REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO 79549 DE 2022
(11 NOVIEMBRE 2022)

"Por la se inicia una investigación administrativa y se formulan cargos"

Radicación 21-433282

VERSIÓN ÚNICA

EL DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES

En ejercicio de sus facultades legales, en especial las conferidas por el 19 y 21 de la Ley 1581 de 2012, y los numerales 4 y 10 del artículo 17 del Decreto 4886 de 2011, modificado por el artículo 7 del Decreto 092 de 2022, y

CONSIDERANDO

PRIMERO: Que mediante radicado 21- 433282 - -1 del 12 de noviembre de 2022, el laboratorio técnico forense de la Superintendencia de Industria y Comercio ("SIC"), radicó el documento denominado "Acta de preservación de páginas Web – pre investigación, Acta N. 180-21" (el "Acta de Preservación"), en la cual se evaluaron: (i) el portal web (ii) el aplicativo móvil versión Android, y; (iii) el asistente virtual VIANCA ("Vianca") de WhatsApp de propiedad de la sociedad comercial **AEROVÍAS DEL CONTINENTE AMERICANO S.A.** -pudiendo usar las siglas AVIANCA o AVIANCA S.A. (la "Investigada" y/o "AVIANCA"), con el fin de verificar el cumplimiento del Régimen General de Protección de Datos Personales, entre otras actuaciones preliminares.

1.1. Radicado 21- 433282 - -1 del 12 de noviembre de 2022, el laboratorio técnico forense de la Superintendencia de Industria y Comercio ("SIC"), radicó el documento denominado "Acta de preservación de páginas Web – pre investigación, Acta N. 040-22" (el "Acta de Preservación"), de cuyo contenido se destaca los siguientes apartes en relación con el cumplimiento del Régimen General de Protección de Datos:

(a) Con respecto a la página web de Avianca en el portal https://www.avianca.com/co/es/

Frente al proceso de registro en el portal web, en la opción de registro se indica lo siguiente:

> *"El formulario recolecta los datos Email, código de verificación (cuyo propósito y uso se describe en la sección dedicado a la app, por tratarse del mismo procedimiento en la misma página), nombre, apellido e ingresar una contraseña. Adicional contiene un checkbox con la leyenda "¡Deseo recibir ofertas exclusivas y personalizadas por ser MyAvianca! Consultar condiciones" el cual contiene un enlace a la página https://www.avianca.com/co/es/newsletter/aceptacion-comercial/ el cual aloja el documento "Autorización de uso de datos personales para finalidades comerciales" donde se encuentra el texto Política de privacidad el cual permite acceder a la página https://www.avianca.com/co/es/sobre-nosotros/informacion-legal/politica-de-privacidad/ que contiene la Política de Privacidad, como se observa en la imagen 5: [1]*


Autorización de uso de datos personales para finalidades comerciales

Mediante la marcación de la casilla correspondiente declaras ser mayor de edad, además aceptas, autorizas y consientes a AEROVÍAS DEL CONTINENTE AMERICANO S.A. AVIANCA, al igual que las demás aerolíneas integradas bajo Avianca Holdings S. A.(en adelante Avianca) con registro: RNI 1001577-6 NIT. Dirección Postal: Calle 770 #57-103 PISO 21 Edificio Green Towers Barranquilla - Colombia, E-mail: habeasdata@avianca.com; Representante en la UE: Aerovías del Continente Americano S.A. Avianca Sucursal en España, con sede en Madrid (C/ Castello, nº 23 - 4º Izquierda, Pmc. +34 91 758 91 22 e-mail habeasdata@avianca.com), a tratar tu información personal con el fin de remitir vía medios electrónicos, información personalizada sobre productos, servicios, nuevos lanzamientos, descuentos, campañas promocionales de publicidad y/o marketing, información que pueda ser de tu interés e información de productos y servicios de terceros con los que Avianca mantenga una relación comercial.

Los datos personales que suministres serán tratados para el envío de comunicaciones comerciales y/o publicitarias a través de medios electrónicos, incluyendo el envío de información personalizada, de acuerdo con la presente autorización. Por lo tanto, ten en cuenta que este tratamiento de datos conlleva el análisis de tu perfil de usuario y/o de cliente para determinar cuáles son tus intereses y preferencias personales con el fin de ofrecerte los productos y servicios que más se ajusten a ti.

Recuerda que facilitar tus datos personales para esta finalidad es voluntario, si quieres darte de baja y no recibir más comunicaciones vía medios electrónicos, podrás hacerlo mediante el enlace habilitado a tal efecto en cada comunicación que remitimos por medios electrónicos. Las peticiones de baja de comunicaciones comerciales se procesan en un plazo de 10 días hábiles desde que recibimos la petición, con lo cual es posible que recibas alguna comunicación comercial entre el momento de la solicitud y la baja efectiva. Así mismo, puedes comunicarte con el/la responsable habeasdata@avianca.com para ejercitar tus solicitudes. Ten en cuenta que podrás retirar tu consentimiento en cualquier momento, pero esta acción no podrá afectar el cumplimiento de las obligaciones legales a cargo de Avianca. Para mayor información sobre el tratamiento de tus datos, puedes consultar nuestra Política de Privacidad

Tienes derecho a obtener confirmación sobre si estamos o no tratando tus datos personales, a acceder a tus datos personales, a solicitar la rectificación de los datos inexactos, o la portabilidad de tus datos en los casos previstos en las normativas aplicables. Para el ejercicio de tus derechos, deberás dirigir una solicitud, adjuntando un documento que acredite tu identidad, donde la descripción de la solicitud de forma clara y especificar el medio de contacto para recibir respuestas.

[1] Radicado 21-433383 - - 1 del 12 de noviembre de 2021, p. 8.

En la parte inferior de la página se encuentra el acceso a los Términos y condiciones, Política de privacidad, Política de cookies, mapa del sitio y Contrato de transporte, las cuales se anexan a la presente acta. [2]

De conformidad con el anexo del Acta de Preservación, estos son los mecanismos por el medio del cual, AVIANCA, adquiere obtiene a autorización previa, expresa e informada de los titulares, destacándose los siguientes[3]:

3.3 ¿CÓMO ACEPTAS ESTA POLÍTICA DE PRIVACIDAD?

Con la aceptación de la presente Política de Privacidad y en los términos de ésta, entregas tu consentimiento libre, expreso e informado a las Compañías para realizar el Tratamiento parcial y/o total de tus datos personales y/o de los datos personales de otros Titulares que te han habilitado para ello, con ocasión de la prestación y ejecución del (los) servicio(s) contratado(s) y para las finalidades establecidas en el presente documento. La aceptación se da especialmente cuando:

- Marcas, señalas y/o diligencias la casilla de verificación y/o el checkbox de aceptación y consentimiento de las Políticas de Privacidad de las Compañías, que se encuentran habilitados en los flujos de reserva, flujos de compra y/o en nuestros sitios web y/o aplicaciones móviles.
- Adquieres alguno de nuestros servicios a través de alguno de los puntos de venta y/o de aten cliente en canales no presenciales como los centros de atención telefónica y/o de contact cen

://www.avianca.com/co/es/sobre-nosotros/informacion-legal/politica-de-privacidad/ 5/

21 9:57 Política de privacidad y protección de datos |Avianca Colombia

- Como potencial Cliente, Viajero y Usuario, cuando buscas o cotizas tus vuelos, productos y/o servicios en nuestros sitios web, aplicaciones móviles y/o contact center y atención telefónica.
- Te registras, completas, participas y/o haces parte de los concursos, promociones y/o convenios que las Compañías tienen para ti (para estos casos, además de aceptar la Política de Privacidad aplicable, puede que tengas que aceptar también los términos y condiciones de la actividad). Diligencias y/o firmas los formatos de autorización definidos por las Compañías en los puntos de atención y de venta físicos, con el fin de recolectar el consentimiento del Titular para el uso de los datos personales, debido a los servicios contratados.
- Firmas y/o compartes con las Compañías, las tarjetas de compensación, EMD (Electronic Miscellaneous Document), MPD (Multiple Purpose Document) y/o cualquiera otro documento que los reemplace y/o sustituya para ser redimidos como medios de pago en las Compañías. Así como, cuando compartes documentos de identificación para validar la Titularidad en los escenarios de transferencia, traspaso y/o cesión del medio de pago, con el fin de evitar un escenario de homonimia y/o de duda razonable en relación con la identidad del Titular y de acuerdo con lo establecido en la Política de Compensaciones de las Compañías.
- Diligencias y/o envías los formatos de autorización para acceder a los beneficios que las Compañías han diseñado para ti (Élite match, Maternidad Élite, Acompañante Consierge y/o cualquiera que los reemplace y/o los complemente).
- Ingresas y/o haces uso de alguna de nuestras instalaciones y/o edificios administrativos o de nuestras salas VIP de propiedad de las Compañías, en las que se cuente con sistemas de video vigilancia o monitoreo CCTV, con el fin de mantener la seguridad de las instalaciones, de nuestros colaboradores y de nuestros Clientes.
- Cuando haces clic y/o respondes a nuestras comunicaciones vía e-mail, e-cards y/o mensajes push-up.
- Cuando envías información personal necesaria para atender tus consultas y/o reclamos, por cualquiera de los canales habilitados y/o cuando haces uso de los canales y formularios de autogestión que las Compañías han desarrollado para ti.
- Cuando utilizas el LiveChat, la asistente virtual Vianca y/o el WhatsApp para la gestión de tus vuelos, atención preferencial, soporte en la gestión de tus vuelos Avianca, asistencia de irregularidades en tus vuelos o equipajes, conocer información de la programación de tus vuelos, información del estado de tus reembolsos y/o para resolver tus dudas.
- Cuando utilizas nuestros sitios web y/o canales digitales y pulsas la función "Continuar" o aceptas en configuración de preferencias el uso de cookies con el fin de seguir navegando y accediendo a nuestro contenido (te recordamos que existen cookies de funcionamiento esenciales que no puedes bloquear).
- Cuando te inscribes y aceptas recibir los boletines informativos "newsletter" que las Compañías tienen para ti.
- Cuando suministras y/o envías a las Compañías documentos tales como: excusas médicas, aptitudes de vuelo, contraindicaciones médicas o instrucciones para el uso dispositivos médicos especializados, autorizas a las Compañías el Tratamiento de la información personal general y sensible contenida en dichos documentos.
- Cuando te auténticas para acceder a My Avianca o a cualquiera de nuestros servicios tecnológicos por medio de: a) tu usuario de redes sociales y/o de correo electrónico, estas aceptando la Política de Privacidad de las Compañías y las Políticas de Privacidad de dichos terceros, por lo tanto, debes consultarlas dirigiéndote a sus propios sitios web con el fin de saber cómo van a ser tratados tus datos personales. b) tu número de viajero frecuente LifeMiles, estas aceptando también la Política de Privacidad de LifeMiles Ltd. disponible para su consulta en www.lifemiles.com c) Las Compañías podrán tratar y/o recolectar tu información personal debido a la interacción que tengas con My Avianca o con cualquiera de los otros servicios tecnológicos; de acuerdo con las finalidades establecidas en la presente Política de Privacidad y las condiciones de uso de nuestros canale

[2] Radicado 21-433383 - - 1 del 12 de noviembre de 2021, p. 11
[3] Radicado 21-433383 - - 1 del 12 de noviembre de 2021, p. 47 – 48.

De conformidad con el anexo del Acta de Preservación, estos son las finalidades que AVIANCA dispuso para el tratamiento de datos personales, adquiere la autorización previa, expresa e informada de los titulares, destacándose los siguientes bajo el lenguaje confuso de "principalmente", dejando entender que pueden existir otros adicionales que no son publicitados[4]:

Las Compañías Tratan tus datos personales principalmente para:

- Ejecutar, procesar, confirmar, cumplir y proveer los servicios de transporte aéreo (doméstico y/o internacional) bajo la ejecución del contrato de transporte.
- Gestionar y administrar todos aquellos aspectos relacionados con tu viaje y/o el servicio contratado (check-in, proceso de embarque, trámites de lista de espera, manejo de equipaje, rutas y/o vuelos en conexión, cambios voluntarios e involuntarios de boletos4 , excepciones pago de penalidades, reembolsos, pago de compensaciones e indemnizaciones, multas menús a la carta, compras previas al vuelo, revistas electrónicas, solicitud y compra de ancillaries o servicios especiales) y todos aquellos servicios complementarios que sean ofrecidos por las Compañías.
- Gestionar las tarjetas de compensación, EMD (Electronic Miscellaneous Document), MPD (Multiple Purpose Document) o cualquiera que los reemplace y/o sustituya y que pueden ser utilizados y/o redimidos como medios de pago en las Compañías. Así como, para validar la Titularidad de los documentos de pago en los escenarios de transferencia, traspaso y/o cesión con el fin de evitar un escenario de homonimia y/o de duda razonable en relación con la identidad del Titular y de acuerdo con lo establecido en la Política de Compensaciones de las Compañías.
- Gestionar y administrar los registros contables de las Compañías y la correspondencia.
- Prevenir, investigar y enjuiciar delitos penales ej.: el fraude, suplantación de identidad, verificación de Titularidad de los medios de pago débito y/o crédito, phishing en línea, robo y uso de medios fraudulentos de pago para obtener condiciones y/o tarifas especiales y/o de los demás instrumentos utilizados por los Clientes, Viajeros y Usuarios para adquirir condiciones especiales en los servicios y productos ofrecidos por las Compañía.
- Contactarnos contigo por medio de los canales que has registrado en tu proceso de reserva para el envío y comunicación de los cambios operaciones y/o actualizaciones de estado de tu viaje, el envío de la tarjeta de embarque, la confirmación de hora y puerta de embarque, actualización de contingencias repentinas e imprevistas y/o de emergencia, así como, las demás comunicaciones operacionales asociadas al servicio contratado, con independencia del canal a través del cual hayas contratado y/o adquirido el servicio y por el medio más expedito posible.

- Compartir, en cumplimiento de nuestras obligaciones legales, tu información personal incluyendo tus datos biométricos, a las autoridades de control y vigilancia5 administrativas, de migración, de policía, judiciales, aduaneras y/o aeronáuticas nacionales e internacionales, así como a las demás entidades gubernamentales que regulan nuestra actividad, para la detección, prevención, aprehensión o persecución del fraude, tráfico ilegal de personas, estupefacientes, fauna y flora, mercancías peligrosas, armas, control fronterizo, aprehensión o persecución del terrorismo, lavado de activos, narcotráfico o demás prácticas Gestionar y administrar los trámites legales en virtud de un requerimiento oficial o reglamentario por parte de las autoridades de control y vigilancia en defensa de la seguridad, los derechos y/o de la propiedad de los Titulares y de las Compañías, de sus canales digitales y/o de sus instalaciones. corruptas o cuando las Compañías de buena fe, consideren que la entrega de la información personal contribuye a la seguridad aérea y de la Organización.
- Gestionar y administrar los trámites legales en virtud de un requerimiento oficial o reglamentario por parte de las autoridades de control y vigilancia en defensa de la seguridad, los derechos y/o de la propiedad de los Titulares y de las Compañías, de sus canales digitales y/o de sus instalaciones.
- Gestionar y administrar, cuando así lo consientas, el envío de boletines y noticias, por medio de correo electrónico, mensajes de texto, web, entre otro tipo de publicidad con información publicitaria y/o comercial acerca de los productos y/o servicios que las Compañías y/o que las empresas y/o terceros asociados tienen para ti. Las Compañías podrán personalizar tu experie con base a tu perfil como Viajero, Cliente y Usuario, dicha acción depende de la región y país que se traten los datos personales y de las obligaciones aplicables para el envío de comunicac

- Si bien las Compañías hacemos todo lo posible por tramitar tus peticiones de baja para comunicaciones comerciales en un plazo de diez (10) días hábiles desde que recibimos la petición, es posible que durante el periodo en el que se surte este proceso de opt-out recibas alguna comunicación comercial. Para más información puedes dirigirte al acápite ¿CÓMO PUEDES EJERCER TUS DERECHOS? de la presente Política6
- Gestionar y atender las quejas, consultas, reclamos, solicitudes y/o sugerencias que realices a las Compañías frente al uso y/o tratamiento de tus datos personales, por medio del canal oficial establecido para ello: habeasdata@avianca.com.
- Gestionar y administrar el canal WhatsApp/Vianca o LiveChat habilitado para dar atención preferencial a nuestros clientes.
- • Gestionar y administrar tu información personal cuando viajas bajo necesidades especiales y/o requieres de asistencia especial a bordo condición de embarazo, enfermedad y/o cirugía reciente, así como cuando viajas con dispositivos médicos especiales u otras condiciones médicas.
- Podemos consultar y actualizar tu información personal, para la ejecución de actividades operacionales, analíticas, estadísticas y de evaluación, de acuerdo con tu nivel de interacción y de satisfacción con la calidad de los servicios ofrecidos de acuerdo con tus preferencias de vuelo y/o necesidades por medio de mensajes pop-up y/o encuestas de satisfacción.
- Podemos compartir tu información personal cuando la prestación del servicio lo requiera y/o lo incluya con representantes comerciales, agencias de viajes, operadores turísticos, compañías de alquiler de vehículos, aseguradoras, proveedores de servicios tecnológicos, sistemas globales de distribución (en adelante, "GDS" por sus siglas en inglés), programas de lealtad, proveedores de infraestructura tecnológica, entre otros, que sean necesarios para la prestación del servicio y para la prestación de este.
- Permitir el acceso a tu información personal a los auditores y/o terceros contratados por las Compañías para llevar a cabo los procesos de auditoría interna y/o externa reglamentados y/o propios de la actividad comercial desarrollada por las Compañías. Solo cuando sea necesario y debido al servicio contratado, podremos compartir tu información personal con las entidades financieras, para procesar pagos, cobros, compensaciones, indemnizaciones y/o reembolsos.
- Permitir el acceso tu información personal a las aseguradoras y/o consultores externos contratados por las Compañías para la ejecución de los servicios prestados.
- Gestionar el almacenamiento y/o procesamiento de tu información personal bajo los estándares de seguridad, confidencialidad, integridad y disponibilidad propios de la industria y en cumplimiento de las regulaciones, estándares y buenas prácticas que nos permita garantizar un nivel adecuado de seguridad de la información, te informamos que podremos contratar terceros externos para los servicios tecnológicos de procesamiento y/o almacenamiento.
- Gestionar la información personal que suministras cuando haces uso de los canales no presenciales (centro de atención telefónica y/o contact center, Apps, chats) te informamos que basándonos en nuestro interés legítimo empresarial podremos grabar y monitorear las llamadas e interacciones en estos canales, con el fin medir la calidad del servicio y ejecutar la trazabilidad y monitoreo de tus solicitudes.
- Transmitir y/o transferir tus datos personales a las Compañías que hacen parte de Avianca Holdings S.A y otros proveedores con ocasión de la prestación del servicio contratado y en cumplimiento de nuestro interés legítimo empresarial. Te informamos que algunas de las Compañías pueden estar establecidas en países y/o territorios distintos al país en el que fueron recolectados inicialmente, por lo tanto, velaremos por dar cumplimiento a los estándares de seguridad y confidencialidad establecidos en este documento.
- Gestionar la cesión de la información personal en caso de cambio de control de una o más Compañías, alguna de las unidades de negocio y/o agentes liquidadores que hacen parte de Avianca Holdings S.A., por fusión, adquisición, quiebra, liquidación, escisión y/o creación, a nueva Compañía y/o entidad. Si como consecuencia del cambio de control, hay cambio en el Responsable del Tratamiento, te informaremos dicha situación con el fin que puedas ejercer t

[4] Radicado 21-433383 - - 1 del 12 de noviembre de 2021, p. 47 – 48.

