Fecha del Informe Final	**Día**	26	**Mes**	06	**Año**	2026
Nombre de la actividad	Seguimiento Ley 1581 de 2012 - Protección de Datos Personales					
Objetivo del Seguimiento	Verificar la aplicación y cumplimiento de las políticas de privacidad y protección de datos personales adoptadas por la Superintendencia Nacional de Salud, en concordancia con las políticas contenidas en la Ley 1581 de 2012					
Alcance	Evaluar los avances y el estado actual de implementación del Sistema de Protección de Datos Personales en la entidad, mediante la revisión de la documentación, procedimientos, políticas, registros, controles y demás evidencias que se encuentren formalmente adoptadas, documentadas y/o en operación a la fecha de realización del seguimiento, de conformidad con los requisitos establecidos en la Ley 1581 de 2012 y su normativa reglamentaria.					
Criterios	• Constitución Política de 1991 – Artículos 209, 269, 270. • Ley 87 de 1993 Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones. • Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.					
Equipo de Seguimiento	Adriana Bello Cortés – Profesional OCI. Luis Alberto Triana Lozada– Contratista OCI. Milton Andrés Ruiz Bonilla - Contratista OCI.					
Tabla de Contenido						

INFORME

El presente seguimiento fue realizado por la Oficina de Control Interno con el propósito de verificar el estado de implementación de las disposiciones establecidas en la Ley 1581 de 2012, sus normas reglamentarias y la Política de Protección y Tratamiento de Datos Personales adoptada por la Superintendencia Nacional de Salud, con el fin de identificar avances, mecanismos implementados y oportunidades de fortalecimiento en materia de protección de datos personales. La evaluación se efectuó sobre los mecanismos, procedimientos, controles, documentos y evidencias que se encontraban implementados, formalizados y operando a la fecha de ejecución del seguimiento.

Para el desarrollo del seguimiento se diseñó una matriz de verificación que incorporó los criterios objeto de evaluación, la cual fue remitida al proceso responsable junto con el requerimiento de la información y evidencias correspondientes. La documentación suministrada fue puesta a disposición en una carpeta compartida para su análisis por parte de la Oficina de Control Interno. Posteriormente, se realizaron entrevistas de seguimiento, mesas de trabajo y requerimientos complementarios dirigidos a diferentes dependencias, con el fin de aclarar información, obtener evidencias adicionales y verificar el cumplimiento de los aspectos evaluados. Los resultados consignados en el presente informe se fundamentan en la información y soportes aportados por las dependencias durante el periodo de ejecución del seguimiento.

A continuación, se presentan los resultados de los criterios evaluados:

Formalización de la Política Institucional de Protección y Tratamiento de Datos Personales

La Superintendencia Nacional de Salud cuenta con la Política de Protección y Tratamiento de Datos Personales, identificada con código E4-PI-1, versión 1, incorporada dentro del Sistema Integrado de Gestión, mediante la cual la Entidad establece los lineamientos institucionales para garantizar la protección de los datos personales tratados en el ejercicio de sus funciones misionales y administrativas. El documento reconoce expresamente el derecho fundamental al hábeas data y su relación con la gestión institucional, constituyéndose en el principal instrumento de direccionamiento para la gestión de la privacidad y protección de datos personales al interior de la Entidad.

Se evidenció que la política incorpora una declaratoria institucional mediante la cual la Superintendencia Nacional de Salud manifiesta formalmente su compromiso de garantizar el cumplimiento de los principios y obligaciones asociados a la protección de datos personales, así como el respeto de los derechos de los titulares de la información.

La política establece el compromiso de implementar medidas técnicas, administrativas y jurídicas orientadas a proteger la confidencialidad, integridad y disponibilidad de los datos personales tratados por la Entidad.

La Política de Protección y Tratamiento de Datos Personales se encuentra publicada para consulta de la ciudadanía en la página web institucional, en el apartado de Transparencia y Acceso a la Información Pública, específicamente en el numeral 6 "*Políticas de privacidad y condiciones de uso*":https://www.supersalud.gov.co/es-co/transparencia-y-acceso-a-la-informacion-publica/informaci%C3%B3n-de-la-entidad/politicas-de-privacidad-y-condiciones-de-uso. Es de anotar que, en la información suministrada por el proceso para el diligenciamiento de la matriz correspondiente al presente seguimiento, se reportó el código de política DIPI04, codificación que se encontraba desactualizada. Esta situación fue puesta en conocimiento del proceso durante la entrevista realizada el 9 de junio de 2026, en la cual se informó que el documento vigente corresponde a la Política de Protección y Tratamiento de Datos Personales identificada con código E4-PI-1, versión 1.

Roles y responsabilidades en la gestión de protección de datos personales

La Política de Protección y Tratamiento de Datos Personales identifica a la Superintendencia Nacional de Salud como responsable del tratamiento de los datos personales. Asimismo, establece una estructura de gobernanza para la implementación y seguimiento de la política, asignando el liderazgo de su despliegue a la Alta Dirección en cabeza del Despacho del Superintendente, e incorporando las figuras de ***Líder de Protección de Datos y Oficial de Protección de Datos***, junto con la participación de dependencias como la Dirección Jurídica, el Grupo de Gestión Documental, el Grupo de Inspección y Vigilancia a las PQRD, el Grupo de Gestión de Correspondencia y la Subdirección de Tecnologías de la Información, entre otras áreas involucradas en el tratamiento de datos personales.

