



SEGUIMIENTO ACCESIBILIDAD LEY DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

**MAYO 2024
OFICINA DE CONTROL INTERNO**

TABLA DE CONTENIDO

1. OBJETIVO	3
2. ALCANCE	3
3. CRITERIOS GENERALES	3
5. METODOLOGÍA	3
6. RESULTADOS DEL SEGUIMIENTO Y ESTADO ACTUAL DE LA IMPLEMENTACIÓN	3
7. CONCLUSIONES	9

1. OBJETIVO

Realizar seguimiento a las acciones tomadas por los responsables de la aplicación de la política de privacidad y protección de datos personales (plan de mejoramiento), según “Informe de Seguimiento Ley de Privacidad y Protección de Datos Personales”, presentado en octubre 2023.

2. ALCANCE

Desde la fecha del último informe presentado hasta el 25 de mayo de 2024.

3. CRITERIOS GENERALES

Leyes 87 de 1993 y 1581 de 2012; Resolución N°225 del 10 de abril de 2023, artículos 9, 11, 12, 14 y 22; “INFORME SEGUIMIENTO LEY DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES” del año 2023, presentado por la Oficina de Control Interno; “PLAN DE TRABAJO: INFORME SEGUIMIENTO LEY DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES – 2024”, aportado por el Grupo Nacional de Atención y Servicio al Ciudadano.

4. METODOLOGÍA

Entrevista.
Inspección en sitio.
Revisión documental.

5. RESULTADOS DEL SEGUIMIENTO Y ESTADO ACTUAL DE LA IMPLEMENTACIÓN

Fundados en lo dispuesto en los artículos 4, literal g) y 12, literal k) de la Ley 87 de 1993, el seguimiento que nos ocupa se surtió retomando los criterios normativos que dieron lugar a los hallazgos, vale decir, los artículos 9, 11, 12, 14 y 22 de la Resolución N°225 del 10 de abril de 2023, “*Por la cual se actualiza la política para el tratamiento de datos personales en el Instituto Nacional de Medicina Legal y Ciencias Forenses*”, mandatos que al ser taxativos son de obligatorio cumplimiento por parte de la entidad.

Con base en el objetivo planteado, la verificación normativa y la aplicación de las técnicas de entrevista, inspección en sitio y revisión documental, a continuación se describen los hallazgos informados y el resultado del seguimiento:

5.1. Hallazgo informado N°1.

(...)

Al tenor de lo anterior, mediante las técnicas de auditoria de observación y circularización, se efectuó un recorrido a los puntos de ingreso a la sede central de la entidad, así como, discrecionalmente, al área de atención a los usuarios del Grupo de Clínica, Psicología y Psiquiatría Forense de la Regional Bogotá, advirtiéndose que si bien las cámaras que capturan imágenes en video en los zonas de acceso cuentan con el letrero de monitoreo, en los lugares donde se registra de manera directa información de los usuarios faltan los avisos de advertencia de tratamiento y confidencialidad de los datos personales; lo que permite inferir razonablemente que se incumple lo dispuesto en el parágrafo primero del artículo 9 de la Resolución N°255 del 10 de abril de 2023.

(...)

En esta línea, atendiendo al hecho que la regulación que nos ocupa es de obligatorio cumplimiento en todas las sedes instituciones dispuestas en el territorio nacional, se adelantó verificación, aleatoria, a las Regionales Norte, Noroccidente, Oriente y Sur, Grupo de Clínica Forense, estableciéndose que en efecto en dichas unidades organizacionales, en concreto, en los puntos de atención donde se recepcionan y

registran datos personales de los usuarios, no se han colocado los avisos donde la entidad debería informar sobre el tratamiento y confidencialidad de los mismos; lo que corrobora el incumplimiento antes relacionado. (Ver imágenes).

(...)”.

5.1.1. Criterio específico incumplido

Resolución N°225 del 10 de abril de 2023, artículo 9. “Recolección de datos personales”.

Con base en lo anterior, en las “CONCLUSIONES” del informe inicial, la Oficina de Control Interno planteó:

“(…)”

En virtud de lo anterior, el Grupo Nacional de Atención y Servicio al Ciudadano, con el apoyo del Grupo Nacional de Tecnologías de la Información y Desarrollo, deberá plantear y ejecutar acciones orientadas a colocar avisos informativos en todos los puntos institucionales de atención, dispuestos en el territorio nacional, donde se recepcionan y registran datos personales de los usuarios, informándoles lo atinente al tratamiento y confidencialidad de los mismos.

(...)”.