- Gestionar, administrar y redimir los beneficios establecidos por las Compañías (Elite match, Maternidad Elite, Acompañante Consierge o cualquiera que los reemplace y/o sustituya). Te informaos que, si eres socio del programa de lealtad operado por LifeMiles Ltd., las Compañías podrán compartir tu información personal con LifeMiles, con el fin de gestionar los beneficios de fidelización a los que tengas derecho (acumulación y/o redención de millas). Para más información del programa LifeMiles, puedes dirigirte a la web oficial: www. lifemiles.com.
- Gestionar y administrar los datos personales de los pasajeros elegibles recolectados por las Compañías para la ejecución del Programa Corporativo "Avianca Corporate" y/o cualquiera que lo reemplace o sustituya de acuerdo con los términos y condiciones del programa.
- Tratar y compartir cuando sea solicitado por la Autoridad competente, los datos personales requeridos (incluyendo datos personales sensibles) para ayudar a controlar, prevenir la introducción, transmisión, mitigación y propagación de enfermedades transmisibles en el caso de epidemias, pandemias, infecciones y/o situaciones de caso fortuito o fuerza mayor u otras intervenciones apropiadas de salud pública, incluida la implementación de restricciones de viaje.
- Gestionar los beneficios, la redención y/o acumulación de millas de acuerdo con las condiciones de la tarifa establecidos para el programa de viajero frecuente de las aerolíneas.
- Gestionar los servicios relacionados con tu equipaje, servicios especiales, objetos olvidados, elementos no declarados y asistencia después del viaje.
- Ejecutar estudios de mercado, estadísticas, encuestas de satisfacción y/o fines analíticos con el fin de optimizar nuestros productos y servicios.

4 Te recordamos que, en los procesos de cambio voluntario de itinerario, ruta y/o nombre del tiquete, tienen sus propias condiciones sujetas a las legislaciones aplicables en cada territorio donde operen las Compañías y a la tarifa que fue adquirida.

5 Las Compañías adscritas a Avianca Holdings S.A. debido a su actividad como transportadores, están obligadas a mantener, suministrar y registrar información personal a las Autoridades locales e internacionales y/o entidades oficiales que regulan la actividad aeronáutica, en concordancia con las leyes aplicables acerca de los pasajeros, carga, mensajería expresa y/o courier, que se encuentren a bordo de sus aeronaves (estatus migratorio, información de visado, documentos de viaje, datos generales de identificación, itinerario, relación de mercancías peligrosas, entre otros) antes de la salida y aterrizaje de los vuelos en el territorio de destino.

6 Le informamos que, en algunos casos de acuerdo con la solicitud de retiro o dada de baja, podemos tener derec ho a continuar proceso sus datos personales bajo finalidades legales tales como, la prestación de su contrato de transporte o para las excepciones legales y/o regulatorias establecidas.

Como usuario de Avianca Services para recibir la prestación del servicio de entrenamientos especializados, capacitaciones y cursos tales como, pero no limitados a: curso de mercancías peligrosas, curso de carga básica y curso de baterías de litios y radiactivos y/o para gestionar los procesos de convalidación y certificaciones de estudios de acuerdo con, lo requerido por la regulación aplicable a los procesos de educación y certificación

Para Deprisa: Administrar la ejecución de los servicios de carga, casillero virtual, paquetería y/o mensajería (premium, estándar y especializada) a nivel nacional e internacional. Para Avianca Cargo: Gestionar los requerimientos para el servicio de transporte de carga aérea de aeropuerto a aeropuerto (como el transporte de animales vivos, carga peligrosa, restos humanos, productos perecederos, medicamentos, entre otros) y para los cuales se recolecte información personal del remitente y/o destinatario de la carga.

Finalmente queremos comunicarle que Las Compañías no venden y/o transan con tu información personal.

(b) Con respecto al acceso al asistente virtual "Vianca" a través de WhatsApp con el número 311-4-00-6797, el Acta de preservación indicó que este asistente permite conocer: (i) tarifas; (ii) realizar compras, cancelaciones, cambios de vuelo, y; (ii) gestionar reservas e información de equipajes:

El acta describe como es el proceso por medio del cual Vianca pone de manifiesto el Aviso de Privacidad ("AP") y la Política de Tratamiento de Información ("PTI")

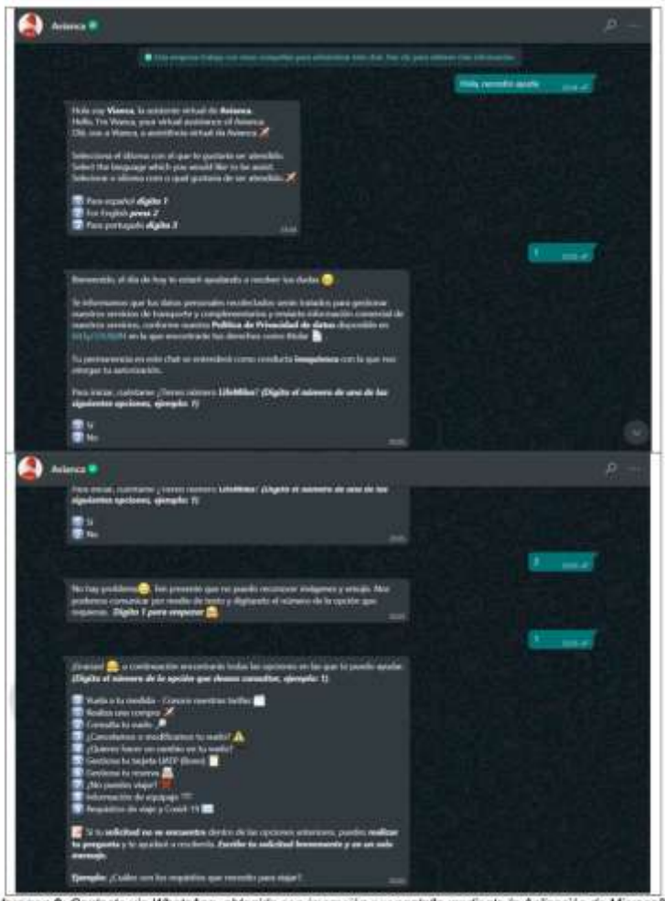


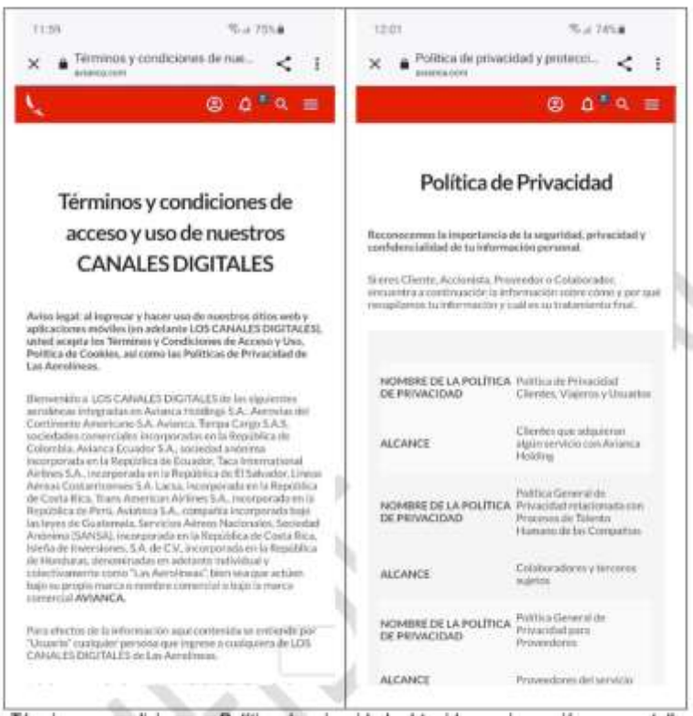
***Imagen 9:** Contacto vía WhatsApp, obtenida con impresión por pantalla mediante la Aplicación de Microsoft*

(c) Con respecto al aplicativo Móvil del Avianca en su versión de Android: *"Se consulta la sección "Acerca de esta app" donde se informa "Comprar boletos, haz check in y conoce el estado de tu vuelo". En la sección "Información de la app" se encuentra que la versión de la aplicación es 7.0.15, la fecha de lanzamiento fue el 26 de diciembre de 2012, y desarrollada por Avianca (. . .)"*[5]

"Finalizada la instalación de la aplicación, se solicita iniciar sesión o crear una cuenta en "MyAvianca" que al ser seleccionada redirige a la página de registro para seleccionar uno de los métodos de inicio se sesión (descritos en la página 7 del presente documento), en caso de seleccionar la opción "Ingresar como invitado"
En la parte inferior de la página se observa la leyenda "Al registrarte confirmas que aceptas nuestros Términos y condiciones y nuestra Política de privacidad" los términos subrayados contienen enlaces a los documentos que indican, los cuales corresponden a los mismos que se acceden desde el sitio web, (. . .)"

[5] Radicado 21-433383 - - 1 del 12 de noviembre de 2021, p. 12.

***Imagen 14:** Ingreso a la aplicación Avianca, obtenida con impresión por pantalla mediante la Aplicación de Microsoft Windows Recortes.*

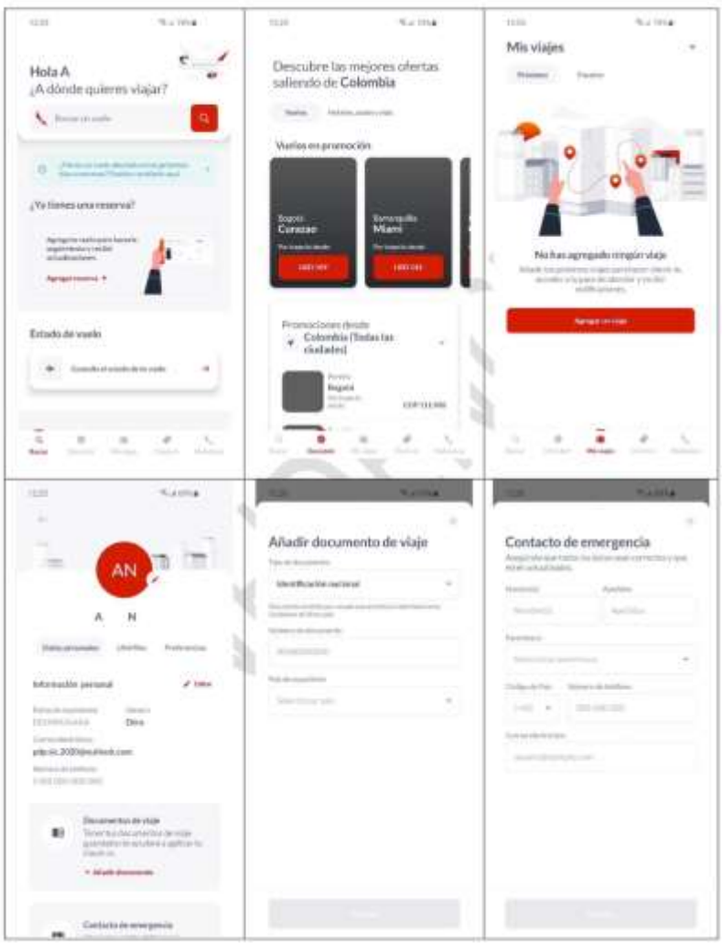


"Finalizado el registro en la app, se muestra la página de búsqueda de vuelos y en la parte inferior de la misma se observan las opciones:

(a) Buscar: que permite la búsqueda de vuelos.
(b) Descubrir: presenta ofertas de vuelos y hoteles.
(c) Mis viajes: permite al usuario registrar próximos vuelos, hacer check in, obtener pases de abordar y recibir notificaciones.
(d) Check in: permite hacer check in de un vuelo.
(e) MyAvianca: permite ver y modificar el perfil de usuario, agregar documentos de viaje

como documento de identificación y pasaporte (solicita número y tipo de documento) adicionalmente solicita información de contactos de emergencia como: nombre, apellido, número de teléfono y correo electrónico.
En caso de acceder por: "ingresar como invitado" se mostrarán únicamente las opciones a, b, c y d."[6]

[6] Radicado 21-433383 - - 1 del 12 de noviembre de 2021, p. 13 - 17



- En relación con el aplicativo, el Acta de Preservación en la sección denominada "Análisis de privacidad Android", indicó lo siguiente:

"Se realiza el análisis de privacidad para la APP Avianca, encontrando quince (15) permisos potencialmente peligrosos por las acciones que la aplicación puede hacer en el Sistema Operativo (para este caso: Android) del teléfono celular donde se instala. Los niveles de gravedad se definen de acuerdo con los niveles de protección de Google (. . .)

Adicional, se encontraron cuatro (4) rastreadores cuya función es recolectar información del usuario o de sus hábitos de navegación, en la imagen se aprecian los mencionados rastreadores:

(d) En n la sección de Observaciones, se destacan las siguientes:

A. "Al ingresar al sitio web Aerovías del Continente Americano S.A. Avianca - https://www.avianca.com se redirige automáticamente a la URL https://www.avianca.com/co/es/, para efectos de la presente preservación se tuvo en cuenta esta última.

B. La URL que contiene el formulario de registro en MyAvianca puede ser accedido desde el sitio web y desde la app, recolecta los datos correo electrónico, nombre y apellido una vez registrado se permite completar la información personal ingresando los datos: fecha de nacimiento, genero, código de país, teléfono de contacto. Adicional solicita los siguientes datos del contacto de emergencia: nombres, apellidos, correo electrónico, código de país y teléfono de contacto, el mencionado formulario no cuenta con un mecanismo de aceptación de tratamiento de datos personales o un acceso a la "Políticas de privacidad". Lo anterior se puede apreciar en las imágenes 16, 17 y 18 de las páginas 16, 17 y 20 respectivamente.

C. De acuerdo con los resultados generados por la herramienta EXODUS la APP Avianca, contiene cuatro (4) rastreadores cuya función es recolectar información del usuario o de sus hábitos de navegación, respecto a este software de rastreo la aplicación no informa al usuario previo a la instalación, en la Imagen 29, página 27 se puede observar el detalle de estos.

D. De acuerdo a la verificación de permisos mediante el uso de la herramienta EXODUS se evidencian 15 permisos (Los permisos son acciones que la aplicación puede hacer en el teléfono) los cuales difieren de los informados al momento de instalar la app, dentro de los permisos solicitados y no informados se encuentran: permiso para realizar llamadas (CALL_PHONE); permiso para leer el estado del teléfono (READ_PHONE_STATE) permite a la aplicación saber el número de teléfono, la información actual de la red móvil, el estado de las llamadas en curso entre otros. Lo descriptor se puede Ver en la Imagen 28, paginal 27.

E. Complementando lo señalado en el documento adjutno a la solicitud, referente a la Política de Privacidad, durante la etapa de registro en MyAvianca, se evidenció que tanto el sitio web como la app dirigen a un formulario (los dos ambientes acceden a la misma URL) de registro el cual no contiene un mecanismo de aceptación diferente al registro por sí mismo mediante el aviso "Al registrarte confirmas que aceptas nuestros Términos y condiciones y nuestra Política de privacidad.", como se observa en la Imagen 3, página 6 y en la Imagen 14, página 14."[7]

1.2. Radicado 21 – 433282 - - 2 del 22 de marzo de 2022, por medio del cual el Despacho realizó el siguiente requerimiento de información a Avianca:

"

(1) Indique el mecanimos fjado por parte de AEROVIAS DEL CONTINENTE AMERICANO S.A. ("AVIANCA") para que los titulares conozcan y acepten la Política de Tratamiento de la informción ("PTI") aplicable tanto para el Portal como para la APP. De igual forma, indique si existe un Aviso de Privacidad aplicable tanto al Portal y/o APP, en los términos establecidos en el D.1377/13 e incorporado en el D.U.R.1074/15-);

(2) Indicar el mecanismo por medio del cual se informa a los titulares de los usuarios del aplicativo móvil Whatsapp ("Vianca") la AP y/o PTI de Avianca destinada para titulares de esta chat de inteligencia artífical. Indicar si el AP o la PTI son las mismas aplicables al Portal y la APP;

[7] Radicado 21-433383 - - 1 del 12 de noviembre de 2021, p. 34.

(3) Indicar que funciones cumplen las siguientes Cookies: (i) Cookie-counter; (ii) Cookie-close; (iii) Avoid -darksite; (iv) Marquesilla-close; (v) Búsqueda 1; (vi) Búsqueda 2; (vii) AVSESSION_ID. De igual forma indique si en su política de Cookies da aviso a los titulares de las funciones de las cookies anteriormente descritas.

