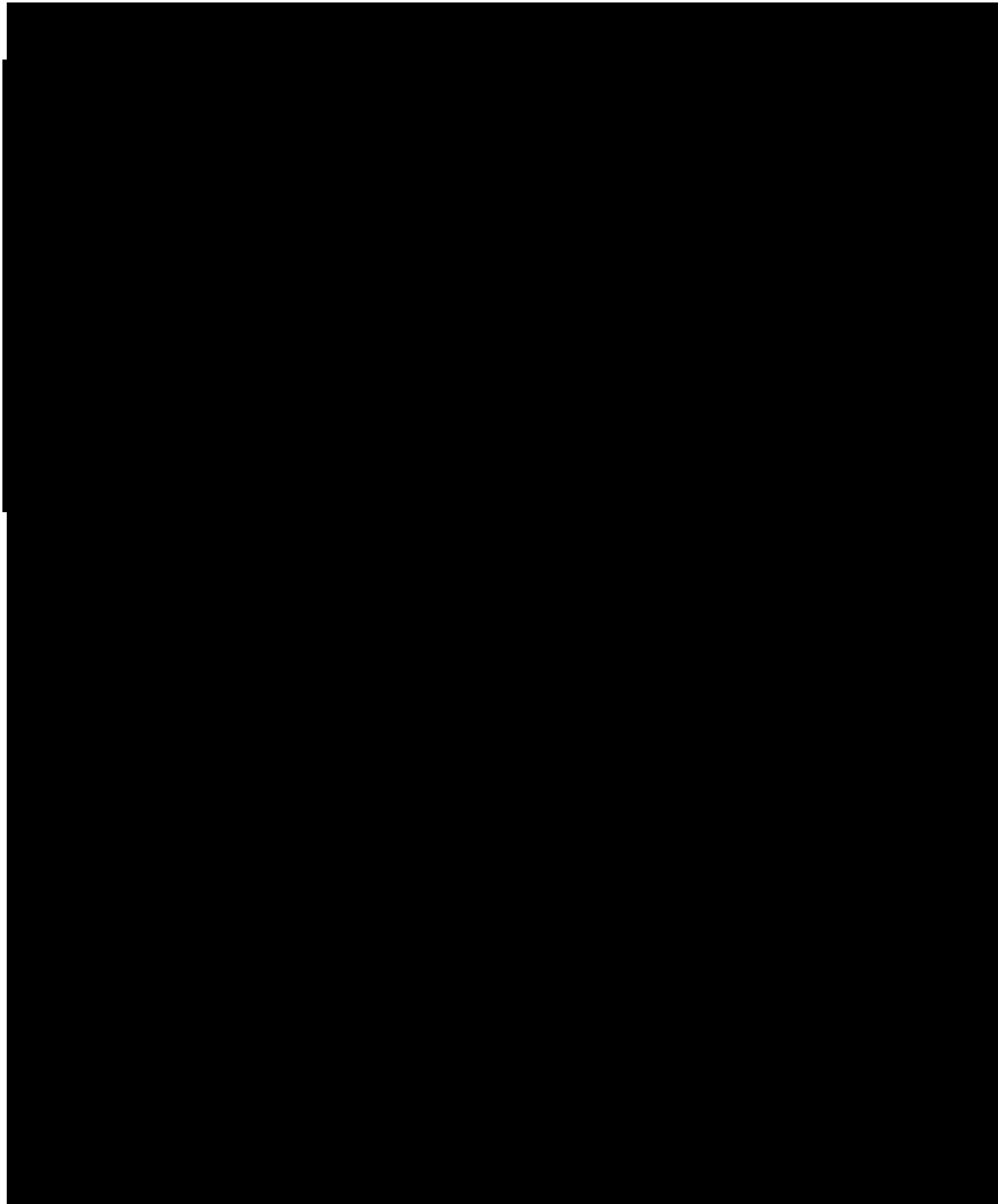


Agencia
Nacional Digital



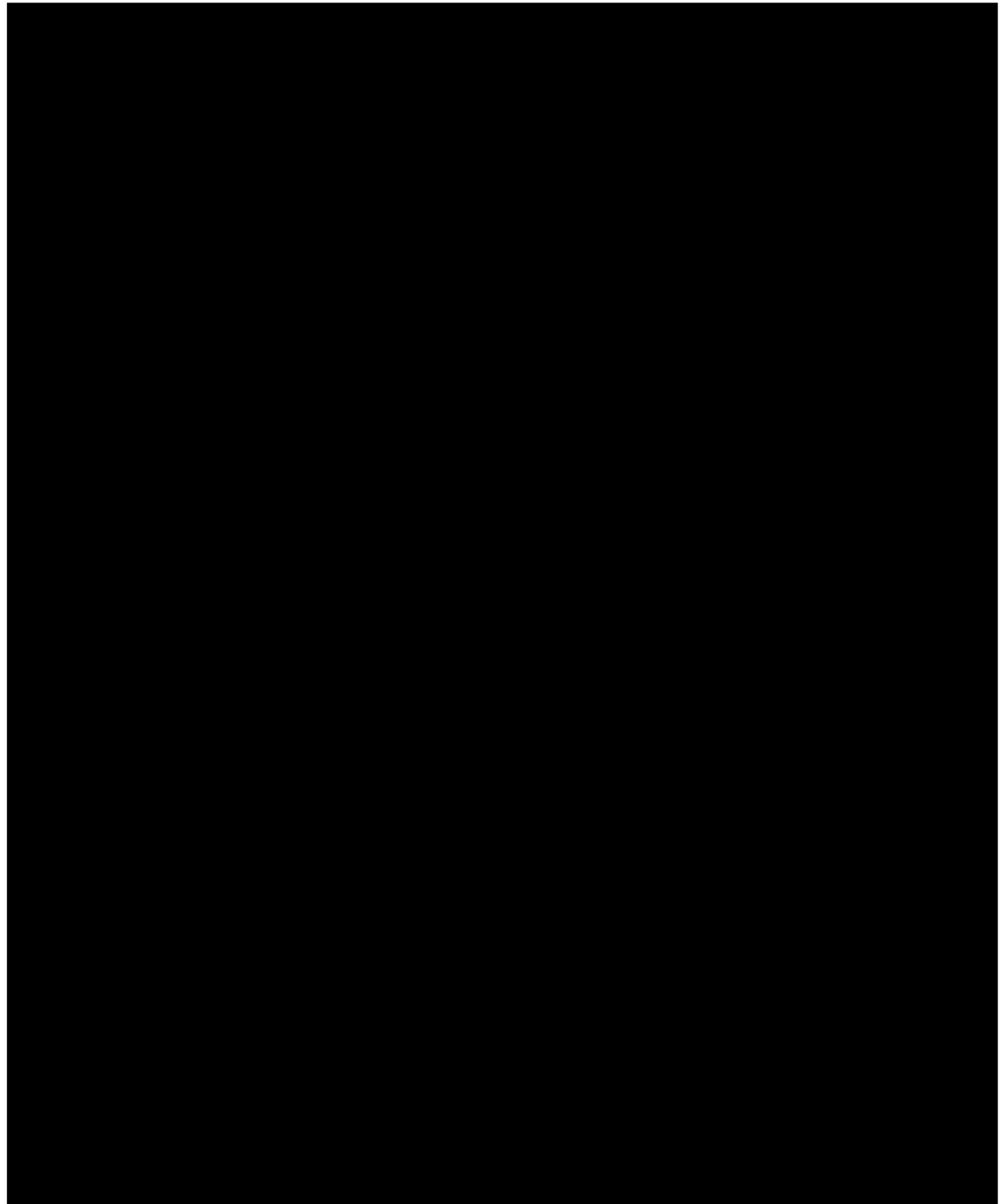


Agencia Nacional Digital



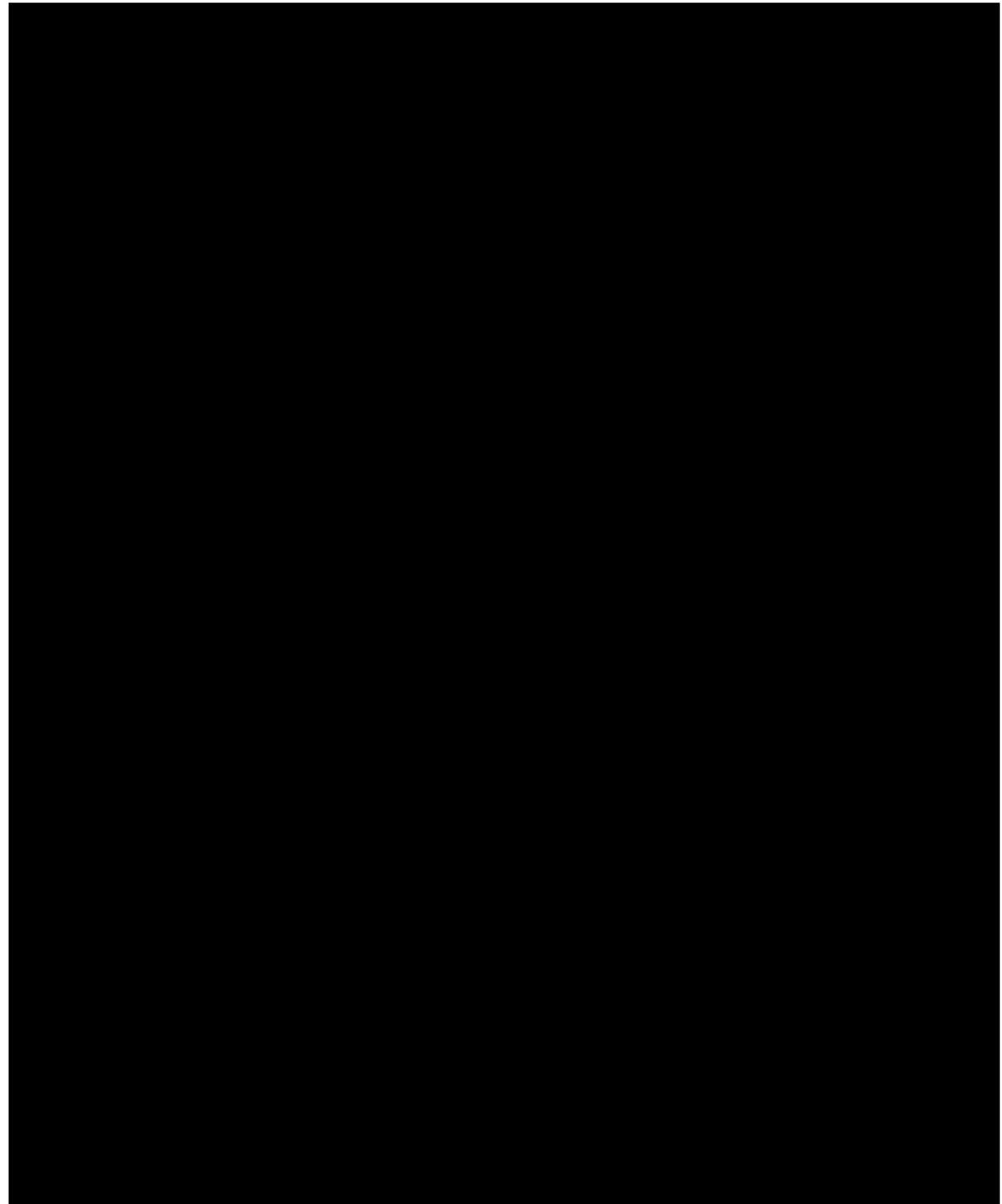


Agencia
Nacional Digital



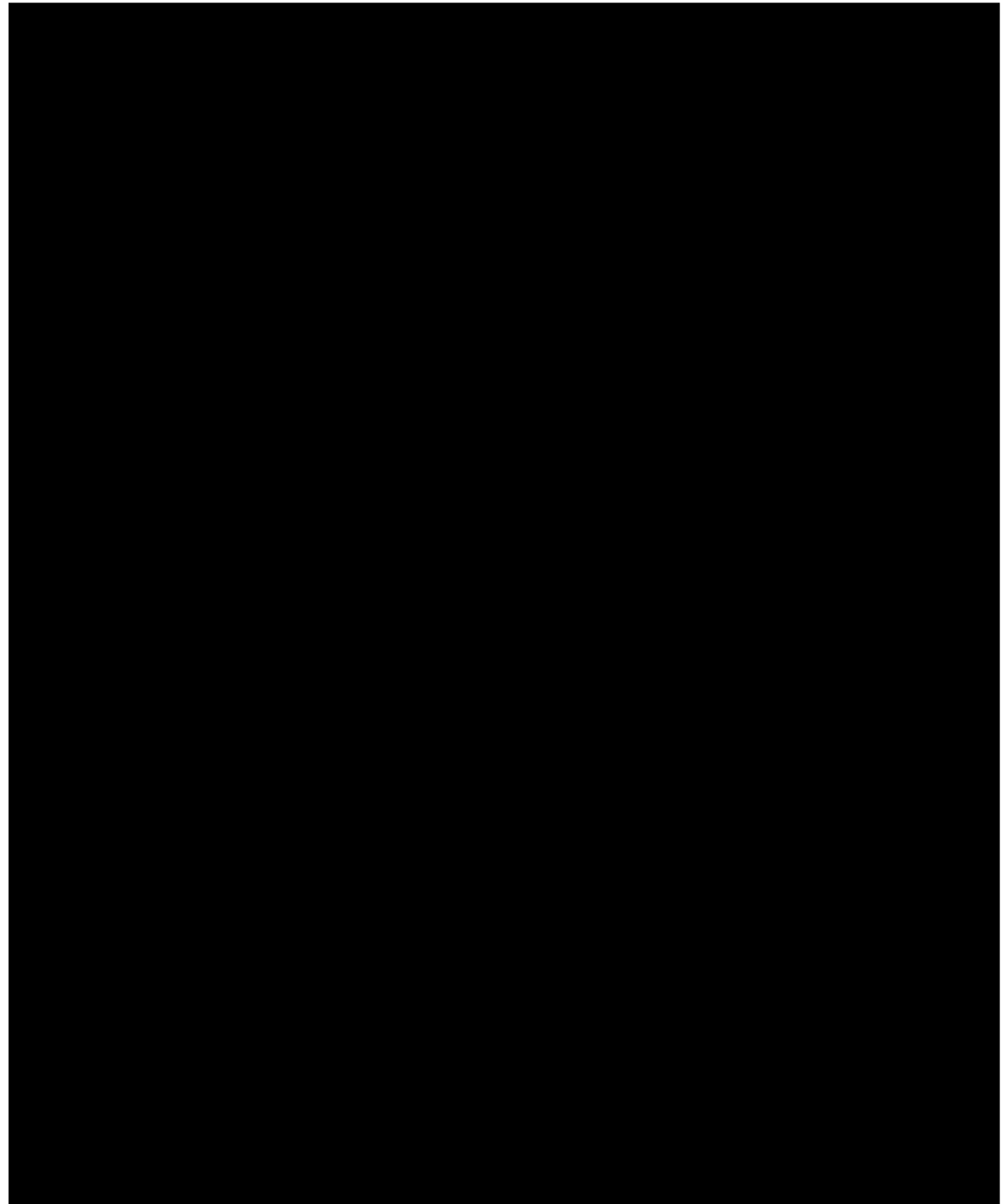


Agencia
Nacional Digital





Agencia
Nacional Digital





Agencia
Nacional Digital



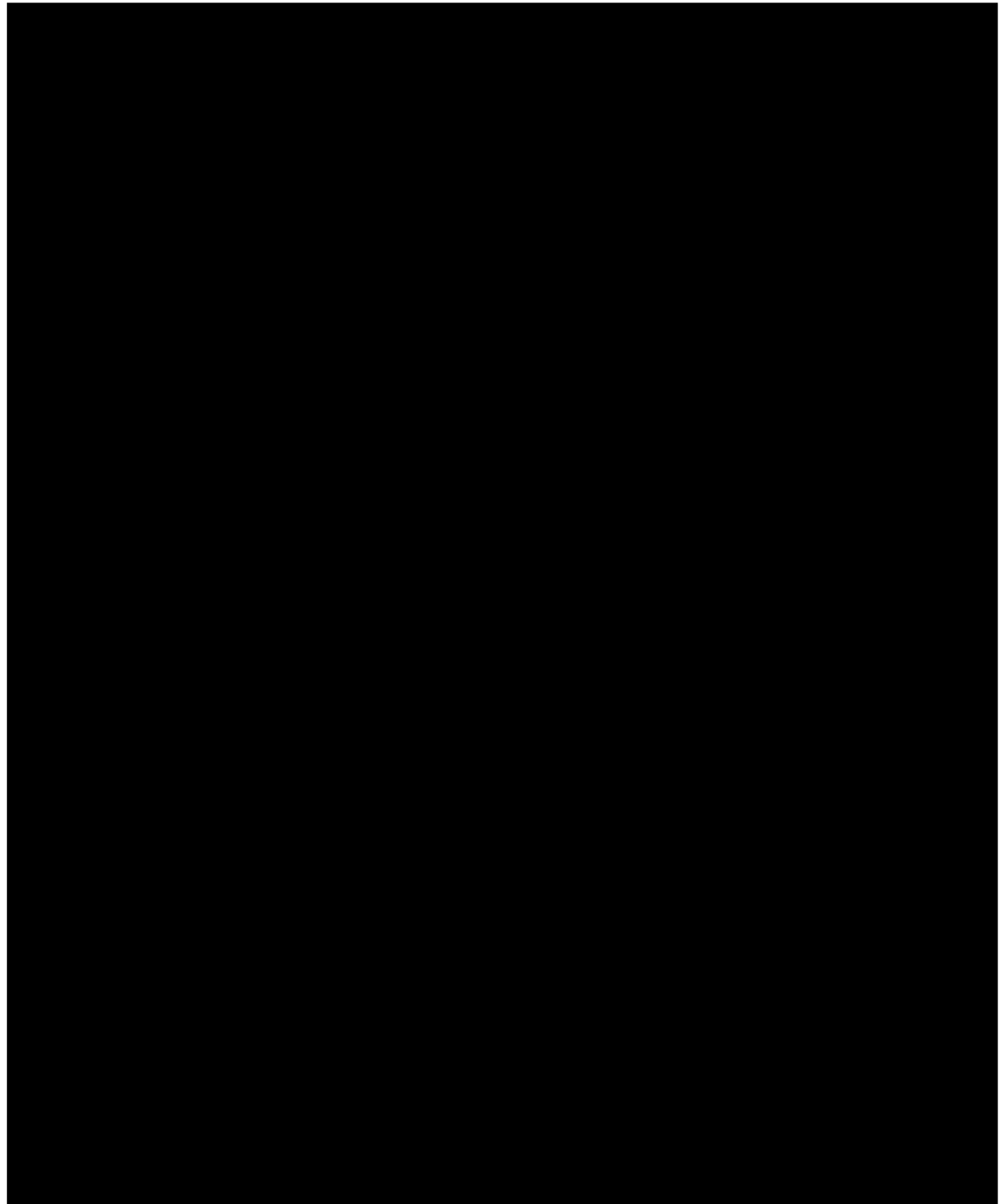


