Agencia Nacional Digital

INFORME FINAL DE AUDITORÍA INTERNA

Informe No. 5 de 2026

Resultados de evaluación realizada al Proceso de Seguridad y Privacidad de la Información

BOGOTÁ, SEPTIEMBRE 2026

CONTENIDO

1. ALCANCE 3
2. CRITERIOS 3
3. OBJETIVO 3
4. RESULTADOS DE LA AUDITORIA 3
4.1. Hallazgos 4
4.2. Observaciones 8
4.3. Fortalezas 5
5. RECOMENDACIONES 7

1. ALCANCE

La auditoría comprenderá una revisión del proceso de Seguridad y Privacidad de la Información de la Agencia Nacional Digital, correspondiente al período comprendido entre el 1 de enero y el 31 de julio de 2026, mediante la verificación selectiva de su documentación y controles, y con base en la información suministrada por el equipo auditado

2. CRITERIOS

- Carta Descriptiva del Proceso Seguridad y Privacidad de la Información - SYPI.PC.01.
- Política General del Sistema de Gestión de Seguridad de la Información (SGSI) - V4.
- Manual de Políticas de Seguridad Digital y de la Privacidad de la Información - V5.
- Política de Tratamiento de Datos Personales - V2.
- SYPI.PR.02 Procedimiento Gestión y Clasificación de Activos de Información.
- SYPI.PR.03 Procedimiento Gestión de Accesos Lógicos - V2.
- SYPI.PR.04 Procedimiento Gestión y Clasificación de Eventos e Incidentes.
- SYPI.GU.02 Guía de Identificación y Clasificación de Activos de Seguridad Digital y de la Información - V3.
- Plan de Seguridad y Privacidad de la Información
- Plan de Tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información
- Ley 1581 de 2012 y Decreto 1377 de 2013 - Protección de Datos Personales.
- Ley 1712 de 2014 - Transparencia y Acceso a la Información Pública.
- Normograma del proceso.

3. OBJETIVO

Evaluar el cumplimiento de la Política General del SGSI, el Manual de Políticas de Seguridad Digital y de la Privacidad de la Información, y los procedimientos y guías asociados al proceso Seguridad y Privacidad de la Información (SYPI) de la Agencia Nacional Digital, así como el avance en la ejecución del Plan de Seguridad y Privacidad

de la Información y del Plan de Tratamiento de Riesgos de Seguridad Digital, con el fin de identificar oportunidades de mejora

4. RESULTADOS DE LA AUDITORIA

La evaluación se efectuó con base en la información solicitada a través de correo electrónico del 18 de agosto de 2026 con dieciocho (18) puntos, por lo que, contrastando las respuestas del proceso con la documentación y evidencias allegadas, de los dieciocho (18) requerimientos, quince (15) cuentan con soporte suficiente para sustentar la evaluación y tres (3) presentan soporte incompleto o no fueron allegados: el seguimiento del mapa de riesgos y sus controles (punto No. 5), la medición de indicadores del proceso (punto No. 16) y el estado y avance del plan de mejoramiento suscrito en el marco de la certificación ISO/IEC 27001:2022 (punto No. 18).

En particular, frente al requerimiento No. 6, el proceso informó que durante el período evaluado no se generaron incidentes de seguridad, dado que el requerimiento estaba orientado a los incidentes gestionados durante el período, no se considera necesaria evidencia documental cuando no se han presentado incidentes.

Con base en el conjunto de evidencias revisadas, se concluye que el proceso presenta un cumplimiento parcial de los criterios evaluados y cuenta con elementos estructurantes del SGSI y controles operando en los aspectos revisados. Se identifican oportunidades de mejora relacionadas principalmente con la disponibilidad del seguimiento al mapa de riesgos, la medición y reporte de indicadores, el seguimiento documentado al plan de mejoramiento y, como aspecto adicional de carácter formal, la consolidación de determinadas evidencias.