Si bien la Política de Protección y Tratamiento de Datos Personales incorpora las figuras de Líder de Protección de Datos y Oficial de Protección de Datos, y la Resolución 2025153040012454-6 de 2025 establece que el funcionario que ejerza el cargo de Oficial de Seguridad de la Información asumirá las funciones de Oficial de Protección de Datos Personales, durante la revisión efectuada no se evidenció la identificación expresa de la dependencia, cargo o funcionario que ejerce el rol de *Líder de Protección de Datos* definido en la política institucional.

Instrumentos para la implementación y divulgación de la protección de datos personales

En desarrollo del presente seguimiento se evidenció que la Superintendencia Nacional de Salud cuenta con documentos formalmente aprobados dentro del Sistema Integrado de Gestión orientados a apoyar la implementación de la Política de Protección y Tratamiento de Datos Personales, entre los cuales se encuentran el "*Manual de Políticas de Seguridad y Privacidad de la Información*" (E4-MN-12), el "*Procedimiento de Gestión de Incidentes de Seguridad de la Información*" (E4-PD-5), el formato E4-FT-16 "*Autorización para uso de información con datos personales*" y el formato E6-FT-3 "*Autorización de uso de imagen de menor de edad*".

A través de estos instrumentos se establecen mecanismos para informar a los titulares o sus representantes sobre el responsable del tratamiento, las finalidades para las cuales se recolectan los datos personales, los derechos que les asisten, los canales dispuestos para su ejercicio y la referencia a la política institucional de protección de datos personales.

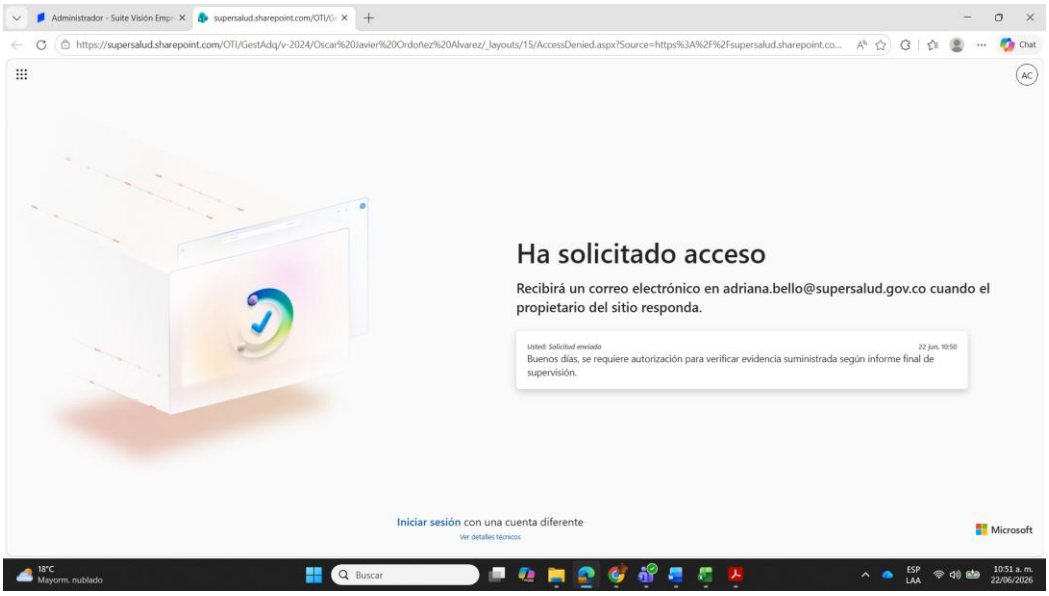
Adicionalmente, el proceso informó que durante la vigencia 2026 se encuentran en construcción, revisión o proceso de formalización diversos instrumentos orientados a fortalecer el Programa Integral de Gestión de Datos Personales, entre los cuales se encuentran avisos de privacidad por categoría de titular, el Manual de Gestión de Datos Personales, el Procedimiento Macro de Protección de Datos Personales, el Procedimiento para la Gestión de Eventos que Comprometan Datos Personales, el Instrumento de Verificación de Terceros y lineamientos asociados al sitio web institucional.

Mecanismos de seguimiento y evaluación de la gestión de protección de datos personales

Como parte de la verificación de los mecanismos institucionales de seguimiento en materia de protección de datos personales, el proceso remitió los informes de supervisión de los Contratos No. 165 de 2024 y No. 102 de 2025, en los cuales se reportan actividades relacionadas con auditorías, diagnósticos de cumplimiento normativo, actualización de instrumentos de protección de datos personales, revisión de procedimientos asociados a la gestión de incidentes y definición de indicadores para el seguimiento de la gestión institucional en esta materia.

No obstante, durante el desarrollo del seguimiento no fue posible verificar el contenido, alcance, resultados y conclusiones de las actividades reportadas, toda vez que la

documentación soporte y las evidencias asociadas se encontraban almacenadas en una carpeta a la cual la Oficina de Control Interno no tuvo acceso. Si bien se solicitó formalmente el acceso a dicha información, a la fecha de elaboración del presente informe no se había recibido respuesta, situación que limitó la validación de los productos reportados y su contribución al cumplimiento de las disposiciones en materia de protección de datos personales.



Trazabilidad de las actualizaciones de la Política de Protección y Tratamiento de Datos Personales

En desarrollo del presente seguimiento se evidenció que el proceso ha adelantado actividades orientadas a la revisión, actualización y fortalecimiento de la Política de Protección y Tratamiento de Datos Personales. Como evidencia de ello, se aportaron los informes finales de supervisión de los contratos suscritos para apoyar la implementación de acciones institucionales en esta materia, en los cuales se relacionan actividades asociadas a la construcción, actualización y fortalecimiento de instrumentos relacionados con la gestión de datos personales.

