



**Agencia
Nacional Digital**



Informe de Re-Test de Ciberseguridad

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

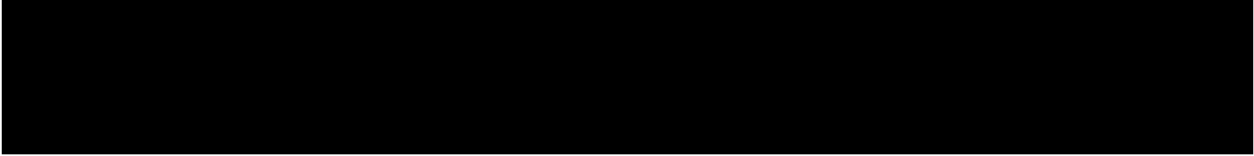
REVISIÓN No.	FECHA	DESCRIPCIÓN	AUTOR DEL CAMBIO
1	09/04/2026	Creación del documento	Virgilio Salgado



Agencia Nacional Digital

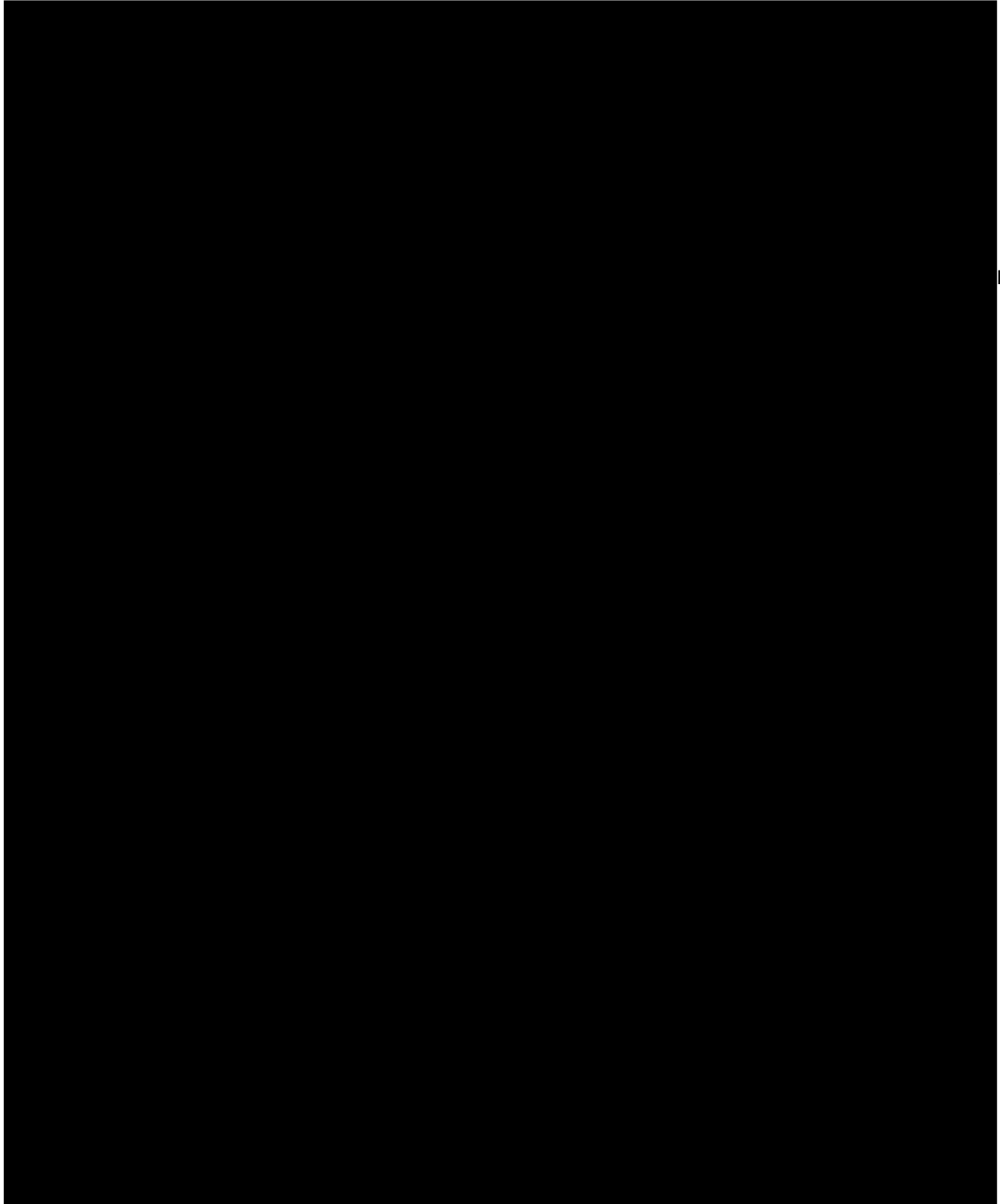


Contenido

1. Introducción	4
2. Objetivo General	4
3. Objetivos Específicos	4
4. Alcance del re-test	5
5. Antecedentes	5
6. Metodología del re-test	6
7. Resultado del re-test.....	6
8. Hallazgo validado en el re-test.....	7
	
