

Cuando ni la Dirección de Impuestos y Aduanas Nacionales (DIAN) se salva de un incidente de seguridad: ataque cibernético

Por: William Alexander López Sandoval

La *data breach*¹ de la DIAN, cuando la ciberseguridad falla y la entidad debe asumir los costos, razón por la cual cobra relevancia contar con un seguros de protección digital (Seguro de ciber-riesgos)

La semana anterior, es decir, en los primeros días del mes de marzo de los corrientes, en diferentes redes sociales y es particular en diferentes grupos de trabajo de WhatsApp dedicados al estudio de derecho de las nuevas tecnologías, entre ellos sobre la Protección de datos, se corría el chisme entre esos pasillos digitales, de que la DIAN (Dirección de Impuestos y Aduanas Nacionales, en adelante la Entidad), había sufrido una exfiltración² de datos personales de más de 18 millones de contribuyentes, a su vez se decía que en la *Dark web*³ estaban vendiendo dicha base de datos por cerca de 2.000 USD para quien la quiera tener, sumándole un aplicativo para obtener más información.

Antes de continuar en esta primera parte, es menester conceptuar sobre Incidentes de seguridad, ya que el mismo está definido en el literal f) del numeral 2.1., del capítulo segundo, del título V de la Circular Única de esta Superintendencia de industria y Comercio (en adelante la SIC), de la siguiente manera: (...) (ii) Incidentes de seguridad. Se refiere a la violación de los códigos de seguridad o la pérdida, **robo y/o acceso no autorizado de información de una base de datos** administrada por el Responsable del Tratamiento o por su Encargado” (...), la negrilla a propósito para contextualizarlo en el presente escrito.

Ya el día 05 de marzo la Entidad, mediante comunicado de prensa No. 033⁴ dio a conocer que:

...“La Dirección de Impuestos y Aduanas Nacionales (DIAN) y CIEL INGENIERÍA, proveedor externo que administra el sistema de agendamiento de citas, adelantan investigaciones técnicas y forenses con el apoyo de proveedores especializados, para determinar si se produjo una exfiltración de información desde los sistemas de la entidad.”...

Y ya el día 06 de marzo la Entidad, mediante comunicado de prensa No. 034⁵ confirmo lo que por los pasillos digitales ya se conocía, que efectivamente había sufrido una exfiltración de datos personales de contribuyentes, pero en ninguno de los comunicados la entidad señala que datos personales fueron exfiltrados / expuestos, o sea, la misma Responsable y/o Encargada de Tratamiento de Datos personales, que es la Entidad, no informa a los contribuyentes y al público en general, entre ellos titulares de los datos personales, si la brecha de seguridad de datos personales

¹ Entiéndase al traducirlo al español, como brecha de datos, más aún, como la violación de la seguridad que sufren los datos personales.

² Entiéndase como exfiltración de datos, conocida también como extrusión o exportación de datos, es el robo de datos: la transferencia intencionada, no autorizada y encubierta de datos desde un ordenador u otro dispositivo. La exfiltración de datos se puede realizar manualmente o automatizarse utilizando malware. Conforme al concepto que maneja IBM, <https://www.ibm.com/es-es/think/topics/data-exfiltration>

³ Conocida como la red oscura, redes centradas en la privacidad llamadas “darknets” Aunque es conocida por actividades delictivas, como mercados de [datos](#) robados, también tiene usos legítimos. Véase: <https://www.ibm.com/es-es/think/topics/dark-web>

⁴ Véase el mismo <https://www.dian.gov.co/Prensa/Paginas/NG-Comunicado-de-Prensa-033-2026.aspx>

⁵ Véase el mismo <https://www.dian.gov.co/Prensa/Paginas/NG-Comunicado-de-Prensa-034-2026.aspx>

expuestos corresponde a datos públicos, semiprivados, privados conforme a lo preceptuado por la Ley 1266 de 2008 o de categoría especial de datos sensibles conforme lo señala la Ley 1581 de 2012.

Ahora bien, los comunicados de prensa (033 y 034), preliminarmente están orientados bajo el principio de Responsabilidad demostrada “*Accountability*”⁶ y de igual forma bajo las instrucciones de la guía de la SIC, sobre el manejo de incidentes de seguridad⁷.

Costos de una brecha de seguridad de datos personales

De acuerdo con los informes anuales de IBM⁸ el costo promedio de una filtración de datos personales, o mejor conocido como un *Data Breach* le está costando a una empresa o entidad gubernamental alrededor de los 4 ´37 millones de dólares americanos (USD), ya que este promedio lo arrojan las cifras de los últimos 6 años así: para el año 2025, el costo aproximado de un *Data Breach* fue de USD 4 ´44 millones; para el año 2024 de USD 4 ´88 millones; para el año 2023 de USD 4 ´45; para el años 2022 de USD 4 ´35 millones; para el año 2021 fue de USD 4 ´24 y en plena pandemia del Covid-19, en el año 2020 fue de USD 3 ´86 millones. (las anteriores cifras, expresadas en millones de USD americanos) (López W.A 2024 P. 92)⁹

¿Por qué los datos que maneja la Entidad de los contribuyentes son de importancia relevante? La entidad como responsable y/o Encargada de Tratamiento de Datos personales de los contribuyentes, maneja bases de datos de carácter tributario y aduanero de los mismos. Dichos datos pueden ser de carácter público, semiprivados, privados y a su vez sensibles (Ley 1266 de 2008 y Ley 1581 de 2012). Toda vez que estos datos lo conforman un conjunto de datos financieros, económicos y jurídicos de personas naturales (nacionales o extranjeras, residentes en el país)¹⁰ o jurídicas, que se utilizan para fiscalizar y recaudar impuestos. Por lo tanto, en estas bases de datos es frecuente encontrar datos personales tales como:¹¹

- Información Exógena (Reportada por terceros): los cuales son datos enviados por bancos, aseguradoras, empleadores y otras entidades, sobre operaciones realizadas con los contribuyentes.