Con el fin de verificar los cambios incorporados a la Política de Protección y Tratamiento de Datos Personales durante el periodo evaluado, se solicitaron las versiones anteriores del documento; sin embargo, estas no fueron remitidas por el proceso. En consecuencia, no se contó con elementos que permitieran efectuar un análisis comparativo de las modificaciones realizadas, su alcance y la trazabilidad de las actualizaciones efectuadas.

Divulgación, apropiación y seguimiento de la Política de Protección y Tratamiento de Datos Personales

En desarrollo del presente seguimiento se evidenció que la entidad ha implementado actividades de socialización y sensibilización en materia de protección de datos personales y seguridad de la información. Entre las evidencias aportadas se encuentran la realización de la conferencia "Protección de datos personales y sensibles: Cumpliendo la normativa" el 9 de octubre de 2025, la publicación y divulgación de la Política de Protección y Tratamiento de Datos Personales durante los meses de noviembre y diciembre de 2025, y la programación de una campaña institucional de sensibilización sobre esta temática para el periodo comprendido entre el 27 de mayo y el 31 de julio de 2026.

Frente a la verificación del conocimiento y aplicación de la Política de Protección y Tratamiento de Datos Personales, el proceso informó que la política establece responsabilidades institucionales para su cumplimiento y aplicación. No obstante, señaló que a la fecha el Programa Integral de Gestión de Datos Personales se encuentra en proceso de implementación documental, razón por la cual las actividades de socialización realizadas han sido básicas y aún no se han implementado mecanismos específicos para verificar el nivel de conocimiento, apropiación o aplicación de la política por parte de funcionarios, contratistas o terceros, tales como evaluaciones, encuestas, mediciones, seguimientos u otros controles.

Transmisión y transferencia de datos personales

Se evidenció que la Política de Tratamiento y Protección de Datos Personales contempla la transmisión o transferencia de datos personales cuando exista fundamento legal para ello y se implementen las medidas contractuales y de seguridad correspondientes. Asimismo, el proceso informó que la entidad incorpora cláusulas de confidencialidad y protección de datos personales en los instrumentos jurídicos que resulten aplicables.

Con el fin de verificar la aplicación de estos controles, la Oficina de Control Interno solicitó información a la Dirección de Contratación, dependencia que informó que, una vez verificadas sus bases de datos, durante el periodo comprendido entre junio de 2025 y mayo de 2026 no se suscribieron contratos, convenios u otros instrumentos jurídicos que contemplaran la transmisión o transferencia de datos personales. En consecuencia, no se identificaron casos en los que hubiera sido procedente la aplicación de los controles contractuales previstos para este tipo de operaciones.

Autorizaciones otorgadas por los titulares

En atención a lo dispuesto en el artículo 9 de la Ley 1581 de 2012 y el capítulo II del Decreto 1377 de 2013, se evaluó el cumplimiento de la obligación relacionada con la obtención de la autorización previa e informada por parte de los titulares para el tratamiento de sus datos personales. En donde la norma establece que dicha autorización debe ser obtenida antes de realizar cualquier operación sobre la información y por un medio que permita su verificación y consulta posterior. En este sentido, se revisaron los mecanismos, procedimientos y soportes implementados por la Entidad para garantizar que las autorizaciones sean recogidas de manera adecuada y que cuenten con evidencia trazable y disponible para efectos de control, consulta y verificación.

De manera aleatoria se validaron elementos (sistemas de información y formatos) así:

Expedientes contractuales:

Para efectos de la verificación, el día 11 de junio de 2026 se solicitó formalmente a la Dirección de Contratación el suministro de las bases de datos correspondientes a los contratos suscritos en las vigencias 2025 y 2026. La información requerida fue remitida mediante correo electrónico el 17 de junio de 2026.

El propósito de esta gestión consistió en constatar, respecto de los contratistas, la existencia de las autorizaciones otorgadas por los titulares y su incorporación en los respectivos expedientes contractuales. Para tal fin, se efectuó una validación aleatoria de diez (10) contratos de prestación de servicios profesionales (OPS) contenidos en los expedientes electrónicos, evidenciándose lo siguiente:

No. Del contrato	Expediente electrónico
20 de 2025	2025940021607000023E
15 de 2025	2025940021607000015E
90 de 2025	2025940021607000086E
21 de 2025	2025940021607000025E
12 de 2025	2025940021607000012E
83 de 2025	2025940021607000074E
274 de 2025	20259400l1607000022E
328 de 2025	20259400l1607000044E
252 de 2025	2025940021607000223E
329 de 2025	20259400l1607000045E

En el marco de la revisión efectuada, no se evidenció formato alguno que acreditara la autorización expresa de los titulares para el tratamiento de sus datos personales. De igual manera, se procedió a verificar si dentro de los estudios previos existía alguna cláusula en la cual la Superintendencia Nacional de Salud (SNS) estableciera la obligación relacionada con la obtención de dicha autorización previa e informada.

Como resultado de esta verificación, se constató la inexistencia de disposiciones contractuales o administrativas que impongan de manera explícita la obligación de recabar la autorización previa e informada de los titulares, lo cual constituye una omisión relevante frente a los principios de legalidad y consentimiento consagrados en la normativa de protección de datos personales.

Mecanismos para el ejercicio de los derechos de los titulares de datos personales

En desarrollo del presente seguimiento se evidenció que la Superintendencia Nacional de Salud cuenta con mecanismos y procedimientos para la atención de consultas y reclamos relacionados con el ejercicio de los derechos de los titulares de datos personales.

