REPÚBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 21478 --- DE 2019

(17 JUN 2019)

Por la cual se imparten órdenes dentro de una actuación administrativa

Radicación 19-40311

VERSIÓN PÚBLICA

EL DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES

En ejercicio de sus facultades legales, en especial las conferidas por los artículos 19 y 21 de la Ley 1581 de 2012 y el artículo 17 del Decreto 4886 de 2011, y

CONSIDERANDO

PRIMERO: Que el inciso 2° del artículo 2° de la Constitución Política de Colombia establece que "*(l)as autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares*".

SEGUNDO: Que el artículo 15 de la Constitución Política de Colombia reconoce bajo la categoría de derecho fundamental la facultad de todas las personas de "*conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas*" y, en relación con el aludido derecho, establece que *"(e)n la recolección, Tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución*".

TERCERO: Que el Congreso de la República de Colombia, en desarrollo del derecho fundamental reconocido en el artículo 15 de la Constitución Política, expidió la Ley Estatutaria 1581 de 2012 "*(p)or la cual se dictan disposiciones generales para la protección de datos personales*".

CUARTO: Que los principios y disposiciones contenidos en la Ley Estatutaria 1581 de 2012 se aplican: i) "*a los datos personales registrados en cualquier base de datos que los haga susceptibles de Tratamiento por entidades de naturaleza pública o privada*"[1] y ii) "*al Tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales*"[2].

En lo que respecta al Tratamiento de datos personales de individuos residentes en el país, realizado, en parte, en un tercer país, la Corte Constitucional, a quien en Colombia "*se le confía la guarda de la integridad y supremacía de la Constitución*"[3], en Sentencia C-748 de 2011[4], fue clara y específica al indicar que el Régimen Colombiano de Protección de Datos Personales (Ley Estatutaria 1581 de 2012) aplica a todo tipo de Tratamiento, aunque parte del mismo ocurra precisamente fuera de las fronteras, o hace uso de equipos situados en Colombia y sobre ellos. Al respecto, precisó la Corte:

> "*Para la Sala, esta disposición se ajusta a la Carta, pues amplía el ámbito de protección a algunos Tratamientos de datos personales que ocurren fuera del territorio nacional, en virtud del factor subjetivo. En un mundo globalizado en el que el flujo transfronterizo de datos es constante, la aplicación extraterritorial de los estándares de protección es indispensable para garantizar la protección adecuada de los datos personales de los residentes en Colombia, pues muchos de los Tratamientos, en virtud de las nuevas tecnologías, ocurren precisamente fuera de*

---

[1] Cfr. Ley 1581 de 2012, art. 2.
[2] Ibidem.
[3] Cfr. Constitución Política, art. 241.
[4] Cfr. Corte Constitucional. Sentencia C-748 de 2011. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

las fronteras. Por tanto, para la Sala se trata de una medida imperiosa para garantizar el derecho al habeas data"[5].

QUINTO: Que para los efectos de la Ley Estatutaria 1581 de 2012 se entiende por dato personal "*(c)ualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables*"[6] y por Tratamiento "*(c)ualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión*"[7].

SEXTO: Que a partir de las anteriores consideraciones se infiere que la Ley Estatutaria 1581 de 2012 se aplica a cualquier operación que se realice sobre piezas de información vinculadas o que puedan asociarse a personas naturales residentes o domiciliadas en la República de Colombia por parte, por ejemplo, de desarrolladores de Aplicaciones Móviles, aunque su sede principal no se encuentre en el territorio colombiano y aun cuando parte del Tratamiento[8] se efectué fuera del mismo.

Al respecto, es menester tener presente que en la actualidad buena parte del Tratamiento de los datos personales se realiza a través de Internet lo que facilita, a modo de ejemplo, que en el territorio colombiano se recolecte la información y fuera del mismo los datos se procesen o usen.

No obstante, ello no significa que por ese fenómeno tecnológico desaparezca la obligación de las organizaciones que operan globalmente de cumplir las normas locales, garantizar, de una manera efectiva y completa, el derecho a la protección de los datos personales y de respetar los derechos humanos, no solo porque parte del Tratamiento se realiza en territorio nacional, sino porque una interpretación distinta podría constituirse en un desconocimiento a la soberanía de los Estados, quienes están facultados para determinar los estándares para la protección de los derechos de sus residentes[9] y, aún más grave, se restringiría el derecho que tiene todo ciudadano a que en la recolección, tratamiento y circulación de sus datos personales cumpla con lo dispuesto en el artículo 15 de la Constitución Política y la Ley 1581 de 2012, "Régimen General de Protección de Datos Personales", como se explicó en detalle párrafos anteriores.

En este sentido, la Corte Constitucional de Colombia ha precisado que "***en Internet (...) puede haber una realidad virtual pero ello no significa que los derechos, en dicho contexto, también lo sean***. *Por el contrario, no son virtuales:* ***se trata de garantías expresas por cuyo goce efectivo en el llamado 'ciberespacio' también debe velar el juez constitucional***"[10] e, igualmente, ha recalcado que *"nadie podría sostener que, por tratarse de Internet, los usuarios sí pueden sufrir mengua en sus derechos constitucionales*" [11] (Negrita y subrayado fuera del texto original).

Como se observa, las actividades que se realicen a través de internet deben ser respetuosas de los derechos humanos y de las normas de cada país, incluidas las de la República de Colombia, porque internet no puede ser un escenario que avale la impunidad o una herramienta para eludir o sustraerse del cumplimiento de aquellas.

SÉPTIMO: Que el artículo 19 de la Ley 1581 de 2012 ordena a la Superintendencia de Industria y Comercio (SIC), como autoridad de protección de datos personales, ejercer vigilancia "*para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley*".

OCTAVO: Que con sujeción a lo establecido en el artículo 21 de la Ley 1581 de 2012, le corresponde a la Superintendencia de Industria y Comercio (SIC) "*impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables*[12] *del Tratamiento y Encargados del Tratamiento a las disposiciones previstas*"[13] en la ley. Adicionalmente, la SIC también puede "*adelantar las investigaciones del caso, de oficio o a petición*

---

[5] Cfr. Corte Constitucional. Sentencia C-748 de 2011. Consideración 2.4.4.
[6] Ibídem, art. 3), literal c).
[7] Ibídem, art. 3), literal g).
[8] Cfr. Ley 1581 de 2012, artículo 3, literal g. "**Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión."
[9] Cfr. Constitución Política, art. 9.
[10] Cfr. Corte Constitucional. Sentencia C-1147/2001. M.P: Manuel José Cepeda Espinosa. Consideración 3. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2001/C-1147-01.htm
[11] Ibídem.
[12] Cfr. Ley 1581 de 2012, artículo 3°, literal e). "**Responsable del Tratamiento:** 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"
[13] Cfr. Ley 1581 de 2012, art. 21, literal d).

de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de habeas data"[14].

NOVENO: Que el artículo 4° de la Ley 1581 de 2012 preceptúa que en el desarrollo, interpretación y aplicación de la aludida ley deberán aplicarse los principios de: i) legalidad; ii) finalidad; iii) libertad; iv) veracidad o calidad; v) transparencia; vi) acceso y circulación restringida; v) seguridad; y, vi) confidencialidad.

En relación a los principios referidos, la Corte Constitucional sostiene lo siguiente:

> *"Para la Corte, el tratamiento de datos, si bien es imprescindible para el normal desarrollo de múltiples ámbitos de la vida social, puede lesionar derechos fundamentales. En consecuencia, tanto en la jurisprudencia como en el ámbito internacional se han fijado una serie de principios para la administración de datos personales, que como mandatos de optimización, tiendan a facilitar la labor de ponderación entre las prerrogativas constitucionales en tensión.*
>
> *(...)*
>
> *Estos principios, buscan impedir el uso abusivo y arbitrario de la facultad informática. Así mismo, deben ser interpretados en concordancia con el segundo inciso del artículo 15 de la Carta, que establece que '(e)n la recolección, tratamiento y circulación de los datos se respetarán la libertad y demás garantías consagradas en la Constitución'.*
>
> *Es decir, el artículo 4 de la Ley Estatutaria define el contexto axiológico dentro del cual debe moverse, el proceso informático. Según este marco general, existen unos parámetros generales que deben ser respetados para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo"*[15].

DÉCIMO: Que el principio de legalidad[16] exige que el Tratamiento de datos personales se realice de la manera que lo indique la ley y sus normas reglamentarias. Por lo tanto, el Tratamiento es una actividad reglada que debe sujetarse lo establecido por la regulación de la República de Colombia.

DÉCIMO PRIMERO: Que el principio de acceso y circulación restringida[17] le otorga el poder a las personas naturales a decidir quiénes pueden acceder a su información personal.

DÉCIMO SEGUNDO: Que el principio de seguridad[18] exige que la información personal sujeta a Tratamiento se maneje con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a esos registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Esto significa que, por regla general, todas las organizaciones que tratan datos personales deben contar con mecanismos de seguridad robustos, ya sea dentro de su organización y cuando o a través de proveedores de servicios externos con la experiencia adecuada. Esto debe incluir mecanismos para: identificar con precisión y rapidez las vulnerabilidades que necesitan corrección; implementar las correcciones adecuadas para que las vulnerabilidades que se presenten se corrijan de forma expedita; y verificar que las vulnerabilidades hayan sido corregidas.

DÉCIMO TERCERO: Que los datos personales pueden ser recogidos de diferentes fuentes, entre ellas: formularios, cookies, aplicaciones móviles, sitios web, redes sociales, registros públicos, programas de fidelización de clientes, etc., y de la siguiente manera: (i) datos personales suministrados directamente por los individuos; (ii) datos personales recolectados como un requisito de un servicio; (iii) datos personales recolectados en cumplimiento de un requisito legal; (iv) datos personales recopilados automáticamente con el uso de un servicio o producto (por ejemplo, datos de transacciones, dirección IP, datos de ubicación); (v) datos personales inferidos mediante el

---

[14] Ibídem, literal b).
[15] Cfr. Corte Constitucional. Sentencia C-748/2011. M.P: Jorge Ignacio Pretelt Chaljub. Consideración 2.6.3.
[16] Ley 1581 de 2012, artículo 4°, literal a). "***Principio de legalidad en materia de Tratamiento de datos:*** *El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen; (...)*".
[17] Ley 1581 de 2012, artículo 4°, literal f). "***Principio de acceso y circulación restringida****: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley; (...)*".
[18] Ley 1581 de 2012, artículo 4°, literal g). "***Principio de seguridad:*** *La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;*"

procesamiento y análisis de los datos suministrados por los individuos o recopilados con el uso del servicio o producto. Dichos datos pueden contener información sobre los intereses, redes, hábitos y comportamientos de los individuos.

DÉCIMO CUARTO: Que por la cantidad y sensibilidad de la información personal que es recolectada en el mundo en línea o en el ciberespacio mediante diversos mecanismos, proceso o tecnologías, la Corte Constitucional en Sentencia C-748 de 2011 subrayó el deber de los proveedores de servicios de redes sociales digitales de reforzar sus medidas de seguridad para proteger la información personal de las personas naturales, pues, según la Corte, "*el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre*"[19].

DÉCIMO QUINTO: Que de conformidad con el último informe publicado por el Departamento Nacional de Estadística (Dane)[20], Colombia registra una población de 45.5 millones de personas, convirtiéndose en el segundo país con mayor población en América del Sur y el tercero en Latinoamérica, en este caso, después de Brasil y México, respectivamente.

DÉCIMO SEXTO: Que según una publicación del director del Departamento Nacional de Planeación Nacional, Colombia para el año 2035 tendrá un estimado de 57,5 millones de habitantes y para el año 2050 la cifra subirá a 61,1 millones[21].

Adicionalmente, progresivamente ha incrementado el número de personas con acceso a internet.

DÉCIMO SÉPTIMO: Que, en lo atinente al Tratamiento de datos personales a través de aplicaciones móviles, esta Dirección considera necesario realizar las siguientes consideraciones:

17.1. Concepto de "Aplicación Móvil"

17.1.1. Una Aplicación Móvil (o una "App") es un programa de software que está diseñado estructuralmente para ejecutarse en un teléfono inteligente (tableta o cualquier otro dispositivo inteligente)[22]. En las fases del diseño, los desarrolladores deciden la medida en que la aplicación accederá y procesará las distintas categorías de datos personales en el dispositivo y/o a través de recursos informáticos remotos (unidades informáticas de los desarrolladores o de terceros)[23].

17.1.2. Una aplicación móvil sirve para una amplia gama de fines como son la navegación en Internet, las comunicaciones (por ejemplo: correo electrónico, telefonía y mensajería), el entretenimiento (juegos, películas o vídeo, y música), las redes sociales, la banca y los servicios basados en la geo-localización[24]. Además, según el informe presentado por la Comisión Federal de

---

[19] Cfr. Ibídem. Consideración. 2.6.5.2.7. "***Principio de seguridad: "Al amparo de este principio, la información sujeta a Tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento***. *De este principio se deriva entonces la responsabilidad que recae en el administrador del dato. El afianzamiento del principio de responsabilidad ha sido una de las preocupaciones actuales de la comunidad internacional, en razón del efecto "diluvio de datos", a través del cual día a día la masa de datos personales existente, objeto de Tratamiento y de ulteriores transferencias, no cesa de aumentar.* ***Los avances tecnológicos han producido un crecimiento de los sistemas de información, ya no se encuentran sólo sencillas bases de datos, sino que surgen nuevos fenómenos como las redes sociales, el comercio a través de la red, la prestación de servicios, entre muchos otros. Ello también aumenta los riegos de filtración de datos, que hacen necesarias la adopción de medidas eficaces para su conservación. Por otro lado, el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre*** *En estos términos, el* ***responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Así, 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". Existe entonces un deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria***." (Negrillas y subrayado fuera del texto original).

[20] Cfr. Departamento Nacional de Estadística (Dane). en: https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/censo-nacional-de-poblacion-y-vivenda-2018/cuantos-somos Consultada el 4 de marzo de 2019.

[21] Cfr. Revista Dinero, En 2050 en Colombia habrá 61,1 millones de habitantes, en http://www.atlasexpansionurbanacolombia.org/ y en: http://www.atlasexpansionurbanacolombia.org/ Consultada el 5 de marzo de 2019.

[22] Cfr. Office of the Information Commissioner of Queensland, Australia, "Privacy and Mobile Apps.", en: https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/privacy-and-mobile-apps. Consultada el 23 de abril de 2019.

[23] Cfr. Grupo de Trabajo del Artículo 29 (Hoy Comité Europeo de Protección de Datos Personales). "Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes.", en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_es.pdf. Consultada el 27 de febrero de 2019.

[24] Ibídem.

Comercio de los Estados Unidos de América, los desarrolladores de aplicaciones móviles integran códigos de terceros para facilitar la publicidad o el análisis dentro de una aplicación[25].

17.1.3. Una aplicación móvil puede recolectar grandes cantidades de datos de carácter personal. Entre ellos, pero no limitado a:

a) Información que es suministrada directamente por la persona cuando ella se registra en la aplicación móvil (por ejemplo: dirección de correo electrónico, nombre de usuario y contraseña, número de teléfono, fecha de nacimiento).

b) Información que se encuentra almacenada en el dispositivo de la persona cuando ella accede la aplicación móvil[26] (por ejemplo: libreta de direcciones y lista de contactos, registros de llamadas, uso de datos de internet, datos del calendario, fotografías, datos sobre la ubicación del dispositivo, los identificadores únicos del dispositivo, etc.[27]).