Agencia
Nacional Digital



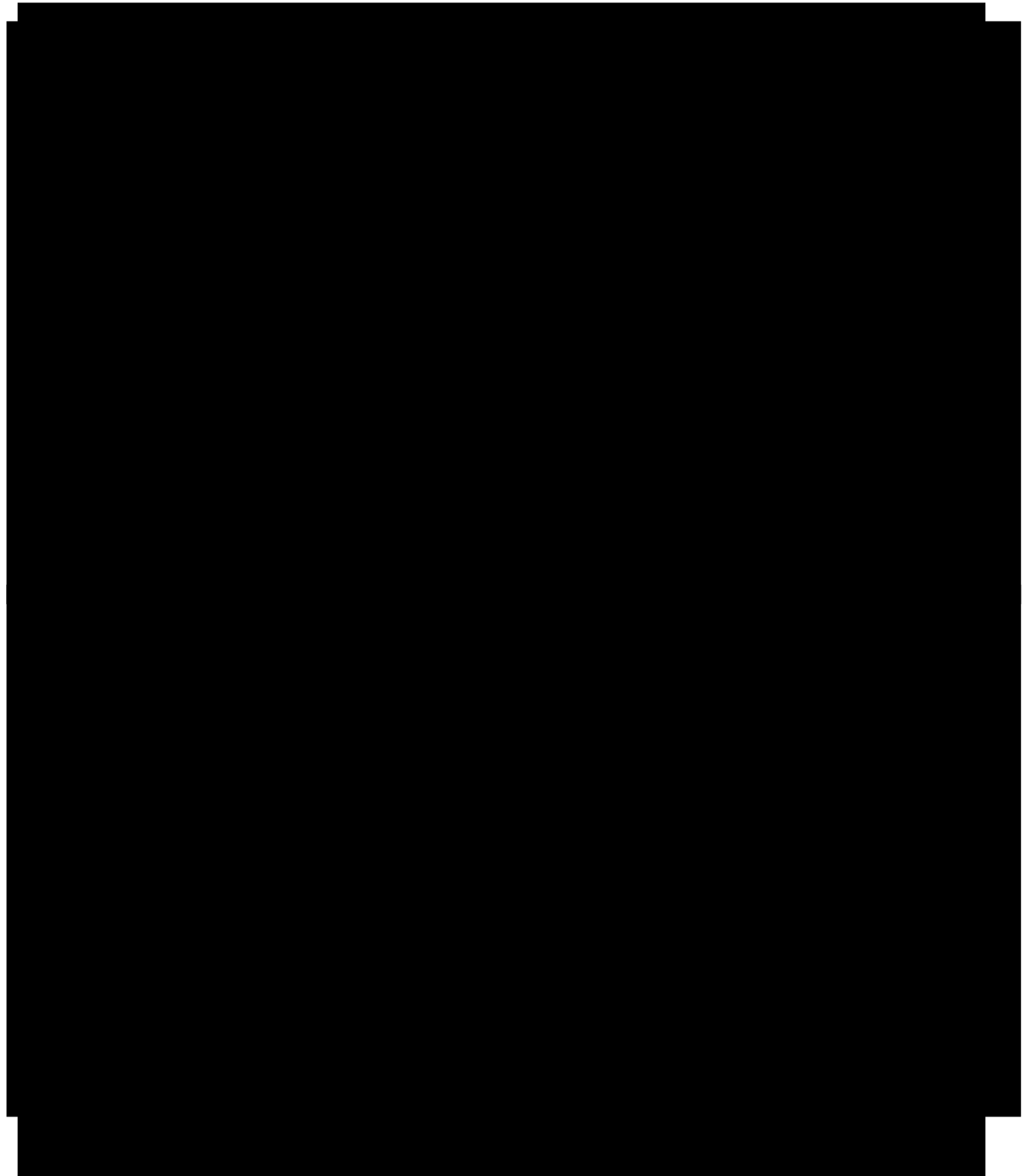


Agencia
Nacional Digital



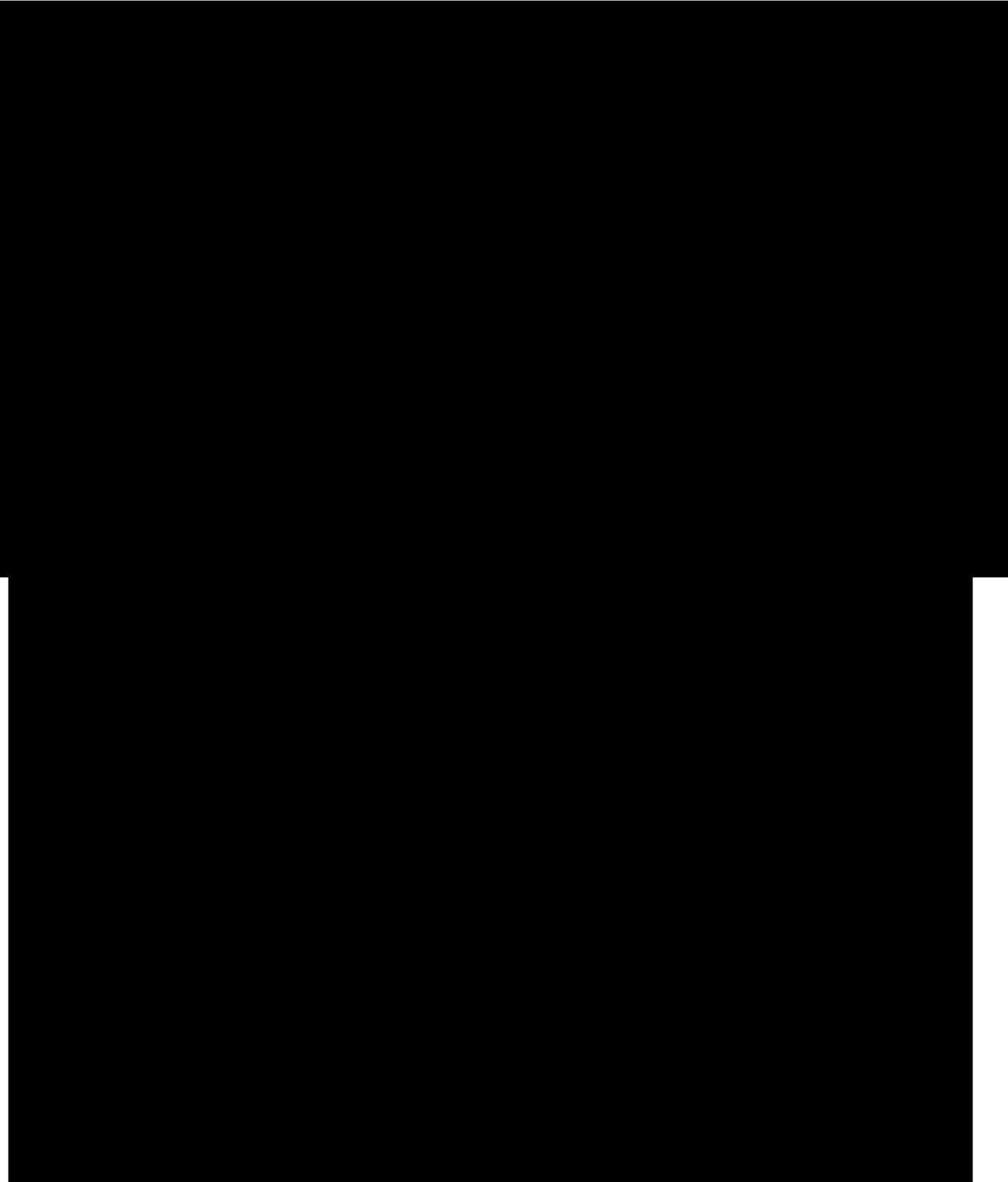


Agencia
Nacional Digital



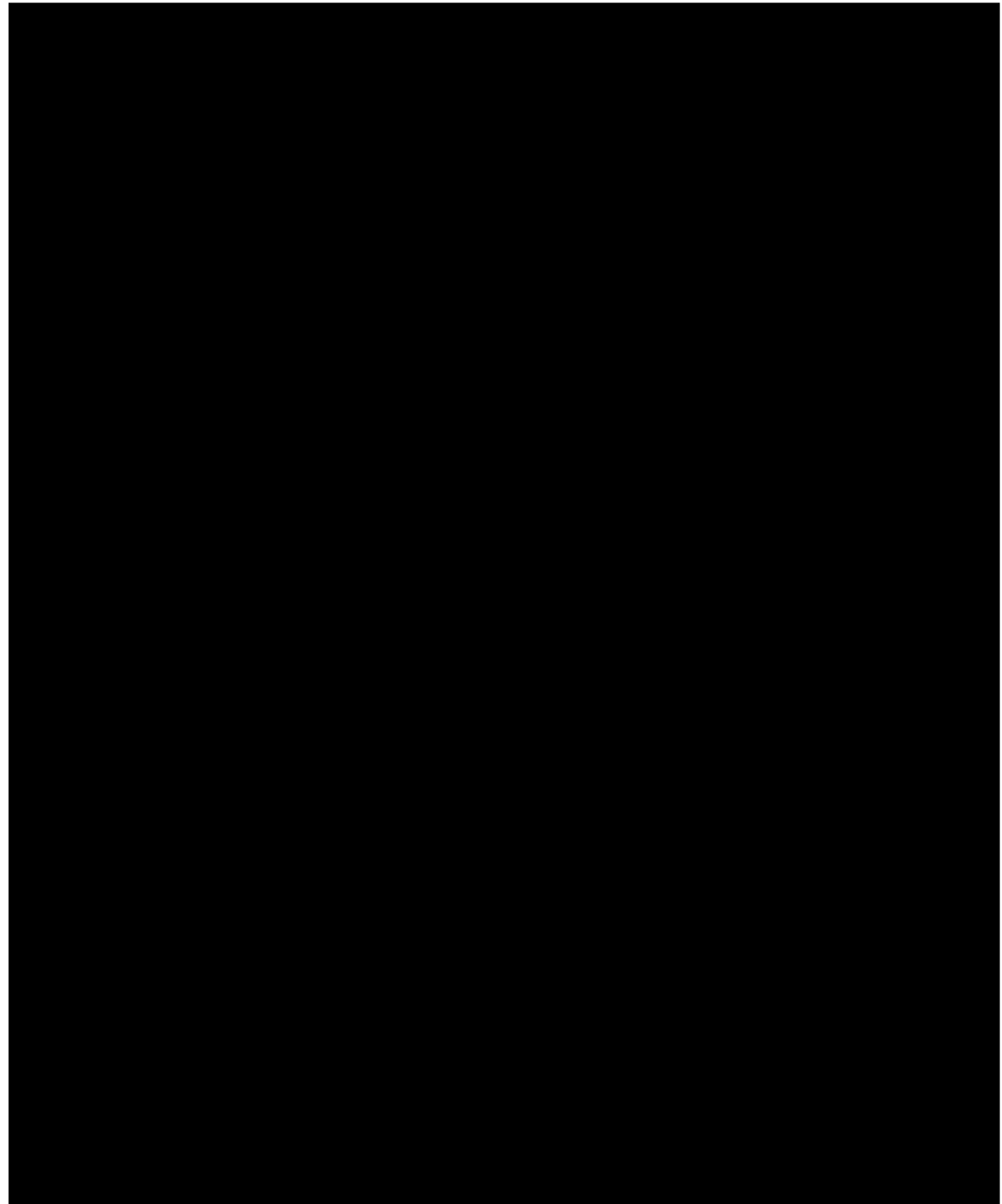


Agencia
Nacional Digital





Agencia
Nacional Digital



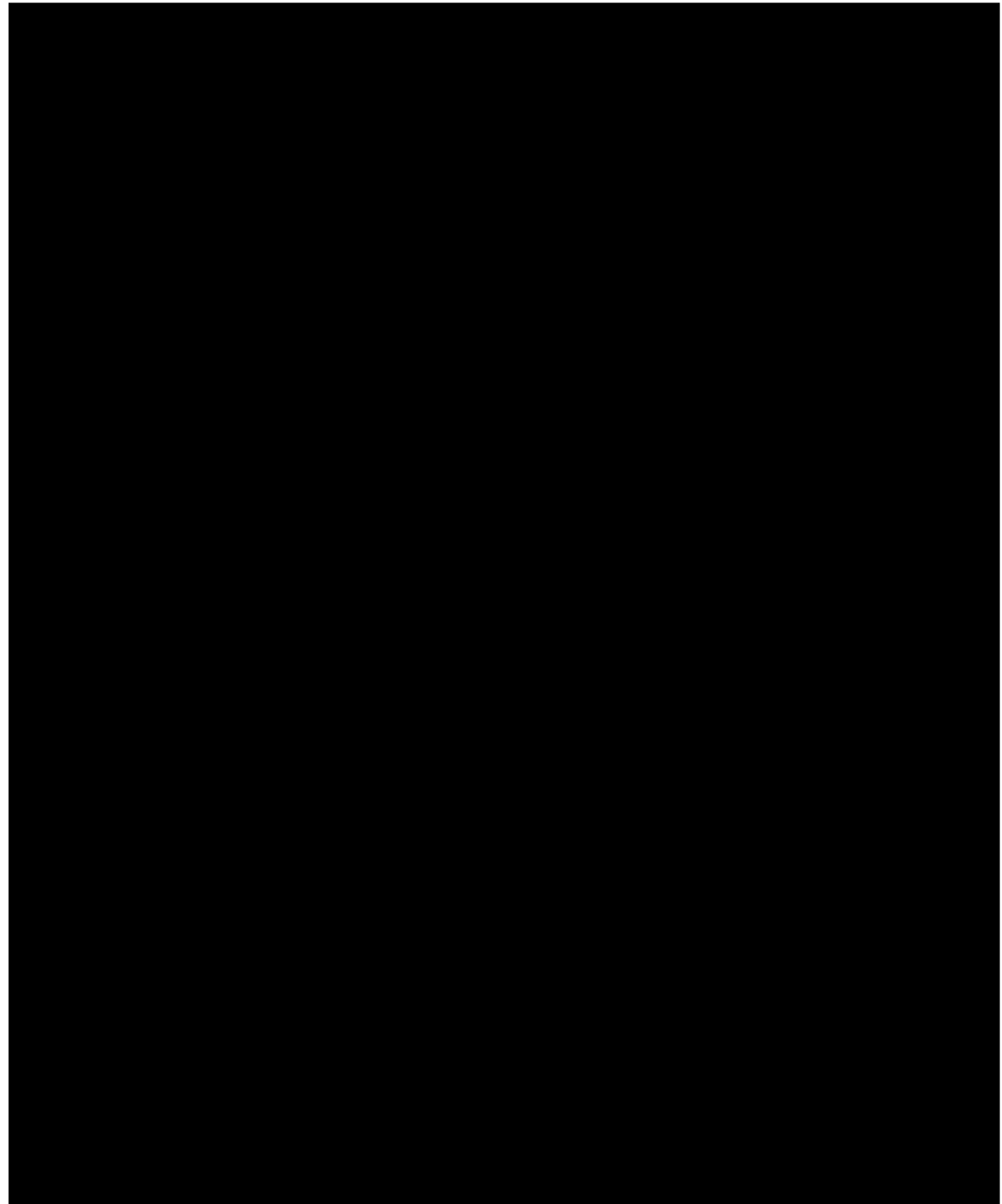


Agencia
Nacional Digital



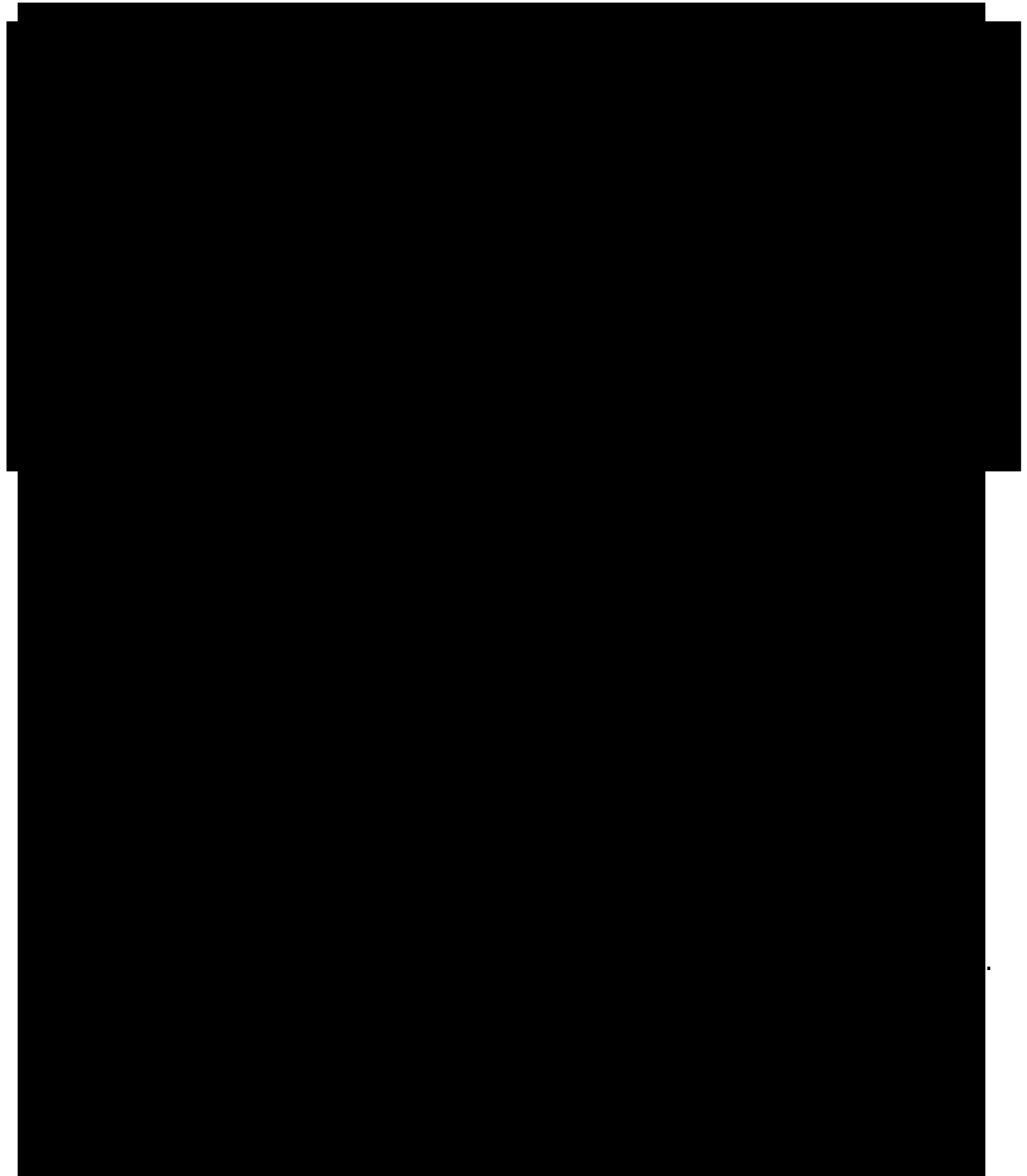