4.1. Hallazgos

En el desarrollo de la presente auditoría no se identificaron hallazgos que constituyan incumplimientos a la normatividad, políticas o procedimientos aplicables al proceso de Seguridad y Privacidad de la Información. Las situaciones identificadas por el equipo auditor, que corresponden a oportunidades de mejora, se relacionan en el numeral siguiente. No obstante, en caso de que el equipo auditor, a partir de las consideraciones que los auditados presenten frente al informe preliminar previo a la reunión de cierre, y lo considere pertinente, el presente informe podrá ser modificado o podrán generarse hallazgos.

4.2. Observaciones

El equipo auditor evaluó de manera integral la totalidad de la documentación, los planes y la normatividad aplicables al proceso Seguridad y Privacidad de la Información: la Carta Descriptiva del proceso, la Política General del SGSI, el Manual de Políticas de Seguridad Digital y de la Privacidad de la Información, la Política de Tratamiento de Datos Personales, los procedimientos y guías del proceso, el Plan de Seguridad y Privacidad de la Información, el Plan de Tratamiento de Riesgos de Seguridad Digital y la normatividad aplicable, contrastando en cada caso la información solicitada. A continuación, se presenta el resultado de esa evaluación, junto con las observaciones que el equipo auditor considera necesarias frente a los aspectos en los que se identificaron oportunidades de mejora.

Observación No. 1. Centralización y consolidación de la evidencia de gestión de accesos lógicos

El proceso allegó 89 formularios de gestión de accesos lógicos, en formato PDF y Excel, distribuidos en los siete meses del período auditado (enero a julio de 2026), que dan cuenta de la totalidad de las solicitudes de acceso tramitadas. No obstante, dicha evidencia se conserva de manera dispersa en archivos individuales, sin un consolidado o base de datos único que totalice y permita el seguimiento agregado de las solicitudes tramitadas (altas, bajas y modificaciones). Esta situación obedece a la ausencia de un registro consolidado que centralice la información contenida en los formularios individuales. En consecuencia, frente a la gestión de accesos lógicos sí se evidencia cumplimiento, al contar con el trámite y soporte de la totalidad de las solicitudes del período; no obstante, se identifica la presente oportunidad de mejora en la consolidación de dicha evidencia.

Respuesta Oficial de Seguridad:

Al momento de la auditoría no se consolidaba la evidencia, razón por la cual se implementará una matriz consolidada institucional para la gestión de accesos lógicos, integrando las solicitudes de creación, modificación y retiro de accesos, con sus respectivas aprobaciones, responsables y evidencias, fortaleciendo la trazabilidad y disponibilidad de la información requerida para seguimiento y auditoría.

Respuesta Equipo Auditor:

Teniendo en cuenta que el proceso auditado no demostró que la observación se encontrara subsanada, se mantiene la observación, y se recomienda consolidar la

evidencia de gestión de accesos lógicos en un registro o matriz único y actualizado que permita medir de forma ágil el volumen, tipo y oportunidad de atención de las solicitudes de acceso y facilite su reporte como indicador del proceso.

Observación No. 2. Medición y reporte de los indicadores de gestión del proceso SYPI

En respuesta remitida por el profesional a cargo de atender la auditoría, al punto 16 se indicó como "Pendiente cargue y soporte" y no allegó el soporte correspondiente a la medición de indicadores, pese a que el SGSI requiere su medición periódica como mecanismo de evaluación del desempeño y de retroalimentación para la mejora continua. Esta situación obedece a la ausencia de un mecanismo consolidado y oportuno para la medición, documentación y reporte de los indicadores de gestión del proceso, y tiene como efecto que se impida verificar su desempeño real y se limite la capacidad de la Alta Dirección y de los responsables del SGSI para identificar oportunamente desviaciones y definir acciones de mejora basadas en datos. En consecuencia, con la información aportada, no se evidencia cumplimiento en la medición y el reporte de los indicadores del proceso SYPI para el período evaluado.