La Dirección precisa, en este punto, que los dispositivos inteligentes[28] están diseñados para que sus sistemas operativos, entre ellos: Apple's iOS, Google's Android, RIM's BlackBerry OS, estén abiertos a las aplicaciones móviles a través de interfaces de programación de aplicaciones ("APIs", por sus siglas en inglés). Sobre este punto, el Comité Europeo de Protección de Datos (antes Grupo de Trabajo del Artículo 29) precisó lo siguiente:

> "*Gracias a las API, los desarrolladores de aplicaciones pueden recoger esos datos de forma continua, acceder a los datos de contacto y registrarlos, enviar mensajes electrónicos, SMS o de redes sociales, leer, modificar o borrar el contenido de las tarjetas SD, grabar sonido, utilizar las cámaras y acceder a imágenes almacenadas, leer el estado y la identidad del teléfono, modificar los parámetros del sistema global y evitar que el teléfono entre en reposo. Las API también pueden proporcionar información sobre el propio dispositivo mediante uno o varios identificadores únicos e información sobre otras aplicaciones instaladas*"[29].

c) Información que está relacionada con las actividades de la persona cuando ella utiliza la aplicación móvil (por ejemplo: historial del uso de la Aplicación, datos de tráfico y localización).

d) Información que es creada por la aplicación móvil con base en los datos que la persona le ha proporcionado a la aplicación móvil o ha sido recolectada por ella (ej. perfilamiento).

17.1.4. Una aplicación móvil organiza la información de acuerdo con las características específicas del dispositivo móvil e interactúa con el soporte físico y las características del sistema operativo del mismo.

17.2 Implementación de prácticas básicas de seguridad de la información

17.2.1. Una práctica básica de seguridad requiere que los métodos de protección definidos e implementados por un desarrollador de aplicaciones móviles (o propietario) incluyan medidas organizativas, como limitar el acceso a "*la necesidad de conocer*", y medidas tecnológicas, como el uso de usuarios y contraseñas y cifrado. Adicionalmente esta Dirección encuentra que son prácticas básicas de seguridad, entre otras, las siguientes:

a) Contar con mecanismos de autenticación (usuarios y contraseñas)[30]. Estas últimas deben almacenarse de una manera cifrada y de forma segura, como un valor criptográfico de

---

[25] Cfr. Federal Trade Commission, Mobile Privacy Disclosures FTC Staff Report | February 2013 # Building Trust Through Transparency", en: https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf. Consultada el 9 de junio de 2019.

[26] Cfr. Grupo de Trabajo del Artículo 29 (Hoy Comité Europeo de Protección de Datos Personales). "Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes.", en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_es.pdf. Consultada el 27 de febrero de 2019.

[27] Ibidem.

[28] En algunos casos, el fabricante del sistema operativo se solapa con el del propio dispositivo y en otros casos, el fabricante de dispositivos es una empresa distinta del proveedor de sistemas operativos

[29] Cfr. Grupo de Trabajo del Artículo 29 (Hoy Comité Europeo de Protección de Datos Personales). "Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes.", en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_es.pdf. Consultada el 27 de febrero de 2019.

[30] Cfr. Comisión Federal de Comercio, App Developers: Start with Security: "If you create credentials for your users (like usernames and passwords), create them securely. For example, a short number string might be an appropriate token for authenticating a user on a game score board, but the same credential wouldn't be appropriate for a social networking app.", en: https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security. Consultada el 9 de junio de 2019.

comprobación aleatoria cifrado[31] (El almacenamiento de contraseñas en texto plano, es decir, entendibles a simple vista, es una práctica insegura y contraria al principio de seguridad establecido en la normatividad en datos personales[32]).

b) Poner a disposición de los usuarios un test de solidez de las contraseñas que eligen, siendo una técnica útil para promover mejores contraseñas (comprobación de entropía).

c) Cifrar los datos en tránsito (por ejemplo, usar SSL / TLS) cuando se autentique usuarios o transfiera información personal.

d) Mantener los datos de producción (es decir, información personal real) separados de los datos de prueba (información ficticia utilizada para desarrollar y probar aplicaciones y sistemas de TI).

e) Proporcionar una capacitación eficaz para el personal sobre el manejo adecuado de los datos personales en custodia o posesión de la organización.

f) Evaluar los riesgos de seguridad generados en el Tratamiento de datos personales, teniendo en cuenta la naturaleza, ámbito, contexto y fines del Tratamiento; asegurar que el programa de seguridad sea el adecuado para proteger los datos contra esos riesgos; y, garantizar que el programa de seguridad sea efectivo en la práctica, pues una clara desconexión entre lo documentado y la práctica genera un alto riesgo para la protección de los datos personales.

g) Identificar con precisión y rapidez las vulnerabilidades que necesitan corrección; implementar los controles adecuados para corregirlas de manera expedita; y verificar que los controles implementados sean efectivos y corrijan la vulnerabilidad.

h) Tomar las medidas técnicas y organizativas necesarias para garantizar la protección de los datos personales que tratan, en todas las fases del diseño y la puesta en práctica de la aplicación móvil.

17.2.2. Los métodos de protección por parte de los desarrolladores de aplicaciones móviles para proteger la información personal deben ser proporcionalmente altos, considerando el volumen, la categoría de titulares y el tipo de datos personales que recolecta una aplicación, así como la sensibilidad que para los titulares puede almacenar una aplicación móvil[33].

17.3. La existencia de riesgos para los derechos y libertades de los individuos frente al Tratamiento de sus datos personales

17.3.1. Si un dato personal es conocido, accedido o sustraído por terceros no autorizados, por ejemplo, piratas cibernéticos, esta situación entraña *per se* un riesgo para los derechos y libertades de los individuos, de gravedad y probabilidad variables.

17.3.2. En los casos en que el dato personal conocido, accedido o sustraído genere o puede generar problemas de usurpación de identidad o fraude, pérdidas financieras, daño para el buen

---

[31] Ibidem: Don't store passwords in plaintext on your server. Instead, consider using an iterated cryptographic hash function to hash users' passwords and then verify against these hash values. (Your users can simply reset their passwords if they forget.) That way, if your server suffers a data breach, passwords aren't left completely exposed."

[32] Mediante Resolución R/01254/2009, la Agencia Española de Protección de Datos Personales sancionó a una empresa por almacenar las contraseñas de sus clientes de manera visible. En: https://www.ecestaticos.com/file/ba38e7429b7ccb9f16684d291932f4b9/1540247088-sancion-interflora.pdf. Consultada en junio 9 de 2019.

[33] Cfr. Al respecto, el Comité Europeo de Protección de Datos (antes Grupo de Trabajo del Artículo 29) resaltó lo siguiente: "**La estrecha interacción con el sistema operativo permite a las aplicaciones acceder a un número de datos significativamente superior a aquél al que tiene acceso un navegador de internet tradicional. Las aplicaciones pueden recoger gran cantidad de datos a partir del dispositivo (datos de ubicación, datos almacenados por el usuario en el dispositivo o datos de los distintos sensores) y procesarlos para proporcionar servicios nuevos e innovadores al usuario final**. Por otro lado, la fragmentación de los numerosos actores que intervienen en el desarrollo de aplicaciones también supone un riesgo grave para la protección de datos. Un determinado dato puede ser transmitido, en tiempo real, desde el dispositivo para ser procesado en cualquier parte del planeta o ser copiado entre cadenas de terceras partes. Algunas de las aplicaciones más populares son desarrolladas por empresas tecnológicas de primer orden, pero muchas otras son diseñadas por pequeñas empresas de nueva creación. Un simple programador con una idea y poco o ningún conocimiento previo sobre programación puede llegar a una audiencia planetaria en un breve espacio de tiempo. Los desarrolladores de aplicaciones que desconozcan las normas de protección de datos pueden crear riesgos significativos para la vida privada y la reputación de los usuarios de dispositivos inteligentes. Simultáneamente, se van desarrollando rápidamente servicios a terceros como la publicidad, que, si son integrados por un desarrollador de aplicaciones sin la debida atención, puede revelar cantidades significativas de datos personales" (Negrita y subrayado agregados). "Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes.", en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_es.pdf. Consultada el 27 de febrero de 2019.

nombre, pérdida de confidencialidad o cualquier otro perjuicio económico o social significativo para los individuos, o se trate de un dato sensible o de información de personas vulnerables, en particular niños, niñas o adolescentes; o en los casos en los que el evento implique una gran cantidad de datos personales y afecte a un gran número de individuos, el riesgo para los derechos y libertades de los individuos es alto.

DÉCIMO OCTAVO: Que este Despacho precisa realizar las siguientes consideraciones sobre el Tratamiento de datos personales realizado a través de las aplicaciones móviles "UBER".

18.4. Sobre las Aplicaciones Móviles "UBER"

18.4.1. "UBER" es una aplicación móvil que permite a las personas ("usuarios") solicitar servicios de movilidad (o de transporte). Dicha solicitud se transmite a otra persona ("conductor"), quien se encuentra conectado a través de la Aplicación "UBER DRIVER".

18.4.2. "UBER" recluta y aprueba a personas para que se conviertan en conductores. "UBER" cobra por proporcionar el servicio de transporte y recolecta una parte de las tarifas que los conductores cobran por cada viaje. Los conductores deciden si está disponible para prestar el servicio y cuáles de las solicitudes aceptan.

18.4.3. UBER ("Uber Eats") también permite conectar a personas (o "clientes"), que solicitan comida u otros artículos a través de la aplicación descargada en su equipo móvil, con otras personas (o "repartidores"), que brindan servicios de entrega a domicilio[34].

18.5. Sobre los datos personales tratados por "UBER"

18.5.1. "UBER" cuenta con un sitio web, en: www.uber.com. La política de privacidad de UBER aplica a todas sus aplicaciones, sitios web, funciones u otros servicios en cualquier parte del mundo[35] y aplica a sus usuarios (personas que viajan), socios conductores (personas que prestan servicios de movilidad individualmente o a través de empresas de transporte asociadas), clientes (personas que ordenan comida u otros artículos) y socios repartidores (personas que brindan servicios de entrega a domicilio).

18.5.2. Según la política de privacidad[36], UBER recolecta la siguiente información personal:

a) Datos que la persona brinda a Uber:

- **Perfil de usuario:** Uber recolecta datos cuando una persona crea o actualiza una cuenta Uber. Esto puede incluir el nombre, correo electrónico, número de teléfono, nombre de usuario y contraseña, dirección, información de pago o bancaria (como la información relacionada para la verificación de pagos), números de ID. oficial (como número de seguro social, licencia de conducir o pasaporte si así lo exige la ley), fecha de nacimiento, foto y firma, información sobre el vehículo o el seguro de los conductores, y la configuración y preferencias que indique en su cuenta Uber.

- **Información de la verificación de antecedentes:** Uber puede que recolecte estos datos si la persona se registra para usar los servicios de Uber como conductor o repartidor, p. ej., su historial de conducción o antecedentes penales (si la ley lo permite). Un proveedor puede recopilar esta información en representación de Uber.

- **Datos demográficos:** Es posible que Uber recopile estos datos, incluso, de encuestas de usuarios. En algunos países, también puede que Uber reciba información demográfica de la persona de terceros.

- **Contenido del usuario:** Es posible que Uber recopile los datos que una persona envía al contactar a soporte, calificar o enviar reconocimientos a otros, o de cualquier otra comunicación que mantenga con Uber.

---

[34] Cfr. Uber. Política de privacidad, en: https://privacy.uber.com/policy. "*Esta política también se aplica a aquellos que proporcionan información a Uber a través de una app para usar nuestros servicios o aquellos cuya información se envía a Uber en relación con sus servicios (como la información de contacto de individuos asociados a los Restaurantes Socios de Uber Eats). A los fines de esta política, se implementará la palabra "usuarios" para referirse a todas aquellas personas sujetas a ella.*". Consultada el 25 de febrero de 2019.

[35] Cfr. Uber. Política de privacidad, en: https://privacy.uber.com/policy. Consultada el 25 de febrero de 2019.

[36] Ibídem.

b) Información creada al usar los servicios de Uber:

- **Ubicación**
  - Dependiendo de los servicios que una persona use y la configuración de la Aplicación o los permisos del dispositivo, Uber puede recopilar los datos de la ubicación exacta o aproximada, que se obtiene a través de servicios como GPS, dirección IP y Wi-Fi.
  - Si es un conductor o repartidor, Uber recopila los datos de la ubicación cuando la Aplicación se ejecuta en primer plano (Aplicación abierta y en pantalla) o en segundo plano (Aplicación abierta, pero no en pantalla) en el dispositivo de la persona.
  - Si es un usuario y autorizó el procesamiento de los datos de ubicación, Uber los recopilará cuando la Aplicación se ejecute en primer plano. En ciertas regiones, Uber recopila esta información cuando la Aplicación se ejecuta en segundo plano si la persona dio su consentimiento a través de la configuración de la Aplicación o los permisos del dispositivo.
  - Los usuarios y clientes pueden usar la Aplicación sin permitir a Uber recopilar los datos de ubicación. Sin embargo, esto puede afectar su funcionamiento. P. ej., si la persona no quiere permitir que Uber recolecte sus datos de ubicación, ella deberá ingresar la dirección del punto de partida manualmente. Además, Uber recopila los datos de ubicación del conductor durante el viaje y se vincularán con su cuenta, incluso, cuando la opción no esté activada.
- **Información de transacciones**
  - Uber recopila detalles sobre las transacciones relacionadas con el uso de sus servicios, incluyendo el tipo de servicios que solicita u ofrece, detalles de los pedidos, información de las entregas, fecha y hora de los servicios brindados, montos cobrados, distancias recorridas y métodos de pago. Asimismo, si alguien usa un código promocional, Uber puede asociar su nombre con esa persona.
- **Información de uso**
  - Uber recopila información sobre cómo la persona interactúa con sus servicios, como la fecha y hora de acceso, funciones de la Aplicación o páginas visitadas, fallas de la Aplicación y otras actividades en el sistema, tipo de navegador, y sitios o servicios de terceros que usó antes de interactuar con nuestra plataforma. En algunos casos, Uber recopila esta información a través de cookies, píxeles de seguimiento y tecnologías similares que crean y mantienen identificadores únicos.
- **Información del dispositivo**
  - Uber puede recopilar información sobre los dispositivos que una persona usa para acceder a sus servicios, como modelos de hardware, dirección IP del dispositivo, sistemas operativos y sus versiones, softwares, nombres de archivos y sus versiones, idiomas preferidos, identificadores únicos del dispositivo, identificadores de publicidad, números de serie, información sobre el movimiento del dispositivo e información sobre la red móvil.
- **Datos de comunicación**
  - Uber permite a los usuarios comunicarse entre ellos y con Uber a través de las Aplicaciones, sitios web y otros servicios. P. ej., los conductores y usuarios, y los repartidores y clientes pueden comunicarse o enviarse SMS entre ellos (en algunos países, sin ver los números de teléfono del otro). Para brindar este servicio, Uber recibe cierta información sobre las llamadas o SMS, incluyendo la fecha y hora de la comunicación y el contenido de esta. Uber también puede usar esta información para los servicios de soporte al cliente (incluida la resolución de conflictos entre los usuarios), con fines de seguridad y protección, para mejorar nuestros productos y servicios, y para análisis.

c) Información de otras fuentes

- Comentarios del usuario, como calificaciones o reconocimientos.
- Usuarios que proporcionen información sobre la persona en relación con los programas de referidos.
- Usuarios u otras personas que proporcionen información en relación con reclamos o conflictos.
- Socios comerciales de Uber a través de los cuales crea o accede a su cuenta Uber, como proveedores de pago, servicios de redes sociales, servicios de música a pedido, Apps o sitios web que usen API de Uber, o cuya API Uber use (como cuando pide un viaje a través de Google Maps).
- Proveedores de seguro (si es un conductor o repartidor).
- Proveedores de servicios financieros (si es un conductor o repartidor).
- Empresas de transporte asociadas (si es un conductor que usa los servicios de Uber a través de una cuenta vinculada a una de estas empresas).
- El propietario de Uber para Empresas o Perfil Familiar que use.
- Fuentes disponibles públicamente.
- Proveedores de servicio de publicidad.
- Uber puede combinar la información que recopile de estas fuentes con otra de la que disponga.

