REPÚBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 74519 DE 2020

(23 NOVIEMBRE 2020)

Por la cual se imparten órdenes dentro de una actuación administrativa

Radicación 20-087350

VERSIÓN ÚNICA

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 esta Dirección requirió **el catorce (14) de abril del 2020** a **ZOOM VIDEO COMMUNICATIONS, INC** para que informara a esta autoridad lo siguiente:

1. *¿Existen ciudadanos Colombianos afectados por incidentes de seguridad presentados en la plataforma Zoom, tales como robo de credenciales de usuarios y la información intercambiada en las reuniones, transferencias de información a Facebook, robo de credenciales de Microsoft, acceso a los perfiles de LinkedIn, entre otros presentados durante el año 2020?*
2. *¿Cuál es la cantidad de ciudadanos o personas residentes en la República de Colombia que se han visto afectados por incidentes de seguridad presentados en la plataforma Zoom durante el año 2020?*
3. *¿Se han presentado reclamos de los ciudadanos o residentes en el Estado Colombiano afectados, si es así cual fue la gestión realizada en estos casos?*
4. *¿Cuáles fueron las medidas para solucionar cada incidente de seguridad y cuáles fueron las medidas para evitar que se presentara nuevamente?*
5. *Para el caso de las reuniones realizadas en ZOOM, las grabaciones guardadas en la nube, ¿los servidores donde se encuentran geográficamente?*
6. *¿Quien tiene acceso a las grabaciones de la nube?*
7. *¿Cuándo se programa una reunión la información recolectada en el registro previo, donde guarda los datos recolectados, quien es Responsable de la información?*
8. *Informe qué datos recolecta en cada plataforma en que funciona la aplicación además de:*
    1. *Nombre de usuario.*
    2. *Dirección física.*
    3. *Dirección de correo electrónico.*
    4. *Número de teléfono.*
    5. *Información de trabajo.*
    6. *Información de perfil de Facebook.*
    7. *Especificaciones de computadora o teléfono.*
    8. *Dirección IP.*
    9. *Ubicación.*
    10. *Zona horaria de los usuarios.*
9. *¿Con qué empresas, plataformas, entidades las aplicaciones de ZOOM realizan intercambio o envió de datos del Titular? Y ¿por qué causa?.*
10. *¿Donde se encuentran y como se obtienen las autorizaciones de los Titulares para el Tratamiento de los datos tratados por los terceros?*
11. *¿Cuál es la información que se comparte y/o trasmite en cada caso?*
12. *¿Que Tratamiento de información o datos es aplicado por cada tercero?*
13. *¿Que políticas de seguridad y privacidad aplicada uno de los terceros a los datos trasmitidos?*
14. *Adjunten las políticas de gestión de vulnerabilidades de las diferentes versiones de ZOOM*
15. *Si las recomendaciones de seguridad para el uso de la plataforma de ZOOM no son atendidas y configuradas por los administradores de las reuniones, qué controles se han implementado para evitar las vulneraciones.*

SEGUNDO: Que el mismo **catorce (14) de abril del 2020** se le informó a **ZOOM VIDEO COMMUNICATIONS, INC**:

"(…) la iniciación de una actuación administrativa a ZOOM VIDEO COMMUNICATIONS, INC la cual se regirá por lo dispuesto en el Capítulo I del Título III de la Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo).

La presente tiene como propósito establecer si ZOOM VIDEO COMMUNICATIONS, INC cumple con la regulación colombiana relativa a los principios de seguridad, acceso y circulación restringida (artículos 4 literales f) y g) y 17 literales d) i) y n) de la Ley 1581 de 2012 en concordancia con el artículo 19 del Decreto 1377 de 2013 incorporado en el Decreto 1074 de 2015). Y, si la misma ha implementado el principio de responsabilidad demostrada en esa materia (artículos 26 y 27 del Decreto 1377 de 2013 incorporado en el Decreto 1074 de 2015)".

TERCERO: Que el **trece (13) de mayo del 2020 ZOOM VIDEO COMMUNICATIONS, INC** respondió el requerimiento en los siguientes términos:

"***La importancia del nuevo papel de Zoom en la pandemia del COVID-19***

Los usuarios están repensando la forma en que Zoom puede ser usado en esta época de distanciamiento social, incluyendo reuniones virtuales, conciertos, happy hours, clubes de lectura, conferencias profesionales, fiestas y sesiones de entrenamiento físico.

Para dar un contexto, a finales de diciembre de 2019, el número de participantes diarios utilizando los servicios de reuniones realizadas en la plataforma Zoom, tanto gratuitas como pagas, era de aproximadamente 10 millones. En abril de este año, Zoom alcanzó más de 300 millones de participantes diarios en reuniones gratuitas y pagas. Zoom ha estado trabajando en todo momento para atender a estos nuevos usuarios en este momento crítico y proteger su privacidad y seguridad.

Zoom ha implementado varias funcionalidades dirigidas a identificar riesgos e incrementar las protecciones a la seguridad y privacidad de sus usuarios. Sin embargo, como ocurre con cualquier desarrollo tecnológico, como el auge de los teléfonos inteligentes o las redes sociales, hay una curva de aprendizaje y un periodo educativo donde los nuevos usuarios deben aprender a utilizar el servicio y entender sus funcionalidades y mejores prácticas implementadas por Zoom para ayudarles a proteger su privacidad y seguridad.

(…)

Medidas de seguridad de Zoom sobre la información personal del usuario

Zoom toma muy en serio la seguridad de la información personal de sus usuarios y, por este motivo, ha puesto en marcha un robusto sistema de controles de seguridad diseñado para proteger los datos personales de los usuarios tratados en sus sistemas o almacenados en la nube. Al respecto, Zoom publicó un informe técnico sobre su programa de seguridad, que se puede encontrar en este enlace: https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf.

Zoom también está comprometido con la protección de la privacidad de los estudiantes menores de edad que podrían tener acceso a la plataforma. La Política de Privacidad de Zoom y la Política de Privacidad para escuelas y distritos (K-12 Cholos & Districts Privacy Policy) reflejan nuestro cumplimiento con los requisitos de la Ley de Protección de la Privacidad Online de los Niños (COPPA – por sus siglas en inglés), la Ley Federal de Derechos Educativos y Privacidad (FERPA – por sus siglas en inglés), la Ley de California sobre Privacidad del Consumidor (CCPA – por sus siglas en inglés), y otras leyes aplicables.

Incidentes de seguridad

Zoom no tiene conocimiento de haber experimentado algún incidente que haya comprometido la seguridad, integridad o disponibilidad de los datos personales de usuarios de Zoom, que estén en Colombia o en otro lugar. Las cuestiones o eventos especificados en esta pregunta y que se examinan a continuación, no afectaron los datos personales de los usuarios de Zoom. No obstante, en aras de la transparencia, y porque Zoom cree que ha resuelto y remediado completamente cualquier presunto o potencial problema o riesgo, Zoom proporciona la siguiente información al respecto:

*i) **Robo de credenciales:** Zoom entiende que esta pregunta se refiere a los informes sobre credenciales de usuarios de Zoom a la venta en la internet oscura (dark web).*

Como cuestión inicial, ninguna credencial de usuario (por ejemplo, nombres de usuario y contraseñas) fue extraída de Zoom. Al respecto, cualquier supuesta credencial de acceso de Zoom sería en realidad una credencial utilizada por usuarios de Zoom en otros sitios web o aplicaciones que fueron extraídas a través de algunos incidentes de

seguridad que implicaron datos personales pero que no involucraron a Zoom. Algunos actores malintencionados afirman ahora que estos conjuntos de credenciales previamente robados pueden utilizarse para acceder a las cuentas de Zoom.