Al respecto, la Política de Protección y Tratamiento de Datos Personales establece los procedimientos para la gestión de solicitudes asociadas al acceso, actualización, rectificación, supresión y revocatoria de la autorización de datos personales, así como los canales dispuestos para su radicación, entre los cuales se encuentran el canal presencial mediante recibo de correspondencia y los Centros de Atención al Ciudadano, el canal telefónico a través de las líneas de atención institucionales y el canal virtual mediante el Sistema de Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD) y el correo electrónico institucional. Adicionalmente, la entidad cuenta con el Procedimiento Gestión de Peticiones, Quejas, Reclamos, Sugerencias, Denuncias y Felicitaciones (PQRSDF) E6-PD-3, mediante el cual se establece el trámite y gestión de las solicitudes presentadas por los titulares de la información.

Durante el seguimiento se verificó la disponibilidad y funcionamiento de los canales virtuales dispuestos para la recepción de solicitudes, evidenciándose su operatividad al momento de la validación realizada por la Oficina de Control Interno.

Supervisión sobre el cumplimiento de obligaciones por parte de terceros

En desarrollo del presente seguimiento se evidenció que la Política de Protección y Tratamiento de Datos Personales, establece como directriz la supervisión y control del cumplimiento de las obligaciones por parte de los terceros que realizan tratamiento de datos personales en nombre de la Superintendencia Nacional de Salud. De igual forma, define como objetivo garantizar que dichos terceros observen el marco normativo aplicable en materia de protección de datos personales e incorpora un indicador orientado a medir el número de contratos revisados con cláusulas de protección de datos vigentes, el cual hace parte del Instrumento del Modelo de Seguridad y Privacidad de la Información.

No obstante, durante el presente seguimiento el proceso no aportó evidencias que permitieran verificar la aplicación, medición y seguimiento del indicador definido en la política institucional, ni demostrar la ejecución de actividades orientadas a supervisar el cumplimiento de las obligaciones en materia de protección de datos personales por parte de proveedores, contratistas u otros terceros que actúan como encargados del tratamiento.

Lo anterior cobra especial relevancia si se tiene en cuenta que, de conformidad con los artículos 17 y 18 de la Ley 1581 de 2012, el responsable del tratamiento debe garantizar que los encargados cumplan las condiciones de seguridad y confidencialidad de la información, mientras que estos últimos deben tratar los datos personales conforme a las instrucciones impartidas por el responsable y abstenerse de utilizarlos para finalidades diferentes a las autorizadas. De igual forma, los lineamientos expedidos por la Superintendencia de Industria y Comercio disponen la necesidad de incorporar y verificar cláusulas de protección de datos personales en los instrumentos contractuales suscritos con terceros.

En consecuencia, se recomienda que el proceso, en articulación con la Oficina Asesora de Planeación, fortalezca los mecanismos de seguimiento y control definidos en la política institucional, implementando acciones que permitan medir de manera efectiva el indicador establecido y acreditar la supervisión del cumplimiento de las obligaciones en materia de protección de datos personales por parte de los terceros que realizan tratamiento de información en nombre de la entidad.

Gestión de riesgos en materia de protección de datos personales

En el marco del seguimiento se solicitó información relacionada con la identificación, evaluación y control de riesgos asociados al tratamiento de datos personales. Durante la gestión del requerimiento se evidenciaron diferentes remisiones entre dependencias respecto de la responsabilidad sobre la información solicitada, involucrando a la Oficina Asesora de Planeación, la Subdirección de Tecnologías de la Información y la Oficial de Protección de Datos, situación que incidió en la oportunidad y trazabilidad de la respuesta suministrada.

Como resultado de la solicitud atendida finalmente por la Oficial de Protección de datos, se remitió una carpeta con los mapas de riesgos correspondientes a los diferentes procesos institucionales; sin embargo, estos no permitieron identificar de manera específica los riesgos asociados a la protección y tratamiento de datos personales ni los controles implementados para su mitigación. Por tal razón, la Oficina de Control Interno solicitó la depuración de la información y la remisión exclusiva de aquellos riesgos relacionados con acceso no autorizado, alteración, divulgación, uso indebido, transferencia o tratamiento inadecuado de datos personales, junto con los controles establecidos para su gestión, sin que se recibiera respuesta a dicho requerimiento. Adicionalmente, durante reunión sostenida con la Oficial de Protección de Datos se informó que la entidad no cuenta con una matriz de riesgos discriminada específicamente para protección de datos personales, sino que hace parte de la matriz de riesgos de seguridad de la información.

No obstante, dentro de la documentación aportada para la verificación de otros criterios se evidenció en el Informe Final de Supervisión del Contrato No. 102 de 2025 que una de las obligaciones contractuales consistió en apoyar la identificación de riesgos asociados al tratamiento de datos personales en los sistemas digitales de la Superintendencia Nacional de Salud, así como proponer acciones de mejora para fortalecer su protección. Igualmente, se registró como entregable el "*Informe de riesgos asociados al tratamiento de datos personales – junio*". En este contexto, llama la atención que durante el presente seguimiento se haya informado que la entidad no cuenta con riesgos asociados a protección de datos personales identificados o discriminados de manera específica, toda vez que la evidencia contractual aportada permite inferir que dicho ejercicio de identificación fue desarrollado en el marco de la ejecución contractual. Esta situación no permitió establecer con claridad la trazabilidad entre los productos obtenidos, los riesgos identificados y su incorporación dentro de los instrumentos institucionales de gestión del riesgo.

Indicadores para el seguimiento de la gestión de protección de datos personales

En desarrollo del presente seguimiento se evidenció que la Política de Protección y Tratamiento de Datos Personales establece directrices, objetivos e indicadores orientados a medir su implementación y cumplimiento, entre los cuales se encuentran el porcentaje de procesos evaluados con cumplimiento normativo en auditorías internas, el porcentaje de bases de datos registradas y actualizadas en el Registro Nacional de Bases de Datos – RNBD, el porcentaje de personal capacitado sobre la política de protección de datos, el número de contratos revisados con cláusulas de protección de datos vigentes y la tasa de cumplimiento de los tiempos de respuesta a las solicitudes de los titulares, entre otros mecanismos de seguimiento asociados al Modelo de Seguridad y Privacidad de la Información.