(4) Indicar, con respecto a la APP, cuáles son las finalidades de específicas por la cual se requiere los siguientes permisos: (i) Cámara; (ii) Internet; (iv) READ_EXTERNAL_STORAGE; (v) READ_PHONE_STATE; (vi) READ_PHONE_STATE; (vi) REQUEST_INSTALL_PACKAGES; (vii) WAKE_LOCK; (viii) WRITE_EXTERNAL_STORAGE; (ix) C2D_MESSAGE. De igual forma, indicar si los titulares están al tanto del acceso estas funcionalidades, y si estas pueden ser desactividadas facilmente por el titular;

(5) Indicar, con respecto a la APP, las razones por las cuales se utilizan los siguientes 4 rastreadores: (i) Demdex; (ii) Google Firebase Analytics; (iii) Microsoft Visual Studio App Center Analytics, y; (iv) Microsoft Visual Studio App Chrases;

(6) Indicar si el desarrollo del Portal y de la APP fue realizado directamente por AVIANCA, o bien, por un tercero. En caso de ser AVIANCA, indicar el área encargada, así como el organigrama de la misma. En caso de que sea un tercero, indicual cual. Así mismo, remitir el contrato de desarrollo de software celebrado con el desarrollador;

(7) Indicar quién realizó el desarrollo del aplicativo o chat de inteligencia artificial de Whatsapp dipuesto para los titulares. En caso de que el desarrollo haya sido realizado por AVIANCA, indicar el área encargada, así como el organigrama de la misma. En caso de que sea un tercero, indicual cual, así como el contrato de desarrollo de software, o similar, celebrado con el desarrollador;

(8) Indicar si durante el período de diseño, desarrollo y de recolección de datos a través del Portal y la App, se realizó un estudio de impacto de privacidad ("Privacy Impact Assessment" o "PIA", por sus siglas en inglés). En caso afirmativo, remita copia completa de dicho estudio tanto para el portal, APP, y el chat de inteligencia artificial de Whatsapp;

(9) Informe si se desarrollo y puso en ejecución un Sistema de Administración de Riesgos asociados al Tratamiento de Datos Personales que les permita "identificar, medir, controlar y mointorear" todos aquellos situaciónes que puedan incidir en la debida administración del riesgo a que están expuestos los titulares por causa u ocasión del tratamiento de sus datos a través portal, APP, y el chat de inteligencia artificial de Whatsapp. En caso afirmativo, remita copia del documento.

(10) Informe que medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole han implementado para que evitar:

(a) Accesos indebidos o no autorizados a la información;
(b) Manipulación de la información;
(c) Destrucción de la información;
(d) Usos indebidos o no autorización de la información, y;
(e) Circulación o suministro de la información a personas no autorizadas.

(11) Informe si dichas medidas de seguridad son objeto de revisión, evaluación y mejora permanente."

1.3. Radicado 21 – 433282 - - 3 del 20 de marzo de 2022, por medio del cual AVIANCA presentó una solicitud de prórroga para dar contestación al requerimiento de información con radicado 21 – 433282 - - 2 del 22 de marzo de 2022;

1.4. Radicado 21 – 433282 - - 4 del 5 de abril de 2022, por medio del cual el Despacho concedió la prórroga solicitada con radicado 21 – 433282 - - 3 del 20 marzo de 2022;

1.5. Radicado 21 – 433282 - - 5 del 19 de abril de 2022, por medio del cual AVIANCA dio contestación al requerimiento de información con radicado 21 – 433282 - - 2 del 22 de marzo de 2022, acompañado de los siguientes anexos:

(a) Certificado de Existencia y Representación Legal.
(b) **Anexo 1:** Manual para la Protección de Datos Personales.
(c) **Anexo 2:** Manual General de Seguridad de la Información.

(d) **Anexo 3:** Manual de Lineamientos Específicos de Seguridad de la Información.
(e) **Anexo 4:** Controles de seguridad aplicados por Avianca.
(f) **Anexo 5:** Flujo de los procedimientos Avianca.
(g) **Anexo 6:** Contrato de servicios de soporte, mantenimiento y desarrollo de aplicaciones tecnológicas - TCS Solution Center.
(h) **Anexo 7:** Carta de levantamiento de confidencialidad con el desarrollador – contrato Amadeus.
(i) **Anexo 8:** Contrato Cellpoint.
(j) **Anexo 9:** Contrato Media Monks.
(k) **Anexo 10:** Contrato WebHelp.
(l) **Anexo 11:** Certificación ISO 22301.
(m) **Anexo 12:** Certificación ISO 27001.
(n) **Anexo 13:** Manual de Riesgos de la Información.
(o) **Anexo 14:** Procedimiento para ejecución de análisis de vulnerabilidades
(p) **Anexo 15**: Procedimiento de monitoreo y gestión de alertas de seguridad de la información y ciberseguridad.
(q) **Anexo 16:** Procedimiento de inteligencia de amenazas de seguridad de la información y ciberseguridad.
(r) **Anexo 17:** Manual General de Monitoreo de Seguridad y Cumplimiento.

1.6. Radicado 21 – 433282 - - 6 del 29 de abril de 2022, por medio del cual el Despacho realizó el siguiente requerimiento de información a Avianca:

(1) Indicar, de acuerdo con la respuesta a la pregunta 4 al primer requerimiento de información, desde qué versión de la App se utilizó por última vez la funcionalidad de cámara. Remitir copia del código fuente de la versión tanto para iOS como para Android;

(2) Indicar, de acuerdo con la respuesta 5 al primer requerimiento de información, cual era la finalidad del rastreador denominado "DEMDEX", indicado también que ocurrió con los datos recolectados por ese rastreador, y la última versión de la App en la que fue utilizada. Remitir copia del código fuente de la versión tanto para iOS como para Android;

(3) Indicar, de acuerdo con la respuesta 5 al primer requerimiento de información, si el uso de los datos personales de los titulares para fines estadísticos, a traves de Google Analytics o herramientas similares, se encuentra contempladas dentro de las finalidades establecidas en el Política de Tratamiento de Información ("PTI");

(4) Indicar, de de acuerdo con la respuesta 8 al primer requerimiento de información y el contrato de desarrollo de software celebrado entre Avianca S.A. ("Avianca") -sus filiales y subsidiarias- con Getcom Servicios S.A.S. (el "desarrollador del chatbot"), espéficiamente la cláusula décima, sección (A), sub-secciones (14), (17), y el anexo 4 del contrato, lo siguiente:

(i) Los mecanismos utilizados para evitar que los empleados de Avianca como del desarrollador del chatbot tenga acceso a los datos personales de los titulares/clientes de Avianca;

(ii) Ubicación y propiedad de los servidores donde se almacena la información personal o bases de datos de los titulares/clientes de Avianca;

(iii) Procedimiento concreto utilizado por Avianca y el desarrollador del chatbot para cumplir con las obligaciones contenidas en la General Data Protection Regulation ("GDPR") de la Unión Europea. Indicar de igual forma si tiene la obligación de cumplir con dicha normativa.

(5) Indicar, de acuerdo con la respuesta 8 al primer requerimiento de información, si Avianca cuenta con certificaciones propias de cumplimiento del principio de responsabilidad demostrada, o bien, certificaciones de cumplimiento de los requerimientos exigidos por la norma ISO27001 e ISO31000 u otras de igual naturaleza?

(6) Indicar, de acuerdo con la respuesta 8 al primer requerimiento de información, si Avianca cuenta con certificaciones propias de cumplimiento del principio de responsabilidad demostrada, o bien, certificaciones de cumplimiento de los requerimientos exigidos por la ISO27001 e ISO31000 u otras de igual naturaleza, e;

(7) Indicar de forma expresa, de acuerdo con la respuesta 9 al primer requerimiento de información, el software y/o el hardware adquirido por AVIANCA para implementar

su firewall perimetral, virtual patching, identificación de eventos de seguridad, y cyberthreats."

1.7. Radicado 21 – 433282 - - 7 del 11 de mayo de 2022, por medio del cual AVIANCA presentó solicitud de prórroga para darle contestación al radicado 21 – 433282 - - 6 del 29 de abril de 2022.

1.8. Radicado 21 – 433282 - - 8 del 16 de mayo de 2022, por medio del cual el Despacho concede una prórroga a AVIANCA para contestar el radicado 21 – 433282 - - 6 del 29 de abril de 2022.

1.9. Radicado 21 – 433282 - - 98 del 28 de junio de 2022, por medio del cual el Despacho requirió a AVIANCA para que diera contestación al radicado 21 – 433282 - - 6 del 29 de abril de 2022.

1.10. Radicados 21 – 433282 - -11 - 12 del 7 de julio de 2022, por medio del cual AVIANCA da respuesta a la información solicitada por parte del Despacho e indicando que la información se remitió mediante correo electrónico a: contactenos@sic.gov.co.

1.11. Radicado 21- 433282 - - 13 del 13 de septiembre de 2022, por medio del cual el Despacho analizó la información relacionada con el supuesto correo enviado por parte del AVIANCA, manifestando que el correo no se encuentra radicado para el expediente dentro de sistema de trámites de la Entidad.

1.12. Radicado 21 – 433282 - - 15 del 15 de septiembre de 2022, por medio del cual AVIANCA dio respuesta al radicado 21 – 433282 - - 6 del 29 de abril de 2022, acompañado de los siguientes documentos y anexos:

(a) Certificado de existencia y representación de Avianca;
(b) Copia del supuesto correo del 27 de mayo de 2022;
(c) Respuesta al oficio el 13 de septiembre de 2022;
(d) Respuesta al oficio del 29 de abril de 2022;
- Anexo 1: Extracto código fuente de la aplicación para IOS.
- Anexo 2: Extracto código fuente de la aplicación para Android.
- Anexo 3: APK de la aplicación para la versión Android.

Con respecto a los anexos a que se hace mención en 1.12.(d), el Despacho certifica que los anexos 1 – 3, no fueron enviados por parte de AVIANCA dentro del radicado con consecutivo 15.

1.13. Radicado 21 – 433282 - - 16 del 27 de septiembre de 2022, por medio del cual el Despacho solicitó a AVIANCA propusiera un mecanismo para remitir los APK solicitados por el Despacho, dando acceso a los correos de los funcionarios a cargo de la Investigación.

1.14. Radicado 21 – 433282 - - 17 del del 29 de septiembre de 2022, por medio del cual AVIANCA informó el mecanismo de acceso a los APK solicitados, y se les dio acceso a los correos de los funcionarios a cargo de la investigación.

SEGUNDO: Que, de la información recaudada en desarrollo de la etapa de averiguación preliminar y del análisis de esta, esta Dirección encontró que, presuntamente, **AEROVÍAS DEL CONTINENTE AMERICANO S.A.** -pudiendo usar las siglas AVIANCA o AVIANCA S.A., habría ejecutado conductas presuntamente violatorias de las normas sobre protección de datos personales, en su condición de Responsables[8] del Tratamiento de datos personales en los términos establecidos por la Ley Estatutaria 1581 de 2012.

TERCERO: FUNCIONAMIENTO DE LOS *TRACKERS* Y COMO A TRAVÉS DE ESTOS SE PUEDE RECOLECTAR INFORMACIÓN PERSONAL Y SOBRE LA PRIVACIDAD DESDE EL EL DISEÑO Y POR DEFECTO (Privacy by Design by Default) Y ACCESO A LOS PERMISOS DEL DISPOSITIVO MÓVIL.

[8] L.1581/12, art. 4(e): Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos

3.1. FUNCIONAMIENTO DE LOS TRACKERS Y COMO A TRAVÉS DE ESTOS SE PUEDE RECOLECTAR INFORMACIÓN PERSONAL

Los *trackers* dentro del entorno de los aplicativos móviles, tal como ocurren con las *cookies* en el entorno web, cumplen la función de rastrear el comportamiento, hábitos de consumido, localización, entre otras, de los Titulares propietarios de los dispositivos donde los aplicativos se encuentran instalados. Los *trackers* son fragmentos de código dentro de la aplicación cuya función es recolectar información arriba mencionadas - comportamiento, hábitos de consumido, localización, entre otras-, también registra datos particulares tales como: (i) modelo de celular donde ejecuta la aplicación; (ii) cantidad de veces de apertura de la aplicación, y (iii) tiempo de uso del aplicativo; (iv) geolocalización; (v) datos personales: (vi) comportamiento del aplicativo frente a fallos, entre otras. Esta información es enviada a servidores, propios o de terceros, donde la información es procesada. Los *trackers* sirven para entre otras cosas, mejorar la funcionalidad y al experiencia del aplicativo frente al usuario.

Al igual que las cookies en los servicios web, todos los *trackers* no recolectan la misma información, sino que cumple distintas finalidades en la recolección, por lo que se pueden categorizar de la siguiente manera:

(1) *Trackers* de Fallos*: Tracker* que permite a los desarrolladores rastrear los fallos dentro de un aplicativo y poder solucionarlos fácilmente.

(2) *Trackers* de perfilación comercial y analítica: *Tracker* que permite crear perfiles sobre los hábitos de navegación del usuario, sin que implique perfilación individual, que permite recolectar información para el posterior envío contenido comercial o de servicios ajustado a los gustos de navegación, manteniendo un grado de anonimidad;

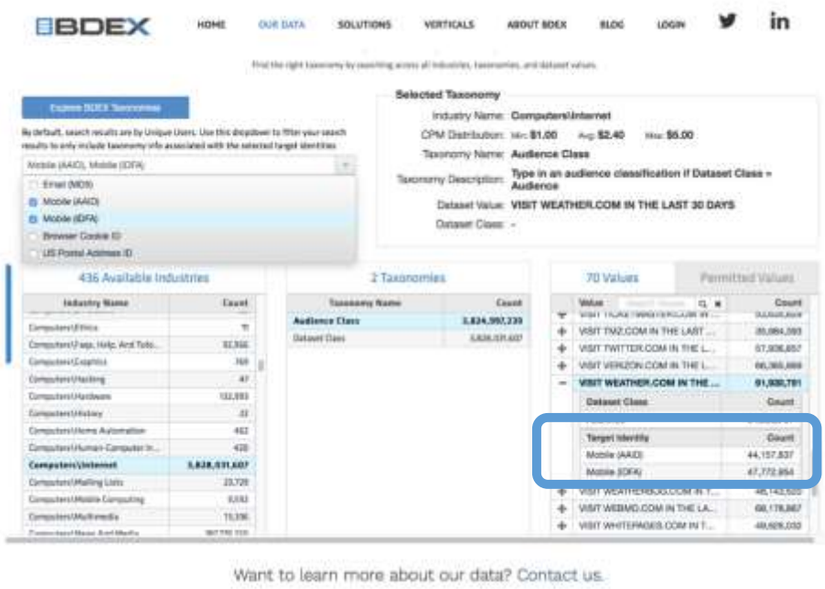
(3) *Trackers* de perfilación personal: *Tracker* que permite crear perfiles individualizados sobre los usuarios, recolectando información personal tal como nombre, dirección, identificación, localización geográfica, entre otros; para fines que pueden ser comerciales, venta de información, estudios demográficos, entre varios.

Trackers de rastreo cruzado: *Tracker* que permite el rastreo de personas a través de dispositivos y plataformas. Este tipo de *trackers* es reciente, pero con un grado de proliferación dentro de los ecosistemas virtuales de algunas compañías

Los *trackers,* dentro del ámbito de los aplicativos móviles, permiten optimizar el funcionamiento de un aplicativo, planificar tareas, el uso de datos para fines estadísticos, y en general, la experiencia de uso para los titulares de los aplicativos, siempre que uso sea de manera trasparente para los titulares, esto es, que su uso sea conocido y aceptado por estos. Ahora, si bien el uso de trackers es valioso para el desarrollador o mejorar de experiencia del usuario dentro determinado aplicativo, también es cierto que en algunas ocasiones, debido a la ausencia de trasparencia en su implementación -componente humano-, esta herramienta tecnológica es implementadas con total desconocimiento de los titulares usuarios del aplicativo, siendo desconocedores de su finalidad e implementación, toda vez que: (i) no le es informada en ningún tipo de documento al público sobre el aplicativo, incluyendo, pero no limitándose, a las Política de Tratamiento de Información o medio de información, y/o; (ii) utilizan mecanismo fraudulentos o engañosos para recolectar y realizar el tratamiento de información bajo una falsa apariencia de legalidad.

La falta de transparencia de los desarrolladores para dispositivos móviles deja a los titulares sin capacidad de identificar la existencia de servicios que recolectar, organizar, y agregar su información personal y actividad en línea a través de la red y las plataformas donde el aplicativo se ejecuta. Esto permite, entre otras cosas, tratar información considerada como confidencial, privada, semi-privada y/o sensible, para ser compartida con terceros -transferencia, transmisión y/o venta, incluyendo, pero no limitándose, a servicios de publicidad, marketing, y vendedores de datos al por mayor; actividades que, por regla general, se realizan sin la autorización de los titulares de los datos

Ahora, a pesar de que en la actualidad, y en una escala diminuta, los usuarios se han concientizado de los datos recolectada dentro de los aplicativos es intercambiada para distintos efectos, ejerciendo acciones para lograr grado de anonimización, ésta termina en manos de los denominados data *brokers* que venden la información al mejor postor sin el consentimiento del titular. Un ejemplo de esto se puede ver en la imagen 1, en la cual se evidencia la cantidad de información que se recolecta mediante *trackers* en dispositivos móviles en el uso del aplicativo del portal weather.com:



Fuente: Imagen 1 Tomada de Apps, Trackers, Privacy, and Regulators A Global Study of the Mobile Tracking Ecosystem, en: https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_05B-3_Razaghpanah_paper.pdf

Esta información es relevante de cara a que, sin el consentimiento de los titulares de las actividades de *tracking* o rastreo dentro de los aplicativos, estos pueden formar perfiles enriquecidos que permiten la individualización de los titulares; información que puede ser comercializada, o bien, en el peor escenario, expuesta a brechas de seguridad como en el caso de Yahoo! [9] con sus brechas de seguridad en los años 2014 y 2016, o bien, EXPERIAN[10], con su brecha de seguridad en Brasil en el año 2021, comprometiendo la información personal de millones de titulares en el mundo.

El problema que se plantea frente al uso de los *trackers*, desde el punto de vista regulatorio, y aún más desde el punto de vista de los generadores de políticas públicas, es identificar si las empresas utilizan estos servicios en sus aplicativos, y como éstas tratan la información de cara al funcionamiento de su operación, y más importante aún, como se articulan de cara a las políticas de tratamiento de información propias y la ley, lo que nos lleva al cuestionamiento de si este tipo de prácticas y/o tecnologías merecen una regulación específica.[11]

A pesar de los anterior, en Colombia, aun cuando no existe una regulación específica sobre *trackers*, la ley 1581 de 2012 entiende que el tratamiento es definido como cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación, supresión, sobre lo cual la Corte Constitucional ha dicho lo siguiente:

> *"[E]l tratamiento es definido como cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. Este vocablo (. . .) es de uso en el ámbito europeo y se encuentra tanto en la Directiva 95/46 del Parlamento Europeo como en los Estándares dictados en la reciente conferencia que se dio en Madrid (España), en la que se definió tratamiento como ´cualquier operación o conjunto de operaciones, sean o no automatizadas, que se aplique a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión´". [12]*

En aplicación de lo anterior, dato personal debe entenderse como aquel datos que por sí solo, o con asocio de otros datos, permite la identificación e individualización de una persona o varias. Por lo tanto, un *tracker*, tal como ocurre con las cookies, puede fungir como un mecanismo automatizado de recolección, clasificación, conservación y utilización de datos que permiten individualizar distintos comportamientos e identidad del titular, lo que en términos del Régimen General de Protección de Datos, que permite formar bases de datos con información que: (i) hace referencia a aspectos exclusivos y propios de una persona; (ii) permite identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; (iii) la propiedad de los datos reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por

---

[9] United Kingdom – Data Breach of 500m Yahoo Accounts, En: https://www.ncsc.gov.uk/news/data-breach-500m-yahoo-accounts (visto: Nov. 3, 2022).