No obstante, Zoom ha investigado esta cuestión y no ha descubierto prueba alguna de que se haya accedido a la información de alguna cuenta de usuario sin autorización. Zoom ha identificado un pequeño número de credenciales válidas (significativamente menos que las cifras comunicadas públicamente) que aparecen en la internet oscura, y en cada caso, Zoom ha bloqueado la cuenta y requerido al usuario relevante que modifique su contraseña. Zoom generalmente recomienda que sus usuarios utilicen contraseñas complejas y seguras que no sean utilizadas en ningún otro lugar y que no hayan sido expuestas en eventuales anteriores violaciones de datos personales.

ii) ***Facebook:*** *Como muchas compañías de tecnología, Zoom usa Kits de Desarrollo de Software ("SDK" – por sus siglas en ingles) para agregar funciones y funcionalidades a sus aplicaciones. Un SDK es un conjunto de códigos informáticos que una empresa proporciona para que otros desarrolladores puedan integrar fácilmente diferentes características provistas por esa empresa en los productos de software de los desarrolladores. Los SDK suelen recolectar y compartir alguna información para funcionar, principalmente información relacionada con las especificaciones técnicas del dispositivo del usuario y no con información específica relativa a los usuarios individuales.*

Acerca de las disrupciones a las reuniones*: Desde que los primeros reportes de estas disrupciones emergieron, Zoom ha dispuesto sus esfuerzos de forma proactiva para educar a los nuevos usuarios no empresariales sobre cómo utilizar las características existentes de Zoom para prevenir la ocurrencia de este tipo de disrupciones en las conferencias. También hemos actualizado la configuración predeterminada de muchos usuarios para habilitar dichas características, y hemos diseñado rápidamente nuevas configuraciones para asistir de forma más eficaz a los usuarios con la seguridad de sus conferencias:*

- *Zoom reajustó las configuraciones predeterminadas para usuarios educativos inscritos en su programa gratuito para proteger con contraseñas las sesiones de Zoom, habilitar salones de espera virtuales (p. ej. el profesor debe dar acceso a cada usuario para entrar la sala de la conferencia), y asegurar que los anfitriones-profesores sean los únicos habilitados para compartir su contenido en la sala de clase virtual (una característica previamente disponible solo para cuentas pagas de Zoom).*
- *Zoom también ha habilitado contraseñas y salas de espera virtual para usuarios gratuitos y aquellos de categoría Single Pro.*
- *Zoom ha desplegado recursos técnicos y legales para responder a los reportes de sitios web, blogs, videos, etc., en donde se publicaron o compartieron enlaces de reuniones, números de identificación de reuniones y/o contraseñas para facilitar la disrupción a las conferencias, y se ha obtenido el bloqueo o la remoción del contenido respectivo.*
- *Zoom ha introducido un nuevo ícono de seguridad que se ubica en la barra de tareas debajo de la ventana de la conferencia que dispone todos los controles de seguridad en un solo lugar y facilita a los usuarios el acceso a herramientas que permiten limitar la compartición de pantalla, bloquear los participantes o reportar participantes no deseados al equipo de Seguridad & Confianza (Trust & Safety) de Zoom.*
- *Zoom ha recientemente actualizado la barra superior para que la identificación de la conferencia no esté visible de forma que se mitigue el riesgo de que esa información sea malintencionadamente compartida y se pudiera habilitar el ingreso de un participante no invitado.*

Es importante destacar que las disrupciones abusivas de las conferencias no son resultado de intrusiones cibernéticas o accesos ilegales que hayan comprometido las medidas de seguridad de Zoom. Por el contrario, dichas disrupciones son producto de usuarios que han compartido públicamente la identificación de las conferencias, y en algunos casos, las contraseñas de las mismas en caso de haber sido determinadas. Una vez alguien tiene acceso a la identificación de una conferencia y a su contraseña (si se configuró una), los actores maliciosos no estarían infiltrándose en la conferencia, sino que estarían ingresando como cualquier otro participante (no obstante que lo haga con intenciones indebidas). Lo anterior no era un inconveniente previo a la crisis global de salud, cuando nuestro servicio era usado predominantemente por usuarios empresariales quienes no tienen motivos para hacer pública la información de sus conferencias. Como resultado, Zoom ha adoptado con celeridad medidas dirigidas a atender este reto y ayudar a nuestros usuarios a evitar disrupciones de esta naturaleza"[1].

[1] Documento con número de radicado 20087350—0000200002.

CUARTO: Que, de conformidad con lo expuesto hasta el momento, la Dirección de Investigación de Protección de Datos Personales se permite exponer las siguientes:

CONSIDERACIONES DE LA DIRECCIÓN DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES

I. Competencia de la Superintendencia de Industria y Comercio para ordenar las medidas que sean necesarias para hacer efectivo el derecho a debido Tratamiento de Datos personales.

El artículo 19 de la Ley Estatutaria 1581 de 2012, establece que "*la Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley*". El artículo 21, por su parte, faculta a esta entidad para, entre otras: "*b) **Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data***. (…) *e) **Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento** y Encargados del Tratamiento a las disposiciones previstas en la presente ley*; (…) f) *Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones*."

Así las cosas, existen expresas y suficientes facultades legales para que esta Superintendencia pueda iniciar investigaciones, así como impartir órdenes o instrucciones para hacer efectivo el derecho que se le ha encargado proteger.

II. La Ley 1581 de 2012 es aplicable a ZOOM VIDEO COMMUNICATIONS, INC porque recolectan Datos personales en el territorio de la República de Colombia a través de *cookies* que instala en los equipos o dispositivos de las personas residentes o domiciliadas en Colombia.

Ordena la Constitución Política de Colombia en su artículo 15 que en cualquier actividad sobre Datos personales se respete la libertad y demás garantías consagradas en la dicha norma. Así, es de vital importancia recordar que el caso bajo estudio hace referencia al cumplimiento de exigencias de naturaleza constitucional referidas al Derecho Fundamental al debido Tratamiento de los Datos Personales de los ciudadanos.

En efecto, el artículo 15 de la Constitución Política Nacional no solo establece que "todas las personas (…) a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas"[2], sino que es tajante en exigir que:

> ***"En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".*** (Destacamos y subrayamos).

Con fundamento en lo anterior, se promulga la Ley Estatutaria 1581 de 2012 que desarrolla, entre otras, el citado derecho constitucional de naturaleza fundamental. En el artículo 2 de la referida norma se dispone lo siguiente:

> "*La presente ley aplicará 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*". (Destacamos y subrayamos).

El término "Tratamiento" no solo se menciona en el artículo 15[3] de la Constitución Política de la República de Colombia, sino que, es determinante para establecer el campo de aplicación de la citada ley, la cual lo define de la siguiente manera:

> ***"Artículo 3. Definiciones.*** *Para los efectos de la presente ley, se entiende por:*
> *(…)*

---

[2] Constitución Política de Colombia. Artículo 15.

[3] El artículo 15 de la Constitución de la República de Colombia dice, entre otras, lo siguiente: " Todas las personas tienen derecho a (…)conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.(Subrayamos)

> *g)* ***Tratamiento:*** *Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión."*

Así las cosas, la Ley Estatutaria 1581 de 2012 es aplicable, entre otras, cuando:

a. El Tratamiento lo realiza el Responsable o Encargado, domiciliados o no en territorio colombiano, que directa o indirectamente, a través de cualquier medio o procedimiento, físico o electrónico, recolecta, usa, almacena o trata Datos personales en el territorio de la República de Colombia. Las anteriores hipótesis son ejemplos de *"tratamiento* [sic] *de datos* [sic] *personales efectuado en territorio colombiano"* a que se refiere la parte primera del mencionado artículo 2.
b. El Responsable o el Encargado no está domiciliado en la República de Colombia ni realiza Tratamiento de Datos dentro del territorio colombiano. Pero, existen normas o tratados internacionales que los obliga a cumplir la regulación colombiana.

La Corte Constitucional, por su parte, en relación con el ámbito de aplicación de ese artículo señaló en la Sentencia C-748 de 2011[4]:

> *"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 las fronteras.*** *Por tanto, para la Sala se trata de una medida imperiosa para garantizar el derecho al habeas data"*[5]*.* (Subrayado fuera de texto).

Es importante señalar que, otras autoridades de protección de Datos personales han concluido que las *cookies* son mecanismos que usan empresas extranjeras para instalarlas en los equipos de las personas de otros países y recolectar sus Datos.

Frente a lo anterior, a finales de 2013 la Agencia Española de Protección de Datos (en adelante AEPD) concluyó lo siguiente con ocasión de una investigación que inició contra Google:

> "*En todo caso, (…),* ***la entidad Google Inc. recurre a medios situados en el territorio español con el fin de captar información en nuestro territorio (utilizando, entre otros, los equipos de los usuarios residentes en España para almacenar información de forma local a través de cookies y otros medios, así como ejecutando código en dichos dispositivos****), sin que la utilización de tales equipos para la recogida de datos se realice exclusivamente con fines de tránsito por el territorio de la Unión Europea, es decir, no se trata de equipos de transmisión, sino que* ***dichos equipos se emplean para la recogida y tratamiento de los datos (…)"***[6]. (Destacamos).