Respuesta Oficial de Seguridad:

En respuesta emitida por el profesional se evidencia que realizó el reporte de los indicadores, los cuales son reporteados al área de planeación.

Respuesta Equipo Auditor:

De conformidad con la evidencia remitida, se subsana la observación, toda vez que se demuestra que se realiza medición periódica de los indicadores. Sin embargo, se reitera que importante definir, medir y reportar de manera periódica los indicadores de gestión del proceso SYPI, remitiendo dicha información al área de planeación, responsable de su seguimiento desde la segunda línea de defensa, y posteriormente a la Oficina de Control Interno, en el marco de su rol de tercera línea, dejando evidencia documental completa de la medición ante los requerimientos de información correspondientes. La ausencia de este reporte durante el período evaluado evidencia una posible omisión en el ejercicio de seguimiento que corresponde a dichas líneas de defensa, por lo cual resulta necesario fortalecer los canales de articulación y reporte entre el proceso, la segunda línea de defensa y el órgano de control interno.

Observación No. 3. Ejecución y seguimiento del Plan de Mejoramiento suscrito en el marco de la certificación ISO/IEC 27001:2022

En respuesta remitida por el profesional a cargo de atender la auditoría, al punto 18 se indicó como "Pendiente cargue y soporte" y no allegó evidencia del estado ni de los avances del plan de mejoramiento suscrito en el marco de la certificación ISO/IEC

27001:2022, pese a que es responsabilidad del proceso ejecutar las acciones correctivas y de mejora allí definidas, así como realizar y documentar el seguimiento periódico a su cumplimiento, en concordancia con el ciclo de mejora continua. Esta omisión obedece a una debilidad en la consolidación, actualización y disponibilidad oportuna de la información de seguimiento al plan de mejoramiento frente a los requerimientos de los órganos de control, y tiene como efecto que el equipo auditor no disponga de elementos objetivos para verificar su cumplimiento, generando el riesgo de incumplimiento de los compromisos adquiridos ante el ente certificador y de afectación de la vigencia de la certificación ISO/IEC 27001:2022. En consecuencia, con la información y evidencia disponibles a la fecha de entrega de información, no se evidencia cumplimiento, por cuanto el proceso no acreditó, ante el requerimiento formal del equipo auditor, la ejecución ni el seguimiento de las acciones correspondientes; la ausencia de soporte no puede sino entenderse, como la no realización de dichas acciones.

Respuesta Oficial de Seguridad:

Al momento de la auditoría no se encontraba actualizado la matriz de seguimiento del plan de mejoramiento incorporando el estado de avance de cada actividad, responsables, fechas de cumplimiento y evidencias asociadas.

Respuesta Equipo Auditor:

Teniendo en cuenta que el proceso auditado no demostró que la observación se encontrara subsanada, se mantiene la observación, y se recomienda eejecutar y realizar seguimiento documentado a cada una de las acciones del plan de mejoramiento suscrito en el marco de la certificación ISO/IEC 27001:2022, y remitir la evidencia correspondiente de manera oportuna y completa ante los requerimientos internos y de los entes de control, de forma que la ausencia de soporte no sea interpretada como incumplimiento en su ejecución.

Observación No. 4. Control de versiones y nomenclatura documental del mapa y la matriz de riesgos de seguridad

El profesional designado para la auditoría allegó el mapa y la matriz de riesgos de seguridad, documento publicado en SIGAND correspondiente a un tablero de control ("Dashboard Avance PTR") que registra acciones de tratamiento de riesgos por proceso, con fechas de seguimiento que se extienden hasta el primer trimestre de 2026 y estados diferenciados (cerrado, en ejecución, no iniciado). Es importante precisar, que no se allegó el seguimiento que, como tal, realiza el área auditada, sino únicamente el documento publicado en SIGAND, sin instrumentos de seguimiento que permitan verificar su actualización y aplicación efectiva durante dicho período.