No obstante, frente a la solicitud de indicadores, reportes y evidencias utilizadas para medir el cumplimiento de la política, el proceso informó que la gestión de protección de datos personales se encuentra en proceso de fortalecimiento e implementación documental a través del Programa Integral de Gestión de Datos Personales y no remitió reportes, mediciones, seguimientos o resultados asociados a los indicadores definidos en la política, por lo que durante el periodo evaluado no se evidenció la aplicación efectiva de dichos mecanismos como herramienta para medir su cumplimiento.

Registro Nacional de Bases de Datos (RNBD)

En desarrollo del presente seguimiento se verificó la identificación de las bases de datos personales reportadas por la entidad ante el Registro Nacional de Bases de Datos (RNBD). Inicialmente, el proceso informó que la identificación de las bases de datos "*debía realizarse con fundamento en las categorías de titulares y las finalidades del tratamiento, diferenciándolas de los repositorios físicos, digitales y demás activos de información*", los cuales, según lo manifestado, hacen parte del Inventario de Activos de Información de la entidad.

Posteriormente, a solicitud de la Oficina de Control Interno, el proceso remitió el archivo denominado "Información RNBD.xls", el cual contenía una hoja denominada "Análisis BD Activas" con ciento ochenta y una (181) bases de datos, información que fue confirmada durante entrevista realizada el 19 de junio de 2026 por la Oficial de Protección de Datos como el universo de bases de datos vigentes.

No obstante, mediante correo electrónico del 22 de junio de 2026, el proceso remitió el documento denominado "*Informe Explicativo reorganización reporte RNBD*", en el cual se plantea una reorganización del esquema de registro de las bases de datos ante el RNBD, orientando su estructuración hacia categorías de titulares de la información.

Durante la revisión de dicho documento se evidenció que la propuesta de reorganización plantea consolidar el registro de las bases de datos personales con fundamento en categorías de titulares de la información (*funcionarios, usuarios, contratistas, proveedores, visitantes, entre otros*), bajo el argumento de que este criterio resulta más coherente para la administración de la privacidad y que los diferentes repositorios físicos, digitales, aplicativos o archivos deben administrarse de manera independiente a través del Inventario de Activos de Información.

No obstante, de acuerdo con la Ley 1581 de 2012, el Decreto Único Reglamentario 1074 de 2015 y los lineamientos impartidos por la Superintendencia de Industria y Comercio, el objeto del Registro Nacional de Bases de Datos corresponde a la inscripción de las bases de datos que contengan datos personales, entendidas como conjuntos organizados de datos personales, independientemente del medio físico o electrónico en el que reposen. En este sentido, tanto las Preguntas Frecuentes de la página de la SIC, como el Manual del RNBD establecen que, previo al registro, el responsable debe elaborar un inventario de las bases de datos existentes, identificando la cantidad de bases de datos, el número de titulares, el tipo de información tratada, las medidas de seguridad, su ubicación y demás características propias **de cada una**, e inscribirlas de manera independiente.

En consecuencia, si bien resulta técnicamente válido diferenciar los conceptos de base de datos y repositorio de información, la propuesta de reorganización basada exclusivamente en categorías de titulares podría no reflejar de manera integral el universo de bases de datos sujetas a registro en el RNBD, toda vez que una misma categoría de titulares puede comprender diferentes bases de datos con finalidades, tratamientos, responsables, ciclos de vida o medidas de seguridad distintas. Esta situación podría afectar la correspondencia entre el inventario institucional de bases de datos y la información reportada ante el RNBD, así como la trazabilidad y consistencia del registro frente a los lineamientos establecidos por la Superintendencia de Industria y Comercio.

Administración de usuarios y control de accesos al Registro Nacional de Bases de Datos (RNBD)

Con el fin de verificar el procedimiento utilizado por la entidad para la administración y

actualización de la información registrada en el Registro Nacional de Bases de Datos (RNBD), la Oficina de Control Interno realizó una validación (vía Teams) mediante acceso en línea a la plataforma, con el acompañamiento del colaborador encargado de su operación. Durante la verificación se evidenció que el ingreso al aplicativo se efectuó utilizando un usuario cuyo nombre no correspondía al colaborador que realizó la autenticación, quien manifestó que se trataba de un usuario genérico.

Como parte de la revisión, se verificó la administración de usuarios registrada en la plataforma, evidenciándose un total de cincuenta (50) usuarios activos con permisos de acceso, distribuidos así: un (1) usuario con rol **Responsable**, doce (12) usuarios con rol **Administrador** y treinta y siete (37) usuarios con rol **Operativo**. Posteriormente, la Oficina de Control Interno confrontó dicha información con la base de funcionarios y exservidores administrada por la Dirección de Talento Humano, identificando que únicamente quince (15) de los usuarios registrados mantenían una relación laboral o contractual vigente con la Superintendencia Nacional de Salud, mientras que los demás no registraban vínculo activo con la entidad. Asimismo, se evidenció que el usuario con rol **Responsable**, correspondiente al mayor nivel de privilegio dentro del sistema, tampoco mantenía relación laboral o contractual vigente.