[10]

[11] Alrededor del mundo las agencias y los creadores de políticas públicas, han desarrollado normativas que protegen a los derechos y datos personales de los titulares de forma relativamente exitosa. Cada jurisdicción tiene sus propias Reglas en contra la recolección de ilegal e invasiva mediante el uso de trackers: (i) Estados Unidos: Mediante la Children's Online Privacy Protection Act ("COPPA"), prohibió la recolección de datos personales de niños y menores de 13 años sin el consentimiento de los padres, incluyendo al recolección mediante trackers. Sin embargo, se evidenció que compañías violaron esta prohibición realizaron la recolección de este tipo de información, siendo multados por la Federal Trade Commision; (ii) Unión Europea: Mediate la General Data Protection Regulation ("GDPR"), creo reglas estrictas en el uso de tracking para la recolección de datos personales. Sin embargo, dada la envergadura del continente, y la cantidad de aplicativos existentes en los varios ecosistemas para dispositivos móviles, es difícil darles cumplimiento a estas regulaciones.

[12] Corte Constitucional [C.C.] SentenciaC-748/11, M.P. Jorge Ignacio Pretelt Chaljub, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 25) (Colom.)

parte de un tercero de manera lícita o ilícita, y; (iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación; caso en el cual, el responsable deberá ceñirse por las normas sobre protección de datos vigentes en Colombia, en especial la aplicación de los principios rectores para la administración de datos de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad consagrados en el artículo 4 de la Ley 1581 de 2012.

Por tanto, los trackers son mecanismos automatizados de recolección de datos personales que, sin impedir su avance tecnológico y benéfico para los titulares, deben cumplir con la regulación de tratamiento de datos personales en Colombia establecida por el Régimen General de Protección de Datos Personales, incluyendo, pero no limitándose, a la obtención por parte de los responsable de la autorización, previa e informada el titular, la implementación de las medidas de protección de la información accediendo solo a la información necesaria para la finalidad del aplicativo, y cumplimiento del principio de Responsabilidad Demostrada.

Finalmente, es necesario anotar que el Régimen General de Protección de Datos Personales no riñe con el avance de la tecnología, por el contrario, apoya su avance para mejorar la calidad de vida de los titulares, pero abogando, desde un punto de vista de neutralidad tecnológica, para que cualquier avance tecnológico, donde se realice la recolección y tratamiento de datos personales, sea respetuosos con todos los principios y reglas del debido tratamiento de datos personales.

3.2. SOBRE LA PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO (*Privacy by Design by Default*) Y ACCESO A LOS PERMISOS DEL DISPOSITIVO MÓVIL.

La privacidad desde el diseño y por Defecto (*"Privacy by Design and by Default" o "*PDyPD") es una teoría creada en los años 90 la cual busca que cualquier avance tecnológico donde se encuentre implicada la privacidad de las personas no solo diera cumplimiento a las regulaciones sobre la materia, sino que también esta fuera diseñada con respeto a la privacidad, y que esta visión fuera parte del núcleo esencial de desarrollo de productos y/o servicios por parte del fabricante y/o desarrollador.

Es así que, poniendo en práctica esta teoría, a finales del año 2020, la Global Privacy Assembly, aprobó el documento denominado RESOLUTION ON ACCOUNTABILITY IN THE DEVELOPMENT AND THE USE OF ARTIFICIAL INTELLIGENCE; el cual persuade a las organizaciones que desarrollan o utilizan sistemas de inteligencia artificial (IA) a considerar la implementación de las siguientes medidas: (i) Evaluar el posible impacto en los derechos humanos (incluida la protección de datos personales y los derechos de privacidad) antes del desarrollo y/o uso de la IA; (ii) Probar la solidez, confiabilidad, precisión y seguridad de los datos de la IA antes de ponerla en uso, incluida la identificación de sesgos en los sistemas y los datos que se utilizan que pueden conducir a resultados injustos, y; (iii) Implementar medidas de Responsabilidad Demostrada que sean apropiadas con respecto a los riesgos de interferencia con los derechos humanos. Estos lineamiento son los pilares básico de la incorporación de la privacidad, ética, y seguridad como medida por defecto desde el diseño del aplicativo y/o sistema, y la cual, busca que siempre en el diseño e implementación se realice estudios de impacto de seguridad o Privacy Impact Assessments ("PIA")

Las medidas anteriormente citadas, y sin que signifiquen que sean instrumentos normativos de estricto cumplimiento, sino persuasorios y voluntarios, fueron incorporadas la Superintendencia de Industria y Comercio en las siguiente guías: (i) Guía sobre el tratamiento de datos personales para fines de comercio electrónico; (ii) Guía sobre el tratamiento de datos personales para fines marketing y publicidad, y; (iii) Guía para la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos personales. Lo anterior significa que la PDyPD no aplica exclusivamente a desarrollo tecnológicos donde se encuentre incluida Inteligencias Artificial ("IA"), sino a cualquier avance tecnológico donde se vea implicada la recolección y tratamiento de datos personales. De esta manera ,al introducir la privacidad desde el diseño, se busca garantizar el correcto Tratamiento de los datos utilizados en los proyectos que involucren recolección, uso o tratamiento de datos personales. Así las cosas, el debido tratamiento de la información debe ser un componente esencial del diseño y puesta en marcha de proyectos de desarrollo tecnológico, siendo considerada también una medida proactiva para, entre otras, cumplir con el Principio de Responsabilidad Demostrada (Accountability)[13], orientada en los siguientes principios:

[13] Superintendencia de Industria y Comercio, **Sandbox sobre** privacidad desde el diseño y por defecto en proyectos de inteligencia artificial, en: https://www.sic.gov.co/sandbox-microsite (visto: Nov. 3, 2022).

En suma, la **Privacidad desde el diseño** debe considerarse como la aproximación a la privacidad que asegura la protección de datos en cuál fase de desarrollo e implementación de un sistema ,servicio, producto y/o proceso en cualquier fase de su ciclo de vida; y por su parte, e intrínsecamente ligada a la privacidad desde el diseño, **la privacidad por defecto**, busca que la recolección y tratamiento sea solo para la consecución del propósito específico (vinculado a los principios de minimización de los datos y finalidad específica de los datos), lo cual no quiere decir la adopción de posición op-out total, sino acomodado a la finalidad específica, por lo que se requiera dependerá de los circunstancias específicas y los riesgos que esta recolección y tratamiento signifique para los derechos los individuos.

De este modo, toda tecnología de recolección y tratamiento de datos personales, sin importar su destinación, debe propender a la consecución del objetivo claramente informado al titular a través de cualquier documento y/o medio, solo recolectando los datos mínimos necesarios para la consecución de las finalidades claramente anunciadas, por lo que una recolección y tratamiento de información mediante no tecnologías anunciadas al titular y sin finalidades específicas, constituyen un riegos en el tratamiento de datos, y una posible vulneración al Régimen General de Protección de Datos Personales.

Dicho lo anterior, es necesario indicar que en materia de desarrollo tecnológico de aplicativos móviles ayudan a restringir o dar accesos a varias características del dispositivo, entre ellas, la privacidad del propietario del dispositivo. Es así como en el ecosistema Android, cuyo desarrollo en materia de privacidad es más laxo que otros entornos móviles, los permisos dan acceso a dos características, de acuerdo con el centro para *developers*[14], a saber: (i) **Datos restringidos**: como el estado del sistema y la información de contacto del usuario, y; (ii) **Acciones restringidas**: como conectarte a un dispositivo vinculado y grabar audio. Sin embargo, para acceso a estas dos características, Google desarrollador del sistema operativo Android, indicó que existe 5 tipos de permisos en su entorno: (i) Permisos en el momento de la instalación[15]; (ii) Permisos normales[16]; (iii) Permisos de firma[17]; (iv) Permisos de tiempo de ejecución[18], y (v) Permisos especiales[19].

Con respecto los a permisos de tiempo de ejecución, que permiten el acceso a los datos -información personal privada y/o sensible- y acciones restringidas -tales como las funciones de seguridad del sistema, Google recomienda los siguientes pasos de cara a proteger al usuario: (i) establecer un flujo de trabajo para determinar si es necesario el uso de dichos datos y características; (ii) Aplicar los siguientes principios: transparencia: permitir que el usuario comprende los datos y características que usa el aplicativo y el motivo por el cual los utiliza, control, permitir que el usuario tenga control de los datos y características que comparte con los aplicativos, minimización de datos: el aplicativo acceder y usa solo los datos necesarios para una tarea o acción específica.

Por tanto, los principios de la PDyPD están imbuidos dentro de las pautas de desarrollo fijadas por Google, en especial lo referente a la transparencia, control -enfoque centrado en el usuario-, y

---

[14] Permisos en Android, en: https://developer.android.com/guide/topics/permissions/overview?hl=es-419 (visto: https://developer.android.com/guide/topics/permissions/overview?hl=es-419=) (visto: Nov. 3, 2022)

[15] Los permisos en el momento de la instalación otorgan a tu app acceso limitado a los datos restringidos y permiten que realice acciones restringidas que casi no afectan al sistema o a otras apps. Cuando declaras permisos en el momento de la instalación en la app, el sistema le otorga automáticamente los permisos cuando el usuario la instala. Una tienda de apps le muestra un aviso de permiso en el momento de la instalación al usuario cuando ve la página de detalles de la app, como se muestra en la Figura 2.Android incluye varios subtipos de permisos en el momento de la instalación, incluidos los permisos normales y los de firma.

[16] Estos permisos permiten el acceso a los datos y las acciones que se extienden más allá de la zona de pruebas de tu app. Sin embargo, los datos y las acciones presentan muy poco riesgo para la privacidad del usuario y el funcionamiento de otras apps. El sistema asigna el nivel de protección "normal" a los permisos normales, como se muestra en la página de referencia de la API de permisos.

[17] Si la app declara un permiso de firma definido por otra app, y si ambas están firmadas con el mismo certificado, el sistema otorga el permiso a la primera app en el momento de la instalación. De lo contrario, no se podrá otorgar permiso a esa primera app.

[18] Los permisos de tiempo de ejecución, también conocidos como permisos peligrosos, le otorgan a tu app acceso adicional a datos restringidos y permiten que realice acciones restringidas que afectan de manera más considerable el sistema y otras apps. Por lo tanto, debes solicitar permisos de tiempo de ejecución en tu app antes de poder acceder a los datos restringidos o realizar acciones restringidas. Cuando la app solicita un permiso de tiempo de ejecución, el sistema presenta un mensaje de este permiso, como se muestra en la Figura 3.Muchos permisos de tiempo de ejecución acceden a los *datos privados del usuario*, un tipo especial de datos restringidos que incluye información que puede ser sensible. Algunos ejemplos de datos privados del usuario incluyen la ubicación y la información de contacto. El micrófono y la cámara proporcionan acceso a información particularmente sensible. Por lo tanto, el sistema te ayuda a explicar por qué tu app accede a esta información.El sistema asigna el nivel de protección "peligroso" a los permisos de tiempo de ejecución, como se muestra en la página de referencia de la API de permisos.

[19] Los permisos especiales corresponden a operaciones particulares de la app. Solo la plataforma y los OEM pueden definir permisos especiales. Además, la plataforma y los OEM suelen definir permisos especiales cuando quieren proteger el acceso a acciones particularmente importantes, como el dibujo sobre otras apps.La página **Acceso especial de apps** en la configuración del sistema contiene un conjunto de operaciones que el usuario puede alternar. Muchas de estas operaciones se implementan como permisos especiales.Cada permiso especial tiene sus propios detalles de implementación. Las instrucciones para usar cada permiso especial aparecen en la página de referencia de la API de permisos. El sistema asigna el nivel de protección "appop" a permisos especiales.

minimización de datos, más cuando se pretende al accesos a los permisos de tiempo de ejecución que dan acceso adicional a datos restringidos y permiten que realice acciones restringidas que afectan de manera más considerable el sistema, y a datos privados del titular tales como la ubicación, información de contacto, micrófono, y cámara, entre otros; características las cuales, para Google, son sensibles de cara al titular, por lo cual es necesario solicitar permisos especiales teniendo en cuenta los conceptos de control, transparencia y minimización de datos. No realizar estas actividades puede ser considerado como un acceso indebido o fraudulento por cuanto el acceso no es reconocido por el titular.

CUARTO: Que, de la información y pruebas recolectadas por esta Dirección, y del análisis de las mismas, este Despacho encontró que se habrían ejecutado conductas presuntamente violatorias de las normas sobre protección de datos personales, y en virtud de lo dispuesto en la L. 1581/12, art. 21 (a)[20] y (b)[21] del mismo artículo, se inicia investigación administrativa a través de la formulación de cargos en contra de, por:

4.1. CARGO PRIMERO: La presunta vulneración, en su calidad de responsable, del principio de finalidad (L.1581/12, art. 4(b)) y el deber de informar debidamente sobre la finalidad de la recolección y de los derechos que le asisten por virtud de la autorización otorgada (L.1581/12, art. 17(c)).

La Ley 1581 de 2012 en su artículo 4, literal b, establece el principio rector de finalidad en el cual se establece que: *"El Tratamiento debe obedecer a una finalidad legitima de acuerdo con la Constitución y la ley, la cual deberá ser informada al titular".* Consecuentemente, la Ley 1581 de 2012 en su artículo 17, literal c, establece el deber para el Responsable del Tratamiento de los datos de: *"informar debidamente al titular sobre la finalidad de la recolección y de los derechos que le asisten por virtud de la autorización otorgada".*

En virtud del principio y el deber de finalidad en el tratamiento de datos personales, la Corte Constitucional ha sido enfática en determinar que no es posible la recolección de datos sin un fin legal y legítimo claro, quedando proscrita la recolección de datos sin la clara especificación acerca de su finalidad, o bien, *"(. . .) el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista".*[22]

Por tanto, debe entenderse que, en el periodo de recopilación y posterior tratamiento de los datos, queda prohibido: (i) la recopilación de información personal sin que se establezca el objetivo de su incorporación a la base de datos, y; (ii) la recolección, Tratamiento y/o divulgación de la información personal para un propósito diferente al inicialmente previsto y autorizado por el titular del dato.

Aunado a lo anterior, la finalidad no solo debe ser legitima, sino que la información recolectada debe ser usada para para realizar los fines exclusivos para los cuales fue obtenido el consentimiento, previo, expreso e **informado** por parte del Titular; de manera que, cualquier uso distinto al previamente indicado, requiere ser autorizado por el Titular[23]. Ahora bien, la Corte Constitucional, en interpretación del principio de finalidad, establecidó que existe la posibilidad de que sea dificultoso enunciar, de manera amplia y detallada, los usos de la información, dejando la posibilidad de que se realicen tratamientos no autorizados expresamente siempre que sean compatibles con la finalidad principal autorizada; es así que la Corte Constitucional determinó que *"(. . .) los datos personales deben ser procesados solo en la forma que la persona afectada pueda razonablemente prever. Si, con el tiempo, el uso de los datos personales cambia a formas que la persona razonablemente no espera, debe obtenerse el consentimiento del titular*"[24].

En el presente caso, de acuerdo con el Acta de Preservación bajo el radicado 21 – 433282 - - 1 del 12 de noviembre de 2021, en la sección de "Análisis de privacidad de Android", se observó que la versión para la plataforma Android de Avianca requiere el acceso a 15 permisos que, a consideración del Laboratorio Forense de la Entidad, son peligrosos por "*(. . .) las acciones que la aplicación puede hacer en el Sistema Operativo (para este caso: Android) del teléfono celular donde se instala"*[25]*;* tales como: (i)ACCESS_COARSE_LOCATION: permite enviar la ubicación aproximada del dispositivo

---

[20] Ibidem, art. 21(a): Velar por el cumplimiento de la legislación en materia de protección de datos personales;
[21] Óp.. cit., art. 21(b): Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos
[22] Corte Constitucional [C.C.] Sentencia T-729/02, M.P. Eduardo Montealegre Lynett, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 5) (Colom.).
[23] Corte Constitucional [C.C.] SentenciaC-748/11, M.P. Jorge Ignacio Pretelt Chaljub, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 40) (Colom.) (Interpreta el principio de finalidad de la L.1581/12, y establece su alcance en la sección 2.6.5.2.2.).
[24] Ibidem.
[25] Radicado 21 – 433282 - -1 del 12 de noviembre de 2021, p.29.

móvil, y por tanto del titular a Avianca; (ii) ACCESS_FINE_LOCATION: Permite enviar la ubicación exacta del dispositivo móvil, y por tanto del titular a Avianca; (iii)ACCESS: NETWORK_STATE: Permite leer las conexiones de red; (iv) ACCESS_WIFI_STATE: Permite leer la conexión Wifi; (v) CALL_PHONE: Permite el acceso a las llamadas y números de contacto almacenados en el dispositivo; (vi) CAMERA: Acceso a la cámara del dispositivo; (vii) DOWNLOAD_WITHOUT_NOTIFICATION: Permite realizar descargas en línea sin notificar al titular; (viii) INTERNET; (ix) READ_EXTERNAL_STORAGE: Permite el acceso a la memoria externa del dispositivo móvil, y por tanto, a la información personal del titular; (x) READ_PHONE_STATE: permite hacer lectura del estatus del dispositivo y su identidad; (xi) WAKE-LOCK: Impide que el dispositivo sea bloqueado cuando la aplicación esté en funcionamiento; (xii) REQUEST_INSTALL_PACKAGES: Permite la instalación de nuevos paquetes de información; (xiii) WRITE_EXTERNAL:_STORAGE: permite ingresar a la memoria externa y escribir información en esta; (xiv) C2D_MESSAGE: Previene que otras aplicaciones en registrarse y recibir mensajes de otras aplicaciones; (xv) RECEIVE: permito el uso de los datos o conexión a la red.

fuente: Radicado 21 - 433282 - - 1 del 12 del noviembre de 2022, p.29

Fuente: Radicado 21 - 433282 - - 1 del 12 del noviembre de 2022, p.30

Adicionalmente, el radicado 21 – 4332822 - - 1 del 12 de noviembre de 2021, el Acta de Preservación, indicó que adicionalmente, el aplicativo móvil contiene 4 rastreadores que recolectan *"(. . .) información del usuario o de sus hábitos de navegación (. . .)"*[26], siendo estos rastreadores, los siguientes: (i) Demdex: Permite recolectar información de comportamiento de navegación del titular, incluyendo la información personal del titular tal como la identificación a través de dispositivos, análisis predictivo de hábitos de consumo, ofrecimiento comercial mediante geolocalización, ubicación en tiempo real; (ii) Google Firebase Analytics; Permite recolectar información de uso y comportamiento dentro del aplicativo, o del comportamiento externo que tenga el usuario. De acuerdo con el manual de desarrollo del tracker, permite el acceso a eventos dentro del aplicativo (errores y acciones) y opciones del usuario, lo cual permite la personalización del aplicativo, entre otras características, el idioma y/o la localización geográfica; (iii) Microsoft Visual Studio App Center Analytics: ayuda a estudiar y entender aspectos y comportamiento del aplicativo durante su uso, y; (iv) Microsoft Visual Studio App Center Crashes: Permite la creación de un log de los errores del aplicativo y ser enviado al desarrollador.