DÉCIMO NOVENO: Que sobre el modelo de negocio de "UBER" y la responsabilidad respecto del Tratamiento de los datos personales de los residentes o domiciliados en la República de Colombia, la Dirección se permite precisar los siguientes aspectos:

19.1. Sobre el grupo de compañias "UBER"

19.1.1. UBER TECHNOLOGIES, INC. es una corporación registrada en Delaware, Estados Unidos de América, con sede principal en 1455 Market Street, San Francisco, California 94103, Estados Unidos de América[37].

19.1.2. UBER B.V. es una sociedad domiciliada en los Países Bajos[38], con domicilio social en Mr. Treublaan 7, 1097 DP, Ámsterdam, Países Bajos, inscrita en la Cámara de Comercio de Ámsterdam con el número 56317441[39].

19.1.3. UBER COLOMBIA SAS se encuentra registrada desde el 15 de febrero de 2015[40] en la Cámara de Comercio de la ciudad de Bogotá, Colombia, identificada con el Nit. 900.676.165-2, con domicilio social y centro de negocios en la ciudad de Bogotá, Colombia.

19.1.4. Según el certificado de existencia y representación legal de UBER COLOMBIA SAS., UBER TECHNOLOGIES, INC., ejerce situación de control indirecta sobre UBER COLOMBIA SAS (Subordinada) a través de las sociedades UBER INTERNATIONAL C.V, UBER INTERNATIONAL B.V., y UBER INTERNATIONAL HOLDING B.V[41].

19.1.5. El objeto social de UBER COLOMBIA SAS es "*desarrollar actividades de promoción y venta de espacios publicitarios*" en el territorio colombiano, con el fin de, de conformidad con la respuesta de UBER COLOMBIA SAS del 4 de enero de 2018, generar ingresos económicos a UBER TECHNOLOGIES INC.

19.1.6. UBER cuenta, de una manera efectiva y real, con centros de ayuda para que las personas se conviertan en socio conductor en el territorio colombiano (Ciudades: Bogotá – Centro Comercial San Rafael, Centro Comercial Plaza Claro, Servitek, Medellín - Centro Comercial Tierragro-, Cali, Bucaramanga, Barranquilla, Cúcuta, Ibagué, Montería, Pereira y Popayán). También cuenta con un contacto telefónico (Valledupar y Santa Marta)[42].

---

[37] Cfr. Autoriteit Persoonsgegevens, "Dutch DPA: fine for data breach Uber", en: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_uber.pdf. Consultada el 4 de marzo de 2019.
[38] Cfr. Ibidem.
[39] *Cfr. Legal UBER B.V. TÉRMINOS Y CONDICIONES", en: https://www.uber.com/legal/terms/co/ Consultada el 7 de junio de 2019.*
[40] Folios 17-21.
[41] Cfr. Ibidem.
[42] Cfr. Uber. *Centros de activación Uber en Colombia*, en: https://www.uber.com/es-CO/blog/centros-de-activacion-uber-en-colombia. Consultada el 12 de junio de 2019.

19.1.7. La política de privacidad como la política de términos y condiciones de uso está disponible globalmente en el sitio web de "UBER" y aplica, salvo la política "Uber Freight Privacy Policy". Dice textualmente el texto de política de privacidad de UBER:

> "*Esta política describe la forma en la que Uber y sus filiales recopilan y utilizan la información personal para proporcionar servicios. Esta política se aplica a todos los usuarios de nuestras apps, sitios web, herramientas y otros servicios en cualquier lugar del mundo, a menos que se aplique una política de privacidad independiente, como la Uber Freight Privacy Policy.*".
> *En concreto, esta política se aplica a:* ***Pasajeros:*** *usuarios que solicitan o reciben un servicio de transporte.* ***Conductores:*** *usuarios que prestan servicios de transporte a título individual o mediante empresas de transporte.* ***Destinatarios de entregas:*** *usuarios que solicitan entregas de comida u otros artículos.* ***Repartidores:*** *usuarios que prestan servicios de entrega.*
>
> *La política también se aplica a aquellas personas que proporcionan información a Uber en el ámbito de una app para usar nuestros servicios y a aquellas cuya información reciba Uber como consecuencia de la prestación de sus servicios (p. ej., información de contacto de personas relacionadas con restaurantes asociados a Uber Eats). Todas las personas sujetas a esta política se denominan 'usuarios' en el contexto de la misma.*"[43].

19.1.8. Se concluye, en este punto, que UBER TECHNOLOGIES, INC., UBER B.V. y UBER COLOMBIA SAS son tres agentes o compañías que hacen parte del grupo "UBER", que, en virtud del reparto de funciones dentro del grupo, intervienen conjuntamente en el desarrollo, la distribución y la explotación de los servicios de "UBER", incluida las aplicaciones que están disponibles en territorio colombiano, descargadas a través de dispositivos móviles dentro del territorio colombiano y usadas por personas domiciliadas o residentes en el territorio colombiano para los fines señalados en la política de privacidad de "UBER".

19.2. Sobre el Tratamiento de los datos personales por parte del grupo de compañías "UBER"

19.2.1. UBER TECHNOLOGIES, INC. es el propietario de las Aplicaciones Móviles "UBER", que están disponibles para su descarga en las tiendas de aplicaciones (o distribuidor de aplicaciones) Apple App Store y Google Play Store[44], respectivamente.

19.2.2. De conformidad con la investigación realizada por la Autoridad de Protección de Datos de los Países Bajos (Autoriteit Persoonsgegevens), UBER TECHNOLOGIES, INC., es la empresa responsable de la política de privacidad y de las medidas de seguridad con respecto a la protección los datos personales que trata para sus propósitos comerciales[45].

Adicionalmente, el contrato de computación en la nube Amazon Web Services -"AWS" S3-, donde se almacena las copias de seguridades, completas y parciales, de las bases de datos de UBER, fue suscrito entre UBER TECHNOLOGIES, INC., y AMAZON, respectivamente, de conformidad con la investigación realizada por la Autoridad de Protección de Datos de los Países Bajos (Autoriteit Persoonsgegevens)[46].

19.2.3. De conformidad con la política de privacidad de UBER, UBER B.V. es la compañía que formalmente tiene la calidad de "Responsable del Tratamiento", es decir, quien, según dicho documento, define los fines y propósitos del tratamiento, de los datos de las personas que residen fuera del territorio de los Estados Unidos. Se cita la política:

> "Si vive en los Estados Unidos, el controlador de datos para la información que nos proporciona o que recopila Uber o sus filiales es el siguiente:
>
> Uber Technologies, Inc. 1455 Market Street San Francisco, California, 94103
>
> **Si vive en la Unión Europea o en otro lugar, el controlador de datos es el siguiente:**

---

[43] Cfr. Uber. Política de privacidad, en: https://privacy.uber.com/policy. Consultada el 9 de junio de 2019.
[44] Cfr. Autoriteit Persoonsgegevens, "Dutch DPA: fine for data breach Uber", en: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_uber.pdf. Consultada el 25 de febrero de 2019.
[45] Cfr. Autoriteit Persoonsgegevens, "Dutch DPA: fine for data breach Uber", en: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_uber.pdf. Consultada el 25 de febrero de 2019.
[46] Cfr. Ibidem.

Uber B.V. Mr. Treublaan 7, 1097 DP Amsterdam, the Netherlands."[47]

19.2.4. De conformidad con la respuesta de UBER COLOMBIA SAS del 4 de enero de 2018, UBER COLOMBIA SAS "*tiene acceso a información limitada sobre usuarios y conductores de Colombia, únicamente y exclusivamente, para efectos de prestarle a UBER servicios de mercadeo y publicidad, y servicios operacionales y de soportes de clientes*"[48]. Esta actividad influye en el tratamiento de datos personales a efectos de la venta de espacios publicitarios y de otras actividades de publicidad de "UBER" destinadas a las personas residentes o domiciliadas en Colombia y que sirven para rentabilizar los servicios ofrecidos por UBER.

19.2.5. Es claro que los fines o propósitos por los cuales, los medios y la manera en que se tratan los datos personales de los residentes o domiciliados en la República de Colombia, tanto de aquellos recolectados a través de las aplicaciones móviles "UBER" como de aquellos recolectados directamente por UBER COLOMBIA SAS para prestarle a "UBER" "*servicios de mercadeo y publicidad, y servicios operacionales y de soportes de clientes*", son definidos de manera conjunta por parte de UBER TECHNOLOGIES, INC., UBER COLOMBIA SAS y UBER B.V., para o en relación a todo el circulo de la operación comercial y económica de "UBER" en Colombia.

19.2.6. Además, por su intervención en el desarrollo, la distribución y la explotación de los servicios y productos bajo la marca "UBER", les corresponden a UBER TECHNOLOGIES, INC., UBER COLOMBIA SAS y UBER B.V, por si mismos o conjuntamente, la responsabilidad de velar por el cumplimiento de todos los requisitos establecidos en la Ley 1581 de 2012.

19.3. Sobre la debida diligencia en el Tratamiento de los datos personales por parte de "UBER"

19.3.1. El principio de debida diligencia significa que una organización es responsable de la información personal en su custodia o posesión y debe contar con las medidas necesarias para afrontar los riesgos para los derechos y libertades de las personas frente al Tratamiento de sus datos personales, incluyendo aquellos controles, medidas de seguridad y mecanismos que garanticen de una manera efectiva la protección de los datos personales que proporciona la Ley 1581 de 2012.

19.3.2. UBER cuenta con 75 millones de usuarios y 3 millones de conductores. UBER registra 10 mil millones de viajes realizados en todo el mundo. UBER se encuentra en 65 países y más de 600 ciudades en todo el mundo. UBER registra 15 millones de viajes realizados por día. Hay más de 16,000 empleados en UBER desde 2017[49]. En cuanto a Colombia, UBER cuenta con unos 83.000 conductores y es usado mensualmente por alrededor de 2,1 millones de pasajeros[50], acorde a una entrevista realizada al gerente de UBER y publicada en el periódico El Tiempo.

19.3.3. Recolectar, usar, circular y tratar los datos personales relacionados con esos 83.000 conductores y de 100.000 usuarios, que utilizan UBER por lo menos una vez a la semana[51] en el territorio colombiano exige que UBER sea extremadamente responsable, diligente y profesional con tanta información de seres humanos bajo su posesión o custodia.

19.3.4. Como se señala en la política de privacidad "*aplicable a los usuarios de los servicios de Uber en cualquier lugar del mundo e incluye a los usuarios de las aplicaciones, los sitios web, las herramientas y otros servicios de Uber*", UBER se compromete a no defraudar la confianza de los individuos.

19.3.5. A pesar de las afirmaciones en su política de privacidad relación con su compromiso por "*no defraudar la confianza de sus usuarios*", las fallas en sus políticas de seguridad, como se describirán a continuación, no representa, en la opinión de esta Dirección, a una organización que asume la responsabilidad de otorgar un efecto real y significativo a la protección de los datos personales, rompiendo, bajo esa misma premisa, la confianza depositada por los individuos en la compañía; esto es particularmente preocupante dada la gran cantidad de información personal bajo el control

---

[47] Cfr. Uber. *Política de privacidad*, en: https://privacy.uber.com/policy. Consultada el 25 de febrero de 2019.
[48] Folios 8-11 y 174-25.
[49] Cfr. Uber. "*Las estadísticas. Datos y cifras*", en: https://www.uber.com/es-CO/newsroom/company-info/. Consultada el 25 de febrero de 2019.
[50] https://www.eltiempo.com/tecnosfera/apps/entrevista-con-humberto-pacheco-gerente-general-de-uber-en-la-region-194566. Consultada el 25 de febrero de 2019.
[51] https://www.larepublica.co/internet-economy/mas-de-100000-usuarios-utilizan-uber-por-lo-menos-una-vez-a-la-semana-2256291. Consultada el 25 de febrero de 2019.

de UBER, gran parte de la cual puede ser altamente confidencial (por ejemplo, mensajes privados, números de teléfono, datos de localización, datos financieros, etc.).

VIGÉSIMO: DE LAS FALLAS DE SEGURIDAD DE UBER.

20.1. El uso de "UBER" de la plataforma de servicios de almacenamiento en la nube por Amazon Web Services -"AWS" S3

20.1.1. "UBER" utiliza el servicio de computación en la nube "*Amazon Simple Storage Service*" (*Amazon S3 Datastore*", proporcionado por Amazon Web Services -"AWS"-) tal como lo informó en la respuesta al requerimiento realizado por esta Dirección, visible a folio 9 del expediente.

20.1.2. Amazon Simple Storage Service, en adelante AWS S3, es un *IaaS* («*Cloud Infrastructure as a Service*», infraestructura como servicio), el cual consiste en que un proveedor alquila servidores remotos virtuales a los que puede recurrir el usuario final en virtud de mecanismos y disposiciones que hacen sencillo, eficaz y beneficioso sustituir a los sistemas informáticos de los locales de la empresa, o utilizar la infraestructura alquilada a la vez que dichos sistemas[52]. Amazon S3 almacena los datos dentro de contenedores de archivos "*buckets*" (o "cubos"), a los que se pueden aplicar controles de acceso individuales.

20.1.3. AWS S3 almacena las copias de seguridad, completas y parciales, de las bases de datos de UBER. Las copias de seguridad contienen una amplia gama de información personal de usuarios y conductores, incluyendo, entre otro tipo de información, nombres, apodos o "*nickname*", direcciones de correo electrónico, direcciones de residencia (o postales), números de teléfono, identificadores únicos de dispositivos, registros de viaje, geo-localización, información y números de licencia de conducir. Los archivos también incluyen documentos proporcionados por los conductores de UBER, como recibos de registro de vehículos, prueba de documentos de seguro e imágenes de licencias de conducir.

20.1.4. El contrato AWS S3, como se señaló anteriormente, fue suscrito entre UBER TECHNOLOGIES, INC., y AMAZON, respectivamente, de conformidad con la investigación realizada por la Autoridad de Protección de Datos de los Países Bajos (Autoriteit Persoonsgegevens)[53].

20.2. Acceso no autorizado a los datos personales almacenados en la nube AWS S3

20.2.1. El 22 de noviembre de 2017[54] en la sección UBER Colombia, el señor Dara Khosrowshahi, director ejecutivo o "*CEO*" de UBER anunció públicamente que un incidente de seguridad había afectado información personal almacenada por ellos en un servidor en la nube de un proveedor externo. Señaló el señor Khosrowshahi en su comunicado:

> *"Como CEO de Uber, es mi trabajo establecer nuestro camino hacia el futuro, el cual comienza con construir una compañía de la que cada empleado, socio conductor o usuario pueda estar orgulloso. Para que eso ocurra, debemos ser honestos y transparentes mientras trabajamos para reparar nuestros errores del pasado.*
>
> *Hace poco me enteré que a finales de 2016 dos individuos ajenos a la Compañía obtuvieron de forma inapropiada acceso a datos de usuarios almacenados en un servidor en la nube alojado por un proveedor externo que utilizábamos. El incidente no violó nuestros sistemas corporativos o nuestra infraestructura.*
>
> *Nuestros expertos forenses no han visto ninguna indicación acerca de que la ubicación de viajes, números de tarjetas de crédito, números de cuentas bancarias, números de seguro social o fechas de nacimiento hayan sido descargados. Sin embargo, los individuos pudieron acceder a archivos que contenían una cantidad significativa de otra información, entre la que se incluye:*
>
> *Los nombres y los números de licencia de conducir de cerca de 600,000 socios conductores en Estados Unidos. Ellos pueden encontrar más información aquí.*

---

[52] Cfr. Grupo de Trabajo del Artículo 29 (Hoy Comité Europeo de Protección de Datos Personales). "Dictamen 05/2012 sobre la computación en nube.", en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf. Consultada el 25 de febrero de 2019.

[53] Cfr. Autoriteit Persoonsgegevens, "Dutch DPA: fine for data breach Uber", en: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_uber.pdf. Consultada el 25 de febrero de 2019.

[54] Cfr. Uber. Incidente de seguridad de datos en 2016, https://www.uber.com/es-CO/newsroom/incidente-de-seguridad-de-datos-en-2016/ Consultada el 25 de febrero de 2019.