Durante la validación, el colaborador informó que los usuarios registrados con permisos activos podrían realizar el registro o modificación de la información en el RNBD; sin embargo, manifestó que, por decisión operativa, dichas actividades actualmente son ejecutadas exclusivamente por el grupo de Protección de Datos. Lo anterior evidencia la existencia de usuarios habilitados con capacidad de acceso y administración sobre la plataforma, pese a que no participan en su operación ni mantienen vinculación vigente con la entidad, situación que podría afectar los principios de control de acceso, trazabilidad y administración de cuentas de usuario.

RESULTADOS

NO CONFORMIDADES:

NC 1: Debilidades en la administración de usuarios y control de accesos al Registro Nacional de Bases de Datos (RNBD): Durante el presente seguimiento se evidenció que el acceso al Registro Nacional de Bases de Datos (RNBD) se realizó mediante credenciales que no correspondían a la identidad del colaborador que efectuó la autenticación. Así mismo, se identificó la existencia de usuarios con permisos activos, incluido el usuario con rol Responsable, que no mantienen vinculación laboral o

contractual vigente con la entidad y que conservan la posibilidad de acceder y efectuar modificaciones sobre la información registrada en la plataforma.

Esta situación incumple las disposiciones establecidas en el Manual de Políticas de Seguridad y Privacidad de la Información (E4-MN-12) y en el Modelo de Seguridad y Privacidad de la Información (MSPI) respecto de la administración de identidades y el control de accesos. Lo anterior obedece, presuntamente, a debilidades en la gestión y depuración de las cuentas de usuario y en la aplicación de controles para garantizar el uso de credenciales individuales y la deshabilitación oportuna de accesos que ya no son requeridos. Como consecuencia, se incrementa el riesgo de accesos o modificaciones no autorizadas sobre la información registrada en el RNBD, afectando su integridad, trazabilidad, confiabilidad y la responsabilidad sobre las actuaciones realizadas en la plataforma.

NC 2: Falta de autorización para el tratamiento de datos personales de contratistas o inclusión en los estudios previos : Se constató que en una muestra de diez (10) contratos de prestación de servicios ejecutados durante la vigencia 2025, la Entidad recolectó, almacenó y procesó datos personales y documentación soporte de los contratistas (tales como cédulas de ciudadanía, hojas de vida, certificaciones bancarias, Certificado de examen médico pre ocupacional de ingreso, Tarjeta profesional o matrícula profesional, RIT, RUT y registros de antecedentes entre otros) sin contar con la debida autorización previa, expresa e informada para el tratamiento de datos personales firmada por los titulares de la información.

Lo anterior no permite evidenciar el cumplimiento de lo establecido en la normatividad vigente, así:

- **Ley Estatutaria 1581 de 2012 (Artículo 9):** Establece que la recolección y tratamiento de datos personales requiere de la autorización previa, expresa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.
- **Decreto 1074 de 2015:** Regula la obligatoriedad de los responsables del Tratamiento de implementar políticas y formatos que garanticen el derecho al *Habeas Data*.

El incumplimiento se originó posiblemente por la inexistencia de un control obligatorio dentro del *checklist* o lista de chequeo de la etapa precontractual que exija la firma del formato de autorización de datos como requisito para la suscripción del contrato; falta de articulación y capacitación entre el Oficial de Protección de Datos y la Dirección de Contratación.

NC 3: Ausencia de protección técnica (anonimización o encriptación) de la información contenida en las tablas de la base de datos ORFEO2: Durante el presente seguimiento se evidenció que la información de salud recibida de forma digital a través de las peticiones, quejas, reclamos, denuncias y demás solicitudes de información, almacenada en las tablas **PQRD_REGISTRADOS_RADICADOS**, **PQRD_AFECTADOS** y **PQRD_PETICIONARIOS**, no cuenta con mecanismos de protección como cifrado o técnicas de anonimización que impidan su lectura directa. Esta situación incumple el principio de seguridad previsto en el artículo 4, literal g), y el deber de confidencialidad establecido en el literal h) de la Ley 1581 de 2012, así como el principio de responsabilidad demostrada (Accountability) y las directrices técnicas del Programa Integral de Gestión de Datos Personales de la Superintendencia de Industria y Comercio.

NC 4: Deficiencias en la Identificación, Conciliación y Control de Bases de Datos Personales: Durante el presente seguimiento se evidenciaron inconsistencias en la información suministrada para acreditar el inventario de las bases de datos personales de la entidad. En primer lugar, el inventario remitido por el proceso no identificó las dependencias responsables de la administración de cada una de las bases de datos reportadas ante el Registro Nacional de Bases de Datos (RNBD).

Adicionalmente, no se observó concordancia entre el número de bases de datos reportadas en las diferentes fuentes consultadas, evidenciándose diferencias entre la información publicada en el portal institucional (185 bases de datos), la registrada ante la Superintendencia de Industria y Comercio en las vigencias 2025 y 2026 (184 bases de datos) y el inventario suministrado por la Oficial de Protección de Datos (181 bases de datos). Así mismo, no fue posible verificar la correspondencia de esta información con el inventario de activos de información de la vigencia 2025, debido a que dicho soporte no fue suministrado durante el seguimiento.

Esta situación incumple lo dispuesto en el artículo 25 de la Ley 1581 de 2012 y las disposiciones reglamentarias contenidas en el Decreto 1074 de 2015 relacionadas con el Registro Nacional de Bases de Datos, al no contar con información consistente y verificable que permita acreditar la identificación y administración de las bases de datos personales de la entidad. Lo anterior pudo obedecer a debilidades en los mecanismos de administración, actualización y conciliación de la información reportada, generando el riesgo de inconsistencias en el inventario institucional, afectando la confiabilidad de la información registrada ante el RNBD y el adecuado cumplimiento de las obligaciones asociadas a su administración.