En cuanto a las web cookies, **ZOOM VIDEO COMMUNICATIONS, INC (**en adelante Zoom) hace referencia a las *web cookies*, en su *Política del uso de cookies*[7] de la siguiente manera*:*

> *"****Zoom Video Communications, Inc. («Zoom») y nuestros socios usan cookies o tecnologías similares*** *para analizar tendencias, administrar y seguir los movimientos de los usuarios cuando visitan nuestro sitio web o usan nuestros Productos,* ***y para recopilar información sobre usted: desde dónde accede a nuestro sitio web o Productos y cómo usa nuestros Productos y servicios, y para proporcionarle información sobre los productos de Zoom que podría tener interés en comprar****.*

---

[4] Cfr. Corte Constitucional. Sentencia C-748 de 2011. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm
[5] Cfr. Corte Constitucional. Sentencia C-748 de 2011. Consideración 2.4.4.
[6] La AEPD concluyó lo siguiente: "*la Agencia Española de Protección de Datos también es competente para decidir sobre el tratamiento llevado a cabo por un responsable no establecido en territorio del Espacio Económico Europeo que ha utilizado en el tratamiento de datos medios situados en territorio español, por lo que debe concluirse, igualmente, que la LOPD es aplicable al presente supuesto y procedente la intervención de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 2.1.c) de la LOPD*" (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución R/02892/2013 del 19 de diciembre de 2013. Procedimiento sancionador PS/00345/2013 instruido a las entidades Google Inc. y Google Spain, S.L. Madrid, España).
La parte pertinente de la regulación española - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal- sobre su ámbito de aplicación dice lo siguiente:
"*Artículo 2 Ámbito de aplicación.*
1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.
Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:
a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
c) ***Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito****. (…)".* (Destacamos).
[7] Política del uso de cookies: https://zoom.us/es-es/cookie-policy.html Obtenido el 3 de noviembre de 2020.

> *¿Qué son las cookies y cómo las usa Zoom?*
>
> *Las **cookies son pequeños archivos de texto que se colocan en su ordenador** los sitios web y servicios que visita o a los que accede. Se usan ampliamente para que los sitios web y servicios operen y funcionen con una mayor eficiencia y **para proporcionar información sobre la experiencia de nuestros usuarios** durante el uso o interacción con nuestros sitios web, productos, servicios y anuncios. Algunas cookies duran solo el tiempo de su sesión web y caducan cuando sale del navegador; otras cookies pueden durar más tiempo que su sesión web, incluso después de que salga del navegador, por ejemplo, para recordarle cuando regresa a nuestro sitio web". (*Destacamos).

En adición, la Política de Privacidad de Zoom afirma que: "***Al igual que muchas empresas, utilizamos servicios de publicidad que tratan de adaptar los anuncios en línea a sus intereses basándose en la información recogida a través de cookies y tecnologías parecidas en nuestras Páginas de marketing**. Esto se llama publicidad en función de intereses. Puede obtener más información y optar por no utilizar cookies en nuestras Páginas de marketing haciendo clic en el enlace No vender mis datos personales en el pie de página de esta página web. Tendrá que establecer sus preferencias desde cada dispositivo y cada navegador web del que desee rechazar su uso"*[8]. (Destacamos).

Entonces, se concluye por parte de esta autoridad que, sin lugar a dudas, una *cookie* es un archivo que se instala en los equipos o dispositivos (bien sea celular, computador portátil, u otro) de los titulares en la República de Colombia con el objetivo de realizar alguna operación o conjunto de operaciones sobre aquellos Datos personales en territorio colombiano. Por ejemplo, la recolección de Datos personales en territorio colombiano. Por tanto, **ZOOM VIDEO COMMUNICATIONS, INC**, realiza un Tratamiento de Datos personales en el territorio colombiano sujeto a las disposiciones de la Ley 1581 de 2012.

III. ZOOM VIDEO COMMUNICATIONS, INC tienen la obligación de cumplir la legislación Colombiana, así como las órdenes y requerimientos de esta autoridad, en cumplimiento de la Ley 1581 de 2012.

La regulación sobre Tratamiento de Datos personales debe aplicarse al margen de los procedimientos, metodologías o tecnologías que se utilicen para recolectar, usar o tratar ese tipo de información. La ley colombiana permite el uso de tecnologías para tratar datos pero, al mismo tiempo, exige que se haga de manera respetuosa del ordenamiento jurídico. Quienes crean, diseñan o usan "innovaciones tecnológicas" deben cumplir todas las normas sobre Tratamiento de Datos personales.

Entonces, es importante decir que nuestra Constitución Política Nacional establece:

> Artículo 4 *"(…) Es **deber de los nacionales y de los extranjeros** en Colombia acatar la Constitución y las leyes, y respetar y obedecer a las autoridades"*[9].
>
> Artículo 333 *"(…) La actividad económica y la iniciativa privada son libres, dentro de los límites del bien común. Para su ejercicio, nadie podrá exigir permisos previos ni requisitos, sin autorización de la ley. La libre competencia económica es un derecho de todos que supone responsabilidades*. **La empresa, como base del desarrollo, tiene una función social que implica obligaciones**". (Destacamos).

De esta manera, es la misma Constitución Política la que dispone el cumplimiento de la normatividad a los extranjeros que estén en este territorio. La cual, además, incluye el sometimiento a la ley en general, así como a las órdenes de autoridades administrativas, entre otras.

IV. El respeto por las leyes en el ciberespacio.

En el ciberespacio no desaparecen ni disminuyen los derechos de las personas. El ciberespacio ha sido caracterizado por ser un escenario global no delimitado por fronteras geográficas en donde las actividades suceden dentro de la arquitectura tecnológica de la Internet. Aunque se trata de un "mundo virtual", sus ciudadanos son miles de millones de personas reales ubicadas en prácticamente cualquier lugar del "mundo físico" cuyas actividades tienen impacto o consecuencias en el "mundo real".

A pesar que el campo de acción de la Internet desborda las fronteras nacionales, para la Corte Constitucional el nuevo escenario tecnológico y las actividades en Internet no se sustraen del respeto

---

[8] Obtenido el 3 de noviembre de 2020 en el enlace: https://zoom.us/es-es/privacy.html

[9] "*Dicho reconocimiento genera al mismo tiempo la responsabilidad en cabeza del extranjero de atender cabal y estrictamente el cumplimiento de deberes y obligaciones que la misma normatividad consagra para todos los residentes en el territorio de la República pues, así lo establece, entre otras disposiciones, el artículo 4o. inciso segundo de la Carta (…)".* Corte Constitucional, Sentencia C-1259 de 2001

de los mandatos constitucionales . Por eso, concluyó dicha entidad 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]. Recalca dicha Corporación que, "***nadie podría sostener que, por tratarse de Internet, los usuarios sí pueden sufrir mengua en sus derechos constitucionales***"[11]. (Destacamos).

Por su parte, en la respuesta que **Zoom**[12] allegó a esta entidad se afirma que: "*entre el 1 y el 28 de abril de 2020, usuarios en Colombia se unieron a reuniones de Zoom más de 17 millones de veces*". Es decir, **Zoom** tiene la obligación constitucional y legal de garantizar a los usuarios de por lo menos diez y siete (17) millones de reuniones el debido Tratamiento de sus Datos personales y el correcto ejercicio de sus derechos fundamentales en el ciberespacio.

Entonces, es relevante tener presente que **Zoom** trata Datos personales de los usuarios de por lo menos diez y siete (17) millones de reuniones. Lo cual, genera la obligación de ser extremadamente diligente y garantizar la efectividad real (no formal) de los derechos de los Titulares de los Datos personales en aquel ciberespacio.

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

Los Datos personales pueden ser recogidos por diferentes fuentes, entre ellas: formularios, cookies, aplicaciones móviles, sitios web, redes sociales, registros públicos, programas de fidelización de clientes, etc. Todas estas formas de recolección, entre otras, son manifestaciones de: 1) Datos personales suministrados directamente por los titulares, 2) Datos personales recolectado en cumplimiento de un requisito legal, 3) Datos personales recopilados automáticamente con el uso de un servicio o producto (por ejemplo, datos de transacciones, direcciones IP, datos de ubicación), y 4) Datos personales inferidos mediante el Tratamiento y análisis de los datos suministrados por los individuos o recopilados con el uso del servicio o producto. Estos datos, sin lugar a dudas, también son de gran interés para terceros que no han sido autorizados para el Tratamiento de dicha información.

Si un Dato personal es conocido, accedido o sustraído por terceros no autorizados, por ejemplo, piratas cibernéticos, resulta *per se* en un riesgo para los derechos y libertades de los individuos, de gravedad y probabilidades variables.

Considerando la cantidad y sensibilidad de la información personal que es recolectada en el ciberespacio mediante diversos mecanismos, procesos y tecnologías, la Corte Constitucional en Sentencia C-748 de 2011 subrayó el deber de los Responsables del Tratamiento de reforzar sus medidas de seguridad para proteger la información personal de los Titulares. Lo anterior como resultado de que "*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"*[13].

Entonces, existen riesgos para los derechos y libertades de los titulares cuando su información personal es conocida, accedida o sustraída por terceros no autorizados. En particular, cuando versen sobre Datos sensibles o de niños, niñas y adolescentes.