Información personal de 57 millones de usuarios alrededor del mundo, incluyendo a los socios conductores mencionados anteriormente. Esta información incluye nombres, direcciones de correo electrónico y números de teléfono. Los usuarios pueden encontrar más información aquí.

Al momento del incidente, tomamos medidas de inmediato para asegurar los datos y bloquear cualquier acceso no autorizado. Al mismo tiempo, identificamos a los atacantes y nos aseguramos que los datos descargados fueran destruidos. Además, implementamos medidas de seguridad para restringir accesos y fortalecer los controles en nuestras cuentas de almacenamiento de datos en la nube.

Puede que muchos se pregunten por qué estamos hablando de esto ahora, un año después de ocurrido el incidente. Yo me hice la misma pregunta, así que inmediatamente solicité una investigación acuciosa acerca de lo ocurrido y cómo lo manejamos. Lo que descubrí, particularmente acerca de nuestra falla a la hora de notificar a las personas y a las autoridades el año pasado, me ha llevado a adoptar varias medidas:

- *He solicitado a Matt Olsen, co-fundador de una firma consultora de ciberseguridad, ex consejero general de la Agencia Nacional de Seguridad de EE.UU. y director del Centro Nacional para el Contraterrorismo, que me ayude a analizar cómo podemos guiar y estructurar nuestros equipos de seguridad y decidir nuestros siguientes pasos. Con efecto inmediato, dos de las personas que lideraron la respuesta a este incidente, no seguirán relacionados a la Compañía.*
- *Estamos notificando individualmente a los socios conductores cuyos números de licencia de conducir fueron descargados.*
- *Estamos ofreciendo a estos conductores servicio gratuito de servicios de verificación de crédito y protección ante robo de identidad.*
- *Estamos notificando a las autoridades regulatorias.*
- *Si bien no hemos visto evidencia de fraude o uso indebido relacionado a este incidente, estamos monitoreando las cuentas afectadas y las hemos notificado para brindarles protección adicional ante fraudes.*

Nada de esto debió haber ocurrido, y no intentaré justificarlo. Si bien no puedo borrar el pasado, sí puedo comprometerme a nombre de cada empleado de Uber a que aprenderemos de estos errores. Estamos cambiando la forma en que trabajamos, poniendo la integridad en el centro de cada decisión y esforzándonos para ganar la confianza de nuestros clientes"

20.2.2. El 29 de noviembre de 2017[55], el Grupo de Trabajo del Artículo 29 (Hoy Comité Europeo de Protección de Datos) publicó el siguiente comunicado de prensa:

"El WP29 estableció un grupo de trabajo en el caso de violación de datos UBER. Este grupo de trabajo, liderado por la DPA holandesa, estará compuesto en esta etapa por representantes de las APD francesas, italianas, españolas, belgas y alemanas, así como ICO, y coordinará las investigaciones nacionales sobre este importante tema"

20.2.3. El 4 de enero de 2018, UBER COLOMBIA SAS le informó a esta Dirección que el número de colombianos afectados por el incidente de seguridad se estima en 267.000 y que UBER está adoptando los pasos necesarios para evitar futuros incidentes de seguridad como el reportado por parte de su director ejecutivo, empezando por el cambio de personal y otras acciones correctivas.

20.2.4. El 12 de abril de 2018[56], la Comisión Federal de Comercio de los Estados Unidos de América informó que UBER había aceptado expandir el acuerdo que había suscrito con dicha autoridad en el año 2017 por las fallas de seguridad presentadas en sus sistemas de almacenamiento en la nube, incluyendo los siguientes eventos: (i) el ataque cibernético que sufrió en Amazon S3 entre octubre y noviembre de 2016 y (ii) la omisión de informar el evento a los usuarios o a la FTC durante más de un año, a pesar de que UBER era objeto de una investigación en curso por parte de dicha autoridad.

---

[55] Cfr. Grupo de Trabajo del Artículo 29 (Hoy Comité Europeo de Protección de Datos Personales -EDPB). Cita el comunicado de prensa: "WP29 has established a taskforce on the UBER data breach case. The WP29 established a taskforce on the UBER data breach case. This taskforce, led by the Dutch DPA, will be composed at this stage of representatives from the French, Italian, Spanish, Belgian and German DPAs as well as from the ICO and will coordinate the national investigations on this important issue.", en: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=609786. Consultado el 20 de febrero de 2019.

[56] Cfr. The Federal Trade Commission (FTC), en: https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security. Consultado el 22 de febrero de 2019.

20.2.5. El 27 de noviembre de 2018[57], la Oficina del Comisionado de Información de Gran Bretaña (ICO) impuso una sanción monetaria de 385.000 libras esterlinas contra UBER por incumplir su obligación de proteger la información personal durante un ciber-ataque por el incidente de seguridad ocurrido entre octubre y noviembre de 2016.

20.2.6. El 27 de noviembre de 2018[58], la Autoridad de Protección de Datos de los Países Bajos (Autoriteit Persoonsgegevens) impuso una multa de 600.000 a UBER B.V. y UBER TECHNOLOGIES, INC., por el incidente de seguridad ocurrido entre octubre y noviembre de 2016 y que afectó la información personal de los conductores y usuarios en los Países Bajos.

20.2.7. El 20 de diciembre de 2018[59], la Comisión Nacional de Informática y de las Libertades de Francia (CNIL) impuso una multa de 400.000 euros a UBER FRANCE SAS., una compañía propiedad de UBER TECHNOLOGIES INC., y UBER B.V., por incumplir su obligación de garantizar la seguridad de los datos personales frente al incidente de seguridad ocurrido por el incidente de seguridad ocurrido entre octubre y noviembre de 2016.

20.2.8. A la luz de lo anterior, esta Dirección encuentra que UBER falló en sus políticas y prácticas para hacer garantizar la protección efectiva de los datos personales bajo su custodia o posesión y respecto al incidente de seguridad que sufrió por dicha compañía entre octubre y noviembre de 2016.

VIGÉSIMO PRIMERO: Actuaciones y decisiones de autoridades internacionales en relación con los incidentes de seguridad que han puesto en riesgo los datos personales en custodia o posesión de UBER

Que para los fines de la presente resolución, esta Dirección considera importante hacer referencia a las órdenes y sanciones emitidas contra UBER por las diferentes autoridades nacionales de protección de datos (o comisionados de privacidad), la Comisión Federal de Comercio de los Estados Unidos de América, el acuerdo suscrito con la Oficina del Fiscal General de California y aprobado por una corte estatal y una audiencia desarrollada por el Comité del Senado sobre Comercio, Ciencia y Transporte del Senado de los Estados Unidos, en relación con los incidentes de seguridad que han puesto en riesgo los datos de los individuos en custodia o posesión de UBER.

21.1. The Federal Trade Commission (FTC) de los Estados Unidos de América

21.1.1. El 15 de agosto de 2017[60], la Comisión Federal de Comercio de los Estados Unidos de América ("The Federal Trade Commission"), en adelante la "FTC", por sus siglas en inglés, encontró los siguientes hallazgos en las políticas de UBER[61]:

a) UBER falló en su deber de contar con una política estricta de control de acceso interno a los datos personales de los usuarios y conductores y que el acceso por parte de los empleados estaba siendo monitoreado de una manera muy cerca y con sistemas de auditorías. En este punto, indicó la FTC: UBER desarrolló un sistema automático para monitorear el acceso de los empleados a los datos personales de los usuarios en diciembre de 2014, pero el sistema no fue diseñado o dotado de personal para realizar un monitoreo continuo frente al acceso a los datos por parte de los miles de empleados y trabajadores contingentes de UBER.

b) Aproximadamente en el mes de agosto de 2015, UBER dejó de usar un sistema automatizado que había desarrollado en diciembre de 2014 y comenzó a desarrollar un nuevo sistema de monitoreo automatizado. Desde agosto de 2015 hasta mayo de 2016, UBER no realizó un seguimiento oportuno de las alertas automáticas relacionadas con el posible uso indebido de la información personal de los usuarios y, durante los primeros seis meses de ese período, UBER solo supervisó el acceso a la información de la cuenta que pertenecía a un conjunto de usuarios de alto perfil, como sus ejecutivos. Por lo tanto, UBER no supervisó el acceso interno a la

---

[57] Cfr. The Information Comissioner's Office, ICO, en: https://ico.org.uk/media/2553890/uber-monetary-penalty-notice-26-november-2018.pdf Consultado el 22 de febrero de 2019.
[58] Cfr. Autoriteit Persoonsgegevens, en: https://www.autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fine-data-breach-uber Consultado el 22 de febrero de 2019
[59] Cfr. Commission Nationale de l'informatique et des libertés, CNIL, en: https://www.cnil.fr/fr/uber-sanction-de-400000eu-pour-une-atteinte-la-securite-des-donnees-des-utilisateurs Consultado el 22 de febrero de 2019.
[60] Cfr. The Federal Trade Commission (FTC), en: https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data Consultado el 22 de febrero de 2019.
[61] Cfr. The Federal Trade Commission (FTC), en: https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_complaint.pdf Consultado el 22 de febrero de 2019.

información personal y se enteró una vez un empleado le informó específicamente que un compañero de trabajo había participado en un acceso inapropiado a la información personal.

c) A pesar de que UBER informaba que los datos estaban almacenados de una manera segura dentro de sus sistemas de almacenamiento, UBER falló en su obligación de contar con las medidas razonables para prevenir accesos no autorizados a los datos personales almacenados en el servidor Amazon S3. Entre otras cosas, se detectó:

   i. Hasta septiembre de 2014, UBER falló en implementar controles de acceso razonables para proteger los datos almacenados en Amazon (-AWS-) S3. En esa medida, UBER:
      - falló en requerir que los programas e ingenieros que acceden a AWS S3 (o también escrito como Amazon S3 en la presente resolución) usen claves de acceso distintas y, en lugar de ello, UBER permitió que todos los programas e ingenieros usarán una simple clave de acceso "*AWS*"; esta clave proporciona privilegios completos administrativos sobre todos los datos en AWS S3;
      - falló en restringir el acceso a los sistemas basados en funciones de trabajo de los empleados; y,
      - falló en requerir la autenticación multi-factor para acceder a AWS S3.

   ii. Hasta septiembre de 2014, UBER falló en implementar una política de capacitación y orientación de seguridad razonables;

   iii. Hasta septiembre de 2014, UBER falló en contar con un programa escrito de seguridad de la información;

   iv. Hasta marzo de 2015, la información personal confidencial almacenada en AWS S3 se realizó en texto simple, incluidos los respaldos de la base de datos, en lugar de cifrar la información.

d) Como consecuencia de las fallas en los controles de acceso, un intruso pudo acceder a la información personal de los consumidores almacenada en AWS S3, mediante una clave de acceso que uno de los ingenieros de UBER había publicado en "*GitHub*"; sitio web de código compartido utilizado por desarrolladores de software (La clave publicada públicamente otorgó privilegios administrativos completos a todos los datos y documentos almacenados en AWS S3).

e) El intruso accedió a un archivo que contenía información personal, sin medidas de cifrado, relacionada con conductores de UBER, incluidos más de 100,000 nombres y números de licencia de conducción, 215 nombres de cuentas bancarias y números de enrutamiento nacional y 84 nombres de números de seguridad social. El archivo también contenía otra información de los conductores de UBER, incluidas direcciones físicas, direcciones de correo electrónico y dispositivos móviles, números de teléfono, "*ID*" de dispositivo e información de la localización de los viajes que los conductores proporcionaron a UBER.

f) UBER no había descubierto el incidente hasta septiembre de 2014; momento en que dicha organización tomó medidas para evitar un mayor acceso no autorizado.

21.1.2. Como consecuencia de los anteriores hallazgos, UBER acordó con la FTC implementar las siguientes medidas[62]:

a) Establecer, implementar y mantener un programa comprensivo de privacidad, incluyendo: (i) la designación de un empleado (o empleados) para coordinar y ser responsable por el programa de privacidad; (ii) la identificación de los riesgos; (iii) la designación e implementación de controles y procesos razonables para hacer frente a dichos riesgos y un monitoreo regular de la efectividad de esos controles y procesos; y, (iv) la evaluación y ajustes del programa de privacidad.

b) Obtener de una tercera parte calificada, independiente y objetiva una evaluación inicial y evaluaciones bianuales en relación con los controles de seguridad implementados por UBER para proteger los datos personales.

---

[62] Cfr. The Federal Trade Commission (FTC), en: https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data Consultado el 22 de febrero de 2019

21.1.3. El 12 de abril de 2018[63], la FTC informó que UBER había aceptado expandir el acuerdo que había suscrito con dicha autoridad en el año 2017, incluyendo lo relacionado con (i) el ataque cibernético que sufrió en AWS S3 entre octubre y noviembre de 2016 y (ii) su omisión de informar el evento a los usuarios y a la FTC durante más de un año, a pesar de que esa organización era objeto de una investigación en curso por parte de la FTC. La FTC encontró los siguientes hallazgos[64]:

a) Aproximadamente el 14 de noviembre de 2016, UBER se enteró de otra violación que afectó la información personal almacenada en AWS S3. Una vez más, los intrusos obtuvieron acceso a Amazon S3 utilizando una clave de acceso que un ingeniero de UBER había publicado en "*GitHub*".

b) Las claves estaban en texto sin formato (o texto en archivo plano) en el código que se publicó en un repositorio privado de "*GitHub*".

c) UBER había otorgado a sus ingenieros acceso a los repositorios de "*GitHub*", a través de cuentas individuales de "*GitHub*", a los que ellos generalmente accedían a través de direcciones de correo electrónico personales.

d) UBER no tenía una política que prohibiera a los ingenieros reutilizar las credenciales. Tampoco requería para que se habilitara la autenticación de múltiples factores al acceder a los repositorios de "*GitHub*" de UBER.

e) Los intrusos dijeron que accedieron a la página de "*GitHub*" de UBER, en ese caso, utilizando contraseñas que anteriormente estaban expuestas en otras violaciones de datos importantes, con lo que descubrieron la clave de acceso en texto sin formato.

f) Los intrusos descargaron 16 archivos de AWS S3, entre el 13 de octubre de 2016 y el 15 de noviembre de 2016. Estos archivos contenían información personal del consumidor sin cifrar y relacionada con los usuarios y conductores ubicados en los EE. UU., incluido, entre otras cosas, aproximadamente 25.6 millones de nombres y direcciones de correo electrónico, 22.1 millones de nombres y números de teléfonos móviles, y 607.000 nombres y números de licencias de conducir. Casi toda la información personal expuesta se recopiló antes de julio de 2015 y se almacenó en archivos de copia de seguridad de base de datos no cifrados.

g) UBER descubrió la violación el 14 de noviembre de 2016 o alrededor de esa fecha, cuando uno de los atacantes se contactó con ellos para informarle que había accedido a las "bases de datos" de UBER y exigirle un pago de seis cifras.

h) UBER pagó a los atacantes $ 100,000 a través del tercero que administra el programa de recompensas de errores (o "*bug bounty*") de UBER.

i) UBER creó el programa de recompensas por errores (o "*bug bounty*") para pagar recompensas financieras a cambio de la divulgación responsable de vulnerabilidades de seguridad graves en sus sistemas. Sin embargo, los atacantes, en este caso, eran diferentes de los destinatarios legítimos que podían a acceder a una recompensa de errores, pues, según la conclusión de la FTC, los atacantes explotaron maliciosamente la vulnerabilidad y adquirieron información personal relacionada con millones de consumidores de UBER.

j) UBER no reveló la violación a los consumidores afectados hasta el 21 de noviembre de 2017, es decir, más de un año después de que dicha organización descubrió la violación.

k) A pesar de que la FTC estaba adelantando una investigación no pública contra UBER relacionada, en ese caso, con sus prácticas de seguridad, en particular, las implementadas en la cuenta en AWS S3, UBER no reveló la existencia de la violación a la FTC hasta noviembre de 2017.