5.1.2. Acción formulada en el plan de mejoramiento

Ninguna. El responsable del proceso no formuló correcciones o acciones correctivas.

5.1.3. Resultado del seguimiento.

En desarrollo de la actividad que nos ocupa, se advirtió con la muestra tomada (*Recepción Nivel Central, Edificio de Docencia y Regional Occidente*) que persiste el incumplimiento a lo normado, como quiera que el responsable del proceso no planteó ni ejecutó acciones orientadas a colocar avisos informativos atinentes al tratamiento y confidencialidad de los datos personales de los usuarios, en la totalidad de los puntos institucionales de atención dispuestos en el territorio nacional; hallazgo que no fue objetado por las personas entrevistadas durante la reunión de seguimiento celebrada el 2024/05/24.

5.1.4. Evidencia documental aportada

Al no formularse corrección o acción correctiva, no se aportó ninguna evidencia.

5.2. Hallazgo informado N°2.

“(…)”

Si bien el liderazgo del proceso de implementación de la política de tratamiento de datos está a cargo del Grupo Nacional de Atención y Servicio al Ciudadano, resulta evidente que para el desarrollo e implementación de un plan para revolver los incidentes de seguridad que afecten los datos personales bajo custodia o posesión de la entidad, se debe contar, inexorablemente, con el apoyo del Grupo Nacional de Tecnologías de la Información y Desarrollo, quien durante la entrevista presencial indicó que tal actividad no se había abordado, argumentando que no se ha adelantado ninguna reunión conjunta para conocer los posibles incidentes a la seguridad de los datos; circunstancia de hecho por la cual, se incumple lo dispuesto en el parágrafo único del presente artículo.

(...)”.

5.2.1. Criterio específico incumplido

Resolución N°225 del 10 de abril de 2023, artículo 11. Seguridad de la Información.

En consonancia, la Oficina de Control Interno expuso en las “CONCLUSIONES” del informe inicial:

“(…)

En virtud de lo anterior, el Grupo Nacional de Atención y Servicio al Ciudadano, con el apoyo del Grupo Nacional de Tecnologías de la Información y Desarrollo, deberá adelantar la gestión orientada a conocer los incidentes de seguridad que han afectado, a la fecha, los datos personales bajo custodia o posesión de la entidad; así como desarrollar e implementar un plan para resolverlos y neutralizar la posible ocurrencia.

“(…)”.

5.2.2. Acción formulada en el plan de mejoramiento.

“(…)”

Adelantar la gestión orientada a conocer los incidentes de seguridad que han afectado, a la fecha, los datos personales bajo custodia o posesión de la entidad; así como desarrollar e implementar un plan para resolverlos y neutralizar la posible ocurrencia.

“(…)”.

5.2.3. Resultado del seguimiento.

Mediante entrevista realizada a la coordinadora del Grupo Nacional de Tecnologías de la Información y Desarrollo, manifestó que: “(…) *las bases de datos misionales y administrativas a cargo del grupo no se ha presentado ningún incidente de seguridad que pueda afectar la información y datos allí consignados (…)*”. (sic)

Con relación al desarrollo e implementación de un plan para resolver y neutralizar la posible ocurrencia de incidentes de seguridad que puedan afectar los datos personales bajo custodia o posesión de la entidad, manifestó: “(…) *se implementó el procedimiento DG-A-P-038, el cual se encuentra en actualización (…)*”; pronunciamiento que nos lleva a inferir razonablemente que se viene cumpliendo con el mandato normativo en cuestión.

5.2.4. Evidencia documental aportada

- Procedimiento “GESTIÓN DE INCIDENTES DE TECNOLOGÍAS DE INFORMACIÓN”, Código: DG-A-P-083, Versión: 2.
- Procedimiento “GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN”, Código: DG-A-P-038, Versión: 3.

5.3. Hallazgo informado N°3.

“(…)”

Frente al tema de tener un nivel de acceso a la información limitado a parámetros previamente definidos, así como a la fijación de medidas técnicas de control para restringirlo solo a las personas autorizadas, la coordinación del Grupo Nacional de Atención y Servicio al Ciudadano, como líder del proceso, indico que ello era del resorte funcional del Grupo Nacional de Tecnología de la Información y Desarrollo, quien a su vez, a la misma pregunta, manifestó que este grupo no tiene la autonomía para definir los niveles de acceso a la información, como tampoco para establecer los perfiles de los servidores y contratistas; señalando que son los dueños de los procesos quienes lo deben hacer.

En este entendido, se incumple el artículo 12 de la Resolución N°225 del 10 de abril de 2023.