VI. Del deber de conservar la información bajo condiciones de seguridad.

La seguridad de la información es una condición crucial del Tratamiento de Datos personales. Recolectada la información, debe ser objeto de medidas de diversa índole para evitar situaciones indeseadas que puedan afectar los derechos de los titulares y de los mismos Responsables y Encargados del Tratamiento. El acceso, la consulta y el uso no autorizado o fraudulento, así como la manipulación y pérdida de la información son los principales riesgos, pero no los únicos, que se quieren mitigar a través de medidas de seguridad de naturaleza humana, física, administrativa y/o técnica.

La seguridad de la información ha sido una preocupación del legislador colombiano 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*"[14].

---

[10] República de Colombia. Corte Constitucional. Sentencia C-1147 del 31 de octubre de 2001.
[11] República de Colombia. Corte Constitucional. Sentencia C-1147 del 31 de octubre de 2001.
[12] Documento "20087350-- 0000200002" página 7.
[13] República de Colombia. Corte Constitucional. Sentencia C-748 del 6 de octubre de 2011. Considerando 2.6.5.2.7
[14] República de Colombia. Corte Constitucional. Sentencia C-748 de 2011.

Por su parte, la seguridad de los Datos personales no se limita a situaciones de infiltración o burla de las medidas de seguridad que han implementado los Responsables y Encargado del Tratamiento. La Ley 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 fuera de texto).*

Nótese que **la redacción del principio de seguridad tiene un criterio eminentemente preventivo**, lo cual obliga a los Responsables y Encargados del Tratamiento ha adoptar medidas apropiadas y efectivas para **evitar** afectaciones a la seguridad de la información. **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.

VII. **Del Tratamiento de Datos personales realizado por ZOOM VIDEO COMMUNICATIONS, INC.**

Al revisar la Política de Privacidad[15], se encuentra la siguiente información[16] relacionada con los datos que recolecta la plataforma Zoom y la forma como los trata.

Primero, es importante destacar que **ZOOM VIDEO COMMUNICATIONS, INC.** aclara que solo será Responsable del Tratamiento de los Datos personales relacionados con la prestación del servicio, más no los que surjan de las interacciones durante cualquier sesión a la que un usuario de Zoom asista, como: "grabaciones o transcripciones de reuniones o llamadas".

---

[15] Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842

[16] Las capturas de pantalla que se presentan a continuación son extraídas del Análisis técnico de la información entregada por Zoom Video Communications, Inc, contenido lo anterior en el expediente 20-87350, realizado el Bogotá, 15 de septiembre de 2020 por el Grupo de Investigaciones Administrativas de Protección de Datos Personales.

Los datos personales que tratamos y cómo los usamos

En la siguiente tabla se describe el tratamiento de los datos personales por parte de Zoom como controlador de datos. La tabla no cubre el contenido del cliente, incluidos datos personales sobre usted que se puedan incluir en el contenido del cliente —tales como las grabaciones o transcripciones de reuniones o llamadas— porque el cliente (el titular de la cuenta de Zoom), en lugar de Zoom, controla cómo se procesa el contenido del cliente. Cualquier pregunta sobre el tratamiento del contenido del cliente se debe dirigir directamente al cliente.

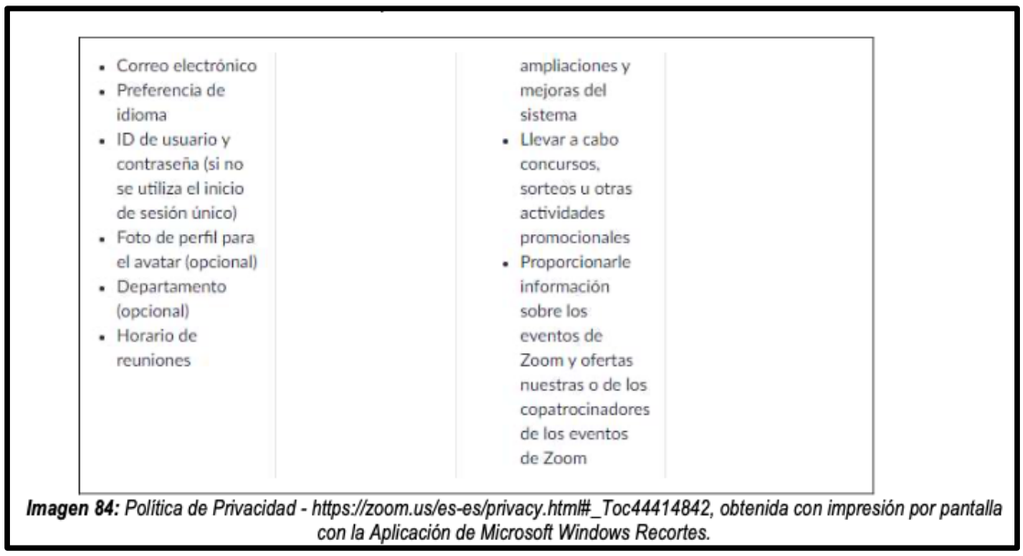
Imagen 82: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

A continuación, se encuentra una tabla en la que se describen detalladamente los datos que Zoom recolecta y el Tratamiento que les da, como se puede ver a continuación:

Tratamiento de datos personales

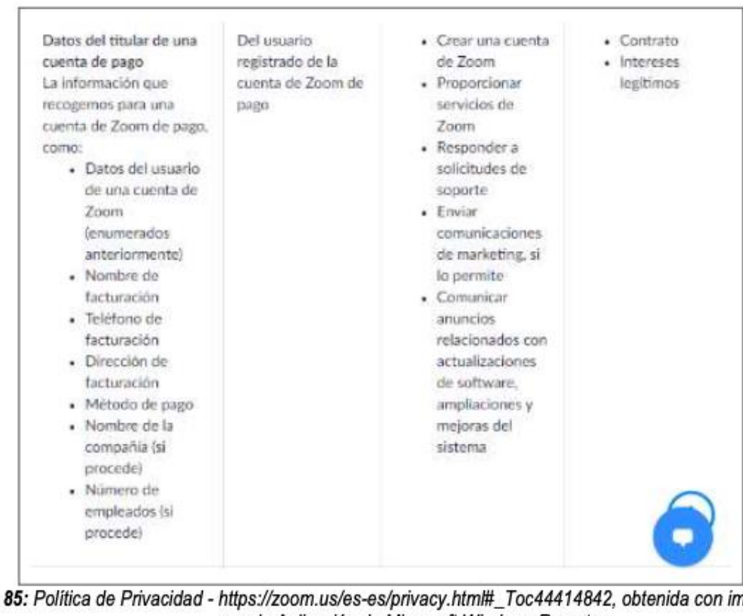
Tipos de datos personales	Cómo los obtenemos	Qué hacemos con ellos	Fundamento jurídico (Se aplica solo en el EEE, y solo según lo dispuesto en el Reglamento General de Protección de Datos (RGPD) de la UE)
Datos del usuario de una cuenta La información que recogemos cuando crea una cuenta de Zoom gratuita, como: • Fecha de nacimiento (solo para fines de verificación de la edad. **Zoom no conserva ni utiliza esta información para ningún otro propósito**) • Nombre • Apellido(s) • Teléfono (opcional)	Del usuario registrado de la cuenta de Zoom gratuita	• Inscribirle en los Servicios • Mostrar su avatar de usuario a los participantes de reuniones • Proporcionarle soporte • Enviar comunicaciones de marketing, si lo permite • Comunicar anuncios relacionados con actualizaciones de software,	• Contrato • Intereses legítimos

Imagen 83: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*



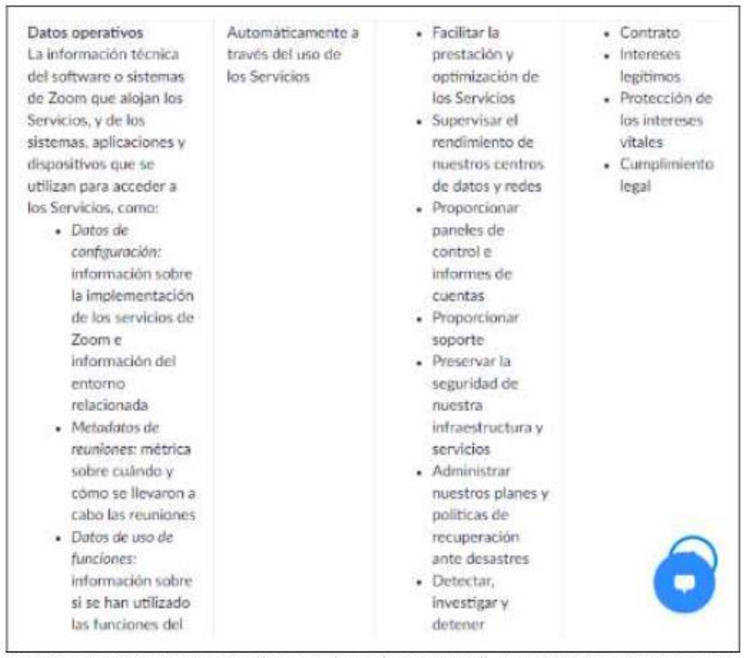
• Correo electrónico • Preferencia de idioma • ID de usuario y contraseña (si no se utiliza el inicio de sesión único) • Foto de perfil para el avatar (opcional) • Departamento (opcional) • Horario de reuniones		ampliaciones y mejoras del sistema • Llevar a cabo concursos, sorteos u otras actividades promocionales • Proporcionarle información sobre los eventos de Zoom y ofertas nuestras o de los copatrocinadores de los eventos de Zoom