---

[63] Cfr. The Federal Trade Commission (FTC), en: https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security. Consultado el 22 de febrero de 2019.

[64] Cfr. The Federal Trade Commission (FTC), en: https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_complaint_0.pdf. Consultado el 22 de febrero de 2019.

21.1.4. Como consecuencia de lo anterior, UBER acordó con la FTC implementar las siguientes medidas[65]:

a) Establecer, implementar y mantener un programa comprensivo de privacidad, incluyendo: (i) la designación de un empleado o empleados para coordinar y ser responsable por el programa de privacidad; (ii) la identificación de los riesgos; (iii) la designación e implementación de controles y procesos razonables para hacer frente a dichos riesgos y un monitoreo regular de la efectividad de esos controles y procesos; (iv) la revisión, evaluación y respuesta a informes de vulnerabilidad de seguridad de terceros, incluso a través de un programa de "recompensas de errores" o similar; y, (v) la evaluación y ajustes del programa de privacidad.

b) Obtener de una tercera parte calificada, independiente y objetiva una evaluación inicial y evaluaciones bianuales en relación con los controles de seguridad implementados por Uber para proteger los datos personales

c) Dentro de un tiempo razonable después de la fecha de descubrimiento de un Incidente cubierto por UBER, pero en cualquier caso, a más tardar 10 días después de la fecha en que UBER notifique por primera vez a cualquier entidad gubernamental federal, estatal o local de los EE. UU., el incidente, presentar un informe a la FTC sobre el evento ocurrido.

d) Entregar una copia de la orden suscrita con la FTC a su Alta Gerencia, incluyendo a sus empleados, dependiendo del caso en concreto

21.1.5. El 28 de octubre de 2018[66], la FTC informó que ella había aprobado el acuerdo final con UBER TECHNOLOGIES, INC., en los siguientes términos[67]:

a) Establecer, implementar y mantener un programa comprensivo de privacidad, incluyendo: (i) la designación de un empleado o empleados para coordinar y responder por el programa de privacidad; (ii) la identificación de los riesgos; (iii) la designación e implementación de controles y procesos razonables para hacer frente a dichos riesgos y un monitoreo regular de la efectividad de esos controles y procesos; y, (iv) la evaluación y ajustes del programa de privacidad.

b) Obtener de una tercera parte calificada, independiente y objetiva una evaluación inicial y evaluaciones bianuales en relación con los controles de seguridad implementados por UBER para proteger los datos personales.

c) Presentar un informe a la FTC sobre la ocurrencia de incidentes de seguridad. Así como, entregar una copia de la orden a la Alta Gerencia de UBER, incluyendo a sus empleados, dependiendo del caso en concreto

21.2. The Information Commissioner's Office (ICO) del Reino Unido de Gran Bretaña e Irlanda del Norte

21.2.1. El 27 de noviembre de 2018[68], la Oficina del Comisionado de Información del Reino Unido de Gran Bretaña e Irlanda del Norte (The Information Commissioner's Office, ICO), en adelante "ICO" por sus siglas en inglés, anunció que esa autoridad impuso una sanción monetaria de 385.000 libras esterlinas contra UBER B.V., UBER LONDON LIMITED, UBER BRITANNIA LIMITED, UBER SCOT LIMITED y UBER NIR LIMITED, en adelante UBER BV y UBER UK, en conjunto "UBER"), bajo la sección 55ª del "Data Protection Act 1998". ICO encontró los siguientes hechos:

a) Entre el 13 de octubre y el 15 de noviembre de 2016, respectivamente, la información personal almacenada por UBER en Amazon S3 o AWS S3 fue objeto de un ciberataque externo.

---

[65] Cfr. The Federal Trade Commission (FTC), In the Matter of Uber Technologies, Inc., a corporation, en: https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_decision_and_order.pdf. (Traducción no official). Consultado el 22 de febrero de 2019. Nota: Puede consultar el documento completo en su idioma original en el link.

[66] Cfr. The Federal Trade Commission (FTC), en: https://www.ftc.gov/news-events/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber Consultado el 22 de febrero de 2019. (Traducción no oficial). Consultado el 22 de febrero de 2019. Nota: Puede consultar el documento completo en su idioma original en el link.

[67] Cfr. The Federal Trade Commission (FTC), en: https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_decision_and_order.pdf (Traducción no oficial). Consultado el 22 de febrero de 2019. Nota: Puede consultar el documento completo en su idioma original en el link.

[68] Cfr. The Information Comissioner's Office, ICO, en: https://ico.org.uk/media/action-weve-taken/mpns/2553890/uber-monetary-penalty-notice-26-november-2018.pdf (Traducción no oficial). Consultado el 22 de febrero de 2019. Nota: Puede consultar el documento completo en su idioma original en el link.

b) Los atacantes le informaron a UBER que ellos habían accedido al repositorio de "*GitHub*", usando nombres de usuarios y contraseñas de otras cuentas de empleados de UBER, las cuales, según la decisión, habían sido violado anteriormente.

c) Los atacantes efectuaron dicho acceso por un relleno de credenciales "*credential stuffing*", un proceso mediante el cual los pares de nombres de usuarios y contraseñas comprometidos se inyectan en los sitios web hasta que se comparan con una cuenta existente, que luego se piratea "*hijacked*" con fines fraudulentos. Los atacantes le dijeron a UBER que habían identificado las contraseñas de las cuentas de "*GitHub*", pertenecientes a 12 de los empleados de UBER.

d) Habiendo accedido a la cuenta de UBER en Amazon S3, los atacantes descargaron el contenido de 16 archivos. En un informe de auditoría forense realizado por UBER, se encontró que esos archivos contenían la siguiente información:

   i. Registros de aproximadamente 32 millones de usuarios establecidos fuera del territorio de los Estados Unidos. Los registros incluían: nombre completo, número de celular, dirección de correo electrónico y ubicación (o localización) del registro inicial de aquellos usuarios quien habían activado la funcionalidad de los datos de ubicación, como se refleja en los archivos de UBER el 24 de junio de 2015. También incluían versiones con sal y hash de algunas contraseñas de usuario, actuales y anteriores, en un archivo actualizado por última vez en agosto 20 de 2015.
   ii. Registros de aproximadamente 3.7 millones de usuarios establecidos fuera del territorio de los Estados Unidos. Esos registros, en algunos casos, incluían: (i) los números de licencia de los conductores; y (ii) los resúmenes de las rutas suministradas por los conductores, por ejemplo, cuánto pagaron los conductores en una semana, un resumen por viaje, el tipo de viaje y cuándo se creó la factura.

e) Amazon S3 fue usado en el tiempo relevante para almacenar los anteriores datos, incluyendo, datos personales adicionales. La credencial podría acceder alrededor de 100 "*buckets*" dentro de S3. Alguna de la información en esos "*buckets*" fue accedida por los atacantes durante el ataque.

f) Los atacantes alertaron a UBER el 14 de noviembre de 2016 sobre el incidente. Ellos requirieron un pago de al menos $100.000 para revelar como ellos habían accedido a las cuentas de Amazon S3 y le advirtieron que ellos no iban a proceder a destruir los datos que ellos habían descargado hasta que el pago por parte de UBER fuera recibido.

g) En respuesta a la solicitud de los atacantes, UBER: (i) tomó pasos para poner para poner fin al ataque, rotando la clave comprometida que se encuentra en "*GitHub*" que proporcionó acceso a Amazon S3, incluida la cuenta de servicio XXX, y solicitando la autenticación de dos factores para acceder a los repositorios privados de "*GitHub*"; y, (ii) pagar a los atacantes la suma de $100,000, a través del tercero que administra el programa "*bug bounty*" (Este programa invita a expertos en seguridad de la información externos a encontrar vulnerabilidades en el sistema de UBER y divulgar el método de compromiso a Uber, en cambio de una recompensa); y, (iii) obtuvieron un seguro de los atacantes que los datos descargados habían sido destruidos.

21.2.2. Conforme a lo anterior, ICO concluyó lo siguiente:

a) Los acuerdos de seguridad adoptados por UBER fueron de hecho inadecuados, por las siguientes razones:
   i. Las políticas y prácticas de UBER no cubrieron adecuadamente los riesgos presentados por el uso de las plataformas de terceros, como "*GitHub*", sin un sistema de autenticación multifactor.
   ii. UBER no ordenó el uso de dos factores de autenticación para acceder a los repositorios privados de Uber en "*GitHub*".
   iii. A pesar de que la política de seguridad de la información de UBER se refiere a no usar "*Uber's Onelogin password*", UBER no prohibió expresamente a su personal el re-uso de las credenciales en las plataformas de terceros, incluido "*GitHub*". En ese tiempo, los atacantes fueron capaz de obtener acceso a las cuentas "*GitHub*" de 12 empleados, en la medida en que dichos empleados habían reusado sus "*GitHub*" credenciales en otras plataformas.
   iv. Las credenciales fueron obtenidas en texto simple en una pieza de código que fue almacenada en "*GitHub*". UBER ha confirmado que mientras ellos no tenían una política

escrita y formal sobre esa materia, su lineamiento, sin embargo, era que los ingenieros no tienen credenciales codificadas en formato de texto simple.

v. UBER había adoptado una herramienta para la herramienta *'secrets'*, con el fin de generar y gestionar las credenciales de cuenta en Amazon S3. A pesar de que esa herramienta permitía a los ingenieros rotar o configurar la rotación de las credenciales de la cuenta de Amazon S3, la credencial no había sido rotada. UBER no fue capaz de explicar por qué esa credencial no había sido rotada, a pesar de que ellos creen que eso fue atribuido a un error humano en la herramienta más que cualquier falla o falla adecuada para probarlo.

b) La decisión de UBER de tratar el evento ocurrido en la plataforma Amazon S3 como una recompensa de errores "o *bug bounty*", en lugar de un incidente de seguridad, demuestra, según la decisión, una falla de la organización en la toma de decisiones. ICO reconoce que el programa "*bug bounty*" puede ser una práctica legítima para el pago de recompensas financieras para la divulgación responsable de vulnerabilidades de seguridad. Sin embargo, frente al incidente ocurrido, UBER no siguió los pasos descritos en su programa de recompensas, en la medida en que los atacantes no reunían los requisitos que deben cumplir los destinatarios legítimos de su programa; en cambio de identificar una vulnerabilidad y divulgar la misma responsablemente a UBER, los atacantes maliciosamente explotaron la vulnerabilidad e intencionalmente adquirieron información personal relacionada a los usuarios de UBER.

c) Teniendo en cuenta el estado del desarrollo tecnológico, el costo de la implementación de cualquier medida, la naturaleza de la información personal y el daño que podría resultar de un mal uso frente a los datos personales de los individuos, las prácticas de UBER, descritas en la decisión, constituyen insuficiencias en los acuerdos de UBER para asegurar la seguridad de la información en el sistema S3.

21.3. The Commission Nationale de l'informatique et des libertés (CNIL) de Francia

21.3.1. El 20 de diciembre de 2018,[69] la Comisión Nacional de Informática y de las Libertades de Francia (La Commission Nationale de l'informatique et des libertés, CNIL), en adelante CNIL por sus siglas en francés, anunció que esa entidad el 19 de diciembre había sancionado a UBER FRANCE SAS, una compañía propiedad de UBER TECHNOLOGIES INC., y UBER B.V.,[70] por no garantizar la seguridad y confidencialidad de los datos personales[71]. La CNIL encontró lo siguiente:

a) UBER sostiene que solo UBER B.V. puede considerarse responsable del Tratamiento y que UBER TECHNOLOGIES INC., solo actúa como encargado de UBER B.V., y como tal, la empresa UBER TECHNOLOGIES INC. redactó pautas de gestión de datos, capacitó a nuevos empleados del grupo, firmó contratos con empresas de terceros y gestionó las consecuencias de la violación de datos.

b) Se recuerda que, de acuerdo con el dictamen del Grupo de Trabajo del Artículo 29 (Hoy Comité Europeo de Protección de Datos) No. 1/2010 del 16 de febrero de 2010, sobre los conceptos de controlador y encargado, un encargado que adquiere un papel importante en la determinación de los propósitos o medios esenciales de Tratamiento son más un (co) responsable del Tratamiento que un encargado.

c) Es UBER TECHNOLOGIES INC., la entidad que gestionó el incidente de seguridad en datos personales y fue UBER TECHNOLOGIES INC., quien, a través de un artículo publicado por su director general "o *CEO*", reveló al público la existencia del incidente de seguridad en datos personales.

d) Es UBER TECHNOLOGIES INC., quien ha escrito varios documentos claves relacionados con la gestión de los datos personales recopilados, incluidas las directrices que aplican a todas las entidades del grupo UBER. También es esta entidad la que se encarga de capacitar a los nuevos empleados del grupo.

---

[69] Cfr. La Commission nationale de l'informatique et des libertés (CNIL), en: https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037830841&fastReqId=413824161&fastPos=1. (Traducción no oficia). Consultado el 4 de marzo de 2019. Puede consultar el documento completo en su idioma original en el link.

[70] Cfr. La Commission nationale de l'informatique et des libertés (CNIL), en: https://www.cnil.fr/fr/uber-sanction-de-400000eu-pour-une-atteinte-la-securite-des-donnees-des-utilisateurs. (Traducción no oficial). Consultado el 4 de marzo de 2019. Puede consultar el documento completo en su idioma original en el link.

[71] Cfr. La Commission nationale de l'informatique et des libertés (CNIL), en: https://www.cnil.fr/fr/uber-sanction-de-400000eu-pour-une-atteinte-la-securite-des-donnees-des-utilisateurs. (Traducción no oficial). Consultado el 4 de marzo de 2019. Puede consultar el documento completo en su idioma original en el link.

e) Se considera que la multitud de campos de acción en los que interviene UBER TECHNOLOGIES INC., testifica de su papel determinante en la determinación de los fines y los medios de Tratamiento. Como resultado, las empresas UBER B.V. y UBER TECHNOLOGIES INC., deben ser calificados conjuntamente como corresponsables del Tratamiento.

21.3.2. Siguiendo lo anterior, la CNIL destacó lo siguiente:

a) A pesar de la recomendación de la plataforma "*GitHub*", le correspondía a la compañía, como responsable, adoptar las políticas que garantizaran la seguridad de la información almacenada en "*GitHub*" que, si no constituía en sí mismos, los datos personales (eran claves de acceso a los servidores [...]), sin embargo, permitían el acceso directo a una gran cantidad de datos relacionados con los usuarios del servicio UBER.

b) Se considera que la ausencia de un proceso relacionado con el retiro de los usuarios y contraseñas de los antiguos ingenieros constituye una negligencia importante, pues la empresa no pudo garantizar que las personas que habían abandonado UBER no siguieran accediendo a los proyectos desarrollados en "*Github*".

c) Se recuerda, en este punto, que en el área de la autenticación, es importante garantizar que las credenciales para conectarse de forma segura a servidores que contienen una gran cantidad de datos personales no puedan ser reveladas. Por lo tanto, es imperativo que dichos identificadores no se almacenen en un archivo que no esté protegido.

d) La decisión de la empresa muestra que, por un lado, era consciente de que los identificadores de acceso estaban potencialmente presentes en su código fuente y, por otro lado, que la presencia de dicha información dentro de "*GitHub*" era una fuente de riesgo.

e) Se considera que cuando se hace que los empleados se conecten de forma remota a los servidores utilizados por una empresa, asegurar esta conexión es una precaución básica para preservar la confidencialidad de los datos procesados.

f) En conclusión, UBER fue negligente al no implementar algunas medidas básicas de seguridad y no tomó todas las precauciones necesarias para evitar que terceros no autorizados tuvieran acceso a los datos procesados, lo que se constituye en una violación de la ley.