[26] Ibidem, p. 30.

Fuente: Radicado 21 - 433282 - - 1 del 12 del noviembre de 2022, p.30

En virtud de lo anterior, el Despacho mediante radicados 21-433282 - - 2 del 22 de marzo de 2022[27] y 21 – 433282 - - 6 del 29 de abril de 2022[28], requirió a AVIANCA respecto a los *trackers* y permisos, a lo cual AVIANCA, mediante radicados 21- 433282 - - 5 del 9 de abril de 2022 y 21-433282 - - 11 del 7 de julio de 2022, dio respuesta en los siguientes términos, respectivamente:

> ***"(. . .)*** *Informamos al Despacho que los permisos (i) READ_EXTERNAL_STORAGE, (ii) READ_PHONE_STATE (iii) REQUEST_INSTALL_PACKAGES (iv) WRITE_EXTERNAL_STORAGE, y (v) C2D_MESSAGE, no son usados por la aplicación móvil. Teniendo en cuenta lo anterior, a continuación, relacionamos el objetivo, la finalidad y los momentos del proceso en donde se usan los permisos restantes cuestionados por el Despacho:*
>
> ***Permiso de Cámara:***
>
> - ***Objetivo de usarlo:*** *En las versiones más antiguas de la aplicación, este permiso habilitaba que las personas pudieran tomarse una foto para completar su perfil, sin embargo, las nuevas versiones de esta aplicación no soportan esta funcionalidad. La funcionalidad no se ha removido, pues en un futuro se planea volverla a habilitar, no obstante, hoy en día no es usada.*
> - ***Finalidad de la información recopilada con estas herramientas:*** *La única funcionalidad del permiso era poder tomar una foto para modificar el perfil del usuario.*
> - ***En que partes del proceso se usan:*** *Hoy en día no se usa.*
>
> *(1)* ***Permiso de Internet: Objetivo de usarlo****: El objetivo del permiso es la conexión con servicios externos para la funcionalidad general de la aplicación.*
> *(2)* ***Finalidad de la información recopilada con estas herramientas:*** *Permitir el flujo de información que puede ser consultada o visualizada por los usuarios por medio de la aplicación.*
> *(3)* ***En que partes del proceso se usan:*** *Durante todo el proceso de uso de la aplicación.*
>
> - ***Permiso de WAKE_LOCK:***
>
> *(1)* ***Objetivo de usarlo:*** *Este permiso tiene como objetivo mantener la app activa cuando hay una tarea en el "background" de la aplicación que no se terminó de ejecutar.*
>
> *(2)* ***Finalidad de la información recopilada con estas herramientas:*** *mantener la aplicación con información actualizada.*
>
> *(3)* ***En que partes del proceso se usan:*** *Se usa en la sección "Mis vuelos" dentro de la aplicación"*
>
> *(. . .)* ***Respuesta:*** *Informamos al Despacho que actualmente la APP de Avianca no utiliza el rastreador "Demdex". Teniendo en cuenta lo anterior, a continuación, relacionamos el objetivo, la finalidad y los momentos del proceso en donde se usan los otros 3 rastreadores de la aplicación móvil de Avianca identificados por el Despacho:*
>
> • ***Microsoft Visual Studio App Center Analytics:***

---

[27] Radicado 21-433282 - - 2 del 22 de marzo de 2022: *"(4) Indicar, con respecto a la APP, cuáles son las finalidades de específicas por la cual se requiere los siguientes permisos: (i) Cámara; (ii) Internet; (iv) READ_EXTERNAL_STORAGE; (v) READ_PHONE_STATE; (vi) READ_PHONE_STATE; (vi) REQUEST_INSTALL_PACKAGES; (vii) WAKE_LOCK; (viii) WRITE_EXTERNAL_STORAGE; (ix) C2D_MESSAGE. De igual forma, indicar si los titulares están al tanto del acceso estas funcionalidades, y si estas pueden ser desactivadas fácilmente por el titular;(5) Indicar, con respecto a la APP, las razones por las cuales se utilizan los siguientes 4 rastreadores: (i) Demdex; (ii) Google Firebase Analytics; (iii) Microsoft Visual Studio App Center Analytics, y; (iv) Microsoft Visual Studio App Crashes."*

[28] Radicado 21-433282 - - 6 del 29 de abril de 2022: *"(2) Indicar, de acuerdo con la respuesta a la pregunta 4 al primer requerimiento de información, desde qué versión de la App se utilizó por última vez la funcionalidad de cámara. Remitir copia del código fuente de la versión tanto para iOS como para Android; (3) Indicar, de acuerdo con la respuesta 5 al primer requerimiento de información, cuál era la finalidad del rastreador denominado "DEMDEX", indicado también que ocurrió con los datos recolectados por ese rastreador, y la última versión de la App en la que fue utilizada. Remitir copia del código fuente de la versión tanto para iOS como para Android;"*

Objetivo: *Esta herramienta es usada por Avianca para monitorear el comportamiento de la APP y el uso que se da de la misma. Por ejemplo, la herramienta permite dar visibilidad sobre (i) países con mayor número de instalaciones, (ii) lenguaje de uso, (iii) tipo de dispositivos más usados, (iv) duración de las sesiones en la aplicación, y (v) cantidad de usuarios, entre otros.*

o ***Finalidad de la información recopilada con esta herramienta:*** *Teniendo en cuenta lo anterior, la herramienta se utiliza con la finalidad de tener un muestreo y análisis del uso de la aplicación. Lo anterior, sin realizar captura de datos personales de los usuarios.*

o ***En que partes del proceso se usa:*** *La herramienta entra en funcionamiento y registra datos desde el momento en que se inicializa la APP, cuando se cambia de idioma en la APP, cuando se interactúa con el Login y/o cuando llegan las notificaciones sobre la aplicación.*

Microsoft Visual Studio App Crashes*.*

o ***Objetivo:*** *El objetivo principal de la herramienta es poder realizar un seguimiento y control a los errores inesperados la APP. En este sentido, la herramienta no captura datos personales o sensibles de los usuarios, sino que registra datos de rendimiento y fallas propias de la aplicación.*

o ***Finalidad de la información recopilada con esta herramienta:*** *Identificar posibles errores en la APP.*

o ***En que partes del proceso se usa****: La herramienta entra en funcionamiento cuando registra algún error técnico no controlado.*

Google Firebase Analytics*;*

o ***Objetivo:*** *El objetivo de usar Firebase Analytics es realizar un seguimiento de los análisis de la aplicación (iOS y Android), con el fin de generar estadísticas de los usuarios, ventas y productos. Generar estadísticas que permitan una medición correcta de los eventos de ventas y autogestión realizados en este canal.*

o ***Finalidad de la información recopilada con esta herramienta:*** *Poder ejecutar un correcto estudio del comportamiento del usuario dentro de la APP y por ende tener una mayor efectividad de la comunicación con usuarios.*

o ***En que partes del proceso se usa****: La herramienta se usa en el proceso de pago, proceso de reserva, etc.: Se emplean en los procesos de eventos de Login de usuario, cuando se agregan productos (Addtocart) o remover productos (Removefromcart), o cuando un usuario realiza una selección de vuelos, detalle de vuelo."*
"Respuesta: Aclaramos al Despacho que el rastreador "Demdex" no ha sido usado en la aplicación móvil Avianca, en la medida en que esta es una aplicación "Adobe", la cual no es soportada por la tecnología que usan las aplicaciones móviles de la compañía. Por lo tanto, no habría estado disponible ni en la versión OS, ni en la versión Android de la misma.
Adicionalmente, informamos al Despacho que según hemos investigado internamente aun si la aplicación usara este rastreador, el mismo no permite la recolección, captura, o almacenamiento de datos personales de usuarios, debido a que su finalidad es realizar un muestreo general del uso y de la navegabilidad de los usuarios en una página web, sin realizar perfilación o individualización de dichas interacciones. (. . .)
Respuesta: Aclaramos al Despacho que la herramienta Google Firebase Analytics no pretende ser usada con el propósito de capturar datos personales a través los canales digitales de Avianca, por lo que Avianca no almacenaría datos personales de clientes mediante el uso de esta herramienta. Lo anterior, teniendo en cuenta que tal y como se expuso en la respuesta a la pregunta 5 del requerimiento de información referenciado por el Despacho, el objetivo de usar esta herramienta es generar estadísticas generales sobre el comportamiento de usuarios en las aplicaciones móviles, sin que esto implique una individualización y/o perfilación de cada uno de los usuarios.
En este sentido, los análisis realizados mediante el uso de la precitada herramienta se direccionan hacia la mejora de los canales y/o plataformas mediante enfoques descriptivos que permitan conocer, por ejemplo: (i) el total de visitas del sitio, (ii) el total de transacciones realizadas, y (iii) las páginas de error, entre otros.
Adicionalmente, la intención de no recoger datos personales se hace aun más evidente si se tiene en cuenta que las mismas políticas de Google Analytics no admiten la captura de datos personales, por lo que usar la herramienta con este objetivo constituiría una pérdida de la licencia con la que actualmente se cuenta.
Al respecto las políticas de Google Analytics indican:

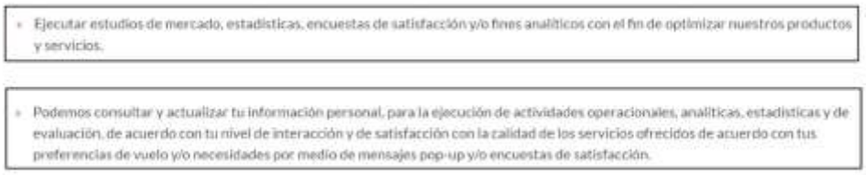
Prácticas recomendadas para evitar enviar información personal identificable

Evite el envío de información personal identificable a Google al recoger datos de Analytics

Para proteger la privacidad del usuario, las políticas de Google exigen que no se transmita información que Google pueda utilizar o reconocer como información personal identificable (IPI). Esto incluye información como, por ejemplo, direcciones de correo electrónico, números de móvil personales o números de identificación personal. Dado que las leyes son diferentes en cada país o territorio y como Google Analytics puede utilizarse de distintas formas, consulte a un abogado si tiene dudas sobre si ciertos datos se consideran información personal identificable.

De acuerdo a lo anterior, reiteramos al Despacho que no es intención de Avianca contar con métricas, modelos o dimensiones de datos personales recolectados por medio del uso de la herramienta Google Firebase Analytics.

Ahora bien, aunque Avianca no pretende recolectar datos personales de usuarios mediante el uso de esta herramienta, informamos al Despacho que, dentro de las finalidades de la Política para el tratamiento de datos personales de Avianca, se encuentran incluidas las finalidades estadísticas como se evidencia a continuación:



- Ejecutar estudios de mercado, estadísticas, encuestas de satisfacción y/o fines analíticos con el fin de optimizar nuestros productos y servicios.

- Podemos consultar y actualizar tu información personal, para la ejecución de actividades operacionales, analíticas, estadísticas y de evaluación, de acuerdo con tu nivel de interacción y de satisfacción con la calidad de los servicios ofrecidos de acuerdo con tus preferencias de vuelo y/o necesidades por medio de mensajes pop-up y/o encuestas de satisfacción.

Esta información, contrastada con la normativa sobre protección de datos personales, permite establecer de manera preliminar, que las finalidades que AVIANCA informa a sus titulares mediante la Política de Tratamiento de Información ("PTI") resultan demasiado generales, incluso inespecíficas, puesto que: (i) se accede a funciones del dispositivo que resultan inexplicables y peligrosas tales como: ACCESS_COARSE_LOCATION, ACCESS_FINE_LOCATION, CAMERA, READ_EXTERNAL_STORAGE, READ_PHONE_STATE, y WRITE_EXTERNAL_STORAGE, y (ii) la utilización del tracker denominado DEMDEX, permite recolectar información de comportamiento de navegación del titular, incluyendo la información personal del titular tal como la identificación a través de dispositivos, análisis predictivo de hábitos de consumo, ofrecimiento comercial mediante geolocalización, ubicación en tiempo real, lo cual permite crear perfiles específicos de los titulares sin su consentimiento; vulnerando en principio el Régimen General de Protección de Datos puesto que contraría el principio de finalidad contenido en el literal (b) del artículo 4, y el deber contenido en el artículo literal (c) del artículo 17 de la Ley 1581 de 2012, de informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten a los por virtud de la autorización, por cuanto no existe una finalidad dentro de la PTI analizada por el Laboratorio Forense de la SIC, así como la remitida por AVIANCA, que permita inferir que esta compañía está habilitada por parte del titular a: (i) ingresar a características del sistema y datos -privados y sensibles- considerados como peligrosos, e; (ii) implementar herramientas tecnológicas como un *tracker* como DEMDEX[29], el cual permite su perfilación para diversos usos, incluyendo, pero no limitándose, a su geolocalización; ambas actividades ejecutadas sin el consentimiento del titular. Así mismo, es necesario anotar que, con respecto a la finalidad de algunas de las citadas funciones, AVIANCA no dio respuesta concreta sobre los motivos de su implementación y uso, ya que, según la investigada, no se encuentran implementados en la versión actual de software.

Por tanto, se encuentra a AVIANCA, en su condición responsable del tratamiento de información mediante el aplicativo "AVIANCA" de la plataforma Android, presuntamente vulneró el principio y deberes contenidos en el artículo 4(b) y artículo 17 (c) de la ley 1581 de 2012, por los motivos arriba indicados.

4.2. CARGO SEGUNDO: La presunta vulneración, en su calidad de Responsable, del principio de seguridad (L.1581/12, art. 4(g)) en concordancia con el deber de conservar la información la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento (L.1581/12, art. 17(d)).

[29] Este Tracker ha sido ategorizado por este Despacho como un rastreador o *tracker* de perfilación personal y rastreo cruzado entre plataformas para efectos comerciales no definidos.

El principio de seguridad establecido por el literal (g) del artículo 4 de la Ley 1581 de 2012, estableció de forma expresa que el responsable del tratamiento deberá implementar 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. Por su parte, y de forma concordante, la misma norma en su artículo 17 literal (d) establece la obligación para el responsable de conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado.

Nótese que **la redacción del principio y el deber de seguridad tienen 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 sobre las personas. Proteger la información es una condición crucial del tratamiento de datos personales. Una vez recolectada debe ser objeto de medidas de diversa índole para evitar situaciones indeseadas que pueden afectar los derechos de los titulares y de los mismos responsables y encargados del tratamiento. El acceso, la consulta y el uso no autorizado o fraudulento, así como la manipulación y pérdida de la información son los principales riesgos que se quieran mitigar a través de las medidas de seguridad de naturaleza humana, física, administrativa, técnica o de cualquier otra índole.

Del texto del literal (d) precitado artículo 17 de la Ley Estatutaria 1581 de 2012 se concluye, entre otras, que las medidas de seguridad deben estar dirigidas a evitar que se presente cualquier tipo de irregularidad que, entre otras, facilite o permita que una persona no autorizada un acceda a los datos personales de otras personas, situación que adquiere mayor importancia, sí se tiene en cuenta la existencia de datos de carácter sensible. Por lo tanto, las actividades tendientes a mitigar posibles fallas en las medidas de seguridad adoptadas deben tener un carácter permanente y ser monitoreadas para establecer su pertinencia y efectiva protección de los datos personales. Con respecto a lo anteriormente expuesto, la Corte Constitucional ha establecido que:

> *"(. . .) [E]l Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Asíí, por ejemplo, en materia de redes sociales, empieza a presentarse una preocupación de establecer medidas de protección reforzadas, en razón al manejo de datos reservados. En el año 2009, el Grupo de Trabajo Sobre Protección de Datos de la Unión Europea señaló que en los 'Servicios de Redes Sociales' o 'SRS' debe protegerse la información del perfil en el usuario mediante el establecimiento de 'parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos´"*[30].

De lo anterior debe entenderse entonces, que la norma busca establecer un elemento preventivo para que los Responsables, al igual que los Encargados, cuando sea el caso, adopten las medidas necesarias y efectivas de carácter reforzado para así evitar afectaciones a la seguridad de la información de los Titulares. El acceso, consulta y/o el uso no autorizado o fraudulento, así como la manipulación y pérdida de la información son los principales riesgos que se buscan mitigar a través de las medidas de seguridad de naturaleza humana, física, administrativas, técnicas, y de cualquier índole que refuercen las medidas tomadas.

En el caso de Avianca, y como se indicó para el cargo primero, el Laboratorio Técnico Forense de la de la SIC, mediante el Acta de Preservación - Acta número 180-21, con radicado 21 – 433282 - - 1 del 12 de noviembre de 2021, específicamente en la sección de "Análisis de privacidad de Android", indicó que la versión 7.0.15 del aplicativo AVIANCA para la plataforma Android requiere el acceso a 15 permisos que, a consideración del Laboratorio Forense de la Entidad, son peligrosos por "*(. . .) las acciones que la aplicación puede hacer en el Sistema Operativo (para este caso: Android) del teléfono celular donde se instala"*[31]*;* tales como: (i) ACCESS_COARSE_LOCATION; (ii) ACCESS_FINE_LOCATION:; (iii)ACCESS: NETWORK_STATE; (iv) ACCESS_WIFI_STATE; (v) CALL_PHONE; (vi) CAMERA; (vii) DOWNLOAD_WITHOUT_NOTIFICATION:; (viii) INTERNET; (ix) READ_EXTERNAL_STORAGE; (x) READ_PHONE_STATE; (xi) WAKE-LOCK; (xii) REQUEST_INSTALL_PACKAGES; (xiii) WRITE_EXTERNAL:_STORAGE; (xiv) C2D_MESSAGE; (xv) RECEIVE; de las cuales hay que destacar 6 como peligrosos: (i) ACCESS_COARSE_LOCATION; (ii) ACCESS_FINE_LOCATION: (iii) CALL_PHONE: (iv) CAMERA, (v) READ_EXTERNAL_STORAGE; (vi) READ_PHONE_STATE, tal como se indica en las imágenes adjuntas, donde junto al signo de exclamación en rojo se muestran como "peligroso" o "especial"

---

[30] Corte Constitucional [C.C.] SentenciaC-748/11, M.P. Jorge Ignacio Pretelt Chaljub, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 40) (Colom.) (Interpreta el principio de Seguridad de la L.1581/12, y establece su alcance en la sección 2.6.5.2.7.).