Imagen 84: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*



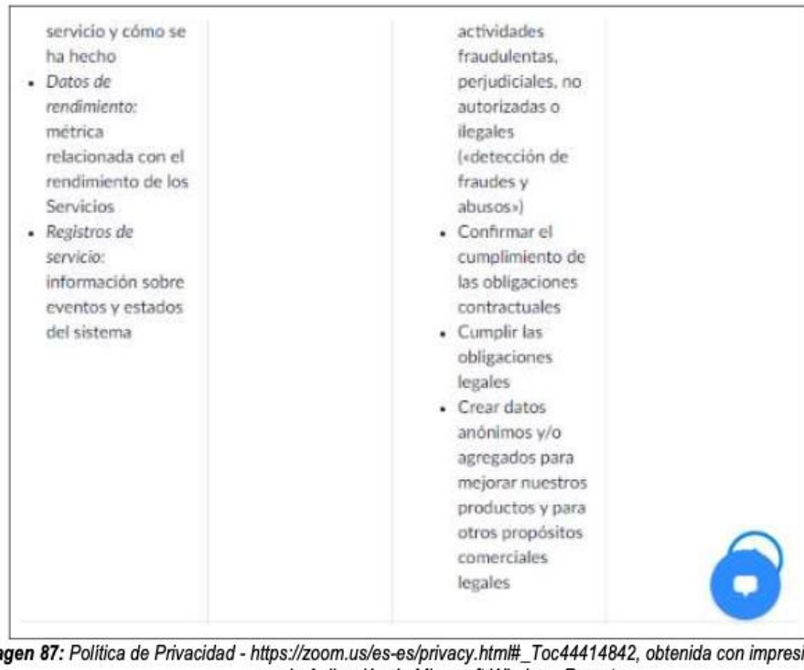
Datos del titular de una cuenta de pago La información que recogemos para una cuenta de Zoom de pago, como: • Datos del usuario de una cuenta de Zoom (enumerados anteriormente) • Nombre de facturación • Teléfono de facturación • Dirección de facturación • Método de pago • Nombre de la compañía (si procede) • Número de empleados (si procede)	Del usuario registrado de la cuenta de Zoom de pago	• Crear una cuenta de Zoom • Proporcionar servicios de Zoom • Responder a solicitudes de soporte • Enviar comunicaciones de marketing, si lo permite • Comunicar anuncios relacionados con actualizaciones de software, ampliaciones y mejoras del sistema	• Contrato • Intereses legítimos

Imagen 85: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*



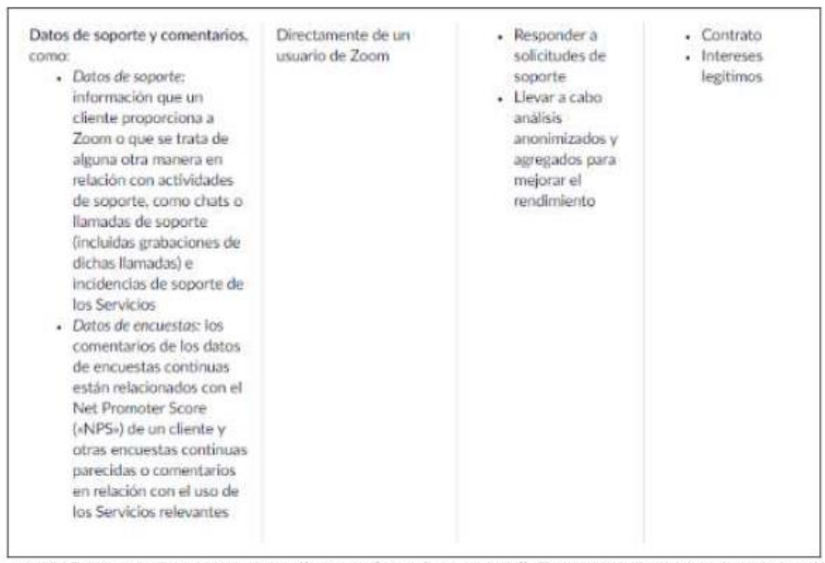
Datos operativos La información técnica del software o sistemas de Zoom que alojan los Servicios, y de los sistemas, aplicaciones y dispositivos que se utilizan para acceder a los Servicios, como: • *Datos de configuración:* información sobre la implementación de los servicios de Zoom e información del entorno relacionada • *Metadatos de reuniones:* métrica sobre cuándo y cómo se llevaron a cabo las reuniones • *Datos de uso de funciones:* información sobre si se han utilizado las funciones del	Automáticamente a través del uso de los Servicios	• Facilitar la prestación y optimización de los Servicios • Supervisar el rendimiento de nuestros centros de datos y redes • Proporcionar paneles de control e informes de cuentas • Proporcionar soporte • Preservar la seguridad de nuestra infraestructura y servicios • Administrar nuestros planes y políticas de recuperación ante desastres • Detectar, investigar y detener	• Contrato • Intereses legítimos • Protección de los intereses vitales • Cumplimiento legal

Imagen 86: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*



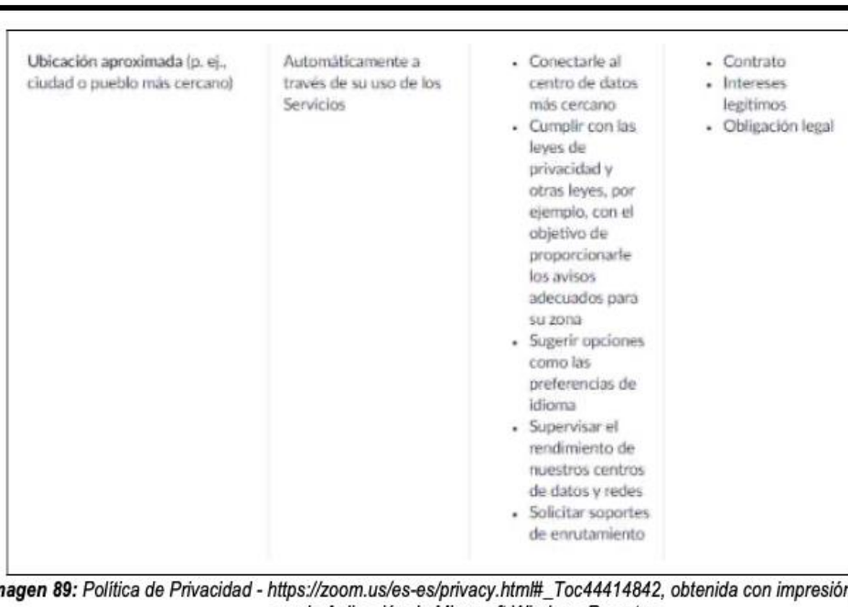
servicio y cómo se ha hecho • *Datos de rendimiento:* métrica relacionada con el rendimiento de los Servicios • *Registros de servicio:* información sobre eventos y estados del sistema		actividades fraudulentas, perjudiciales, no autorizadas o ilegales («detección de fraudes y abusos») • Confirmar el cumplimiento de las obligaciones contractuales • Cumplir las obligaciones legales • Crear datos anónimos y/o agregados para mejorar nuestros productos y para otros propósitos comerciales legales	

