Superintendencia de Industria y Comercio

Bogotá D.C., 20 de septiembre de 2024

Magistrada,
**DIANA ALEXANDRA REMOLINA BOTIA**
Presidente
Consejo Superior de la Judicatura
regnal@cendoj.ramajudicial.gov.co

Asunto: Radicación: 24-191514
Trámite: 384
Evento: 330
Actuación:530
Folios: 6

Respetada Magistrada:

La Delegatura de Protección de Datos Personales, Autoridad Nacional de Protección de Datos Personales, agradece los esfuerzos que se han venido desarrollando en el Consejo Superior de la Judicatura para garantizar el debido Tratamiento de los datos personales, de acuerdo con lo establecido en la Ley 1581 de 2012. En particular por su apoyo, colaboración y disposición con ocasión a la visita administrativa realizada los días 16 y 17 de mayo de 2024, a las dependencias del Consejo Superior de la Judicatura relacionada con el incidente de seguridad presentado en el servidor del proveedor de servicios de telecomunicaciones IFX NETWORKS el 12 de septiembre de 2023.

Las entidades estatales que conforman las ramas del poder público recolectan, usan, circulan y tratan Datos Personales. Como tales, son Responsables de su Tratamiento y deben cumplir con todos los deberes constitucionales y legales.

Es factible que para ciertas actividades acudan a terceros (contratistas, empresas de seguridad, proveedores de tecnologías, otras entidades públicas, etc.) que actúan como Encargados del Tratamiento.

Conforme con el artículo 15 superior y la jurisprudencia de la Corte Constitucional, las personas tienen el derecho a conocer, actualizar y rectificar toda la información que se haya recogido sobre ellas en Bases de Datos o archivos de entidades públicas y privadas. Además, señala que *"en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".* Esta disposición fue desarrollada por la Ley Estatutaria 1581 de 2012, y ratificada por la sentencia de la Corte Constitucional C- 748 del 2011.

Dado que las entidades estatales tratan datos personales y sensibles de millones de personas deben obrar conforme a la Constitución y a la ley. Esta Dirección se permite

presentar las siguientes recomendaciones con el fin de que sean tenidas en cuenta por el CSJ para prevenir incidentes de seguridad que puedan comprometer la información de los titulares tratada a través de sus plataformas.

| | |
|---|---|
| **Articulación de dependencias** | A partir de la creación de la Unidad de Transformación Digital e Informática como respuesta al incidente de seguridad presentado, se recomienda articular las actividades con otros miembros que tengan a cargo actividades tecnológicas, esto con el fin de mejorar los procesos y garantizar la seguridad de la información. |
| **Implementación de sistemas de gestión tecnológica** | Continuar con la implementación de las mejoras planificadas para optimizar la gestión y seguridad de la información. Dicha implementación deberá extenderse a las zonas del país donde aún se utilicen tecnologías que no se adapten o se encuentren obsoletas, ya que éstas pueden representar un riesgo para la seguridad de la información que manejan, e incluso para la seguridad de la infraestructura digital de la rama judicial a los procesos de integración entre ellas. |
| **Evaluaciones y Auditorías a terceros** | A través de la dependencia competente para ello, es necesario realizar las evaluaciones y auditorías a los proveedores de servicios enfocándose en los análisis de riesgos asociados con la tercerización de los servicios y con aquellos a los que puede estar expuesta la información allí almacenada. |
| **Identificación de malas prácticas** | A medida que se realice la implementación de las mejoras en la infraestructura tecnológica de la entidad, es necesario identificar si existen malas prácticas en la gestión de los recursos tecnológicos y la información de la entidad. Esto permitirá mejorar los procesos de gestión y aseguramiento de la información, así como la calidad de los servicios prestados. |
| **Revisión y evaluación periódica** | Revisar periódicamente los planes de contingencia establecidos para dar continuidad al servicio que presta la entidad en caso de que se presente una brecha de seguridad, así mismo, realizar pruebas de esos planes para garantizar su eficacia y asegurar un funcionamiento normal. |
| **Gestión de almacenamiento de las grabaciones de audiencias** | En la medida que las grabaciones de las audiencias realizadas en los diferentes despachos judiciales fueron las más afectadas con el incidente de seguridad, es indispensable que se modifique el proceso de gestión almacenamiento de las grabaciones que se realicen, esto con el fin de garantizar su seguridad, disponibilidad y optimizar el uso del espacio con el tiempo. |
| **Descentralización de información** | Explorar métodos alternativos para la visualización de la información que permitan descentralizar los datos generados por la rama judicial. Esto garantizará que, en caso de una contingencia, no se vea comprometida toda la información generada por la rama judicial. |
| **Centralización de soporte técnico en las seccionales** | Centralizar el soporte técnico proporcionado a las diferentes secciónales de la entidad para así estandarizar los procesos de monitoreo, control, gestión y otras actividades relacionadas con la gestión de las tecnologías de la información. |
| **Gestión de riesgos** | Estandarizar los procesos de revisión y actualización de los procesos relacionados con la gestión de riesgos, en los que se establezcan los tiempos de actualización. Además, se sugiere crear manuales que estandaricen el diseño y registro de las actualizaciones, y centralizar estos documentos o para su difusión y conocimiento en toda la organización. |

Las anteriores recomendaciones o sugerencias tienen su fundamento en los principios: de seguridad, circulación restringida, Responsabilidad Demostrada, y la corresponsabilidad en el Tratamiento desarrollados en la Ley 1581 de 2012.