“(…)”.

5.3.1. Criterio específico incumplido.

Resolución N°225 del 10 de abril de 2023, artículo 12. Nivel de acceso a la información de datos personales.

En esta línea, la Oficina de Control Interno, en las “CONCLUSIONES” del informe inicial, resaltó:

“(…)

En virtud de lo anterior, el Grupo Nacional de Atención y Servicio al Ciudadano, con el apoyo del Grupo Nacional de Tecnologías de la Información y Desarrollo, deberá definir un nivel de acceso a la información, limitado a parámetros previamente establecidos, así como los perfiles de los servidores públicos y contratistas para que puedan acceder a los datos personales recolectados, almacenados y usados por las distintas unidades organizacionales en el ejercicio de su deber funcionales.

“(…)”.

5.3.2. Acción formulada en el plan de mejoramiento.

“(…)”

Definir un nivel de acceso a la información, limitado a parámetros previamente establecidos, así como los perfiles de los servidores públicos y contratistas para que puedan acceder a los datos personales recolectados, almacenados y usados por las distintas unidades organizacionales en el ejercicio de su deber funcionales.

“(…)”.

5.3.3. Resultado del seguimiento.

En desarrollo de la técnica de entrevista, la coordinación del Grupo Nacional de Tecnologías de la Información y Desarrollo, indicó que: “(…) *quien define el acceso al aplicativo que interactúa con las bases de datos es el responsable del proceso y define el perfil y el nivel de acceso a la información (…)*”, agregando que: “(…) *eso no está contemplado en ninguno de los procedimientos por eso es necesario modificarlos (…)*”; pronunciamiento que permite colegir que se mantiene el incumplimiento de la norma citada en el numeral 5.3.1.

5.3.4. Evidencia documental aportada.

Dado que no se ejecutaron correcciones o acciones correctivas por parte del responsable del proceso, no se aportaron evidencias documentales.

5.4. Hallazgo informado N°4.

“(…)”

Frente al hecho que el Instituto Nacional de Medicina Legal y Ciencias Forenses ha suscrito un contrato para que, a través de un tercero, se preste el servicio de vigilancia en todo el territorio Nacional, se advirtió que dicho operador usa una base de datos denominada “Total Integration System” - (TIS), de propiedad de la Compañía Interamericana de Seguridad y Servicio Ltda. - (C.I.S.), en la cual registra datos personales de los usuarios de la entidad, empleando esta una sola contraseña para todos los operarios, lo que implica que cualquiera de ellos puede acceder al sistema y consultar la información recaudada; lo que deja en evidencia que carecen de niveles de acceso y no se han establecido perfiles para los guardas, aumentándose el riesgo de fuga de datos.

Con base en lo anterior, se adelantó entrevista a los supervisores de la compañía de vigilancia Avizor Seguridad Ltda., manifestando desconocer la política para el tratamiento de datos personales implementada por la institución, a pesar que mediante el oficio N°0047-GNASC-OFPL-DG-2023 del 2023-09-29, el líder del proceso solicitó a la coordinación del Grupo Nacional de Gestión Administrativa, la socialización de la Resolución N°225 del 10 de abril de 2023, entre los guardas de seguridad de la empresa en mención.

Con relación a la disposición final de la base de datos antes citada, agregaron que vencido el plazo de ejecución y, por ende, obligaciones contractuales, esta será entregada y dejada bajo custodia de la institucional por un término de dos (2) años; término que agotado dará lugar a borrar la totalidad de la información y formatear nuevamente el disco.

Sin perjuicio de lo anterior, la entidad, a través de su comisionista, no ha exigido a la persona jurídica Bursagan S.A., ni a los prestadores del servicio de vigilancia, el cumplimiento de la política para el tratamiento de datos personales implementada por el Instituto Nacional de Medicina Legal y Ciencias Forenses; lo que permite colegir el incumplimiento a lo dispuesto en el artículo 14 de la Resolución N°225 de 2023.

(...)"

5.4.1. Criterio específico incumplido

Resolución N°225 del 10 de abril de 2023, artículo 14. Bases de Datos con datos personales manejadas por terceros.

Acorde con lo expuesto, en las "CONCLUSIONES" del informe inicial, la Oficina de Control Interno señaló:

"(...)

En virtud de lo anterior, el Grupo Nacional de Atención y Servicio al Ciudadano, con el apoyo del Grupo Nacional de Tecnologías de la Información y Desarrollo, deberá socializar ante todos los contratistas de la entidad la política para el tratamiento de datos personales implementada en el Instituto Nacional de Medicina Legal y Ciencias Forenses, exigir su cumplimiento y definir la forma de que estos hagan la entrega de las Bases de Datos que contengan datos personales de los usuarios del Instituto, una vez cesen las obligaciones contractuales.