21.4. The Dutch Data Protection Authority (Dutch DPA) de los Países Bajos

21.4.1. El 6 de diciembre de 2018[72], la Autoridad de Protección de Datos de los Países Bajos (Autoriteit Persoonsgegevens), en adelante la "Dutch DPA", por sus siglas en inglés, encontró que UBER incumplió la regulación holandesa en protección de datos personales. La Dutch DPA concluyó que:

a) UBER BV (en adelante UBV) y UBER TECHNOLOGIES INC. (en adelante UTI) celebraron un "*Acuerdo de procesamiento de datos*" el 31 de marzo de 2016. En dicho acuerdo, UBV y UTI acordaron que UBV fuera el responsable del Tratamiento de los datos personales de los usuarios ubicados fuera del territorio de los Estados Unidos y que UTI procesaría los datos como encargado del Tratamiento para UBV.

b) UTI suscribió un contrato de almacenamiento en la nube (o "*cloud*") con Amazon (AWS S3). El propósito de dicho contrato era almacenar las copias de seguridad de los datos personales.

c) El 14 de noviembre de 2016, UTI fue informada de una vulnerabilidad en su seguridad de datos. En esa fecha, UTI recibió un correo electrónico en el cual una persona le informó que él y su equipo habían descubierto una vulnerabilidad importante en la seguridad de los datos del grupo Uber. La persona tuvo acceso al almacenamiento de AWS S3 durante el período del 13 de octubre de 2016 al 15 de noviembre de 2016, a través de los datos de inicio de sesión almacenados en un repositorio privado de "*GitHub*" del grupo UBER.

d) El 15 de noviembre de 2016, UTI remedió la violación de datos. La violación de datos hizo que UTI contratara un experto forense. El experto investigó en qué medida los atacantes tenían

[72] Cfr. Autoriteit Persoonsgegevens, "Dutch DPA: fine for data breach Uber", en: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_uber.pdf. (Traducción no oficial). Consultado el 1 de marzo de 2019. Puede consultar el documento completo en su idioma original en el link.

acceso a los datos personales almacenados en los servidores de Amazon. Encontró, en este punto, que 57,383,315 usuarios de UBER estuvieron involucrados en la violación de datos, de los cuales 25,606,182 eran estadounidenses y 31,777,133 eran no eran estadounidenses. La investigación llevada a cabo por el experto muestra que 31 tipos de datos personales estuvieron involucrados en la violación de datos.

e) El 25 de octubre de 2017, UBV se dio cuenta de lo que UBER llama "*un incidente de seguridad de TI*" en 2016, que estaba siendo investigado y que potencialmente podría crear un ciclo de medios. Una discusión tuvo lugar entre UTI y UBV el 4 de noviembre de 2017. Durante esta discusión, UTI indicó que hubo un incidente de seguridad. El 21 de noviembre de 2017, el actual CEO de UTI publicó una noticia en el sitio web de UBER para informar al público sobre la violación de datos. Ese mismo día, UBV informó sobre la violación de la seguridad de los datos personales a la Dutch DPA.

f) UBV y UTI son co-responsables del Tratamiento. En efecto, la Dutch DPA considera que: (i) UBV junto con UTI determinan los propósitos y los medios para el procesamiento de los datos personales; y, (ii) UTI y UBV toman decisiones (conjuntas) con respecto al establecimiento de objetivos y medios para el procesamiento de datos. La Dutch DPA recuerda, en este punto, que el responsable del Tratamiento es aquel que determina el propósito y los medios del procesamiento de los datos. Él puede hacer esto solo, pero también con otros.

g) Los datos personales procesados por el grupo UBER están respaldados y almacenados en AWS S3 en los Estados Unidos. El procesamiento de los datos personales para realizar copias de seguridad se realiza en el marco del proceso de negocio regular (diario) del grupo UBER y, como tal, puede considerarse como parte del servicio normal a los usuarios de la Aplicación UBER.

h) UTI también determina (en parte) los recursos para el procesamiento. Es importante tener en cuenta que incluso si alguien simplemente determina los medios, puede ser responsable del Tratamiento.

i) La Dutch DPA enfatiza que UTI determina (parcialmente) el propósito del procesamiento y, por lo tanto, ya puede calificarse como responsable conjunto con UBV.

j) La Dutch DPA aclara, en este punto, que la responsabilidad conjunta también está determinada por la aplicación de una política de privacidad uniforme y la determinación por parte de UTI de la política de seguridad de la información, así como el desarrollo, la oferta y las actualizaciones de las Aplicaciones UBER que se tratarán a continuación y el manejo de la violación de datos por parte de UTI.

k) UTI también toma decisiones importantes con respecto al almacenamiento y tiene un alto grado de control, por ejemplo, es UTI la que ha firmado un acuerdo con Amazon para el almacenamiento de copias de seguridad y la violación de datos afectó los datos personales almacenados en las copias de seguridad en el almacenamiento AWS S3 (externo) en los Estados Unidos.

l) La Dutch DPA señala que las decisiones fácticas sobre el manejo de la violación de datos, sobre las cuales se enteró UBV casi un año después de la fecha en que se produjo la violación de datos, fueron tomadas de manera independiente, y solo por el personal de UTI. Existe por el XXX de UTI, sin conocer UBV y darle la oportunidad de influir en ella, las medidas específicas tomadas. Estas medidas se centran en el cifrado de archivos en los depósitos de AWS S3 y requieren una autenticación de dos factores para los servicios que utiliza el grupo UBER y que son accesibles a través de Internet

m) La Dutch DPA confirma que UTI toma decisiones de manera independiente y, de hecho, tiene control sobre la forma en que se maneja una violación de datos, incluido el pago de la recompensa a los atacantes, con el fin de "proteger los datos de nuestros consumidores".

n) Frente a la violación, la Dutch DPA retoma el informe que presentó un forense contratado por UBER, quien encontró que personas no autorizadas obtuvieron acceso al llamado repositorio privado de "*GitHub*" de UBER, utilizando nombres de usuario y contraseñas previamente filtrados. Estas personas no autorizadas descargaron archivos de este almacenamiento de AWS S3 por primera vez el 13 de octubre de 2016 y por última vez el 15 de noviembre de 2016. Indica

que la fuga de datos duró casi cinco semanas. Durante ese período, personas no autorizadas podrían, en cualquier caso, acceder a los datos personales de los clientes de UBER. Esto incluía datos personales sin cifrar, como el nombre, el apellido, la dirección de correo electrónico y los números de teléfono de los usuarios holandeses de UBER.

o) Señala que, en este caso, personas no autorizadas descargaron archivos de UBER en su almacenamiento AWS S3 y, por lo tanto, tuvieron acceso a los datos personales de los clientes de UBER que contenían esos archivos, hubo un procesamiento ilegal y las consecuencias adversas para la protección de datos personales. Por eso, en opinión de la Dutch DPA, hay graves consecuencias adversas.

p) El tamaño de los datos personales involucrados en la violación de datos o el incidente de seguridad, la gran cantidad de diferentes tipos de datos personales, el tipo de datos personales (nombres, direcciones de correo electrónico y números de teléfono), así como el hecho de que se trata de datos personales de clientes específicos de una empresa que opera a nivel mundial, hacen que los datos personales sean extra atractivo para terceros por ejemplo, para ser revendidos para actividades tales como '(*spear) phishing*', publicidad no deseada (*spam*) y / o compras telefónicas no deseadas.

q) El impacto y la gravedad de la violación de los datos y, por lo tanto, respaldan la conclusión de la Dutch DPA de que existe la posibilidad considerable de consecuencias adversas graves para los individuos, también se puede deducir del hecho de que UBER acudiera a un subcomité de Senado de los Estados Unidos.

r) Cuando UBER se dio cuenta de la violación de los datos y de los datos personales que participaron en este proceso a mediados de noviembre de 2016, hubo motivos suficientes para informar a las partes interesadas sobre las consecuencias desfavorables, como el riesgo de *phishing* (por ejemplo). En ese momento era un riesgo real y eso no podía ser razonablemente excluido.

s) En la opinión de la Dutch DPA, la administración de UTI era consciente de la gravedad de la violación de datos y querían evitar que se hiciera público. Esto se muestra, en primer lugar, por la velocidad con la que UTI aceptó el pago de una cantidad a los detectores de la violación de datos. En segundo lugar, el monto pagado a los reporteros es sustancialmente más alto de lo habitual. En tercer lugar, acordó obligaciones de confidencialidad adicionales con los atacantes o denunciantes frente al incidente.

t) En opinión de la Dutch DPA, la violación ha dañado seriamente la confianza en el manejo de datos personales.

21.5. The Office of the Attorney General of California

21.5.1. El 26 de septiembre de 2018[73], el Fiscal General de California, señor Xavier Becerra, y el Fiscal del Distrito de San Francisco, señor George Gascón, publicaron en la página web de sus oficinas un acuerdo suscrito por todos los 50 fiscales generales de los EE.UU, el distrito de Columbia y UBER, para resolver las acusaciones que UBER TECHNOLOGIES, INC., había violado las normas estatales sobre la seguridad de la información y de notificación de incidentes de seguridad respecto de la brecha de seguridad que afectó en el año 2016 la información de sus usuarios y conductores. UBER fue acusado de exponer los datos de 57 millones de usuarios y pagar a piratas informáticos (o *hackers*), para encubrir el incumplimiento en lugar de informar a las autoridades correspondientes.

El acuerdo sigue la investigación independiente del Estado de California sobre la omisión de UBER de informar a los más de 174,000 conductores de California sobre el incidente de seguridad que afectó su información personal (nombres y los números de las licencias de conducir). En lugar de notificar a los conductores como lo exige la ley, UBER cubrió el incidente y luego pagó a los *hackers* US$100,000 a cambio de su silencio. La compañía no notificó a la policía ni al público el incumplimiento hasta noviembre de 2017, cuando fue descubierta por una revisión interna realizada por la Junta Directiva de UBER.

---

[73] Cfr. The Office of the Attorney General for Falifornia, "California Attorney General Becerra, San Francisco District Attorney Gascón Announce $148 Million Settlement with Uber over 2016 Data Breach and Cover-Up", en: https://oag.ca.gov/news/press-releases/california-attorney-general-becerra-san-francisco-district-attorney-gasc%C3%B3n (Traducción no oficial) Consultado el 1 de marzo de 2019. Puede consultar el documento completo en su idioma original en el link.

21.5.2. Además de las sanciones civiles, el acuerdo también requiere que UBER[74]:

a) Implementar y mantener prácticas sólidas de seguridad de datos.

b) Cumplir con las leyes estatales en relación con su recopilación, mantenimiento y protección de la información personal, así como el informe de incidentes de seguridad de datos.

c) Representar de manera precisa y honesta las prácticas de privacidad y seguridad de los datos para garantizar una mayor transparencia en la forma en que se protege la información del conductor y del cliente de la empresa.

e) Desarrollar, implementar y mantener un programa integral de seguridad de la información con un funcionario ejecutivo que asesora al personal ejecutivo clave y a la Junta Directiva de UBER.

f) Reportar cualquier incidente de seguridad de datos a los estados trimestralmente durante dos años.

g) Mantener un Programa de Integridad Corporativa que incluya una línea directa para informar sobre conductas indebidas, informes trimestrales a la junta directiva, implementación de los principios de privacidad y un código anual de capacitación sobre conducta

21.5.3. El acuerdo fue aprobado por el Juez de la Corte Superior del estado de California para el estado de San Francisco, señor Richard Ulmer.

21.6. The Office of the Australian Information Commissioner (OAIC), the Office of the Privacy Commissioner for Personal Data of Hong Honk (PCPD), the Office of the Privacy Commissioner of Canada (OPC), el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), the National Privacy Commission of the Philippines y the Office of the Privacy Commissioner of New Zealand (OPC).

Con ocasión del comunicado de prensa del 22 de noviembre de 2017 por parte del señor Dara Khosrowshahi, director ejecutivo o "*CEO*" de UBER, (i) la Oficina del Comisionado de Información de Australia (The Office of the Australian Information Commissioner, OAIC)[75]; (ii) la Oficina del Comisionado de Privacidad para la Protección de los Datos de Hong Kong (The Office of the Privacy Commissioner for Personal Data of Hong Kong, PCPD)[76]; (iii) la Oficina del Comisionado de Privacidad de Canadá, OPC[77], el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[78], (iii) la Comisión Nacional de Privacidad de las Filipinas (The National Privacy Commission of the Philippines)[79]; la Oficina del Comisionado de Privacidad de Nueva Zelanda (The Office of the Privacy Commissioner of New Zealand)[80], en adelante "OPC", por sus siglas en inglés, anunciaron que habían requerido, a los representantes de UBER en esos países, información relacionada con el incidente de seguridad que ocurrió entre octubre y noviembre de 2016, el tipo de datos afectados, la cantidad de usuarios afectados en esos respectivos países y las medidas implementadas que había implementado UBER para evitar incidentes de seguridad en el futuro.

21.7 Congreso de los Estados Unidos de América

---

[74] Cfr. The Office of the Attorney General of California. Copia del fallo final en: https://oag.ca.gov/system/files/attachments/press-docs/uber-final-judgmentscanned_0.pdf Consultado el 1 de marzo de 2019. Puede consultar el documento completo en su idioma original en el link.

[75] Cfr. The Office of the Australian Information Commissioner (OAIC)", en: https://www.oaic.gov.au/media-and-speeches/statements/uber.

[76] Cfr. The Office of the Privacy Commissioner for Personal Data of Hong Kong, PCPD, en: https://www.pcpd.org.hk/tc_chi/news_events/media_enquiry/enquiry_20171122.html.

[77] Cfr. The Office of the Privacy Commissioner of Canada (OPC), en: https://www.priv.gc.ca/en/about-the-opc/opc-operational-reports/reporting-of-opc-spending/drr_index/2017-2018/drr_2017-18/.

[78] Cfr. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), en: http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-389-17.pdf.

[79] Cfr. The National Privacy Commission (NPC), en: (i) https://www.privacy.gov.ph/2017/11/statement-privacy-commissioner-raymund-enriquez-liboro-personal-data-breach-sustained-uber-2016/; (ii) https://www.privacy.gov.ph/2017/11/statement-privacy-commissioner-raymund-enriquez-liboro-npcs-november-23-meeting-uber-ph/; (iii) https://www.privacy.gov.ph/2017/12/latest-statement-privacy-commissioner-raymund-enriquez-liboro-uber-personal-data-breach/; y, (iv) https://www.privacy.org.nz/news-and-publications/statements-media-releases/privacy-commissioner-monitoring-uber-data-breach/. Consultado el 26 de febrero de 2019.

[80] Cfr. The Office of the Privacy Commissioner of New Zealand, en:

21.7.1. El 6 de febrero de 2018, el Comité del Senado sobre Comercio, Ciencia y Transporte del Senado de los Estados Unidos realizó la audiencia[81]: "Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers"[82], con el testimonio del Director de Seguridad de la Información o "Chief Information Security Officer" de UBER TECHNOLOGIES, INC., señor John Flynn, UBER.

21.7.2. El senador Jerry Moran precisó en el inicio de la audiencia que el hecho de que UBER tardara aproximadamente un año en notificar (o reportar) a los usuarios afectados genera señales de alerta dentro de este Comité, en cuanto a qué cuestiones sistémicos le impidieron a UBER notificar sobre dicha situación a los afectados.

21.7.3. Chief Information Security Officer de UBER TECHNOLOGIES, INC.

En su testimonio[83] ante el comité, el señor John Flynn se enfocó en tres temas, a saber: [84](i) la importancia de los programas de recompensas frente a las amenazas cibernéticas; (ii) su perspectiva sobre el incidente de seguridad de datos sucedido en UBER en el 2016; y, (iii) las lecciones aprendidas con posterioridad al incidente[85]. Frente al segundo punto, se cita parte del testimonio[86]:

a) Con posterioridad al correo electrónico que UBER recibió de unos agentes externos (intrusos) sobre una vulnerabilidad encontrada por ellos, incluyendo la exigencia del pago de una recompensa, UBER investigó y determinó que el individuo y otra persona que trabajaba con él habían obtenido acceso a ciertas copias archivadas de las bases de datos y archivos de UBER ubicados en el entorno de almacenamiento de datos en la nube privada de UBER en Amazon Web Services ("AWS").

b) El acceso de los intrusos comenzó el 13 de octubre de 2016 y los intrusos no tuvieron más acceso después del 15 de noviembre de 2016.

c) Los datos provenían de archivos de respaldo almacenados en un contenedor AWS S3. S3 significa "servicio de almacenamiento simple".

d) El intruso encontró una credencial contenida en el código en un repositorio privado para los ingenieros de UBER en "*GitHub*", que es un sitio de terceros que permite a las personas colaborar sobre el código.

e) UBER tomó las medidas inmediatas para implementar la autenticación multifactor para "*GitHub*" y rotó la credencial de AWS utilizada por el intruso.

f) Se inició el proceso de eliminación del código adicional de "*GitHub*" que podría considerarse sensible y confirmando la rotación de llaves. Se dejó de usar "*GitHub*", excepto para elementos como el código fuente abierto.