10. Conclusión	11
11. Recomendaciones	12

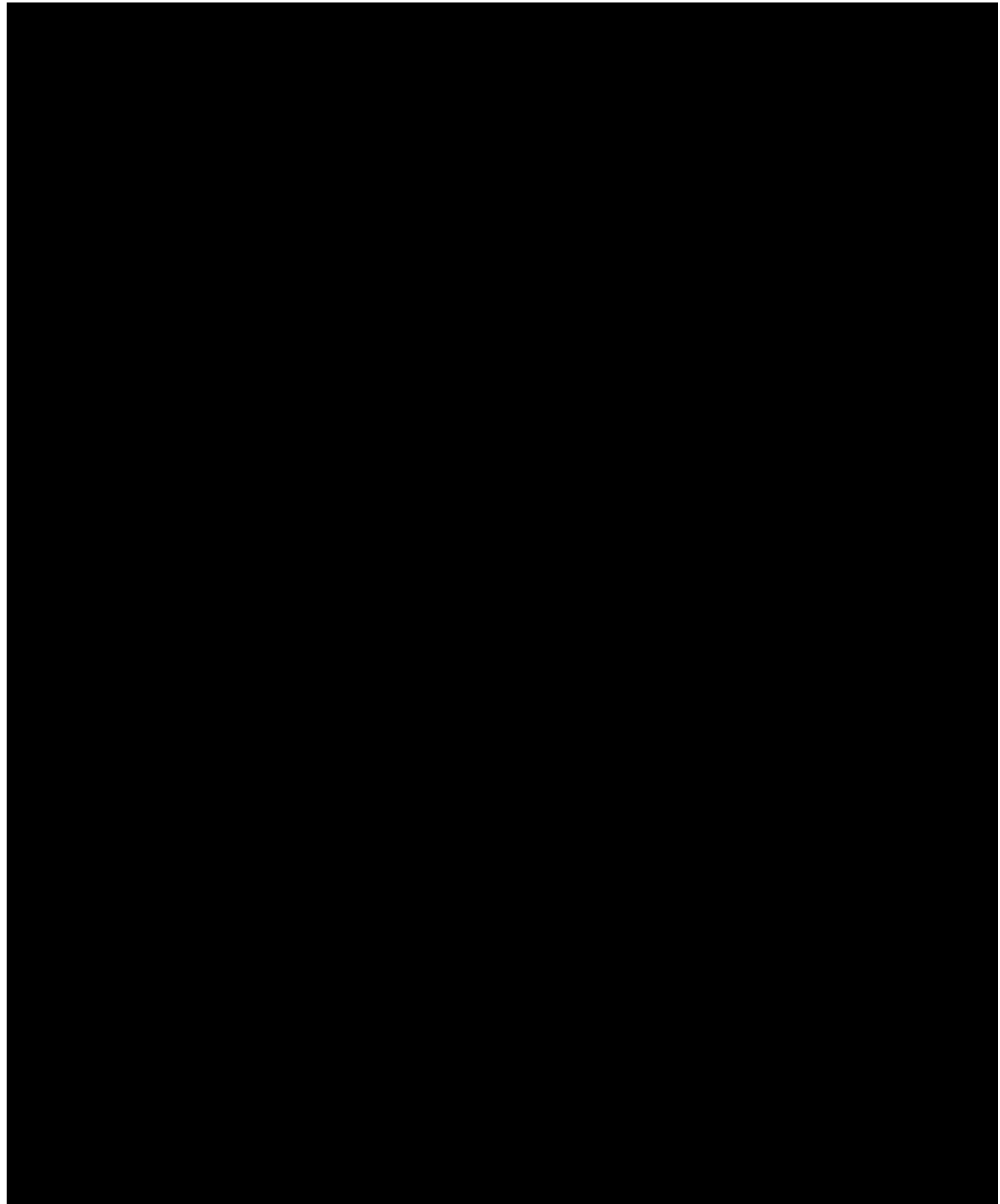


Agencia Nacional Digital



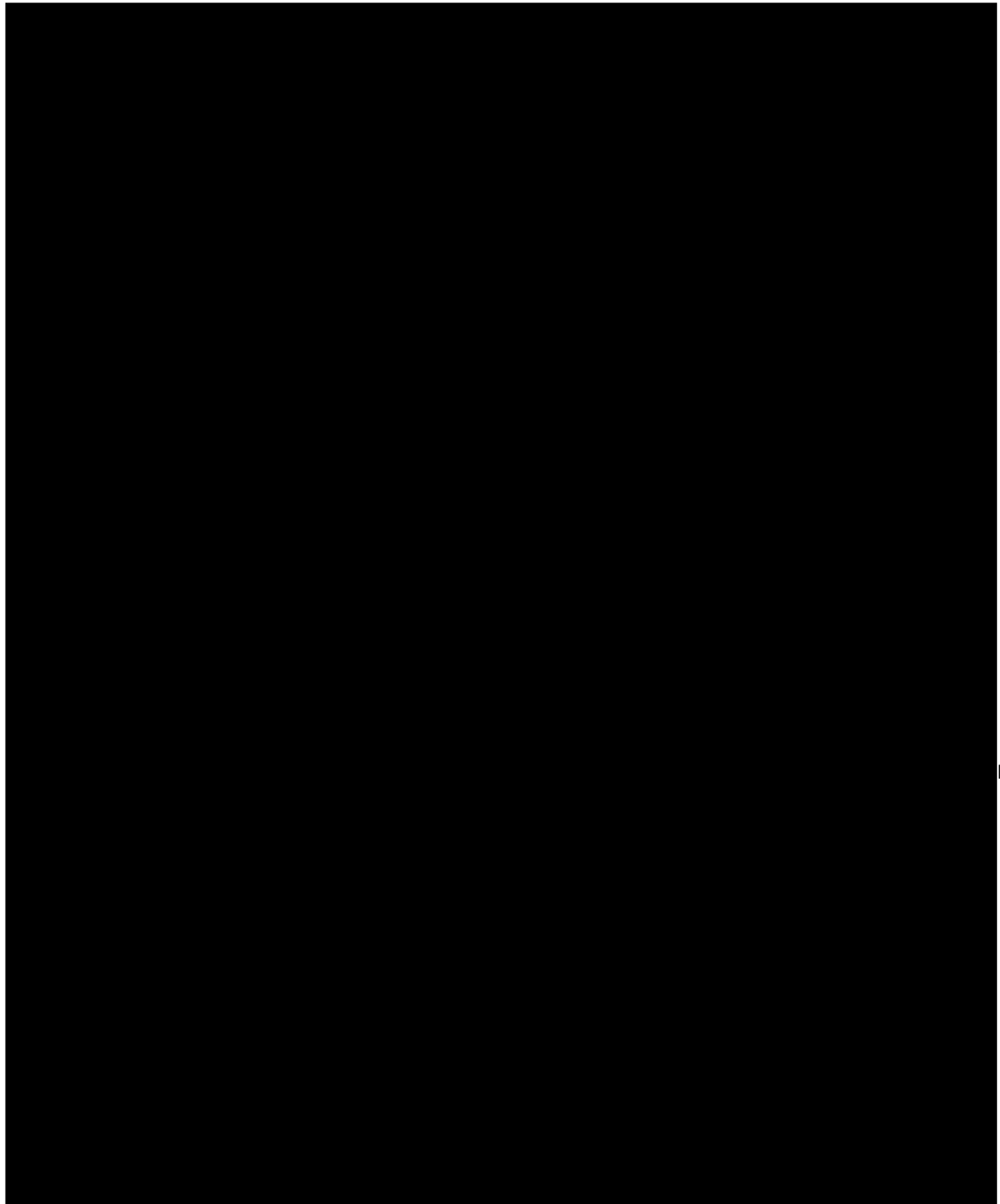


Agencia
Nacional Digital



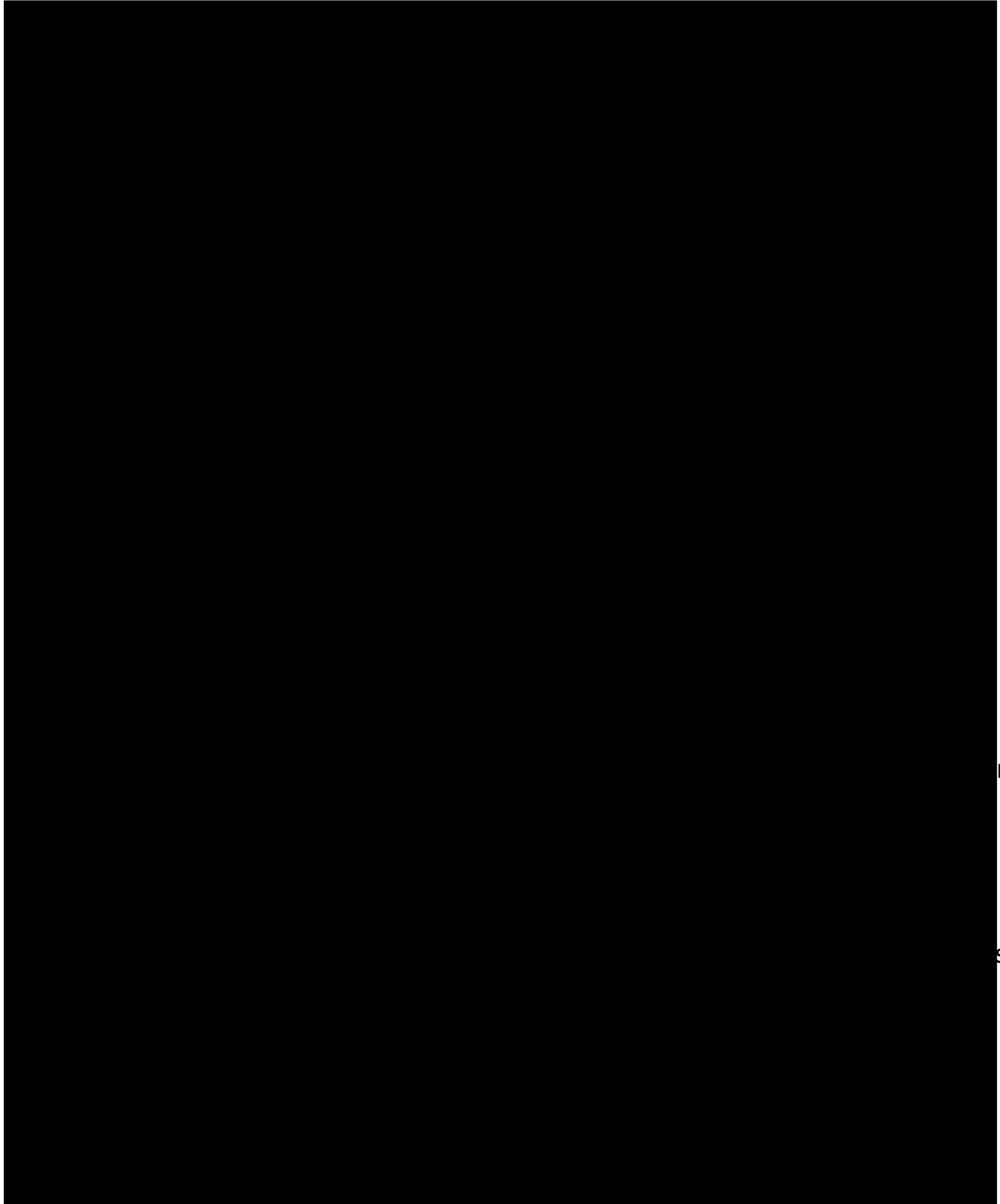


Agencia
Nacional Digital





Agencia
Nacional Digital





Agencia
Nacional Digital





Agencia
Nacional Digital



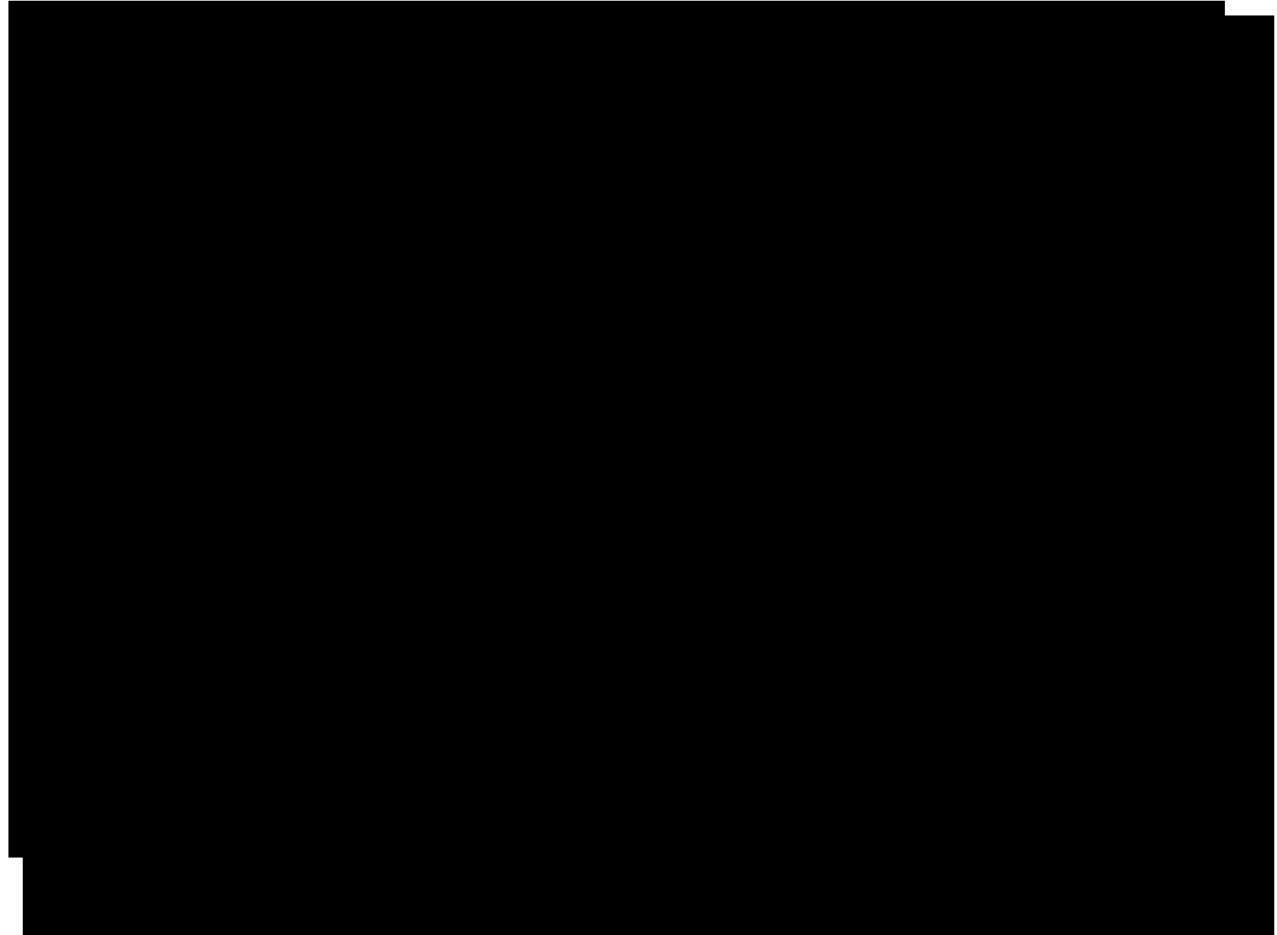


Agencia
Nacional Digital





Agencia
Nacional Digital



10. Conclusión

Con base en los resultados obtenidos durante el presente re-test, concluimos que la plataforma [REDACTED] **no superó