(...)"

5.4.2. Acción formulada en el plan de mejora.

"(...)

Socializar ante todos los contratistas de la entidad la política para el tratamiento de datos personales implementada en el Instituto Nacional de Medicina Legal y Ciencias Forenses, exigir su cumplimiento y definir la forma de que estos hagan la entrega de las Bases de Datos que contengan datos personales de los usuarios del Instituto, una vez cesen las obligaciones contractuales.

(...)"

5.4.3. Resultado del seguimiento.

En desarrollo de esta actuación se entrevistó al supervisor de la compañía de vigilancia Avizor Seguridad Ltda., la cual presta sus servicios en las sedes institucionales ubicadas en la ciudad de Bogotá, quien indicó que en efecto ya se había socializado entre sus trabajadores la política para el tratamiento de datos personales implementada en el Instituto Nacional de Medicina Legal y Ciencias Forenses.

En consonancia, en la reunión celebrada el 2024/05/24, la coordinación del Grupo Nacional de Atención y Servicio al Ciudadano precisa que no se ha realizado dicha actividad respecto a los demás contratistas de la institución, porque no sabe quiénes son y que: *“(…) se deberá socializar la política a los contratistas y dar una directriz para que los contratos que suscriban la entidad deben tener los requisitos de la ley de protección de datos. Contactar con las unidades organizacionales para socializar la política de protección de datos personales (…).”* (sic)

Acorde a lo expuesto, tampoco se ha definido un mecanismo para exigir a los contratistas el cumplimiento de la política para el tratamiento de datos personales implementada en el Instituto Nacional de Medicina Legal y Ciencias Forenses, ni para la entrega de las Bases de Datos que, eventualmente, creen para registrar datos personales de los usuarios de la entidad, una vez cesen las obligaciones contractuales con la misma; circunstancia de hecho que permite advertir que se mantiene el incumplimiento de la disposición legal aquí abordada.

5.4.4 Evidencia documental aportada.

Al no ejecutarse correcciones o acciones correctivas, el responsable del proceso no aporta ninguna evidencia.

5.5. Hallazgo informado N°5.

“(…) Sobre el particular, la coordinación del Grupo Nacional de Tecnologías de la Información y Desarrollo indica que ninguna de las unidades organizacionales a que refiere el presente artículo ha reportado las Bases de Datos creadas y usadas en las mismas y que contengan datos personales cuyo tratamiento automatizado o manual se realice por parte de la entidad; lo cual implica que se viene incumpliendo el deber que contempla la norma. (…)”

5.5.1. Criterio específico incumplido

Resolución N°225 del 10 de abril de 2023, artículo 22. Reporte de creación o uso de Bases de Datos.

Dado lo detectado, la oficina de Control Interno indicó en las “CONCLUSIONES” del informe inicial, que:

“(…) En virtud de lo anterior, el Grupo Nacional de Atención y Servicio al Ciudadano, con el apoyo del Grupo Nacional de Tecnologías de la Información y Desarrollo, deberá solicitar a los responsables de cada una de las unidades organizacionales de la entidad el reporte de las Bases de Datos creadas y usadas en ellas, que contengan datos personales cuyo tratamiento automatizado o manual se realice por parte de la entidad.

Con base en la información que se recaude, el Grupo Nacional de Tecnologías de la Información y Desarrollo definirá si lo reportado reúne las condiciones de bases de datos personales y, de ser así, procederá a tramitar ante la Superintendencia de Industria y Comercio su inclusión en el Registro Nacional de Bases de Datos — RNBD.

(…)”

5.5.2. Acción formulada en el plan de mejoramiento.

“(…)

* Solicitar a los responsables de cada una de las unidades organizacionales de la entidad el reporte de las Bases de Datos creadas y usadas en ellas, que contengan datos personales cuyo tratamiento automatizado o manual se realice por parte de la entidad.

* Con base en la información que se recaude, el Grupo Nacional de Tecnologías de la Información y Desarrollo definirá si lo reportado reúne las condiciones de bases de datos personales y, de ser así, procederá a tramitar ante la Superintendencia de Industria y Comercio su inclusión en el Registro Nacional de Bases de Datos — RNBD (…).