Adicionalmente, se observa que el archivo aportado conserva en su nombre la referencia al año 2025 ("Matriz de Riesgos de Seguridad_AND - 2025"), pese a corresponder al período 2026 evaluado, lo que resulta inconsistente con la exigencia de que los documentos del SGSI se identifiquen y controlen conforme a su vigencia y período de aplicación, de manera que su nomenclatura sea consistente con el contenido y facilite su trazabilidad. Esta situación obedece a una debilidad en el control de versiones, en la actualización de la nomenclatura de los archivos que soportan la gestión de riesgos del proceso y en la disposición, por parte del área auditada, de instrumentos formales de seguimiento propios para el período evaluado, y tiene como efecto que se dificulte verificar la ejecución real de dicho seguimiento, que la denominación desactualizada del archivo pueda inducir a error sobre la vigencia real de la información, y que se afecte su localización y trazabilidad documental ante partes interesadas y entes de control.

En consecuencia, en cuanto al avance en la ejecución del Plan de Tratamiento de Riesgos de Seguridad Digital, no se evidencia el aporte, por parte del área auditada, del instrumento de seguimiento; se identifica, adicionalmente, una oportunidad de mejora de carácter formal en el control.

Respuesta Oficial de Seguridad:

Al momento de la auditoría no se encontraba actualizado el el archivo aportado conserva en su nombre la referencia al año 2025 ("Matriz de Riesgos de Seguridad_AND - 2025").

Respuesta Equipo Auditor:

Teniendo en cuenta que el proceso auditado no demostró que la observación se encontrara subsanada, se mantiene la observación, y se recomienda robustecer el control de versiones de manera que el nombre del archivo refleje la vigencia y el período a que corresponde, facilitando su trazabilidad y consulta. Así mismo, allegar y mantener disponible el instrumento propio de seguimiento del área auditada para cada período evaluado, de manera que no se limite a la publicación de documentos en SIGAND sin herramientas de seguimiento asociadas.

Observación No. 5. Finalización y aprobación formal del documento "Convenio Interadministrativo 687-2026. Anexo 1 – Informe de Gestión de Controles de Seguridad y Mejora Continua.

Frente al Anexo 1 – Informe de Gestión de Controles de Seguridad y Mejora Continua, allegado, se reporta un avance de revisión del 100% en controles organizacionales,

85% en controles de personas, 85% en controles físicos y 90% en controles tecnológicos; sin que se logre evidenciar un real cumplimiento de los niveles de efectividad de los controles, en razón a que el documento allegado corresponde a una versión en borrador, según el control de cambios, en el cual se registra la participación de quienes intervienen en su elaboración sin que conste su cierre o aprobación formal, lo que indica que el ejercicio de revisión de controles se encuentra en curso y no ha sido concluido a la fecha de corte de la auditoría. Esta situación obedece a que el proceso aún no ha formalizado ni aprobado el resultado definitivo del ejercicio de revisión de controles del período. Su efecto es que, a la fecha, no se cuenta con un documento definitivo y formalmente aprobado sobre el estado de los controles de seguridad, lo que limita la posibilidad de utilizar dicho informe como soporte concluyente del nivel de cumplimiento o de efectividad. En consecuencia, si bien se evidencia un avance significativo en el ejercicio de revisión de controles, no se evidencia cumplimiento en cuanto a la finalización y aprobación formal de dicho ejercicio.

Respuesta Oficial de Seguridad:

Al momento de la auditoría no se encontraba finalizado el **"Convenio Interadministrativo 687-2026. Anexo 1 – Informe de Gestión de Controles de Seguridad y Mejora Continua.**

Respuesta Equipo Auditor:

Teniendo en cuenta que el proceso auditado no demostró que la observación se encontrara subsanada, se mantiene la observación, y se recomienda finalizar y formalizar la aprobación del Informe de Gestión de Controles de Seguridad y Mejora Continua (Anexo 1), dejando constancia de su cierre en el control de cambios, de forma que los porcentajes de avance de revisión no se confundan con niveles de cumplimiento.