Imagen 87: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*



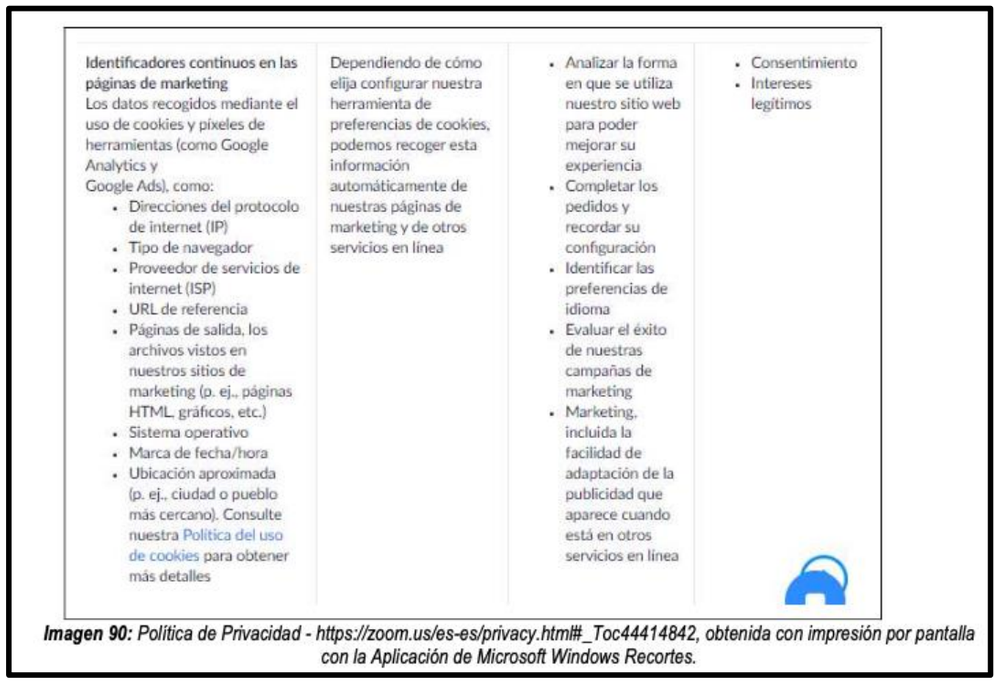
Datos de soporte y comentarios, como: • *Datos de soporte:* información que un cliente proporciona a Zoom o que se trata de alguna otra manera en relación con actividades de soporte, como chats o llamadas de soporte (incluidas grabaciones de dichas llamadas) e incidencias de soporte de los Servicios • *Datos de encuestas:* los comentarios de los datos de encuestas continuas están relacionados con el Net Promoter Score («NPS») de un cliente y otras encuestas continuas parecidas o comentarios en relación con el uso de los Servicios relevantes	Directamente de un usuario de Zoom	• Responder a solicitudes de soporte • Llevar a cabo análisis anonimizados y agregados para mejorar el rendimiento	• Contrato • Intereses legítimos

Imagen 88: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*



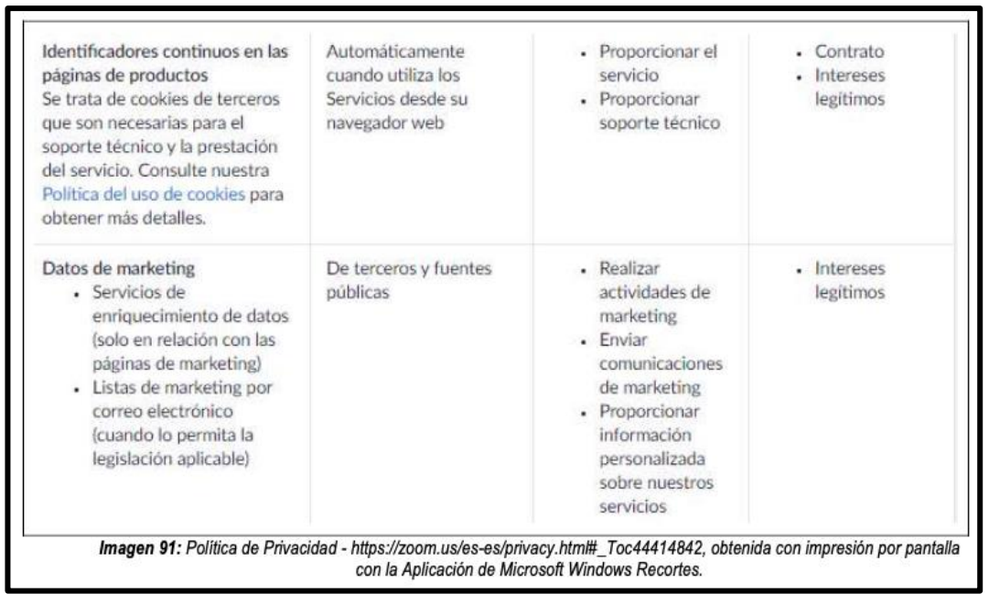
Ubicación aproximada (p. ej., ciudad o pueblo más cercano)	Automáticamente a través de su uso de los Servicios	• Conectarle al centro de datos más cercano • Cumplir con las leyes de privacidad y otras leyes, por ejemplo, con el objetivo de proporcionarle los avisos adecuados para su zona • Sugerir opciones como las preferencias de idioma • Supervisar el rendimiento de nuestros centros de datos y redes • Solicitar soportes de enrutamiento	• Contrato • Intereses legítimos • Obligación legal

Imagen 89: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*



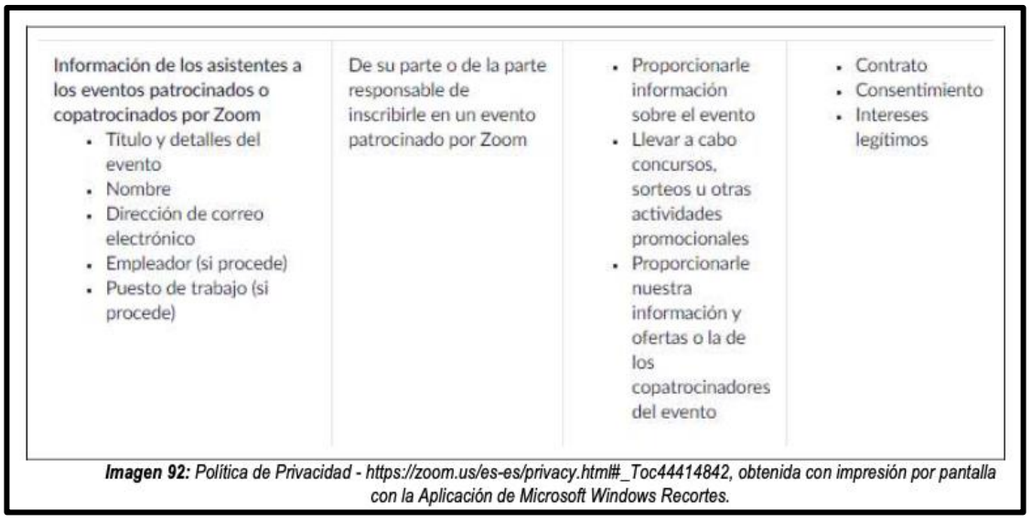
Identificadores continuos en las páginas de marketing Los datos recogidos mediante el uso de cookies y píxeles de herramientas (como Google Analytics y Google Ads), como: • Direcciones del protocolo de internet (IP) • Tipo de navegador • Proveedor de servicios de internet (ISP) • URL de referencia • Páginas de salida, los archivos vistos en nuestros sitios de marketing (p. ej., páginas HTML, gráficos, etc.) • Sistema operativo • Marca de fecha/hora • Ubicación aproximada (p. ej., ciudad o pueblo más cercano). Consulte nuestra Política del uso de cookies para obtener más detalles	Dependiendo de cómo elija configurar nuestra herramienta de preferencias de cookies, podemos recoger esta información automáticamente de nuestras páginas de marketing y de otros servicios en línea	• Analizar la forma en que se utiliza nuestro sitio web para poder mejorar su experiencia • Completar los pedidos y recordar su configuración • Identificar las preferencias de idioma • Evaluar el éxito de nuestras campañas de marketing • Marketing, incluida la facilidad de adaptación de la publicidad que aparece cuando está en otros servicios en línea	• Consentimiento • Intereses legítimos

Imagen 90: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*



Identificadores continuos en las páginas de productos Se trata de cookies de terceros que son necesarias para el soporte técnico y la prestación del servicio. Consulte nuestra Política del uso de cookies para obtener más detalles.	Automáticamente cuando utiliza los Servicios desde su navegador web	• Proporcionar el servicio • Proporcionar soporte técnico	• Contrato • Intereses legítimos
Datos de marketing • Servicios de enriquecimiento de datos (solo en relación con las páginas de marketing) • Listas de marketing por correo electrónico (cuando lo permita la legislación aplicable)	De terceros y fuentes públicas	• Realizar actividades de marketing • Enviar comunicaciones de marketing • Proporcionar información personalizada sobre nuestros servicios	• Intereses legítimos