5.5.3. Resultado del seguimiento.

Durante la entrevista realizada a la coordinadora del Grupo Nacional de Tecnologías de la Información y Desarrollo informa: “(...) no se han solicitado, se realizará una acción de mejora para solicitar bases de datos a las unidades organizacionales (...)” (sic); agregando que: “(...) sé que certificación y genética han creado bases de datos (...)”.

Con base en lo anterior, se infiere que el GNTID no tiene conocimiento de cuantas bases de datos de este tipo se han creado y manejan en la entidad y, por ende, no tiene información nueva para su inclusión en el Registro Nacional de Bases de Datos — RNBD; razón por la cual, se evidencia que se mantiene el incumplimiento al mandato normativo que nos ocupa.

5.5.4 Evidencia documental aportada.

El responsable del proceso no aportó ninguna evidencia.

6. CONCLUSIONES.

Con fundamento en los resultados del seguimiento a la implementación de la política para el tratamiento de datos personales en el Instituto Nacional de Medicina Legal y Ciencias Forenses, la Oficina de Control Interno evidenció que solo uno de los cinco hallazgos informados recibió tratamiento efectivo por parte del responsable del proceso, lo cual implica que se mantiene un nivel de incumplimiento del 80% frente a los mismos; circunstancia de hecho por la cual, el líder debe replantear el: “**PLAN DE TRABAJO: INFORME SEGUIMIENTO LEY DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES – 2024**”, aportado el 2024/04/11, y, por ende, generar un plan de mejoramiento para subsanar y corregir en fecha cierta las causas que dieron origen a los hallazgos administrativos incluidos en el presente informe.

Téngase que un plan de mejoramiento debe estar integrado por el conjunto de correcciones o acciones correctivas a ejecutar en tiempo real por el responsable de la implementación de disposiciones legales, de un proceso o de un procedimiento auditado, en procura de dar cumplimiento a la obligación de subsanar y corregir las causas que dieron origen a los hallazgos identificados y relacionados en un informe emitido por la Oficina de Control Interno en ejercicio de su función.

Como quiera que estamos en presencia de disposiciones de orden legal su acatamiento es de carácter obligatorio e inmediato, circunstancia de hecho por la cual, el responsable del proceso, dentro de los diez (10) días hábiles siguientes al recibo del presente informe deberá aportar a la Oficina de Control Interno un plan de mejoramiento que contemple las correcciones de fondo o acciones correctivas efectivas para mitigar en fecha cierta las causas que dieron origen a los hallazgos administrativos especificados en el informe de seguimiento.

INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES

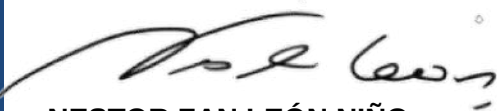
INFORME SEGUIMIENTO LEY DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

Página 10 de 10

La no presentación del plan de mejoramiento dentro del término antes citado y, como consecuencia, la probable reiteración de los hallazgos, dará lugar a que esta Oficina de Control Interno solicite ante las instancias competentes el inicio de las actuaciones disciplinarias a que haya lugar, por presunta inobservancia de lo dispuesto en el numeral 1 del artículo 38¹ de la Ley 1952 de 2019.

Finalmente, es procedente indicar que los hallazgos reportados y planteamientos de la Oficina de Control Interno fueron socializados y tratados con la coordinadora del Grupo Nacional de Atención y Servicio al Ciudadano, responsable del proceso, y con la coordinación del Grupo Nacional de Tecnologías de la Información y Desarrollo, en la reunión de seguimiento celebrada el 2024/05/24; tal como se advierte en el acta suscrita.

Atentamente,


NESTOR FAN LEÓN NIÑO.

Jefe Oficina de Control Interno.

	Nombre, apellido y cargo	Firma	Fecha
Elaboró	Edgar Ramos Saldaña – Profesional Especializada OFCI.		2024/05/29
Revisó/Aprobó	Néstor Fan León Niño - Jefe Oficina de Control Interno.		2024-05-29
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las disposiciones legales y reglamentarias vigentes, razón por la cual se presenta para revisión y eventual firma.			

¹ **Artículo 38. Deberes.** Son deberes de todo servidor público:

1. Cumplir y hacer que se cumplan los deberes contenidos en la Constitución, los tratados de derechos humanos y derecho internacional humanitario, los demás ratificados por el Congreso, las leyes, los decretos, las ordenanzas, los acuerdos distritales y municipales, los estatutos de la entidad, los reglamentos y los manuales de funciones, las decisiones judiciales y disciplinarias, las convenciones colectivas, los contratos de trabajo y las órdenes superiores emitidas por funcionario competente.