[31] Radicado 21 – 433282 - -1 del 12 de noviembre de 2021, p.29.

Fuente: Radicado 21 - 433282 - - 1 del 12 del noviembre de 2022, p.29

Fuente: Radicado 21 - 433282 - - 1 del 12 del noviembre de 2022, p.30

De igual forma, mediante el Acta de preservación, el Equipo Técnico Forense de la SIC indicó que el aplicativo móvil de AVIANCA para la plataforma Android contiene 4 rastreadores que recolectan *"(. . .) información del usuario o de sus hábitos de navegación (. . .),* donde se debe poner especial atención al rastreador denominado Demdex: el cual Permite recolectar información de comportamiento de navegación del titular, incluyendo la información personal del titular tal como la identificación a través de dispositivos, análisis predictivo de hábitos de consumo, ofrecimiento comercial mediante geolocalización, ubicación en tiempo real:

fuente: Radicado 21 - 433282 - - 1 del 12 del noviembre de 2022, p.29

En razón a los anteriores hallazgos, el Despacho mediante los radicados 21-433282 - - 2 del 22 de marzo de 2022[32] y 21 – 433282 - - 6 del 29 de abril de 2022[33], requirió a AVIANCA respecto los permisos y tracker, y las medidas de seguridad para proteger la información de los titulares, a lo cual AVIANCA, mediante radicados 21- 433282 - - 5 del 9 de abril de 2022 y 21-433282 - - 11 del 7 de julio de 2022, dio respuesta en los siguientes términos, respectivamente:

> ***"(. . .)*** *Informamos al Despacho que los permisos (i) READ_EXTERNAL_STORAGE, (ii) READ_PHONE_STATE (iii) REQUEST_INSTALL_PACKAGES (iv)*

[32] Radicado 21-433282 - - 2 del 22 de marzo de 2022: *"(4) Indicar, con respecto a la APP, cuáles son las finalidades de específicas por la cual se requiere los siguientes permisos: (i) Cámara; (ii) Internet; (iv) READ_EXTERNAL_STORAGE; (v) READ_PHONE_STATE; (vi) READ_PHONE_STATE; (vi) REQUEST_INSTALL_PACKAGES; (vii) WAKE_LOCK; (viii) WRITE_EXTERNAL_STORAGE; (ix) C2D_MESSAGE. De igual forma, indicar si los titulares están al tanto del acceso estas funcionalidades, y si estas pueden ser desactivadas fácilmente por el titular;(5) Indicar, con respecto a la APP, las razones por las cuales se utilizan los siguientes 4 rastreadores: (i) Demdex; (ii) Google Firebase Analytics; (iii) Microsoft Visual Studio App Center Analytics, y; (iv) Microsoft Visual Studio App Crashes."*

[33] Radicado 21-433282 - - 6 del 29 de abril de 2022: *"(2) Indicar, de acuerdo con la respuesta a la pregunta 4 al primer requerimiento de información, desde qué versión de la App se utilizó por última vez la funcionalidad de cámara. Remitir copia del código fuente de la versión tanto para iOS como para Android; (3) Indicar, de acuerdo con la respuesta 5 al primer requerimiento de información, cuál era la finalidad del rastreador denominado "DEMDEX", indicado también que ocurrió con los datos recolectados por ese rastreador, y la última versión de la App en la que fue utilizada. Remitir copia del código fuente de la versión tanto para iOS como para Android;"*

WRITE_EXTERNAL_STORAGE, y (v) C2D_MESSAGE, no son usados por la aplicación móvil. Teniendo en cuenta lo anterior, a continuación, relacionamos el objetivo, la finalidad y los momentos del proceso en donde se usan los permisos restantes cuestionados por el Despacho:

Permiso de Cámara:

- ***Objetivo de usarlo:*** *En las versiones más antiguas de la aplicación, este permiso habilitaba que las personas pudieran tomarse una foto para completar su perfil, sin embargo, las nuevas versiones de esta aplicación no soportan esta funcionalidad. La funcionalidad no se ha removido, pues en un futuro se planea volverla a habilitar, no obstante, hoy en día no es usada.*
- ***Finalidad de la información recopilada con estas herramientas:*** *La única funcionalidad del permiso era poder tomar una foto para modificar el perfil del usuario.*
- ***En que partes del proceso se usan:*** *Hoy en día no se usa.*

(1) ***Permiso de Internet: Objetivo de usarlo****: El objetivo del permiso es la conexión con servicios externos para la funcionalidad general de la aplicación.*

(2) ***Finalidad de la información recopilada con estas herramientas:*** *Permitir el flujo de información que puede ser consultada o visualizada por los usuarios por medio de la aplicación.*

(3) ***En que partes del proceso se usan:*** *Durante todo el proceso de uso de la aplicación.*

- ***Permiso de WAKE_LOCK:***

(4) ***Objetivo de usarlo:*** *Este permiso tiene como objetivo mantener la app activa cuando hay una tarea en el "background" de la aplicación que no se terminó de ejecutar.*

(5) ***Finalidad de la información recopilada con estas herramientas:*** *mantener la aplicación con información actualizada.*

(6) ***En que partes del proceso se usan:*** *Se usa en la sección "Mis vuelos" dentro de la aplicación"*

(. . .) ***Respuesta:*** *Informamos al Despacho que actualmente la APP de Avianca no utiliza el rastreador "Demdex". Teniendo en cuenta lo anterior, a continuación, relacionamos el objetivo, la finalidad y los momentos del proceso en donde se usan los otros 3 rastreadores de la aplicación móvil de Avianca identificados por el Despacho:*

Nótese de que las respuestas dadas en los radicados 21- 433282 - - 5 del 9 de abril de 2022 y 21-433282 - - 11 del 7 de julio de 2022, evadieron por completo dar respuesta sobre los siguientes permisos:(i) READ_EXTERNAL_STORAGE, (ii) READ_PHONE_STATE (iii) REQUEST_INSTALL_PACKAGES (iv) WRITE_EXTERNAL_STORAGE, y (v) C2D_MESSAGE, aludiendo que no son utilizados por el aplicativo, sin embargo, como ya se anotó en el Acta de Preservación, estos se encuentran o encontraban activos para la versión 7.0.15 del aplicativo AVIANCA.

La utilización de estos permisos y tracker constituye una posible vulneración al Régimen General de Protección de Datos por cuanto su implementación resulta contraria con el principio de seguridad definido por el artículo 4(g) de la Ley 1581 de 2012, que el responsable debe implementar 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; de forma concordante, la misma norma en su artículo 17 literal (d) establece la obligación para el responsable de conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado, por cuanto, aun cuando es un criterio preventivo, las medidas técnicas son ausentes en el aplicativo Avianca versión versión 7.0.15 de la plataforma Android, toda vez que, de forma inadvertida para los titulares, y sin que medie su autorización expresa, previa e informada, se tiene acceso a funciones consideradas esenciales del dispositivo móvil en el cual se encuentra instalado, pudiendo accede AVIANCA, a funciones tales como: (i) cámara; (ii) localización por red y geolocalización por GPS; (ii) memoria externa del dispositivo; (iii) acceso a llamadas y agenda del teléfono, y (iv) lectura del estado de información del dispositivo; medidas que pueden poner en riesgo la información personal privada y sensible de los titulares, más cuando estas no son advertidas a estos a través de las respectivas PTI y/o Aviso de Privacidad, generando de esta forma un riesgo de adulteración, pérdida, consulta, uso o acceso no autorizado por parte de personal de AVIANCA o terceros de mala Fe.

De igual forma, la implementación de un *tracker* como DEMDEX pone en riesgo la información privada y sensible de los titulares, toda vez que no es una herramienta tecnológica sobre la cual pueda el Responsable, una vez implementada, tener control sobre la destinación de la información, lo cual preliminarmente rompe el deber preventivo de evitar afectaciones a la seguridad de la información sobre las personas una vez son recolectadas, además que permite que terceros puedan formar perfiles enriquecidos de información sin el consentimiento del titular, contradiciendo el mandato de

acceso indebidos o de mala de establecidos por la norma, generando de igual forma un riesgo adulteración, pérdida, consulta, uso o acceso no autorizado.

Así mismo, se vulnera, en principio, el mandato de la Corte Constitucional[34] sobre la implementación de "*(. . .) parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos´",* puesto que los implementados dentro del aplicativo Avianca versión 7.0.15 del aplicativo AVIANCA para la plataforma Android, languidecen en relación con respecto a la intimidad de los titulares. En este punto se debe destacar lo informado por parte del laboratorio técnico Forense de la Entidad en los siguientes términos: *"De acuerdo a la verificación de permisos mediante el uso de la herramienta EXODUS se evidencian 15 permisos (Los permisos son acciones que la aplicación puede hacer en el teléfono) los cuales difieren de los informados al momento de instalar la app, dentro de los permisos solicitados y no informados se encuentran: permiso para realizar llamadas (CALL_PHONE); permiso para leer el estado del teléfono (READ_PHONE_STATE) permite a la aplicación saber el número de teléfono, la información actual de la red móvil, el estado de las llamadas en curso entre otros"*[35]

Por tanto, se encuentra que la investigada, como Responsable del tratamiento de información mediante el aplicativo "AVIANCA" de la plataforma Android, presuntamente vulneró el principio y los deberes contenidos en el literal (g) del artículo 4(g) y el literal (d) artículo 17 de la Ley 1581 de 2012, por los motivos anteriormente expuestos.

4.3. CARGO TERCERO: La presunta vulneración, en su calidad de responsable, del principio de libertad (L.1581/12, art. 4(c)) y el deber de abstenerse de utilizar medios engañosos para recolectar y realizar el tratamiento de datos personales (D.1377/13, art. 4 - incorporado por el D.U.R. 1074/15-)

El principio de libertad, establecido por en el literal (c) del artículo 4 de la Ley 1581 de 2012, orienta a que la actividad de recolección y tratamiento de información solo puede ejercerse cuando el titular a otorgado su consentimiento expreso, previo e informado para dichas actividades. Así mismo, reafirma la norma que los datos personales no puede ser obtenidos sin el consentimiento del titular, solo pudiendo ser relevado por un mandato legal o judicial por parte de un juez de la república. Así mismo, por remisión expresa de la norma, y armonía con la Ley 1581 de 2012, el artículo 4 del Decreto 1377 de 2013, ordena que el tratamiento de datos personales debe limitarse a aquellos datos pertinentes y adecuados para la finalidad informada al titular -minimización de datos Personales-. De igual forma, esta norma obliga al Responsable a no *"(. . .) utilizar medios engañosos o fraudulentos para recolectar y realizar el tratamiento de información".*

En el caso en concreto de AVIANCA, el Acta de Preservación con radicado 21-433282 - - 1 del 12 de noviembre de 2021, indicó que el aplicativo para la plataforma móvil Android denominado "AVIANCA": (i) tiene acceso a las siguientes características consideradas como peligrosas: ACCESS_COARSE_STATE, ACCESS_FINE_LOCATION, CALL_PHONE, CAMERA, READ_EXTERNAL_STORAGE, READ_PHONE_STATE, y WRITE_EXTERNAL:_STORAGE[36]; (ii) implementó un *tracker* denominado DEMDEX" que tiene fines estadísticos, razón por la cual se requirió a la sociedad investigada al referente, mediante radicados 21-433282 - - 2 del 22 de marzo de 2022[37] y 21 – 433282 - - 6 del 29 de abril de 2022[38], indicando que con respecto a los permisos *"(. . .) (i) READ_EXTERNAL_STORAGE, (ii) READ_PHONE_STATE (iii) REQUEST_INSTALL_PACKAGES (iv) WRITE_EXTERNAL_STORAGE, y (v)*

[34] Corte Constitucional [C.C.] SentenciaC-748/11, M.P. Jorge Ignacio Pretelt Chaljub, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 40) (Colom.) (Interpreta el principio de Seguridad de la L.1581/12, y establece su alcance en la sección 2.6.5.2.7.).

[35] Radicado 21 – 433282 - - 1 del 12 de noviembre de 2021, p. 34.

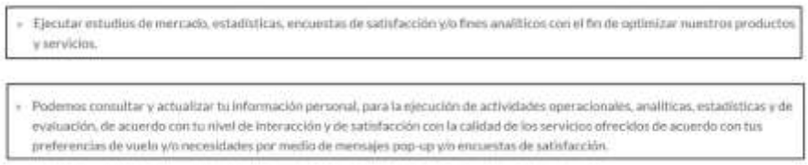
[36] Radicado 21-433282 - - 1 del 12 de noviembre de 2022, p. 29 – 30.

[37] Radicado 21-433282 - - 2 del 22 de marzo de 2022: *"(4) Indicar, con respecto a la APP, cuáles son las finalidades de específicas por la cual se requiere los siguientes permisos: (i) Cámara; (ii) Internet; (iv) READ_EXTERNAL_STORAGE; (v) READ_PHONE_STATE; (vi) READ_PHONE_STATE; (vi) REQUEST_INSTALL_PACKAGES; (vii) WAKE_LOCK; (viii) WRITE_EXTERNAL_STORAGE; (ix) C2D_MESSAGE. De igual forma, indicar si los titulares están al tanto del acceso estas funcionalidades, y si estas pueden ser desactivadas fácilmente por el titular;(5) Indicar, con respecto a la APP, las razones por las cuales se utilizan los siguientes 4 rastreadores: (i) Demdex; (ii) Google Firebase Analytics; (iii) Microsoft Visual Studio App Center Analytics, y; (iv) Microsoft Visual Studio App Crashes."*

[38] Radicado 21-433282 - - 6 del 29 de abril de 2022: *"(2) Indicar, de acuerdo con la respuesta a la pregunta 4 al primer requerimiento de información, desde qué versión de la App se utilizó por última vez la funcionalidad de cámara. Remitir copia del código fuente de la versión tanto para iOS como para Android; (3) Indicar, de acuerdo con la respuesta 5 al primer requerimiento de información, cuál era la finalidad del rastreador denominado "DEMDEX", indicado también que ocurrió con los datos recolectados por ese rastreador, y la última versión de la App en la que fue utilizada. Remitir copia del código fuente de la versión tanto para iOS como para Android;"*

C2D_MESSAGE, no son usados por la aplicación móvil."[39], y frente al *tracker* que *"(. . .)*actualmente la APP de Avianca no utiliza el rastreador ´Demdex´"[40]

Posteriormente, mediante radicado 21 -433282 - - 6 del 29 de abril de 2022, se le requirió a la sociedad investigada lo siguiente: *"(3) Indicar (. . .) si el uso de los datos personales de los titulares para fines estadísticos, a través de Google Analytics o herramientas similares, se encuentra contempladas dentro de las finalidades establecidas en el Política de Tratamiento de Información ("PTI")",* a lo cual le dieron respuesta de la siguiente forma mediante radicado 21-433282 - -15 del 15 de septiembre de 2022: *"(. . .) Avianca no pretende recolectar datos personales de usuarios mediante el uso de esta herramienta, informamos al Despacho que, dentro de las finalidades de la Política para el tratamiento de datos personales de Avianca, se encuentran incluidas las finalidades estadísticas como se evidencia a continuación*[41]*:*



- Ejecutar estudios de mercado, estadísticas, encuestas de satisfacción y/o fines analíticos con el fin de optimizar nuestros productos y servicios.

- Podemos consultar y actualizar tu información personal, para la ejecución de actividades operacionales, analíticas, estadísticas y de evaluación, de acuerdo con tu nivel de interacción y de satisfacción con la calidad de los servicios ofrecidos de acuerdo con tus preferencias de vuelo y/o necesidades por medio de mensajes pop-up y/o encuestas de satisfacción.

Se evidencia entonces, a pesar de que AVIANCA indicó que no busca recolectar información personal de los titulares, y aun teniendo la finalidad para dichos efectos, el lenguaje usado en la PTI resulta muy general con respecto a la implementación del *tracker* DEMDEX, el cual estaba presente para la versión 7.0.15. del aplicativo, llevando al Despacho a concluir, preliminarmente, que el tratamiento de información por parte de AVIANCA mediante esta herramienta informática no tiene el consentimiento de los titulares, pues no informa para ningún efecto que sus datos personales han sido recolectando, incluyendo geolocalización, para efectos desconocidos o comercialización. En ese mismo sentido, no se advierte que se haya informado en las PTI, como en ningún otro documento público, a los titulares que el aplicativo en su versión 7.0.15., y de forma automática, activa permisos de tiempo de ejecución, considerados peligrosos por Google, y tal como se refleja en el radicado 21-433282 - - 12 de noviembre de 2012, y que permiten el acceso a datos y acciones restringidas, por lo cual se recomienda adquirir la autorización del titular bajo los principios de la Privacidad desde el Diseño y por Defecto de transparencia, control, y solicitud mínima de datos. Sin la presencia de estos elementos, en especial el de transparencia, ya que no existe elementos para indicar que estas funciones están siendo accedidas por el aplicativo, y que el titular no tiene control sobre estas, se entiende, preliminarmente que AVIANCA está accediendo a información adicional a la necesaria para ejecutar la finalidad de su aplicativo, lo que indica que, de forma presunta, está ejecutando acciones consideradas fraudulentas para recolectar y tratar información personal de los titulares usuarios de su aplicación.

De esta manera, se concluye que AVIANCA, como responsable del tratamiento de información, presuntamente vulneró el literal (c) del artículo 4 de la Ley 1581 de 2012, y el deber contenido por remisión expresa, en el artículo 4 del Decreto 1377 de 2008.

QUINTO: PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA *(ACCOUNTABILITY)* EN EL TRATAMIENTO DE LOS DATOS PERSONALES (L.1581/12, ART. 26 Y D.1377/13, ART. 26 -Y 27- INCORPORADO EN EL D.1074/13).