LIMITACIONES:

LM 1: Disponibilidad y oportunidad de la información sobre riesgos de protección de datos personales: Durante la ejecución del seguimiento se presentaron dificultades para obtener información específica relacionada con la identificación, evaluación y control de riesgos asociados al tratamiento de datos personales. Aunque la solicitud inicial fue realizada oportunamente, se generaron sucesivas remisiones entre dependencias respecto de la responsabilidad sobre la información requerida, inicialmente hacia la Oficina Asesora de Planeación, posteriormente hacia la Subdirección de Tecnologías de la Información y, finalmente, nuevamente hacia la Oficial de Protección de Datos, situación que incidió en la oportunidad de la respuesta y redujo el tiempo disponible para su análisis.

OBSERVACIONES:

OBS 1: Inconsistencia en la identificación de la documentación aplicable: Durante el diligenciamiento de la matriz de verificación del presente seguimiento, el proceso reportó la Política de Protección y Tratamiento de Datos Personales bajo el código DIPI04 y remitió documentación asociada con codificaciones que no correspondían a los documentos vigentes. Posteriormente, durante la entrevista realizada el 9 de junio de 2026, se aclaró que la documentación vigente había sido actualizada y formalizada bajo nuevas codificaciones dentro del Sistema Integrado de Gestión, entre ellas la Política de Protección y Tratamiento de Datos Personales identificada con código E4-PI-1, versión 1. Lo anterior evidenció inconsistencias en la referencia e identificación de la documentación aplicable suministrada para el seguimiento, situación que generó reprocesos y posible divulgación o consulta de información desactualizada por parte de los interesados.

OBS 2: Criterio de organización del Registro Nacional de Bases de Datos (RNBD): Durante el presente seguimiento se observó que la propuesta de reorganización del Registro Nacional de Bases de Datos (RNBD) se fundamenta en la consolidación de las bases de datos por categorías de titulares de la información. No obstante, de acuerdo con la Ley 1581 de 2012, el Decreto 1074 de 2015 y los lineamientos impartidos por la Superintendencia de Industria y Comercio, el RNBD tiene por objeto el registro de las bases de datos que contienen datos personales, entendidas como conjuntos organizados de datos personales, las cuales deben identificarse e inscribirse de manera individual, independientemente del medio en el que reposen. En este contexto, aunque resulta técnicamente procedente diferenciar los conceptos de base de datos y repositorio de información, la reorganización propuesta podría no reflejar de manera integral el universo de bases de datos sujetas a registro al

consolidarlas exclusivamente por categorías de titulares, situación que podría afectar la trazabilidad, consistencia y confiabilidad de la información reportada ante el RNBD, así como el adecuado cumplimiento de las obligaciones establecidas en el régimen de protección de datos personales.

OBS 3: Implementar mecanismos que permitan supervisar el cumplimiento de obligaciones por parte de terceros: En el marco del seguimiento efectuado, se evidenció que, si bien la Política de Protección y Tratamiento de Datos Personales establece directrices, objetivos e indicadores orientados a garantizar el cumplimiento de las obligaciones por parte de terceros en el tratamiento de datos, el proceso objeto de seguimiento no acreditó evidencias que permitan demostrar la aplicación y seguimiento del indicador definido. Esta situación limita la verificación del cumplimiento de lo dispuesto en la Ley 1581 de 2012 y en la normatividad expedida por la Superintendencia de Industria y Comercio, que obliga a las entidades a supervisar y controlar a proveedores, contratistas y aliados en materia de seguridad, confidencialidad y respeto de los derechos de los titulares. En consecuencia, se observa para que, en coordinación con la Oficina Asesora de Planeación como segunda línea de defensa del MIPG, se implemente un plan de mejora que asegure la observancia de los principios de legalidad, consentimiento informado, seguridad y confidencialidad, fortaleciendo así la responsabilidad institucional frente al tratamiento de datos personales.

OBS 4: Ausencia de divulgación y socialización de la Política E4-PI-1: Si bien la Superintendencia Nacional de Salud cuenta con una Política de Protección y Tratamiento de Datos Personales formalmente aprobada (E4-PI-1), durante el presente seguimiento se evidenció que la divulgación y socialización de dicho instrumento aún no ha alcanzado la totalidad de las dependencias involucradas en el tratamiento de datos personales. En particular, se identificó que el Grupo Interno de Trabajo de Correspondencia y el Grupo Interno de Trabajo de Gestión Documental manifestaron no conocer la Política E4-PI-1, los formatos asociados ni la forma en que estos deben aplicarse en el desarrollo de sus funciones, situación que difiere de lo establecido en la Declaratoria de la política institucional, la cual dispone que la entidad promoverá su divulgación y socialización tanto al interior de la organización como con los terceros que realicen tratamiento de datos personales en su nombre. Esta situación podría afectar la apropiación y aplicación uniforme de los lineamientos institucionales en materia de protección de datos personales por parte de las dependencias que intervienen en su tratamiento.

OBS 5: Ausencia de documentación actualizada y de elementos técnicos que garanticen el borrado seguro de datos e información: Durante el presente seguimiento se evidenció que el documento E4-MN-3 – Manual para el Borrado Seguro

de Información contiene referencias a formatos identificados con una codificación que ya no se encuentra vigente, lo que hace recomendable su actualización para mantener la coherencia documental del Sistema Integrado de Gestión. Así mismo, se observó que la entidad no dispone de una herramienta tecnológica específica que permita realizar el borrado seguro de la información almacenada en dispositivos de almacenamiento, situación que podría limitar el fortalecimiento de los controles técnicos orientados a garantizar la eliminación definitiva de los datos personales y sensibles, conforme a los principios de seguridad, confidencialidad y responsabilidad demostrada previstos en la Ley 1581 de 2012 y en los lineamientos emitidos por la Superintendencia de Industria y Comercio.