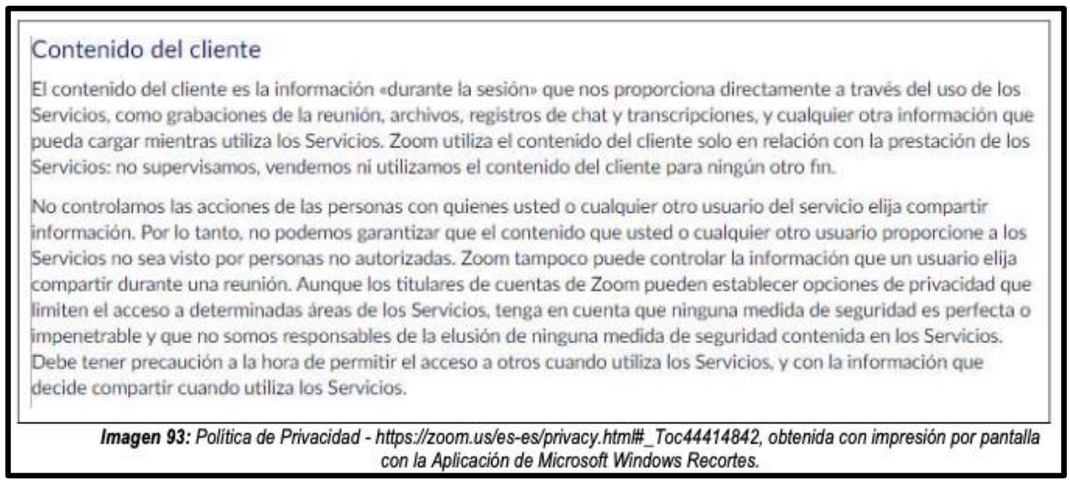
Imagen 91: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*



Información de los asistentes a los eventos patrocinados o copatrocinados por Zoom • Título y detalles del evento • Nombre • Dirección de correo electrónico • Empleador (si procede) • Puesto de trabajo (si procede)	De su parte o de la parte responsable de inscribirle en un evento patrocinado por Zoom	• Proporcionarle información sobre el evento • Llevar a cabo concursos, sorteos u otras actividades promocionales • Proporcionarle nuestra información y ofertas o la de los copatrocinadores del evento	• Contrato • Consentimiento • Intereses legítimos

Imagen 92: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

En la parte final del documento se encuentra el siguiente apartado, en el que se detalla información sobre el contenido que un usuario puede generar durante una reunión en Zoom, además de aquella información relacionada con los productos de Marketing y el programa de referencia de Zoom.



Contenido del cliente

El contenido del cliente es la información «durante la sesión» que nos proporciona directamente a través del uso de los Servicios, como grabaciones de la reunión, archivos, registros de chat y transcripciones, y cualquier otra información que pueda cargar mientras utiliza los Servicios. Zoom utiliza el contenido del cliente solo en relación con la prestación de los Servicios: no supervisamos, vendemos ni utilizamos el contenido del cliente para ningún otro fin.

No controlamos las acciones de las personas con quienes usted o cualquier otro usuario del servicio elija compartir información. Por lo tanto, no podemos garantizar que el contenido que usted o cualquier otro usuario proporcione a los Servicios no sea visto por personas no autorizadas. Zoom tampoco puede controlar la información que un usuario elija compartir durante una reunión. Aunque los titulares de cuentas de Zoom pueden establecer opciones de privacidad que limiten el acceso a determinadas áreas de los Servicios, tenga en cuenta que ninguna medida de seguridad es perfecta o impenetrable y que no somos responsables de la elusión de ninguna medida de seguridad contenida en los Servicios. Debe tener precaución a la hora de permitir el acceso a otros cuando utiliza los Servicios, y con la información que decide compartir cuando utiliza los Servicios.

Imagen 93: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

Las páginas de productos y marketing de Zoom

Por lo general, Zoom trata datos personales de dos maneras distintas a través de sus sitios web y aplicaciones. En primer lugar, Zoom trata los datos personales que obtiene de las páginas web o de las interfaces de las aplicaciones móviles que Zoom utiliza para prestar sus Servicios, como la página de inicio que un usuario visualiza tras hacer clic en un enlace para unirse a una reunión (las «Páginas de productos» de Zoom). Las Páginas de productos también incluyen páginas web y enlaces a los que solo puede acceder el titular de una cuenta de Zoom después de iniciar sesión en su cuenta de Zoom. Las Páginas de productos únicamente proporcionan cookies de terceros que sean necesarias para el soporte técnico y la prestación del servicio. No hay cookies de publicidad en función de intereses en las Páginas de productos.

En segundo lugar, Zoom trata los datos personales obtenidos de sus páginas web que son accesibles sin necesidad de iniciar sesión en una cuenta de Zoom (las «Páginas de marketing» de Zoom). Las Páginas de marketing, como www.zoom.us, están diseñadas para fomentar las ventas de las suscripciones de Zoom. Le informan sobre nuestro producto, planes y precios, características y otra información relacionada.

Al igual que muchas empresas, utilizamos servicios de publicidad que tratan de adaptar los anuncios en línea a sus intereses basándose en la información recogida a través de cookies y tecnologías parecidas en nuestras Páginas de marketing. Esto se llama publicidad en función de intereses. Puede obtener más información y optar por no utilizar cookies en nuestras Páginas de marketing haciendo clic en el enlace No vender mis datos personales en el pie de página de esta página web. Tendrá que establecer sus preferencias desde cada dispositivo y cada navegador web del que desee rechazar su uso. Esta función utiliza una cookie para recordar sus preferencias, por lo que si borra todas las cookies de su navegador, tendrá que volver a establecer su configuración. Para obtener información adicional sobre las cookies o tecnología similar, revise nuestra Política de cookies.

Imagen 94: *Política de Privacidad - https://zoom.us/es-es/privacy.html#_Toc44414842, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

VIII. **Sobre los hallazgos del análisis técnico y las respuestas enviadas por ZOOM VIDEO COMMUNICATIONS, INC**

Al finalizar el análisis técnico y la respuesta enviada por Zoom se destacan los siguientes hallazgos:

Hurto de credenciales

En la respuesta entregada por Zoom (Documento 20087350--0000200002), en la página 4, la compañía se refiere a la pregunta que se le realizó en materia de seguridad en los siguientes términos:

> *"(...) ninguna credencial de usuario (por ejemplo, nombres de usuario y contraseñas) fue extraída de Zoom. Al respecto, cualquier supuesta credencial de acceso de Zoom sería en realidad una credencial utilizada por usuarios de Zoom en otros sitios web o aplicaciones que fueron extraídas a través de algunos incidentes de seguridad que implicaron datos personales pero que no involucraron a Zoom. Algunos actores malintencionados afirman ahora que estos conjuntos de credenciales previamente robados pueden utilizarse para acceder a las cuentas de Zoom.*"

No obstante, en el sitio web BleepingComputer se encuentra un artículo titulado "*Más de 500.000 cuentas de Zoom vendidas en foros de hackers, la web oscura*", en el que se afirma que "*Más de 500.000 cuentas de Zoom se venden en la web oscura y foros de piratas informáticos por menos de un centavo cada una y, en algunos casos, se regalan de forma gratuita*.", como se puede ver a continuación:

Más de 500.000 cuentas de Zoom se venden en la web oscura y foros de piratas informáticos por menos de un centavo cada una y, en algunos casos, se regalan de forma gratuita.

Estas credenciales se recopilan a través de ataques de relleno de credenciales en los que los actores de amenazas intentan iniciar sesión en Zoom utilizando cuentas filtradas en violaciones de datos más antiguas. Los inicios de sesión exitosos se compilan en listas que se venden a otros piratas informáticos.

Imagen 1: *Sitio web BleepingComputer - https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

Cuentas vendidas a granel

Después de ver a un vendedor publicando cuentas en un foro de piratas informáticos, Cyble se acercó para comprar una gran cantidad de cuentas a granel para que pudieran usarse para advertir a sus clientes sobre la posible infracción.

Cyble pudo comprar aproximadamente 530,000 credenciales de Zoom por menos de un centavo cada una a $ 0.0020 por cuenta.

Las cuentas compradas incluyen la dirección de correo electrónico de la víctima, la contraseña, la URL de reunión personal y su HostKey .

Cuentas de Zoom vendidas en foros de hackers

Imagen 2: *Sitio web BleepingComputer - https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

Ahora bien, para ingresar a la aplicación se solicita la dirección de correo electrónico y la contraseña como puede observarse:

Imagen 3: *Inicio de Sesión Zoom - https://zoom.us/signin, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

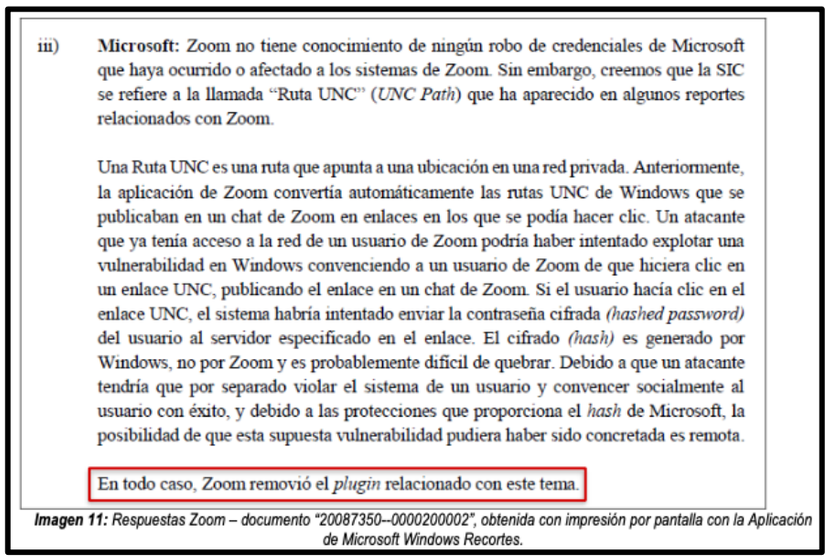
En la parte inferior de la pantalla se encuentra el siguiente mensaje "*Zoom está protegido por reCAPTCHA y la Política de privacidad política de privacidad y las Condiciones de servicio aplicables*", sin embargo, no se ejecuta o muestra algún método de *reCAPTCHA*. Por tanto, esta autoridad encuentra como engañosa y falsa dicha afirmación.