**PRINCIPIO DE SEGURIDAD**

De conformidad con lo establecido en el literal g) del artículo 4 de la Ley 1581 de 2012, *"la información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"*;

**La redacción del principio de seguridad tiene un criterio eminentemente preventivo**, lo cual obliga a los Responsables o Encargados a adoptar medidas apropiadas y efectivas para **evitar** afectaciones a la seguridad de la información de las personas.

Se entiende que las medidas de seguridad de la información deben ser desplegadas por los Responsables, así:

- Las medidas técnicas se han entendido como aquellas que se adoptan para mitigar los riesgos de disponibilidad, confidencialidad e integridad de los datos y de los sistemas de información como el acceso no autorizado o fraudulento por parte del personal de la sociedad o de terceros a una relación comercial.

  Estos riesgos pueden presentarse cuando hay uso no autorizado de los datos personales de los Titulares, cuando no hay disponibilidad de la información de dichos Titulares o del sistema de información y cuando se afecte la integridad de los datos personales.

  Estas medidas técnicas propenden por mejorar los niveles de confianza de los Titulares a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información de la sociedad.

- Las medidas administrativas se refieren a (i) la estructura jerárquica de la entidad, en el sentido de que haya un líder que apruebe la adopción de dichas medidas de seguridad para el funcionamiento óptimo del organismo y (ii) la implementación de procedimientos y documentación que tienda a demostrar el compromiso de la entidad con la seguridad de la información. Para ello, la sociedad debe asegurar que haya implementado un sistema para garantizar la trazabilidad de la información y el no-repudio de la misma frente a los accesos informáticos.

- Las medidas humanas se refieren a los métodos de capacitación de personal y de formación de personal para asegurar que éste realiza todas las medidas que sean pertinentes para evitar la puesta en riesgo de los datos personales y de la seguridad de la información.

Es oportuno tener en cuenta las siguientes dimensiones del principio de seguridad de la información:

- Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren;

- Confidencialidad: propiedad o característica consistente en que la información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados; y

- Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Por lo anterior, el Responsable del Tratamiento debe garantizar a los titulares que el procedimiento que éste lleva a cabo para tratar sus datos personales desde la fase de recolección hasta la fase de supresión o eliminación total de sus bases de datos, este conforme al Régimen de Protección de Datos Personales.

**PRINCIPIO DE CIRCULACIÓN RESTRINGIDA**

Concordante con lo anterior, el principio de circulación restringida establece que el Tratamiento se sujeta a los límites que se derivan de la naturaleza de los Datos personales, de las disposiciones de la Ley 1581 de 2012 y la Constitución Política. En este sentido, el Tratamiento solo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la ley.
En este orden de ideas, la implementación de medidas útiles para la prevención de riesgos que puedan afectar la seguridad de la información recolectada debe ser considerada como una prioridad para su tratamiento, si bien el Consejo Superior de la Judicatura, realizó todas las acciones necesarias para solucionar la contingencia presentada con el proveedor de los servicios tecnológicos, éstas pueden ser reforzadas y mejoradas para evitar riesgos que en el futuro, puedan comprometer la integridad de la información tratada y almacenada. Y más cuando la base de datos afectada resulta de vital importancia para la seguridad y la justicia de Colombia.

**PRINCIPIO DE RESPONSABILIDA DEMOSTRADA**

Lo anterior adquiere mayor importancia si se tiene en cuenta que, en materia de Tratamiento de Datos personales impera la necesidad de implementar medidas de responsabilidad demostrada o "*accountability'*, el cual exige a los Responsables la

capacidad de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto[1]". Es decir, las entidades publicas deben desplegar su máximo nivel de vigilancia y prevención en la seguridad de sus bases de datos.

**CORRESPONSABILIDAD**

Por último, en el marco de la Responsabilidad demostrada y los criterios establecidos por la Autoridad sobre corresponsabilidad de los Responsables del tratamiento de los datos personales, se **exhorta** a los magistrados del Consejo Superior de la Judicatura: Honorable Diana Alexandra Remolina Botía, Honorable Jorge Enrique Vallejo Jaramillo, Honorable Jorge Luis Trujillo Alfaro, Honorable Aurelio Enrique Rodríguez Guzmán, Honorable Mary Lucero Novoa Moreno a desplegar las medidas útiles, oportunas, eficientes y demostrables para acreditar el total y correcto cumplimiento del régimen constitucional (Art.15 de la Constitución) y estatutario (Ley 1581 de 2012) de protección de datos personales en Colombia; exigible a quienes administran datos personales. En este caso a la máxima autoridad orientadora de la política pública de la justicia en Colombia.

De nuevo agradecemos su colaboración y disposición para superar conjuntamente este incidente de seguridad.

Reciba un cordial saludo,

**CAROLINA GARCIA MOLINA**
**Directora de Investigaciones de Protección de Datos Personales**

Elaboró: Natalia Toro
Revisó: Carolina García
Aprobó: Carolina García

[1] Circular Externa No. 003 del 22 de agosto de 2024.