La regulación colombiana le impone al Responsable o al Encargado del Tratamiento, la responsabilidad de garantizar la eficacia de los derechos del titular del dato, la cual no puede ser simbólica, ni limitarse únicamente a la formalidad. Por el contrario, debe ser real y demostrable. Al respecto, nuestra jurisprudencia ha determinado que "*existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante*". [42]

Adicionalmente, es importante resaltar que los responsables o encargados del tratamiento de los datos, no se convierten en dueños de los mismos como consecuencia del almacenamiento en sus

[39] Radicado 21- 433282 - - 5 del 9 de abril de 2022, p. 8.
[40] Ibidem, p. 9 -10
[41] Radicaso 21-433282 - -15 del 15 de septiembre de 2022, p. 3.
[42] Corte Constitucional [C.C.] Sentencia T-227/03, M.P. Eduardo Montealegre Lynett, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 12) (Colom.).

bases o archivos. En efecto, al ejercer únicamente la mera tenencia de la información, solo tienen a su cargo el deber de administrarla de manera correcta, apropiada y acertada. Por consiguiente, si los sujetos mencionados actúan con negligencia o dolo, la consecuencia directa sería la afectación de los derechos humanos y fundamentales de los titulares de los datos.

En virtud de lo anterior, el Capítulo III del Decreto 1377 de 27 de junio de 2013 -incorporado en el Decreto 1074 de 2015- reglamenta algunos aspectos relacionados con el principio de responsabilidad demostrada. Por su parte, el artículo 26[43] *-Demostración-* establece que, "*los responsables del tratamiento de datos personales deben ser capaces 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*". Así́, resulta imposible ignorar la forma en que el Responsable o Encargado del Tratamiento debe probar poner en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación. Es decir, se reivindica que un administrador no puede utilizar cualquier tipo de políticas o herramientas para dicho efecto, sino solo aquellas que tengan como propósito lograr que los postulados legales sean realidades verificables, y no solo se limiten a creaciones teóricas e intelectuales. El artículo 27*-Políticas Internas Efectivas-*, exige que los responsables del tratamiento de datos implementen medidas efectivas y apropiadas que garanticen, entre otras: "(*...) 3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, con respecto a cualquier aspecto del tratamiento*."[44]

Con el propósito de dar orientaciones sobre la materia, la Superintendencia de Industria y Comercio expidió el 28 de mayo de 2015 la *"Guía para implementación del principio de responsabilidad demostrada (accountability)*". El término "*accountability"*, a pesar de tener diferentes significados, ha sido entendido en el campo de la protección de datos como el modo en que una organización debe cumplir (en la práctica) las regulaciones sobre el tema, y la manera en que debe demostrar que lo puesto en práctica es útil, pertinente y eficiente.

Conforme con ese análisis, las recomendaciones que trae la guía a los obligados a cumplir la Ley 1581 de 2012, son:

(1) Diseñar y activar un programa integral de gestión de datos (en adelante PIGDP). Esto, exige compromisos y acciones concretas de los directivos de la organización. Igualmente requiere la implementación de controles de diversa naturaleza;

(2) Desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP, y;

(3) Demostrar el debido cumplimiento de la regulación sobre tratamiento de datos personales.

El principio de responsabilidad demostrada *–accountability-* demanda implementar acciones de diversa naturaleza para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El mismo, exige que los responsables y encargados del tratamiento adopten medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia. Dichas acciones o medidas, deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los datos personales.

El principio de responsabilidad precisa menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. Requiere apremiar acciones concretas por parte de las organizaciones para garantizar el debido tratamiento de los datos personales. El éxito del mismo, dependerá del compromiso real de todos los miembros de una organización. Especialmente, de los directivos de las organizaciones, pues, sin su apoyo sincero y

---

[43] D.1377/13, art. 26: El texto completo del artículo 26 del Decreto 1377 de 2013 ordena: *"Demostración. Los responsables del tratamiento de datos personales deben ser capaces 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, en una manera que sea proporcional a lo siguiente: (1) La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente. (2) La naturaleza de los datos personales objeto del tratamiento. (3) El tipo de Tratamiento (4) Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta de las medidas de seguridad apropiadas evidencia sobre la implementación efectiva*

[44] D.1377/13, art. 27: *"Políticas internas efectivas. En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberían garantizar: 1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este decreto. 2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación. 3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento. La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto".*

decidido, cualquier esfuerzo será insuficiente para diseñar, llevar a cabo, revisar, actualizar y/o evaluar los programas de gestión de datos. Adicionalmente, el reto de las organizaciones frente al principio de responsabilidad demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas. Como se ha manifestado, exige que se demuestre el cumplimiento real y efectivo en la práctica de sus funciones.

En este sentido, desde el año 2006 la Red Iberoamericana de Protección de Datos (RIPD) ha puesto de presente que, "*la autorregulación sólo* [sic] *redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que* ***no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales****".*[45] (Énfasis añadido)

El principio de responsabilidad demostrada busca que los mandatos constitucionales y legales sobre tratamiento de datos personales sean una realidad verificable y redunden en beneficio de la protección de los derechos de las personas. Por eso, es crucial que los administradores de las organizaciones sean proactivos respecto del tratamiento de la información. De manera que, por iniciativa propia, adopten medidas estratégicas, idóneas y suficientes, que permitan garantizar: (i) los derechos de los titulares de los datos personales, y; (ii) una gestión respetuosa de los derechos humanos

En el caso de AVIANCA, se le solicitó, mediante los radicados 21-433282 - - 2 del 22 de marzo de 2022[46] y 21 – 433282 - - 6 del 29 de abril de 2022[47], que informara sobre las medidas tendientes al cumplimiento del principio de responsabilidad demostrada, y a lo cual dieron respuesta mediante los radicados 21- 433282 - - 5 del 9 de abril de 2022 y 21-433282 - - 11 del 7 de julio de 2022, en los siguientes términos:

> *"(. . .)* ***Respuesta:*** *Avianca cuenta con un proceso definido para gestionar los riesgos asociados a las leyes de protección de datos personales y se tienen implementadas medidas de seguridad y controles, para proteger la confidencialidad, integridad y disponibilidad de los datos de carácter personal de los Titulares, garantizando los derechos de estos y el cumplimiento regulatorio, mitigando amenazas como: acceso, modificación o eliminación no autorizada de los datos.*
>
> *Este proceso además de asegurar el cumplimiento normativo disminuye los posibles impactos financieros, reputacionales, operacionales y legales que se pueden generar por causa de la materialización de los riesgos. La metodología para gestionar los riesgos se basa en la norma ISO31000 (Contexto, identificación, análisis, valoración, tratamiento, comunicación, monitoreo, registro e informe) y se utiliza para: Riesgos estratégicos, proyectos y terceros. Dichos procesos y procedimientos se tienen documentados en el Manual de Riesgos de la Información, el cual es revisado y actualizado anualmente.*
>
> *De acuerdo con lo anterior, dicho Manual establece tres (3) tipos de riesgos, sobre los cuales se implementan diferentes controles para su mitigación como se evidencia a continuación:*
>
> • ***Riesgos estratégicos:***
> *Los riesgos estratégicos corresponden a los riesgos cuya materialización pueden generar impactos importantes a Avianca afectando el cumplimiento de los objetivos estratégicos del negocio, para este caso particular, se tiene identificado el riesgo de Incumplimiento de las leyes de datos personales.*
>
> *La documentación de los riesgos se realiza en una matriz diseñada de tal forma que cumpla con la metodología establecida y que tenga información suficiente y adecuada. Dicha matriz describe los riesgos asociados a la protección de datos personales de los titulares, las posibles causas y consecuencias en relación con la organización y en relación con los titulares, los controles implementados, la calificación de la probabilidad e impacto, y los planes de acción para los riesgos residuales fuera del apetito de riesgos*

---

[45] Red Iberoamericana de Protección de Datos. Grupo de trabajo temporal sobre autorregulación y protección de datos personales. Mayo de 5 de 2006. En aquel entonces, la RIPD expidió un documento sobre autorregulación y protección de datos personales que guarda cercana relación con "accountability" en la medida que la materialización del mismo depende, en gran parte, de lo que internamente realicen las organizaciones y definan en sus políticas o regulaciones internas.

[46] Radicado 21 – 433282 – 2 del 22 de marzo de 2022: *"(8) Indicar si durante el periodo de diseño, desarrollo y de recolección de datos a través del Portal y la App, se realizó un estudio de impacto de privacidad ("Privacy Impacto Assessment" o "PIA", por sus siglas en inglés). En caso afirmativo, remita copia completa de dicho estudio tanto para el portal, APP, y el chat de inteligencia artificial de WhatsApp; (10) Informe que medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole han implementado para que evitar:(a) Accesos indebidos o no autorizados a la información; (b) Manipulación de la información; (c)Destrucción de la información;(d) Usos indebidos o no autorización de la información,y; (e) Circulación o suministro de la información a personas no autorizadas. (11) Informe si dichas medidas de seguridad son objeto de revisión, evaluación y mejora permanente."*

[47] Radicado 21 – 433282 - - 6 del 29 de abril de 2022: *"(7) Indicar de forma expresa, de acuerdo con la respuesta 9 al primer requerimiento de información, el software y/o el hardware adquirido por AVIANCA para implementar su firewall perimetral, virtual pachanga, identificación de eventos de seguridad, y cyberthreats."*

de Avianca. La periodicidad de revisión es por lo menos semestral o cada vez que se requiera.

Para ilustración del Despacho a continuación allegamos un ejemplo de un riesgo en la matriz:

• ***Riesgos de terceros:***

Avianca cuenta con un proceso para identificar los tipos de contrataciones y los riesgos que estas puedan tener frente al nivel de implementación de medidas técnicas para la protección de datos personales.

En este caso, a los contratos que requieran implementar medidas técnicas para la protección de datos personales, les son incluidos una cláusula en el contrato relacionada con la seguridad de la información y el tratamiento de datos personales, y adicionalmente, se solicita el cumplimiento de las políticas de seguridad de la información para terceros de Avianca, la cual se encuentra publicada en el siguiente enlace:https://www.avianca.com/co/es/sobre-nosotros/informacion-legal/politica-de-privacidad/.

Adicionalmente, Avianca solicita al proveedor el certificado ISO27001 (estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005). En caso de que los proveedores no se encuentren certificados, Avianca pide sus políticas de seguridad y de la información, para hacer una revisión de que los estándares necesarios para la seguridad y tratamiento de los datos personales se encuentren debidamente cumplidos. Al respecto reiteramos que el cumplimiento de este tipo de procedimientos es monitoreado y revisado de forma constante, para actualizar las certificaciones y verificar el ambiente de control de seguridad de la información que tienen los proveedores.

Teniendo en cuenta lo anterior, le hacemos notar al Despacho que la aplicación de estas medidas da cuenta de los análisis de riesgo que se realizan sobre la contratación de proveedores como es el caso de la compañía WebHelp, quien, como se mencionó anteriormente, es el proveedor encargado de prestar los servicios de contact center para Avianca, dentro de los que se encuentra el Chat de respuestas automatizadas de WhatsApp.

Al respecto de este caso particular, le informamos al Despacho que el contrato con este proveedor cuenta con las cláusulas correspondientes en relación a medidas de seguridad de la información y tratamiento de datos personales. Adicionalmente, el proveedor se encuentra certificado en: ISO27001, ISO22301, AOC (PCI-DSS) y SOC 2 Tipo 2, y respondió de manera satisfactoria en el último control y revisión realizado por Avianca, un cuestionario sobre el nivel de cumplimiento de las políticas de Avianca conforme a sus prácticas de tratamiento de datos personales.

Lo anterior, permite tener una seguridad razonable de que el proveedor tiene implementados controles adecuados y suficientes para garantizar la protección de los datos personales, en los diferentes procesos y sistemas que hacen parte de este alcance normativo.

Como Anexo 11 y 12, allegamos los certificados ISO27001, ISO22301, enviados por el proveedor WebHelp, y como Anexo 13 allegamos el Manual de riesgos de la información.

Riesgos en proyectos:

Se tiene establecido que los proyectos o iniciativas de Avianca que incluyan una adquisición, modificación, y/o cambio de un activo de información, deben cumplir con los lineamientos de seguridad de la información y ciberseguridad para mitigar los riesgos y garantizar el cumplimiento normativo en relación con la protección de datos personales. Para esto, Avianca ha implementado un proceso que implica: (i) Contextualización del proyecto (Incluye preguntas de datos personales), (ii) definición de controles aplicables y evidencias a entregar, (iii) calificación del riesgo inherente y residual, y (iv) concepto para el paso a producción.

Para ilustración del Despacho, a continuación, allegamos un ejemplo de los controles aplicados sobre la matriz de riesgo de este tipo de proyectos:

Tema	Evidencia	¿Quién emite la evidencia?	¿Quién revisa la evidencia principal o el cumplimiento del control?
11. TRANSVERSAL	ALMACENAMIENTO Y TRANSFERENCIA DE INFORMACIÓN Evidencias donde se logre identificar los protocolos utilizados para el almacenamiento o transferencia de la información confidencial o sensible. Ejemplo de evidencias: pantalla donde se utilice algoritmos de cifrados utilizados, de la aplicación o línea de comando donde se evidencien los protocolos. CERTIFICADOS DIGITALES - Si es aplicación web expuesta a internet, se debe proporcionar la URL, la cual será sometida al análisis de fortaleza de cifrado, tamaño de la llave, soporte de protocolos. El resultado (rating) del análisis debe ser grado A o B, resultados con grado C,E o F no serán admitidos. - Si se trata de un webservice que no necesariamente este incrustado en una aplicación en internet, proporcionar la pantalla del certificado en donde se muestre los algoritmos de cifrado utilizados. - Informar al área de seguridad operativa, si el certificado será administrado por el proveedor o por AVIANCA para evitar futuras interrupciones del servicio.	Proyecto	Seguridad Operativa
4. EXTERNO - LPDP	Diagrama de Arquitectura de la solución donde se puedan observar los componentes y flujos de los datos	Proyecto	Protección de datos personales
9. INTERNO - LPDP	Diagrama de Arquitectura de la solución donde se puedan observar los componentes y flujos de los datos	Proyecto	Protección de datos personales
4. EXTERNO - LPDP	Soporte suministrado por el proveedor donde se pueda observar que se cumple con el requerimiento, que se pueda observar la leyenda de autorización y el log de la	Proveedor	Protección de datos personales
9. INTERNO - LPDP	Soporte o pantalla de la leyenda de autorización de datos personales y el log donde se pueda observar y almacenar la autorización del titular de los datos.	Proyecto	Protección de datos personales
4. EXTERNO - LPDP	Soporte suministrado por el proveedor donde se pueda observar que se cumple con el requerimiento	Proveedor	Protección de datos personales
9. INTERNO - LPDP	Evidencia de la implementación de la autorización segregada del envío de comunicaciones comerciales	Proyecto	Protección de datos personales
4. EXTERNO - LPDP	Soporte suministrado por el proveedor donde se pueda observar que se cumple con el requerimiento	Proveedor	Protección de datos personales
9. INTERNO - LPDP	Evidencia de la opción de darse de baja para comunicaciones comerciales (Opt-out).	Proyecto	Protección de datos personales

Para las iniciativas o proyectos asociados a los cambios en el portal web de Avianca, en la app o en aplicaciones integradas, se cumple con el proceso establecido (este puede variar respecto a años anteriores, dado la madurez del proceso), siempre y cuando el cambio pueda impactar la seguridad de la información o la protección de datos personales."

(. . .)

Ahora bien, adicional a los procedimientos y controles descritos, y especialmente en atención a implementar medidas para evitar: (i) Accesos indebidos o no autorizados a la información; (ii) Manipulación de la información; (iii) Destrucción de la información; (iv) Usos indebidos o no autorización de la información, y; (v) Circulación o suministro de la información a personas no autorizadas, le hacemos notar al Despacho que Avianca, basada en los principios fundamentales de seguridad de la información como son la confidencialidad, la integridad y la disponibilidad, ha implementado controles de acceso para la autenticación y manejo de roles o perfiles en los sistemas de la organización.

Estos controles tienen como objetivo evitar que personas y/o terceros que no cuenten con la autorización por parte del Titular, o no tengan una justificación de negocio basado en una relación contractual debido a las funciones que desempeña, puedan acceder a la información almacenada en las bases de datos de Avianca. En particular, con el fin de proteger la información personal almacenada en bases de datos, Avianca cuenta con las siguientes medidas de seguridad:

- *Políticas, procedimientos y estándares de seguridad de la información, cuyo objetivo es proteger y preservar la integridad, confidencialidad y disponibilidad de la información y datos personales, independientemente del medio o formato donde se encuentren, de su ubicación temporal o permanente o de la forma en que éstos sean transmitidos.*
- *Implementación de herramientas tecnológicas de seguridad: Firewalls, antivirus, IPS a nivel perimetral y de Endpoint, filtro de correo y de navegación.*
- *Implementación de prácticas de seguridad reconocidas en la industria, que incluyen: transmisión y almacenamiento de información sensible a través de mecanismos seguros, tales como cifrado, uso de protocolos seguros, aseguramiento de componentes tecnológicos, restricción de acceso a la información sólo a personal autorizado, respaldo de información, monitoreo de eventos de seguridad.*
- *Controles de acceso como implementación de mecanismos de autenticación en los diferentes componentes tecnológicos (aplicaciones, servidores, bases de datos), configuración de roles y perfiles basado en el principio del mínimo privilegio, implementación de políticas de seguridad para el establecimiento de contraseñas seguras, configuración de parámetros para el manejo del tiempo de inactividad de usuarios y sesiones, y procedimientos para la gestión de usuarios y accesos que incluyen, la creación, modificación y baja de los mismos.*
- *Así mismo, los terceros contratados por Avianca y que traten información personal de los Titulares en calidad de Encargados, están igualmente obligados a adherirse y dar cumplimiento a las Políticas, Manuales de seguridad de la información, así como a los protocolos de seguridad establecidos, tal como se mencionó en la respuesta 8 del presente requerimiento.*

Adicionalmente, le informamos al Despacho que Avianca cuenta con las siguientes herramientas específicas de seguridad aplicadas a lo largo de toda su operación, con el fin de garantizar la seguridad de la información personal de los Titulares en los términos descritos anteriormente:

- ***Firewall Perimetral**: el firewall de perímetro es un componente transversal con capacidades de detección y prevención de intrusos, que actúa como primer filtro de protección de ataques desde internet hacia la infraestructura interna de la compañía, controla el acceso a los sistemas de información. Este firewall se encuentra licenciado, con mantenimiento y soporte vigente.*
- ***Herramienta de seguridad (Virtual Patching)**: esta es una herramienta que se encuentra instalada en los servidores, y que actúa como escudo virtual a nivel de máquina. Es una solución cuyos objetivos son: mantener los servidores y endpoints con algún grado de obsolescencia tecnológica protegidos, y con actualizaciones de seguridad aplicados, de acuerdo con las liberaciones de los fabricantes.*
- ***Monitoreo de eventos de seguridad**: la compañía cuenta con un SOC (Security Operation Center) el cual opera con disponibilidad 7X24, vigilando eventos de seguridad que se puedan presentar en los servicios de TI.*
- ***Cyberthreats**: es un servicio cuya finalidad es monitorear el uso de las marcas, nombres comerciales, enseñas y demás, cuyos Titulares son las compañías integradas bajo AVH (tales como "Avianca", "LifeMiles", entre otros). Adicionalmente, este servicio está inmerso en Internet, la deep y la dark web, validando información de la compañía que pudiera estar siendo utilizada por terceros no autorizados para fines inescrupulosos.*
- ***Controles de seguridad definidos e implementados en procesos y procedimientos de operación, tales como**: gestión de accesos, contraseñas, tanto en contratación de terceros como frente a colaboradores, atenciones incidentes de seguridad y privacidad, gestión de vulnerabilidades y aseguramiento de plataformas, entre otros.*

- ***Políticas y concientización****: las compañías integradas bajo Investment Vehicle 1 Limited cuentan con Políticas de Privacidad para el Tratamiento de Datos Personales y Manual, así como Política de Seguridad de la Información.*

Finalmente, hacemos notar al Despacho que Avianca informa a los Titulares de los datos personales la forma en que sus datos personales son protegidos en la política de privacidad. Al respecto el numeral 3.11 de dicha política indica:

"3.11 ¿CÓMO PROTEGEMOS TUS DATOS PERSONALES?