⁶ Véase la Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability), en: <https://protecdatalatam.com/wp-content/uploads/2022/03/GUIA-DE-RESPONSABILIDAD-DEMOSTRADA.pdf>

⁷ Véase: GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES en: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf
https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf

⁸ Véase <https://www.ibm.com/reports/data-breach>

⁹ López, W. A. (2024). Los daños por el tratamiento indebido de datos personales y su reparación a través del contrato de seguro. Recuperado de: <http://hdl.handle.net/10554/68409>

¹⁰ Véase el Art. 10. Respecto al alcance de la residencia para efectos tributarios. Del Estatuto Tributario: Decreto Ley 624 de 1989

¹¹ Véase: Manual de Protección de Datos Personales Proceso Información, Innovación y Tecnología Subproceso Seguridad de la Información (DIAN); Versión 03 Código MN-IIT-0062 Año 2024
<https://www.dian.gov.co/atencionciudadano/LMDP/Informacion-Innovacion-y-Tecnologia/Seguridad-de-la-Informacion/Manuales/MN-IIT-0062.pdf>

- Declaraciones Tributarias: documentos donde el contribuyente reporta sus ingresos, egresos, costos, deducciones, patrimonio Y es donde paga sus impuestos (Renta, IVA, Retención en la fuente, retenciones, Impuesto al patrimonio, a la riqueza, etc)¹².
- Registro Único Tributario (RUT): El cual identifica, ubica y clasifica a los contribuyentes, sujetos de obligaciones tributarias.
- Datos de otras entidades: La Entidad también puede obtener información de otras entidades le permiten complementar y cruzar los datos de los contribuyentes y así realizar seguimientos para determinar el cumplimiento de las obligaciones con la entidad y/o identificar posibles conductas que requieran revisión y seguimiento.

Por lo anterior, la información que maneja la Entidad de los contribuyentes es un caldo de cultivo, entendido como aquel ambiente propicio para los ciberdelincuentes, por lo que el incidente de seguridad que sufrió hace unos días la Entidad no es menor, máxime cuando a raíz de dicha vulneración de datos personales, se pueden desprender una serie de delitos informáticos donde el/los contribuyentes serán los más afectados por esa falla de seguridad. Como lo señala la [GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES](#) en el paso N°. 3, relacionado a “Identificar los daños para las personas, las organizaciones y el público en general”. Aunque la entidad en sus comunicados 033 y 034 reitera que la información de carácter tributario y aduanera no fue expuesta – filtrada.

Para finalizar esta primera parte y no menos importante, surge preguntas como: ¿está obligada la entidad (DIAN) de notificar esta brecha de seguridad a otras entidades de otras jurisdicciones, en el evento que maneje datos personales de personas, por ejemplo, de ciudadanos de la Unión Europea (EU), o solamente a los interesados, afectados? Lo anterior, debido a que en el comunicado de prensa N°. 34 la entidad menciona que “adelantan las acciones correspondientes para reportar el caso a la Superintendencia de Industria y Comercio, como autoridad nacional de protección de datos personales” en Colombia, pero que sucede con los contribuyentes extranjeros que tienen o no, su residencia en Colombia, sino en otra jurisdicción, pero que están obligados a tributar en Colombia, conforme lo preceptuado en el art. 10 del Estatuto Tributario¹³ y dichos datos los almacena y trata la entidad. Lo anterior, debido a que en Colombia el plazo de notificar a la autoridad de protección de datos personales, sobre la brecha de seguridad (Incidentes de seguridad), es de 15 días hábiles:

“deberán reportarse al RNBD por parte de los Responsables del Tratamiento que se encuentran obligados a registrar sus bases de datos en el RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos”

Aunado a lo anterior, la notificación a los titulares de la información, conforme al paso N°. 5 de la Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales, que para los efectos la Entidad generó un comunicado oficial, el N°. 033 y 034, donde brinda a nivel general una recomendación de seguridad, pero surge la pregunta, no es obligatorio un comunicado personal a cada titular de la información afectado, aunque en los dos (2) comunicados la Entidad nunca menciona la cantidad de contribuyentes que se le vulneraron, se filtraron sus datos personales. O

¹²

Véase: <https://www.dian.gov.co/dian/cifras/Paginas/TributosDIAN.aspx#:~:text=Contiene%20la%20informaci%C3%B3n%20estad%C3%ADstica%20producida,nacionales%20en%20cada%20a%C3%B1o%20gravable.>

¹³ Decreto Ley 624 de 1989

es un esfuerzo desproporcionado cuando en realidad la filtración de datos de los contribuyentes es cercano o mayor al millón de personas o como señalan en la *dark web*, que los datos de la brecha de seguridad corresponde a 18 millones de contribuyentes donde fueron expuestos sus datos.

Para la siguiente entrega, llevaré acabo un breve análisis respecto al contrato de seguro de ciber riesgos que tiene contratada la Entidad, a partir de la Póliza de protección digital, que a la fecha del incidente de seguridad la entidad tiene vigente y que, a la luz de los hechos en comento, pudo verse afectada en varias de sus coberturas.