VIGÉSIMO SEGUNDO: Actuaciones de la Dirección de Investigación de Protección de Datos Personales en relación con el incidente de seguridad que afectó datos personales en custodia o posesión de UBER.

---

[81] Cfr. Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security Committee on Commerce, Science and Transportation United States Senate, "*Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers*", en: https://www.commerce.senate.gov/public/index.cfm/2018/2/data-security-and-bug-bounty-programs-lessons-learned-from-the-uber-breach-and-security-researchers. Nota: Los objetivos de la audiencia fueron los siguientes: (i) discutir la violación de datos de UBER en octubre de 2016 y las acusaciones contra UBER sobre los pagos no permitidos para ocultar el incidente de seguridad a través de su programa de recompensas por errores "*bug bounty*"; y (ii) averiguar exactamente qué evitó que UBER notificara de inmediato a los usuarios que se vieron afectados por el incumplimiento de 2016, los detalles de los pagos relacionados y los pasos que UBER está tomando internamente para mejorar sus protocolos de notificación. Consultado el 5 de marzo de 2019.

[82] Cfr. Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security Committee on Commerce, Science and Transportation United States Senate, "Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers. Chairman Jerry Moran." en: https://www.commerce.senate.gov/public/index.cfm/hearings?Id=73871FA8-29AD-4ED5-ABB8-. Consultado el 5 de marzo de 2019.C86B4BE4E0A3&Statement_id=B5A93ABF-68B2-4117-99FE-28610D386362. Consultado el 5 de marzo de 2019. (Traducción no oficial).

[83] Cfr. UBER TECHNOLOGIES, INC., en: https://www.commerce.senate.gov/public/_cache/files/7d70e53e-73e9-4336-a100-67b233084f12/75728554E990488D71625DFA69B05494.uber---john-flynn---testimony.pdf. Consultado el 5 de marzo de 2019. (Traducción no oficial).

[84] Ibídem.

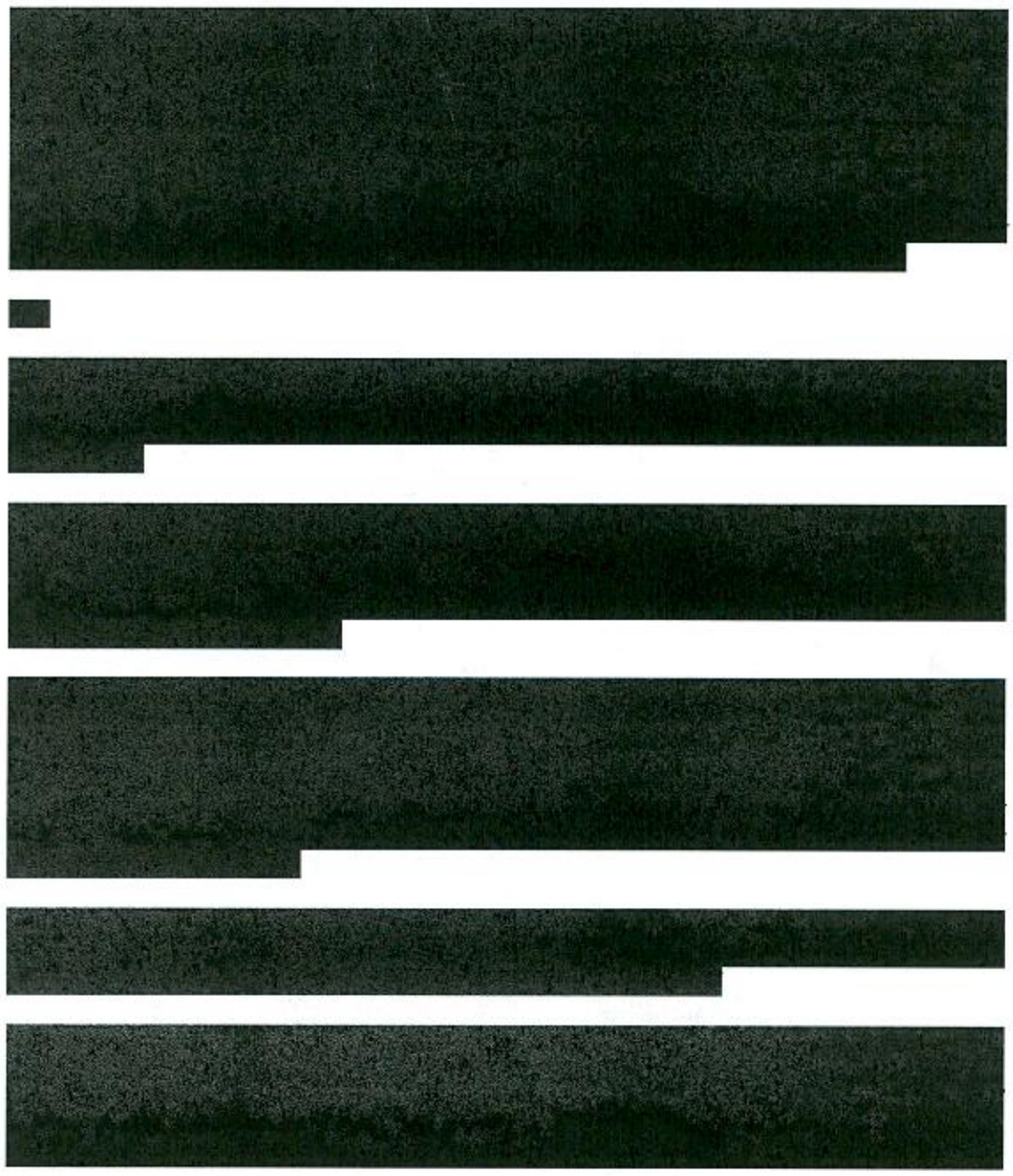
[85] Ibídem.

[86] Ibídem.

A continuación se describirá las diferentes actuaciones adelantadas por esta Dirección para determinar si en el incidente de seguridad que sufrió UBER (a saber: acceso no autorizado al sistema de almacenamiento Amazon Web Services "AWS" S3 por parte de atacantes externos) se comprometió información de personas residentes o domiciliadas en la República de Colombia, así como los informes que remitieron UBER TECHNOLOGIES, INC., UBER COLOMBIA SAS y UBER B.V., en caso en que lo hayan efectuado, respecto de lo ocurrido.

22.1. Que con base en el comunicado de prensa del 22 de noviembre de 2017 del señor Dara Khosrowshahi, director ejecutivo de UBER, esta Dirección requirió preliminarmente a UBER TECHNOLOGIES, INC.[87], UBER COLOMBIA SAS[88] y UBER B.V[89] para que informarán si el incidente de seguridad sufrido había afectado datos personales de ciudadanos colombianos. Las sociedades UBER TECHNOLOGIES, INC y UBER B.V. no remitieron respuestas a los requerimientos efectuados por esta Dirección.

22.2. El 4 de enero de 2018[90], UBER COLOMBIA SAS le informó a esta Dirección que el número de colombianos afectados por el incidente de seguridad se estima en 267.000 y que UBER está adoptando los pasos necesarios para evitar futuros incidentes de seguridad como el reportado por parte de su director ejecutivo, empezando por el cambio de personal y otras acciones correctivas. Se cita la respuesta:



[87] Radicado 19-40311-7 del 2 de mayo de 2019. Guía 4/72 No. CP002561860CO. Guía No. 6959651742. Entregada el 9 de mayo de 2019 Folios 31-34).
[88] Folio 6.
[89] Radicado 19-40311-6 del 2 de mayo de 2019. Guía 4/72 No. CP002561856CO. Guía No. 6959633310. Entregada el 10 de mayo de 2019 Folios 30,33 y 35).
[90] Folios 8-11.

[redacted]

UBER COLOMBIA SAS también le informó a esta Dirección lo siguiente:

[redacted]

[redacted]

22.3. El 15 de mayo de 2018[91], UBER COLOMBIA SAS informó **que UBER TECHNOLOGIES INC. ("UTI"), sociedad con sede en los Estados Unidos, es la entidad encargada de procesar los datos personales que habrían estado involucrados en el incidente de seguridad de datos de 2016**. Se cita la respuesta:

[91] Folios 14-21.

[redacted]

[redacted]

[redacted]

22.4. Con el interés de promover la plena cooperación con la Superintendencia de Industria y Comercio ("SIC"), el 26 de junio de 2018[92] UBER COLOMBIA SAS remitió la información que UBER B.V. y UBER Technologies, Inc. ("UBER") le habían suministrado. Dice el documento:

[redacted]

[92] Folios 22-25.

[redacted]

Así mismo, en el memorial se resumió las medidas correctivas implementadas por UBER para contener, mitigar el impacto y prevenir que en el futuro haya incidentes de esta naturaleza, a saber:

[redacted]

VIGÉSIMO TERCERO: Conclusiones de la Dirección de Investigación de Protección de Datos Personales.

Los derechos de los titulares de los datos personales de los residentes o ciudadanos en Colombia son, como se subrayó al inicio de la presente resolución, merecedores de especial protección constitucional bajo el artículo 15 de la Constitución Política y de la Ley 1581 de 2012, Régimen General de Protección de Datos Personales. En esta oportunidad, las conclusiones a la que arriba esta Dirección son las siguientes:

a) UBER cuenta con unos 83.000 conductores afiliados y es usado mensualmente por alrededor de 2,1 millones de pasajeros en Colombia.

b) UBER usa y circula los datos de manera global y transfronteriza.

c) UBER TECHNOLOGIES, INC., UBER B.V. y UBER COLOMBIA SAS son tres compañías que hacen parte del grupo "UBER", que intervienen en el desarrollo, la distribución y la explotación de los servicios y productos de "UBER", incluida las aplicaciones móviles que están disponibles en territorio colombiano (Véase numeral 19 de la presente resolución).

d) UBER TECHNOLOGIES, INC. es la organización que suscribió el contrato Amazon Web Services "AWS" S3 con AMAZON y es la que, según la investigación de la autoridad de protección de datos de Holanda, está definiendo los propósitos del tratamiento de los datos personales recolectados para el desarrollo, la distribución y la explotación de los servicios y productos "UBER", así como las medidas de seguridad respecto de la información personal almacenada en AWS S3. Por su parte, UBER B.V. es la organización que, según su política de privacidad, se le otorgó formalmente la calidad de "Responsable del Tratamiento" para el tratamiento de datos de ciudadanos y residentes en Colombia, por lo cual está participando conjuntamente con UBER TECHNOLOGIES, INC en esa definición de propósitos o fines. Lo anterior sin perjuicio del papel determinante que juega UBER COLOMBIA SAS en el tratamiento de los datos en esa cadena comercial bajo la marca "UBER" (Véase numeral 19 de la presente resolución).

e) El comunicado de prensa por parte del director ejecutivo o *CEO* de UBER, visible a folio 5 del expediente, reconociendo el incidente de seguridad del año 2016, que afectó los datos personales de 57 millones de usuarios, **de los cuales 267.000 eran personas residentes en la República de Colombia**, las investigaciones y las decisiones de autoridades de protección de datos y del consumidor de Gran Bretaña, Francia, Países Bajos y los Estados Unidos de América, así como el acuerdo que llegó el Fiscal General del estado de California (Estados Unidos de América) aprobado por el Juez de la Corte Superior del Estado de California para el Estado de San Francisco, Richard Ulmer, evidencian que UBER:

(i) No adoptó las medidas de seguridad, suficientes y necesarias, **para impedir que terceras partes (en este caso: atacantes externos) accedieran, sin autorización, al sistema de almacenamiento Amazon Web Services "AWS" S3, y descargaran alrededor de** "*57 millones de cuentas de usuarios con información personal, **de los cuales 267.000 eran residentes colombianos***[93], y de carácter sensible para ellos por las consecuentes que pueden generar el uso de dicha información por parte de esos terceros. Los datos afectados se resumen a continuación:

[redacted]

(ii) No implementó las medidas de seguridad, suficientes y necesarias, para impedir que las credenciales de acceso otorgadas a sus empleados estuvieran disponibles en "texto plano" en "*GutHub*", una plataforma de desarrollo en línea de software para terceros. Dicha situación facilitó que los atacantes conocieran y explotaran esa vulnerabilidad, utilizaran esas credenciales, accedieran al sistema de almacenamiento Amazon Web Services ("AWS") S3, descargaran "[redacted][95], y requirieran a UBER el pago de una suma de dinero[96].

(iii) Falló en detectar, de una manera oportuna y frente a un movimiento inusual de cuentas, que terceros habían accedido al sistema de almacenamiento Amazon Web

[93] Folio 10.
[94] Folio 16.
[95] Folio 9.
[96] Folio 11.

Services ("AWS") S3 y, más grave aún, que habían descargado gran cantidad de información personal. De hecho, según la comunicación remitida por UBER COLOMBIA el 4 de enero de 2018 a esta Dirección, UBER se enteró del acceso no autorizado y la descarga de información personal el 14 de noviembre de 2016, cuando los atacantes se contactaron con su equipo de seguridad para solicitar el pago de una suma de dinero[97]; esto, a pesar de que dicho acceso ocurrió entre el 3 de octubre al 15 de noviembre de 2016. Y, finalmente, el 22 de noviembre de 2017 UBER informó públicamente en su página web que había sufrido un incidente de seguridad. La anterior información se ilustra con el siguiente cuadro.

Fecha	Eventos
3 octubre – 15 de noviembre de 2016	Los atacantes accedieron al sistema de almacenamiento Amazon Web Services ("S3"), y descargaron alrededor de "57 millones de cuentas de usuarios con información personal, de los cuales 267.000 eran residentes colombianos
14 de noviembre de 2016	Los atacantes se comunicaron con UBER para informarle sobre el acceso y descarga de la información personal del sistema de almacenamiento Amazon Web Services ("S3").
22 de noviembre de 2017	UBER reconoció públicamente que, entre el 3 de octubre y el 15 de noviembre de 2016, terceros no autorizados habían accedido, a información personal almacenada del sistema de almacenamiento Amazon Web Services ("S3").

(iv) Fracasó en aplicar sistemas de autenticación multifactor efectivos para todos sus usuarios con el propósito de acceder remotamente de forma segura a los sistemas de almacenamiento con datos personales.

(v) Omitió informar a los individuos afectados en Colombia para que adoptaran por ellas mismas medidas para proteger su información personal en posesión o custodia de UBER, por ejemplo, actualizar (o cambiar) su nombre de usuario y contraseña. La diferencia de un año entre la fecha en que ocurrió el incidente de seguridad y la fecha en que UBER notificó a los individuos afectados generó, en este caso, que estos últimos no pudieran adoptar las medidas que deberían haber tomado si hubieran conocido, de manera completa y oportuna, lo sucedido.

(iv) **Lecciones no aprendidas de incidentes de seguridad anteriores**: La Dirección resalta que, conforme a la investigación que realizó la Comisión Federal de Comercio de los Estados Unidos de América y resumida en esta resolución en el punto 19.1.1., UBER desde el año 2014 tenía conocimiento de las vulnerabilidades en sus controles de acceso y gestión de contraseñas en el sistema de almacenamiento Amazon Web Services ("AWS") S3. Lo que significa que, probablemente, el incidente de seguridad del 2016 se hubiera evitado si, en este caso, UBER hubiera: (i) aprendido de ese incidente; (ii) implementado medidas efectivas para proteger la información personal y (iii) adoptado controles de acceso y gestión de contraseñas seguras y sólidas para acceder al sistema Amazon Web Services AWS ("S3"), sin embargo, por la falta de debida diligencia de la compañía la puerta de entrada a los datos personales para los atacantes continuó abierta y ellos aprovecharon dicha vulnerabilidad.