OBS 6: Debilidades en la parametrización de contraseñas y desalineación en las Políticas de seguridad y privacidad de la información: Durante el presente seguimiento se identificaron oportunidades de mejora relacionadas con la gestión de contraseñas y la actualización de la documentación en materia de seguridad de la información. En particular, se evidenció que la base de datos ORFEO2, soportada sobre PostgreSQL y utilizada para almacenar datos personales e información asociada a las solicitudes radicadas por los ciudadanos, no dispone de un mecanismo que permita parametrizar y administrar políticas de contraseñas, tales como vigencia, longitud mínima, complejidad e historial, razón por la cual no fue posible verificar la fecha del último cambio de las credenciales de acceso.

Así mismo, se observó que el Manual de Políticas de Seguridad y Privacidad de la Información (E4-MN-12) presenta diferencias frente a la configuración vigente del Directorio Activo de Windows, al establecer una longitud mínima de ocho (8) caracteres para las contraseñas, mientras que la configuración implementada exige diez (10) caracteres, correspondiendo esta última a una práctica de seguridad más robusta. Adicionalmente, el citado manual contiene dos numerales identificados como "*Política de control de acceso*" (5.6 y 5.7), con diferente contenido, situación que hace recomendable su revisión y actualización para mantener la coherencia y consistencia del marco documental de seguridad de la información.

RECOMENDACIONES

RM 1: Definición formal del rol de Líder de Protección de Datos: Formalizar la identificación de la dependencia, cargo o funcionario responsable de ejercer el rol de Líder de Protección de Datos previsto en la Política de Protección y Tratamiento de Datos Personales, así como definir su articulación con los demás actores involucrados en la

gestión de protección de datos personales, con el fin de fortalecer la claridad en la asignación de responsabilidades y la coordinación de las actividades asociadas a esta materia.

RM 2: Fortalecimiento de la capacidad operativa del Oficial de Protección de Datos Personales: La Resolución 2025153040012454-6 de 2025 dispone que el funcionario que ejerza el cargo de Oficial de Seguridad de la Información asuma las funciones de Oficial de Protección de Datos Personales. Aunque no se identificaron disposiciones normativas que establezcan incompatibilidad entre ambos roles, se recomienda evaluar periódicamente la suficiencia de los recursos, capacidades y mecanismos de coordinación asociados a dichas funciones, con el fin de garantizar una adecuada gestión tanto de los aspectos relacionados con la seguridad de la información como de aquellos asociados al cumplimiento del régimen de protección de datos personales.

RM 3: Fortalecimiento del marco documental de protección de datos personales: Continuar y priorizar las actividades orientadas a la revisión, aprobación y formalización de los instrumentos documentales que se encuentran en construcción o proceso de actualización. Asimismo, diseñar e implementar mecanismos de evaluación y seguimiento que permitan verificar el conocimiento, apropiación y aplicación de la Política de Protección y Tratamiento de Datos Personales por parte de funcionarios, contratistas y demás actores involucrados, así como medir la efectividad de las actividades de divulgación y sensibilización realizadas por la entidad, con el fin de fortalecer la implementación, estandarización, seguimiento y sostenibilidad de la gestión de protección de datos personales.

RM 4: Implementación de indicadores y mecanismos de seguimiento al cumplimiento de la Política de Protección y Tratamiento de Datos Personales: Implementar y poner en operación los indicadores definidos en la Política de Protección y Tratamiento de Datos Personales, así como los mecanismos de seguimiento asociados, de manera que permitan medir de forma periódica el grado de cumplimiento de los objetivos establecidos, evaluar la efectividad de las acciones implementadas y generar información para la toma de decisiones y el mejoramiento continuo de la gestión de protección de datos personales. Asimismo, documentar y conservar los resultados de las mediciones efectuadas, con el fin de contar con evidencias objetivas que permitan monitorear el avance y cumplimiento de la política institucional.

CONCLUSIONES

Como resultado del presente seguimiento se evidenció que la Superintendencia Nacional de Salud ha adelantado acciones orientadas al fortalecimiento de la gestión de protección de datos personales, entre ellas la adopción de una Política de Protección y Tratamiento de Datos Personales, la implementación de instrumentos asociados, el desarrollo de actividades de socialización y el avance en la estructuración de documentos que soportan el cumplimiento del régimen de protección de datos personales.

No obstante, se identificaron oportunidades de mejora y situaciones que requieren fortalecimiento, relacionadas con la consolidación del inventario y registro de las bases de datos personales, la formalización e implementación de algunos instrumentos documentales, la gestión de riesgos, la operación de indicadores de seguimiento, la administración de usuarios y controles de acceso, así como el cumplimiento de algunos requisitos legales y técnicos asociados al tratamiento y protección de datos personales.

En consecuencia, se hace necesario que el proceso continúe fortaleciendo la implementación del modelo institucional de protección de datos personales, asegurando la articulación entre los instrumentos de gestión, los controles operativos y tecnológicos y el cumplimiento de las obligaciones establecidas en la Ley 1581 de 2012 y su normativa reglamentaria, con el fin de consolidar un sistema de gestión que garantice la adecuada protección de los datos personales tratados por la entidad.

Cordialmente,

GIOVANNY LÓPEZ MEJÍA
Jefe Oficina de Control Interno (e)

Proyectó: Adriana Bello Cortés; Luis Alberto Triana Lozada; Milton Andrés Ruiz Bonilla.

Revisó y aprobó: Giovanny López Mejía, Jefe Oficina Control Interno (e)