Agencia
Nacional Digital



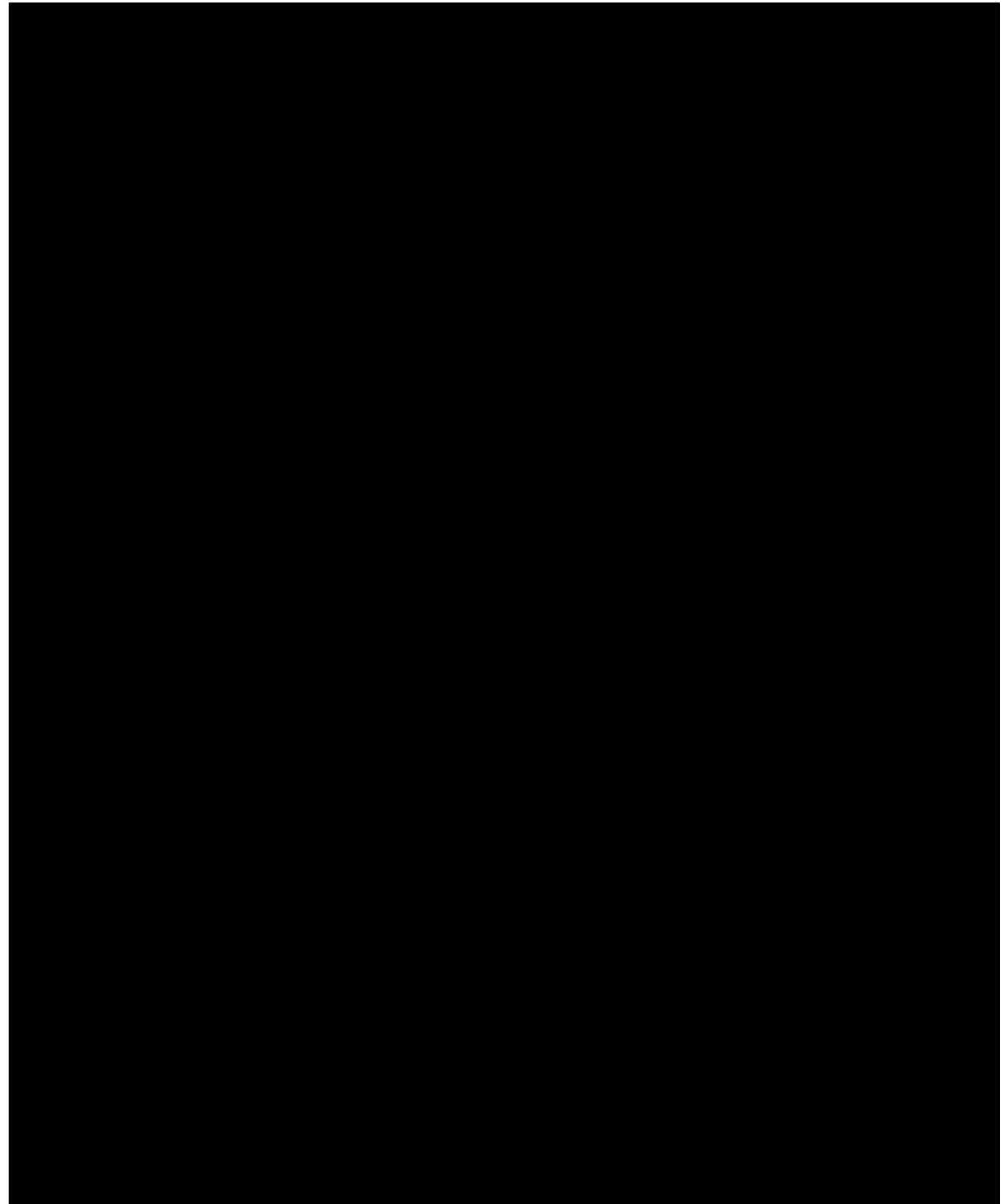


Agencia
Nacional Digital



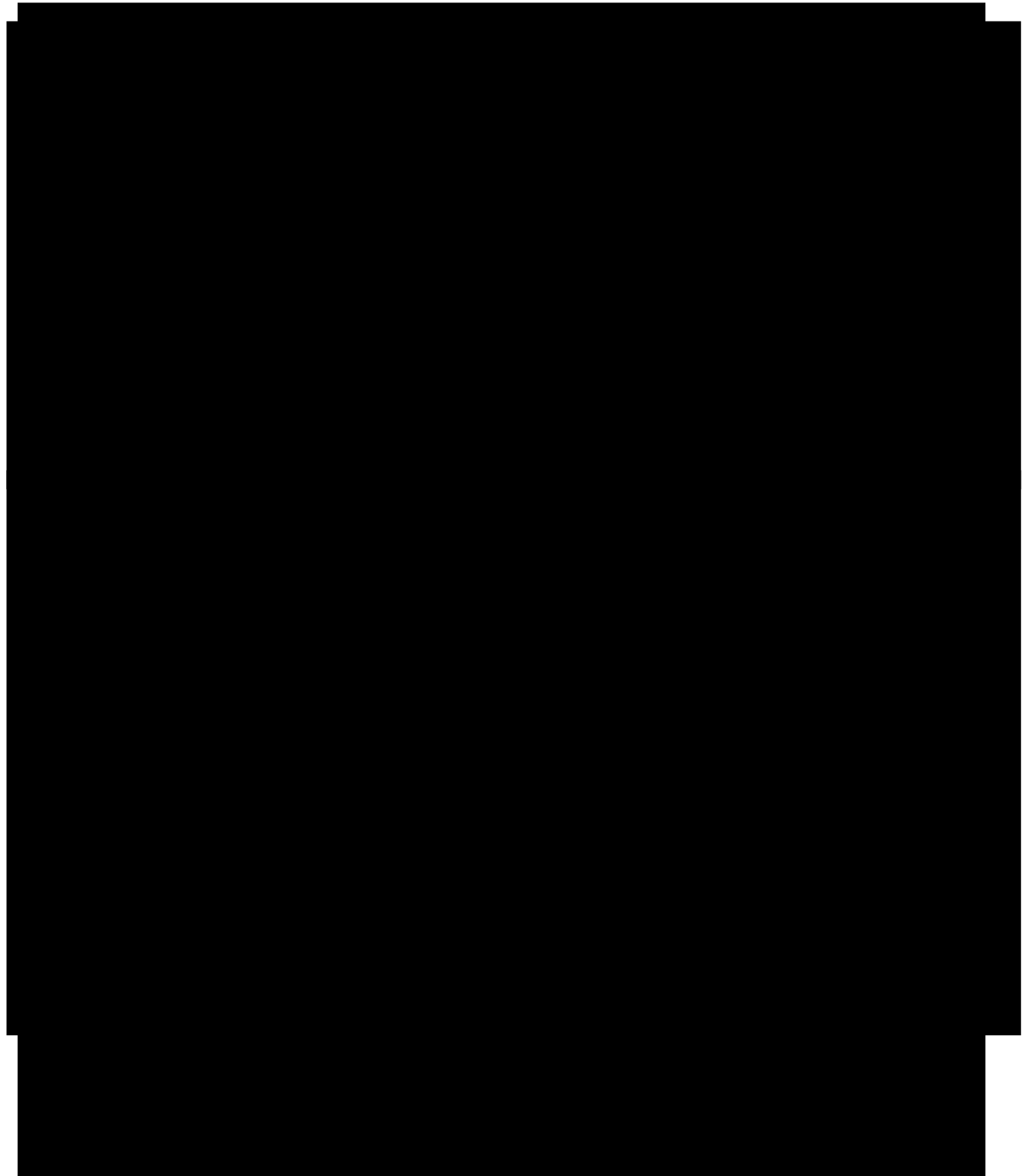


Agencia
Nacional Digital



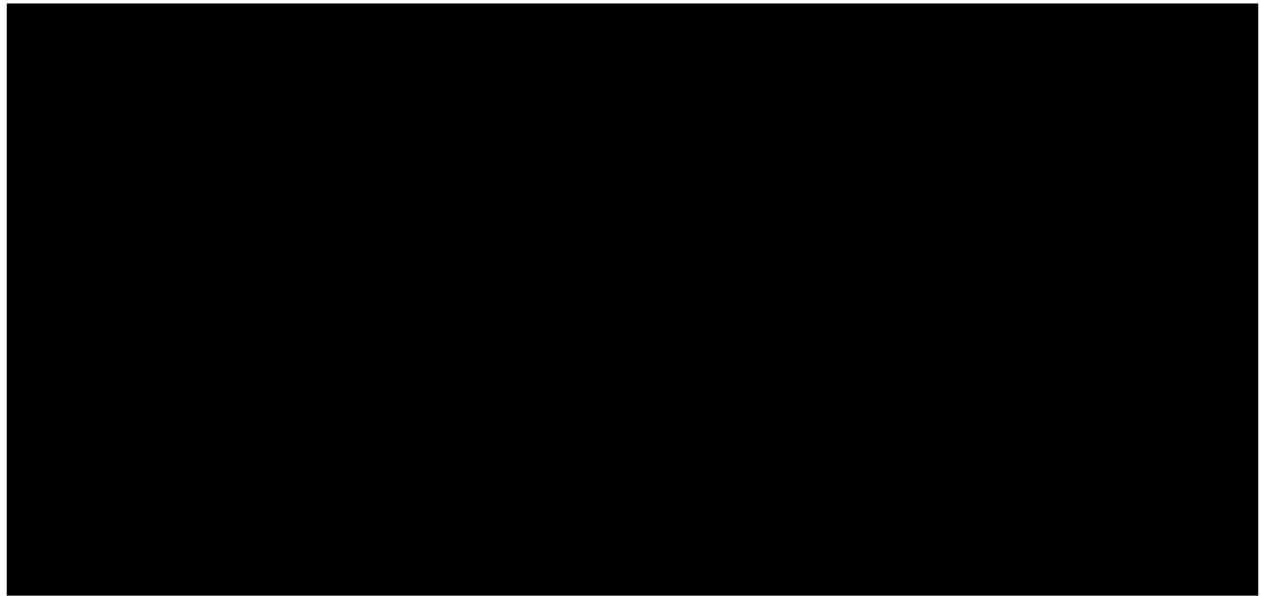


Agencia
Nacional Digital





Agencia
Nacional Digital



7. Conclusión

De acuerdo con los hallazgos identificados durante la presente auditoría