En suma, las medidas de seguridad de UBER no demuestran ser suficientes ni adecuadas para garantizar la seguridad de los datos de millones de personas, en particular frente al acceso por parte de terceros no autorizados (en este caso: atacantes). Lo anterior es extremadamente grave porque la seguridad es un elemento esencial para realizar un debido tratamiento en datos

[97] Folios 8 y 11.

personales, garantizar la confianza depositada mencionada en su política de privacidad y cumplir con lo señalado en la Ley 1581 de 2012.

VIGÉSIMO CUARTO: Que la seguridad de la información es una condición crucial del tratamiento de datos personales. Una vez recolectados deben 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 de los datos. 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 quieren mitigar a través de medidas de seguridad de naturaleza humana, física, administrativa o técnica.

La seguridad ha sido una preocupación del legislador y la Corte Constitucional. Esta última concluyó que "*debe reiterarse que el manejo de información no pública debe hacerse bajo todas las medidas de seguridad necesarias para garantizar que terceros no autorizados puedan acceder a ella. De lo contrario, tanto el responsable como el Encargado del Tratamiento serán los responsables de los perjuicios causados al Titular*"[98].

La seguridad de los datos personales no se limita situaciones de infiltración o burla de las medidas de seguridad que ha implementado un Responsable o Encargado del Tratamiento. La 1581 de 2012 va más allá porque exige lo siguiente:

> "***ARTÍCULO 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES***. *En el desarrollo, interpretación y* ***aplicación*** *de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:*
>
> *(...)*
>
> *g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros* ***evitando*** *su adulteración, pérdida, consulta, uso o* ***acceso no autorizado o fraudulento***;
>
> *(...)*
>
> ***ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO.*** *Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
>
> *(...)*
>
> *d) Conservar la información bajo las condiciones de seguridad necesarias para* ***impedir su*** *adulteración, pérdida, consulta, uso o* ***acceso no autorizado*** *o fraudulento;*
>
> *(...)*
>
> ***ARTÍCULO 18. DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO.*** *Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
>
> *(...)*
>
> *b) Conservar la información bajo las condiciones de seguridad necesarias para* ***impedir*** *su adulteración, pérdida, consulta, uso o* ***acceso no autorizado*** *o fraudulento"*
>
> (Subrayado y negrita agregados)

Nótese que la redacción del principio de seguridad tiene un criterio eminentemente preventivo, lo cual obliga a los Responsables o Encargados del Tratamiento a adoptar las medidas necesarias para evitar posibles afectaciones a la seguridad de los datos. Este carácter preventivo obliga a los Responsable y Encargados a identificar sus vulnerabilidades con el objetivo de implementar o reforzar sus medidas de seguridad.

---

[98] Cfr. Corte Constitucional, Sentencia C-748 de 2011.

Es preciso aclarar que la implementación de las medidas de seguridad por parte de los Responsables y Encargados del Tratamiento no está supeditada o condicionada a que exista un daño o perjuicio de los derechos o intereses que se buscan proteger con la Ley 1581 de 2012. El solo hecho de tratar datos personales es suficiente. Una interpretación en sentido contrario, no solo iría en contra de la naturaleza preventiva que se deriva expresamente de los textos legales citados, sino que privaría a los colombianos de la capacidad de exigir a los Responsables y Encargados que aseguren un nivel adecuado de protección en relación con sus datos.

VIGÉSIMO QUINTO: Que la regulación colombiana exige a UBER cumpla el principio de responsabilidad demostrada respecto de las medidas de seguridad para realizar Tratamiento de datos personales. En efecto, los artículos 2.2.2.25.6.1. y 2.2.2.25.6.1. del Decreto Único Reglamentario 1074 de 2015 (anteriormente artículos 26 y 27 del Decreto 1377 de 2013) dicen lo siguiente:

> *"**Artículo 2.2.2.25.6.1. 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 capítulo, 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, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas**"*
> *(Subrayamos)*
>
> ***Artículo 2.2.2.25.6.2. Políticas internas efectivas.** En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 2.2.2.25.6.1. 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 deberán 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".*
>
> (Subrayado y negrita agregados)

Sobre la responsabilidad demostrada nos remitimos a lo señalado por la Superintendencia de Industria y Comercio mediante la Resolución 83882 del 15 de noviembre de 2018:

La regulación colombiana le impone al Responsable o al Encargado del Tratamiento la responsabilidad de garantizar el cumplimiento de la ley 1581 de 2012, la cual no puede ser simbólica ni formal, sino real y demostrable. Téngase presente que según nuestra jurisprudencia "*existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante*"[99].

Adicionalmente, los Responsables o Encargados del Tratamiento no son dueños de los datos personales que reposan en sus bases de datos o archivos. En efecto, ellos son meros tenedores

[99] Cfr. Corte Constitucional, sentencia T-227 de 2003.

que están en el deber de administrar de manera correcta, apropiada y acertada la información de las personas porque su negligencia o dolo en esta materia afecta los derechos humanos de los titulares de los datos.

En virtud de lo anterior, la sección tercera del capítulo 25 del Decreto Único Reglamentario 1074 de 2015 reglamenta algunos aspectos relacionados con el principio de responsabilidad demostrada. El artículo 2.2.2.25.6.1. -titulado 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*" y dicho decreto.

Nótese como le corresponde al Responsable o al Encargado probar que ha puesto en marcha medidas adecuadas, útiles y eficaces para cumplir la regulación. Lo anterior significa que un administrador no puede utilizar cualquier tipo de política o herramienta para dicho efecto sino sólo aquellas que sirvan para que los postulados legales no sean meras elucubraciones teóricas sino realidades verificables.

El artículo 2.2.2.25.6.2. -denominado POLÍTICAS INTERNAS EFECTIVAS-, por su parte, exige que los Responsables implementen medidas efectivas y apropiadas que garanticen, entre otras, lo siguiente: *"(…) 1. (…) la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este capítulo"*.

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)*"[100]. El término "*accountability*" proviene del mundo anglosajón[101] y a pesar de las diferentes acepciones que puedan darse sobre el significado del mismo, se ha entendido que en la arena de la protección de datos dicha expresión se refiere no sólo al modo como una organización debe cumplir en la práctica las regulaciones sobre el tema, sino a la manera como debe demostrar que lo hecho es útil, pertinente y eficiente.

En línea con lo anterior, la precitada guía recomienda lo siguiente a los obligados a cumplir la Ley 1581 de 2012:

(1) Diseñar y poner en marcha un programa integral de gestión de datos (en adelante PIGDP), lo cual exige compromisos y acciones concretas de los directivos de la organización, así como la implementación de controles de diversa naturaleza que se enuncian en el texto de la guía;

(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[102] 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 implementen medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia. Dichas 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 demanda menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre Tratamiento de datos personales. Éste exige implementar 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, pero, especialmente, de los directivos de las organizaciones ya que sin su apoyo franco y decidido todo esfuerzo será insuficiente para diseñar, implementar, revisar, actualizar y evaluar los programas de gestión de datos.

---

[100] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf
[101] Cfr. Grupo de trabajo de protección de datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 8.
[102] Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humanas y de gestión que involucran procesos y procedimientos.

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 porque exige que se demuestre el cumplimiento real y efectivo en la práctica cuando realizan 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 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***"[103] (Subrayado y negrita agregados).

El principio de responsabilidad demostrada busca, por tanto, 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 capaces de garantizar, entre otras, la seguridad en el Tratamiento de la información.

VIGÉSIMO SEXTO: Que, se reitera, que "UBER" tiene la enorme responsabilidad de garantizar la seguridad de la información de todos sus usuarios, lo cual lo obliga a ser extremadamente diligente en esta labor y a no ahorrar esfuerzos para responder por la seguridad de los datos de miles de millones de personas.

Conforme a lo anterior, esta Dirección considera necesario impartir a UBER directrices con **CARÁCTER PREVENTIVO** para evitar que sucedan incidentes de seguridad como los relacionados en esta resolución que puedan afectar los datos de personas residentes o domiciliadas en la República de Colombia.

VIGÉSIMO SÉPTIMO: Que teniendo en cuenta todo lo anterior, y en especial lo que ordena el principio y el deber de seguridad, así como lo que implica el cumplimiento del principio de responsabilidad demostrada (accountability), este Despacho considera necesario impartir, con **CARÁCTER PREVENTIVO**, las órdenes que se indicarán en la parte resolutiva del presente acto administrativo.

VIGÉSIMO OCTAVO: Que para continuar garantizando el derecho de defensa y contradicción dentro de la presente actuación, el expediente queda a disposición de UBER TECHNOLOGIES INC., UBER COLOMBIA SAS Y UBER B.V. en las instalaciones de esta Superintendencia.

En mérito de lo expuesto, este Despacho

RESUELVE

ARTÍCULO PRIMERO: ORDENAR a las sociedades **UBER TECHNOLOGIES, INC.**, **UBER COLOMBIA SAS** y **UBER B.V.**, en adelante **UBER,** implementar medidas y procedimientos para la adecuación de sus operaciones en la República de Colombia a las disposiciones de la Ley 1581 de 2012, las cuales deberán contener como mínimo los siguientes estándares:

1. Mejorar o robustecer las medidas de seguridad que ha implementado a la fecha de expedición de la presente resolución para garantizar la seguridad de los datos personales, evitando su: (i) acceso no autorizado o fraudulento; (ii) uso no autorizado o fraudulento; (iii) consulta no autorizada o fraudulenta; (iv) adulteración o (v) pérdida.

2. Desarrollar, implementar y mantener un programa integral de seguridad de la información, que garantice la seguridad, confidencialidad e integridad de los datos personales, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El programa deberá constar por escrito, ser sujeto a pruebas periódicas para evaluar su efectividad e indicadores de cumplimiento y tener en cuenta, como mínimo, lo siguiente:

---

[103] Cfr. 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.

a) Los principios rectores establecidos en la Ley 1581 de 2012 y los deberes que de ellos se derivan;
b) El tamaño y la complejidad de las operaciones de UBER;
c) La naturaleza y el ámbito de las actividades de UBER;
d) La cantidad de titulares;
e) La naturaleza de los datos personales;
f) El tipo de Tratamiento de los datos personales;
g) El alcance, contexto o fines del Tratamiento;
h) Las actualizaciones o cualquier tipo de modificación en las Aplicaciones de UBER, sus productos y cualquier otra forma en que UBER utilice, recopile, o comparte los datos recogidos;
i) El acceso a los datos personales por parte de los empleados o contratistas de UBER;
j) El uso de los datos personales de los usuarios por terceros, entre ellos, aliados comerciales, empresas asociadas y desarrolladores de Aplicaciones, si aplica;
k) El uso innovador o aplicación de nuevas soluciones tecnológicas;
l) Los riesgos internos y externos para la seguridad, confidencialidad y disponibilidad de los datos personales; y,
m) Los riesgos para los derechos y libertades de las personas.

3. Desarrollar, implementar y mantener un programa de gestión y manejo de incidentes de seguridad en datos personales, que contemple procedimientos para informar sin dilación indebida a esta Autoridad de protección de datos y a los Titulares de los mismos cuando se presenten incidentes que afecten la confidencialidad, integridad y disponibilidad de los datos personales.

4. Desarrollar, implementar y mantener un programa de capacitación y entrenamiento rutinario para sus empleados y contratistas sobre su política de seguridad de la información, su política de gestión de incidentes de seguridad de datos personales y su política de tratamiento de datos personales (o privacidad) de UBER.

5. Poner en marcha un sistema de monitoreo permanente para verificar si, en la práctica, sus medidas de seguridad son útiles, suficientes o si están funcionando correctamente. En caso que ello no sea así, adoptar las medidas necesarias para garantizar la seguridad de la información.

6. UBER deberá efectuar una auditoría independiente, dentro de los cuatro (4) meses siguientes a la ejecutoria del presente acto administrativo, y cada año después de dicha fecha durante los próximos cinco (5) años, que certifique que cuenta con las medidas técnicas, humanas, administrativas, contractuales y de cualquier otra naturaleza que sean necesarias para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

ARTÍCULO SEGUNDO: Las sociedades **UBER TECHNOLOGIES, INC., UBER COLOMBIA SAS** y **UBER B.V**. deberán cumplir lo ordenado en esta resolución dentro de los **CUATRO (4)** meses siguientes a la ejecutoria del presente acto administrativo y acreditar ante esta Superintendencia las medidas y procedimiento adoptados dentro de los **CINCO (5)** días siguientes al vencimiento de dicho término.

PARÁGRAFO PRIMERO: Para demostrar el cumplimiento deberán remitir, al finalizar dicho plazo, una certificación emitida por una entidad o empresa, nacional o extranjera, independiente, imparcial, profesional y especializada que acredite que se han implementado las medidas ordenadas por esta Dirección y que las mismas están operando con suficiente efectividad para proporcionar el grado de seguridad que exige el principio y el deber de seguridad de la Ley 1581 de 2012 respecto de los datos personales.

PÁRAGRAFO SEGUNDO: La entidad o empresa que emita el certificado será seleccionada por UBER, pero debe ser un tercero cuya gestión esté libre de todo conflicto de interés que le reste independencia y ajena a cualquier tipo de subordinación respecto de UBER.

PARÁGRAFO TERCERO: La entidad o empresa certificadora deberá ser autorizada por la autoridad competente del país de su domicilio, sólo en el caso que la regulación del mismo exija dicha autorización para poder emitir certificaciones. Si en dicho país no se exige lo anterior, bastará

con que la misma sea independiente, imparcial, profesional y especializada en temas de seguridad de la información.

ARTÍCULO TERCERO: Ordenar a **UBER COLOMBIA S.A.S.** que preste su colaboración para que **UBER TECHNOLOGIES, INC.**, y **UBER B.V.** cumplan las instrucciones y órdenes impartidas por esta Superintendencia en esta resolución.

ARTÍCULO CUARTO: Notificar el contenido de la presente resolución a **UBER TECHNOLOGIES, INC., UBER COLOMBIA SAS** y **UBER B.V.,** respetivamente, informándoles que contra el presente acto administrativo procede recurso de reposición ante el Director de Investigación de Protección de Datos Personales y de apelación ante el Superintendente Delegado para la Protección de Datos Personales, dentro de los **DIEZ (10)** días siguientes a la diligencia de notificación.

NOTIFÍQUESE Y CÚMPLASE 17 JUN 2019

Dada en Bogotá, D.C.,

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE SALAZAR MUÑOZ

CEP/CESM

NOTIFICACIÓN:

Investigada:	**UBER TECHNOLOGIES INC.**
Identificación:	Sin identificar
Dirección:	1455 MARKET STREET, 4TH FLOOR
Ciudad:	SAN FRANCISCO, CALIFORNIA, 94103
País:	ESTADOS UNIDOS DE AMÉRICA
Representante:	Sin identificar
Identificación:	Sin identificar

Investigada:	**UBER B.V.**
Identificación:	56317441
Dirección:	MR. TREUBLAAN 7, 1097 DP
Ciudad:	AMSTERDAM
País:	PAÍSES BAJOS
Representante:	Sin identificar
Identificación:	Sin identificar
Correo electrónico:	LERT@uber.com

Sociedad:	**UBER COLOMBIA SAS**
Identificación:	900.676.165-2
Apoderado:	JOHANN SCHOMBERGER TIBOCHA
Identificación:	80.136.989
Dirección:	CALLE 93 NO. 17-45, OFICINA 602
Ciudad:	BOGOTÁ D.C.
País:	COLOMBIA
Correo electrónico:	colombianotifica@uber.com