satisfactoriamente la validación de remediación**, debido a que el hallazgo crítico reportado en la auditoría anterior continúa presente al momento de esta nueva verificación. La permanencia del backdoor confirma que la vulnerabilidad no fue corregida de manera efectiva y que el entorno evaluado sigue manteniendo una vía de acceso no autorizado con capacidad de comprometer la plataforma web y los accesos vinculados a bases de datos institucionales. Desde una perspectiva de riesgo, el resultado del re-test demuestra que la exposición sigue siendo severa y que la plataforma conserva una condición crítica de compromiso. La existencia de controles como el WAF no compensa la permanencia del acceso malicioso, ya que el problema principal radica en que el artefacto o mecanismo de intrusión continúa activo dentro del entorno.



Agencia Nacional Digital



Por lo tanto, se concluye que el estado actual de la plataforma requiere atención inmediata, respuesta prioritaria y acciones correctivas de fondo para lograr el cierre real del hallazgo y evitar una materialización más amplia del riesgo.

11. Recomendaciones

Recomendamos ejecutar de manera inmediata la eliminación total del [REDACTED] archivo malicioso o mecanismo de persistencia identificado dentro del entorno de [REDACTED] acompañando esta acción de una revisión forense y técnica integral del servidor comprometido para descartar la existencia de accesos adicionales, tareas programadas, cuentas ocultas, artefactos persistentes o modificaciones no autorizadas. También debe realizarse la **rotación completa de credenciales** vinculadas a bases de datos, aplicaciones, servicios internos y cuentas administrativas que hayan podido quedar expuestas a partir del hallazgo validado.

De forma complementaria, se recomienda revisar a profundidad la configuración del [REDACTED], endurecer las reglas de protección del servidor, verificar los mecanismos de publicación de aplicaciones y asegurar que no existan rutas temporales, archivos de prueba, artefactos heredados o componentes inseguros dentro del entorno productivo. Finalmente, debe efectuarse un nuevo ciclo de validación posterior a la remediación, con evidencia técnica de cierre, a fin de confirmar que la plataforma ya no conserva vectores explotables y que el riesgo ha sido mitigado de forma efectiva.