de ciberseguridad, concluimos que la entidad presenta un nivel de exposición relevante frente a diferentes debilidades de seguridad detectadas en los activos evaluados. A partir del análisis consolidado del informe, se obtuvo un total de **14 vulnerabilidades identificadas**, de las cuales **7 corresponden a criticidad alta**, lo que representa el **50%** del total, y **7 corresponden a criticidad media**, equivalente al **50%** restante. No se identificaron vulnerabilidades clasificadas con criticidad baja.

Este resultado evidencia que la totalidad de los hallazgos encontrados requiere atención prioritaria, ya que no se trata de observaciones menores o de bajo impacto, sino de debilidades con capacidad real de afectar la confidencialidad, integridad y disponibilidad de la información y de los servicios institucionales. La presencia equilibrada entre vulnerabilidades altas y medias demuestra que la superficie tecnológica evaluada presenta riesgos importantes tanto a nivel de exposición crítica como en configuraciones inseguras, controles deficientes y fallas de endurecimiento que pueden facilitar escenarios de compromiso más severos.

En este sentido, la conclusión general del informe permite establecer que la institución debe adoptar un plan de remediación estructurado, priorizando en primera instancia los hallazgos de criticidad alta, sin dejar de atender de manera oportuna los hallazgos de criticidad media, dado que estos también pueden convertirse en vectores de ataque relevantes si no son corregidos.



Agencia Nacional Digital



Por tanto, la estadística obtenida no solo refleja el estado actual de la seguridad evaluada, sino que también sirve como insumo para la toma de decisiones, la asignación de prioridades técnicas y la implementación de acciones de mejora orientadas al fortalecimiento integral de la postura de ciberseguridad institucional.