La protección, seguridad y confidencialidad de la información y datos personales de los Titulares de la información es de vital importancia para las Compañías. Las Compañías cuentan con políticas, procedimientos y estándares de seguridad de la información, los cuales podrán cambiar en cualquier momento a discreción de las Compañías, y cuyo objetivo es proteger y preservar la integridad, confidencialidad y disponibilidad de la información personal, independientemente del medio y/o formato donde se encuentren almacenados o ubicados, de forma temporal o permanente, así como en la forma en que éstos sean transmitidos. En este sentido, nos apoyamos en herramientas tecnológicas de seguridad e implementamos prácticas de seguridad reconocidas en la industria, que incluyen: transmisión y almacenamiento de información a través de mecanismos seguros, tales como cifrado, uso de protocolos seguros, aseguramiento de componentes tecnológicos, restricción de acceso a la información sólo a personal autorizado, respaldo de información, prácticas de desarrollo seguro de software, Firewalls, antivirus, IPS entre otros.

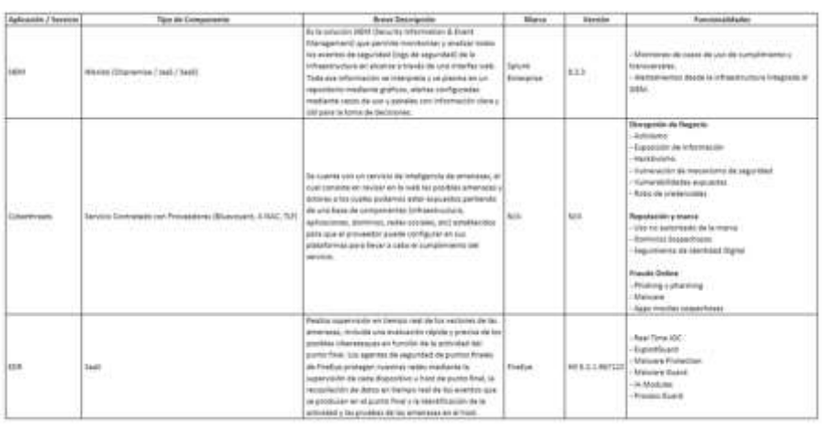
Los terceros contratados por las Compañías (contratistas, consultores externos, colaboradores temporales, etc.) que involucre Tratamiento de información personal de Clientes, Viajeros y Usuarios están igualmente obligados a adherirse y dar cumplimiento a la presente Política de Privacidad, los Manuales de seguridad y privacidad de la información y los protocolos de seguridad de las Compañías Todo contrato de las Compañías con un tercero y/o proveedor (contratistas, consultores externos, colaboradores temporales, etc.) en el que exista Tratamiento de datos personales incluye un acuerdo de confidencialidad y/o Anexo que detalla los compromisos y obligaciones para la protección, cuidado, seguridad y preservación de la confidencialidad, integridad y privacidad de la información personal.

Recuerda que como Titular de la información tú también cumples con un rol en la protección de la información personal, por lo tanto te recordamos que dentro de tus deberes como Titular se encuentran entre otros el de el de no compartir ninguno de tus datos personales (número de reserva, contraseña, número de tiquete, entre otros) con personas no autorizadas para acceder a ellos, mantener un nivel de seguridad adecuado en tus dispositivos electrónicos, evitando que la información que en ellos almacenes sea consultada, modificada y/o sustraída por personas no autorizadas. Las Compañías no asumen ninguna responsabilidad frente a los cambios en los niveles de seguridad indicados por el propietario de sus dispositivos electrónicos".

(. . .)

Respuesta: A continuación, allegamos una tabla en donde se indica cada sistema utilizado por Avianca para implementar el Firewall Perimetral, virtual patching, identificación de eventos de seguridad ("SIEM"), y cyberthreats, con su respectiva Marca, Versión y Funcionalidad:

Servicio	Marca	Version	Funcionalidad
Firewall Perimetral Orgnanisa	Check Point	R80.20 - R80.40	Brindar protección perimetral para todos las oficinas de Avianca Group y sus respectivos Data Centers de SAL, BOG, CEO, MIA, MDE. Las funcionalidades incluidas son: Antimalware, Antibot, AppControl, URL Filtering, DoS, Firewall
Firewall Perimetral Cloud	Check Point	R80.10	Brindar protección perimetral par Infraestructura alojada en Azure en arquitectura de anillo core. Las funcionalidades incluidas son: Firewall
Firewall Perimetral Cloud	Palo Alto	8.1.8	Brindar protección perimetral par Infraestructura alojada en Azure en arquitectura de anillo externo (borde). Las funcionalidades incluidas son: Firewall, Antimalware, URLFiltering, Antibot, DoS, App Control
Virtual Patching	Trend Micro	20.0.393	Protección a Infraestructura EOL, modulos activos: HIPS, Firewall



Aplicación / Servicio	Tipo de Componente	Breve Descripción	Marca	Versión	Funcionalidades
SIEM	Máquina (Diagnóstico / SaaS / SaaS)	En la solución SIEM (Security Information & Event Management) que permite monitorizar y analizar todos los eventos de seguridad (logs de seguridad) de la infraestructura en alcance a través de una interfaz web. Toda esa información se interpreta y se plasma en un repositorio mediante gráficos, alertas configuradas mediante casos de uso y paneles con información clara y útil para la toma de decisiones.	Splunk Enterprise	8.2.3	- Monitoreo de casos de uso de cumplimiento y transversales. - Alertamiento desde la infraestructura integrada al SIEM.
Ciberamenazas	Servicio Contratado con Proveedores (Bluevoyant, X-MAC, TLP)	Se cuenta con un servicio de inteligencia de amenazas, el cual consiste en revisar en la web las posibles amenazas y ataques a los cuales podamos estar expuestos partiendo de una base de componentes (infraestructura, aplicaciones, dominios, redes sociales, etc) establecidos para que el proveedor pueda configurar en sus plataformas para llevar a cabo el cumplimiento del servicio.	N/A	N/A	**Disrupción de Negocio:** - Activismo - Exposición de información - Hacktivismo - Vulneración de mecanismo de seguridad - Vulnerabilidades explotadas - Robo de credenciales **Reputación y marca:** - Uso no autorizado de la marca - Dominios typosquatters - Seguimiento de identidad digital **Fraude Online** - Phishing y pharming - Malware - Apps moviles maliciosas
EDR	SaaS	Realiza supervisión en tiempo real de las acciones de las amenazas, incluida una evaluación rápida y precisa de los posibles interesados en función de la actividad del punto final. Los agentes de seguridad de puntos finales de FireEye protegen nuestras redes mediante la supervisión de cada dispositivo o host de punto final, la recopilación de datos en tiempo real de los eventos que se producen en el punto final y la identificación de la actividad y las pruebas de las amenazas en el host.	FireEye	M.S.1.1.867122	- Real Time IOC - ExploitGuard - Malware Protection - Malware Guard - IA Modules - Process Guard

Así las cosas, lo expuesto por parte de AVIANCA es, *prima facie*, indicio que esta compañía cumple el principio de responsabilidad demostrada establecido por el Régimen General de Protección de Datos; sin embargo, es necesario traer a colación el mandato que trae el artículo 26 del Decreto 1377 de 2013 -incorporado D.1074/13- sobre la implementación de medidas efectivas para el cumplimiento de las obligaciones de la ley 1581 de 2012, puesto que las medidas implementadas por parte de AVIANCA: (i) Manual para la Protección de Datos Personales; (ii) Manual General de Seguridad de la Información; (iii) Manual de Lineamientos Específicos de Seguridad de la Información; (iv) Controles de seguridad aplicados por Avianca; (v) Flujo de los procedimientos Avianca;(vi) Manual de Riesgos de la Información; (vii) Procedimiento para ejecución de análisis de vulnerabilidades; (viii)

Procedimiento de monitoreo y gestión de alertas de seguridad de la información y ciberseguridad, y; (ix) Manual General de Monitoreo de Seguridad y Cumplimiento; no son efectivas para la protección de los datos personales de los titulares de los titulares usuarios del aplicativo Avianca para la plataforma Android, ya que se implementó el uso de permisos y tracker que ponen en riesgo los datos personales de los titulares, por lo que se ven reducidos a una mera declaración retórica simbólica, limitada al cumplimiento de una formalidad.

También es necesario advertir que la remisión de las certificaciones ISO 22301 y 27001 de los proveedores de AVIANCA, no son prueba del cumplimiento propio del principio de responsabilidad demostrada, sino el de un tercero, lo cual pone más en evidencia que las medidas expuestas resultan inefectivas, puesto, como ya se comentó, de ser efectivas, no se hubiese puesto en riesgo la información personal de los titulares de AVIANCA con la implementación de 15 permisos sin la autorización de los titulares, 6 de ellos que ponen en riesgo la información personal y sensible de estos, y la implementación de 1 tracker que permite, nuevamente, sin la autorización de los titulares, por ausencia de una finalidad que permita inferir este tipo de tratamiento, la perfilación del titular para efectos que tampoco es previsible de acuerdo con la autorización originalmente otorgada.

En suma, AVIANCA, de conformidad con lo anteriormente enunciado, y de forma aparente, AVIANCA no cumple con el Principio de Responsabilidad Demostrada establecido por el Régimen General de Protección de Datos en Colombia.

SEXTO: Con el fin de determinar si es procedente o no imponer una de las sanciones establecidas en el artículo 23 de la ley 1581 de 2012 o impartir las órdenes necesarias para hacer efectivo el derecho de habeas data tal como lo menciona el literal b) del artículo 21 de la norma en mención en ejercicio de la función otorgada a esta Superintendencia, que expresamente señalan:

> ***"ARTÍCULO 23. SANCIONES.*** *La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:*
>
> *a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;*
> *b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;*
> *c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;*
> *d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;*
>
> ***PARÁGRAFO.*** *Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva."*
>
> *"**ARTÍCULO 21. FUNCIONES.*** *La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:*
>
> *b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;"*

SÉPTIMO: Que, la L.1955/19, art. 49[48] señala que el *"(a) partir del 1º de enero de 2020, todos los cobros, sanciones, multas, tasas, tarifas y estampillas, actualmente denominados y establecidos con base en el salario mínimo mensual legal vigente, SMMLV, deberán ser calculados con base en su equivalencia en términos de la unidad de valor tributario, UVT. En adelante, las actualizaciones de estos valores también se harán con base en el valor de la UVT vigente.*

De esta manera y de conformidad con la norma antes señalada, si el valor de los cobros, sanciones o multas se encuentran establecidos en salarios mínimos, estos deberán ser calculados con base en su equivalencia en términos de la unidad de valor tributario UVT. Por lo cual, las multas de carácter personal e institucional dispuestas en la L.1581/12, serán determinadas de la siguiente manera:

$$\frac{SMMLV}{\text{UVT vigente 2023}} = SMMLV\ expres \quad \boxed{Multa\ en\ UVT}$$

$$SMMLV\ expresado\ en\ UVT´S * Número\ de\ SMMLV\ a\ convertir = Sanción\ expresada\ en\ UVT´S$$

OCTAVO: Que con el fin de garantizar los derechos fundamentales la sociedad comercial **AEROVÍAS DEL CONTINENTE AMERICANO S.A.** -pudiendo usar las siglas AVIANCA o AVIANCA S.A.- con NIT. 890.100.577 - 6, esta Dirección ha concedido el acceso al presente Expediente digital a esta, por intermedio de su apoderado y/o representante legal al correo electrónico: notificaciones@avianca.com, quienes deben registrarse en calidad de persona natural, exclusivamente con los datos en mención, en el enlace https://servicioslinea.sic.gov.co/servilinea/ServiLinea/Portada.php.

[48] "Por el cual se expide el Plan Nacional de Desarrollo 2018-2022"

En caso de que la sociedad requiera un acceso adicional de consulta del Expediente, deberá dirigir su solicitud en tal sentido desde el correo electrónico de notificación judicial de la sociedad, a los correos electrónicos contactenos@sic.gov.co y habeasdata@sic.gov.co, indicando los nombres y números de identificación de las personas autorizadas, **acreditando para dicho efecto los debidos poderes y/o autorizaciones, según corresponda.**

Si tienen alguna duda o presentan algún inconveniente para la consulta del expediente o requiere más información relacionada con la Protección de Datos Personales, favor comunicarse con el contact center (601) 592 04 00, para que la misma sea atendida en el menor tiempo posible.

En mérito de lo expuesto, esta Dirección

RESUELVE

ARTÍCULO PRIMERO: ABRIR INVESTIGACIÓN y en consecuencia **FORMULAR PLIEGO DE CARGOS** contra de la sociedad comercial **AEROVÍAS DEL CONTINENTE AMERICANO S.A.** -pudiendo usar las siglas AVIANCA o AVIANCA S.A.- con NIT. 890.100.577 - 6, por la presunta contravención de lo dispuesto en:

- **CARGO PRIMERO:** La presunta vulneración, en su calidad de Responsable, del principio de finalidad contenido en el literal (b) del artículo 4 la Ley 1581 de 2012, en concordancia con el deber de informar debidamente sobre la finalidad de la recolección y de los derechos que le asisten por virtud de la autorización otorgada de conformidad con el literal (c) del artículo 17 de la Ley 1581 de 2012.

- **CARGO SEGUNDO:** La presunta vulneración, en su calidad de Responsable, del principio de seguridad contenido en el literal (g) del del artículo 4 la Ley 1581 de 2012 en concordancia con el deber de conservar la información la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de conformidad con el literal (c) del artículo 17 de la Ley 1581 de 2012.

- **CARGO TERCERO:** La presunta vulneración, en su calidad de Responsable, del principio de libertad contenido en el literal (c) del del artículo 4 la Ley 1581 de 2012 y el deber de abstenerse de utilizar medios engañosos para recolectar y realizar el tratamiento de datos personales de conformidad con el Decreto 1377 de 2013, artículo 4 -incorporado en el Decreto 1074 de 2015- .

ARTÍCULO SEGUNDO: NOTIFICAR personalmente el contenido de la presente resolución a la sociedad comercial **AEROVÍAS DEL CONTINENTE AMERICANO S.A.** Avianca pudiendo usar las siglas AVIANCA o AVIANCA S.A.- con NIT. 890.100.577 - 6, para que dentro de los **QUINCE (15)** días hábiles siguientes a la notificación del presente acto, rinda descargos y aporte o solicite las pruebas que pretenda hacer valer dentro del trámite radicado con el número **21 - 433282.**

PARÁGRAFO: En caso de no ser posible la notificación personal al cabo de los **CINCO (5)** días del envío de la comunicación, esta se hará por medio de aviso que se remitirá a la dirección, al número de fax o al correo electrónico que figuren en el expediente o puedan obtenerse del registro mercantil, acompañado de copia íntegra del acto administrativo, de conformidad con lo dispuesto en el artículo 69 de la Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo).

ARTÍCULO TERCERO: ADVERTIR a la investigada que el reconocimiento o aceptación expresa de la presunta infracción antes de la imposición de la sanción a que hubiere lugar, será tenido en cuenta como criterio de atenuación de la responsabilidad al momento de la graduación de las sanciones a imponer conforme a lo dispuesto en el literal f) del artículo 24 de la Ley 1581 de 2012.

ARTÍCULO CUARTO: Para el adelantamiento de la presente investigación, se ordena que, junto con los descargos y las pruebas aportadas, la investigada deberá remitir copia de los estados financieros específicamente, el Balance General y Estado de Pérdidas y Ganancias de los últimos **TRES (3)** años. El referido documento deberá estar suscrito por el Representante Legal y el Revisor Fiscal o por contador público debidamente acreditado, según sea el caso.

ARTÍCULO QUINTO: Contra la decisión contenida en el presente acto administrativo no procede recurso alguno, en los términos del artículo 47 de la Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo).

ARTÍCULO SEXTO: La Superintendencia de Industria y Comercio se permite recordar que los canales habilitados para que los investigados ejerzan sus derechos, den respuesta a requerimientos, interpongan recursos, entre otros, son:

- Correo Superintendencia de Industria y Comercio: contactenos@sic.gov.co

- Sede Principal: Avenida Carrera 7 número 31a - 36, piso 3 y 3ª en la Ciudad de Bogotá de lunes a viernes de 8:00 a.m. a 4:30 p.m.

NOTIFÍQUESE Y CÚMPLASE
Dada en Bogotá D. C., 11 NOVIEMBRE 2022

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE SALAZAR MUNOZ
Firmado digitalmente por CARLOS ENRIQUE SALAZAR MUNOZ
Fecha: 2022.11.11 10:42:07 -05'00'

CARLOS ENRIQUE SALAZAR MUÑOZ

Proyectó: JATS
Revisó: CESM
Aprobó: CESM

NOTIFICACIÓN:

Investigados:

Entidad:	Aerovías del Continente Americano S.A. Avianca pudiendo utilizar las siglas AVIANCA o AVIANCA S.A.
Identificación: NIT.:	890.100.577- 6
Representante Legal:	Ana María Ceballos García
Identificación: C.C. No.	34.561.552
Dirección:	Calle 77B número 57 – 103, piso 21 – Ed. Green Towers
Ciudad:	Barranquilla – Atlántico
Correo electrónico:	notificaciones@avianca.com