4.3. Fortalezas

- Se evidencia la existencia y disponibilidad de una estructura documental del SGSI que comprende la política general, el manual de políticas, los procedimientos, las guías y los planes del proceso, vigente y publicada, la cual constituye una base formal para la gestión de la seguridad y privacidad de la información.
- Se evidenció la disponibilidad de la Declaración de Aplicabilidad (SoA) 2026, debidamente diligenciada con referencia a sus cuatro dominios de control: organizacional, personas, físicos y tecnológicos.
- El informe de gestión de controles reporta avances de revisión del 100% en

controles organizacionales, 85% en personas, 85% en físicos y 90% en tecnológicos. Sin embargo, al momento solo corresponde a un documento en elaboración y los porcentajes representan avance del ejercicio de revisión y no niveles de cumplimiento o efectividad.

- Se evidenció que la totalidad de los Servicios Ciudadanos Digitales fue incluida dentro del alcance del ejercicio de evaluación de seguridad, de los cuales, a la fecha de corte, dos (2) habían culminado la validación de evidencias y nueve (9) se encontraban en proceso de revisión.
- Se dispone de evidencia de la gestión de accesos lógicos del proceso, con 89 registros correspondientes al período enero–julio de 2026, lo que demuestra la operación efectiva del control.
- El proceso cuenta con el Inventario/Matriz de Activos de Información 2026, como soporte del componente de gestión y clasificación de activos de información del SGSI.
- En materia de protección de datos personales, la constancia expedida por la Superintendencia de Industria y Comercio reporta veintidós (22) bases de datos finalizadas y cero (0) pendientes por radicar, con vigencia hasta el 31 de marzo de 2027.

5. RECOMENDACIONES

Con base en la revisión selectiva de la documentación, los controles y las evidencias aportadas, el proceso de Seguridad y Privacidad de la Información presenta un nivel de cumplimiento frente a los criterios evaluados. Se evidencian elementos estructurantes del SGSI y operación de controles en los aspectos revisados, particularmente en la gestión documental, la gestión de activos de información, la gestión de accesos lógicos, la gestión de vulnerabilidades técnicas y la protección de datos personales.

No obstante, se identificaron oportunidades de mejora relacionadas con la disponibilidad del seguimiento propio del área auditada al mapa de riesgos y sus controles, la medición y reporte de indicadores de gestión del proceso, el seguimiento documentado al plan de mejoramiento asociado a la certificación ISO/IEC 27001:2022, la finalización y aprobación formal del ejercicio de revisión de controles de seguridad, y la consolidación de determinadas evidencias. Estas situaciones no permiten concluir, por sí mismas, la inexistencia de los controles; sin embargo, limitan la trazabilidad y la capacidad de demostrar oportunamente su gestión frente a ejercicios de seguimiento y control.

Se recomienda al proceso auditado fortalecer la gestión y atención de los requerimientos de información formulados en el marco de los ejercicios de auditoría y control, procurando dar cumplimiento a los plazos establecidos o acordados y remitir

la información de manera completa y oportuna. Lo anterior, teniendo en cuenta que, durante el desarrollo del presente ejercicio, el profesional designado para atender la auditoría solicitó un plazo adicional para dar respuesta a la solicitud de información, sin embargo, la información fue remitida de manera parcial, situación que dificultó la revisión y verificación oportuna de las evidencias por parte del equipo auditor. La observancia de estos aspectos contribuye a garantizar la adecuada planeación, desarrollo y trazabilidad de los ejercicios de auditoría y control.

Elaboró: Carlos Mario Barrera Sánchez
Contratista Apoyo a Control Interno