Hurto de credenciales de Windows

El robo de credenciales de Windows es una vulnerabilidad en la que los atacantes podían realizar desde el chat de la aplicación de escritorio de la aplicación Zoom para Windows. El robo de las credenciales de inicio de sesión, según el artículo publicado por el portal web "The Hacker News" titulado: "**El nuevo Zoom hack permite a los pitaras informáticos comprometer Windows y su contraseña de inicio de sesión**" se resalta que "*todo lo que un atacante debe hacer es enviar una URL creada (es decir, \\ xxxx \ abc_file) a una víctima a través de una interfaz de chat*."[17] En el mencionado artículo se adjuntan las pruebas realizadas por "Mohamed Baset" en las que se puede ver cómo funciona el ataque.

Imagen 10: *Artículo "El nuevo Zoom hack permite a los pitaras informáticos comprometer Windows y su contraseña de inicio de sesión" - https://thehackernews.com/2020/04/zoom-windows-password.html, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

En relación con lo anterior, en su respuesta la compañía afirma lo siguiente:



iii) **Microsoft:** Zoom no tiene conocimiento de ningún robo de credenciales de Microsoft que haya ocurrido o afectado a los sistemas de Zoom. Sin embargo, creemos que la SIC se refiere a la llamada "Ruta UNC" (*UNC Path*) que ha aparecido en algunos reportes relacionados con Zoom.

Una Ruta UNC es una ruta que apunta a una ubicación en una red privada. Anteriormente, la aplicación de Zoom convertía automáticamente las rutas UNC de Windows que se publicaban en un chat de Zoom en enlaces en los que se podía hacer clic. Un atacante que ya tenía acceso a la red de un usuario de Zoom podría haber intentado explotar una vulnerabilidad en Windows convenciendo a un usuario de Zoom de que hiciera clic en un enlace UNC, publicando el enlace en un chat de Zoom. Si el usuario hacía clic en el enlace UNC, el sistema habría intentado enviar la contraseña cifrada *(hashed password)* del usuario al servidor especificado en el enlace. El cifrado *(hash)* es generado por Windows, no por Zoom y es probablemente difícil de quebrar. Debido a que un atacante tendría que por separado violar el sistema de un usuario y convencer socialmente al usuario con éxito, y debido a las protecciones que proporciona el *hash* de Microsoft, la posibilidad de que esta supuesta vulnerabilidad pudiera haber sido concretada es remota.

En todo caso, Zoom removió el *plugin* relacionado con este tema.

Imagen 11: *Respuestas Zoom – documento "20087350--0000200002", obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

Transferencia de información a Facebook

En diferentes medios de comunicación se reportó que la aplicación Zoom para iOS compartía datos de los usuarios *que la usaban con la red social Facebook, como lo reporta el portal web "Vice" en su artículo titulado "La aplicación Zoom iOS envía datos a Facebook incluso si no tiene una cuenta de Facebook*":

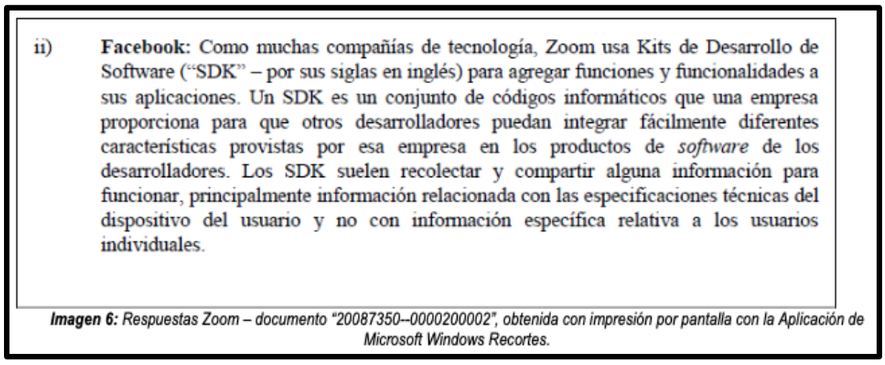
[17] Consultado en: https://thehackernews.com/2020/04/zoom-windows-password.html.

"Eso es impactante. No hay nada en la política de privacidad que aborde eso", dijo Pat Walshe, activista de Privacy Matters que analizó la política de privacidad de Zoom, en un mensaje directo de Twitter.

Al descargar y abrir la aplicación, Zoom se conecta a la API Graph de Facebook, según el análisis de Motherboard de la actividad de la red de la aplicación. Graph API es la principal forma en que los desarrolladores obtienen datos dentro o fuera de Facebook.

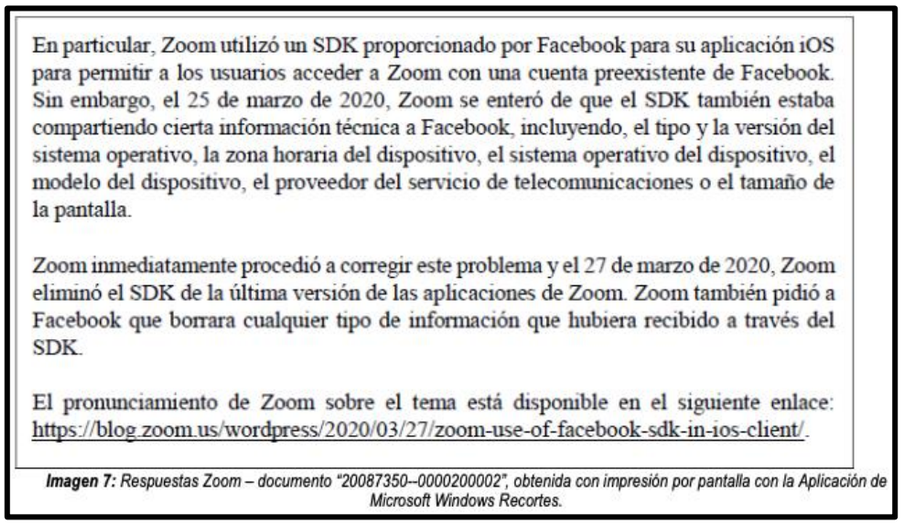
Imagen 4: *Portal web Vice - https://www.vice.com/en/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

De acuerdo con la información entregada por Zoom a esta entidad, en el documento "20087350--0000200002", en la página 4 numeral ii), la compañía afirma que "*el 25 de marzo de 2020,* ***Zoom se enteró de que el SDK también estaba compartiendo cierta información técnica a Facebook, incluyendo, el tipo y la versión del sistema operativo, la zona horaria del dispositivo, el sistema operativo del dispositivo, el modelo del dispositivo, el proveedor del servicio de telecomunicaciones o el tamaño de la pantalla.*** *Zoom inmediatamente procedió a corregir este problema y el 27 de marzo de 2020, Zoom eliminó el SDK de la última versión de las aplicaciones de Zoom. Zoom también pidió a Facebook que borrara cualquier tipo de información que hubiera recibido a través del SDK*." (destacamos), como se puede ver a continuación:



ii) **Facebook:** Como muchas compañías de tecnología, Zoom usa Kits de Desarrollo de Software ("SDK" – por sus siglas en inglés) para agregar funciones y funcionalidades a sus aplicaciones. Un SDK es un conjunto de códigos informáticos que una empresa proporciona para que otros desarrolladores puedan integrar fácilmente diferentes características provistas por esa empresa en los productos de *software* de los desarrolladores. Los SDK suelen recolectar y compartir alguna información para funcionar, principalmente información relacionada con las especificaciones técnicas del dispositivo del usuario y no con información específica relativa a los usuarios individuales.

Imagen 6: *Respuestas Zoom – documento "20087350--0000200002", obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*



En particular, Zoom utilizó un SDK proporcionado por Facebook para su aplicación iOS para permitir a los usuarios acceder a Zoom con una cuenta preexistente de Facebook. Sin embargo, el 25 de marzo de 2020, Zoom se enteró de que el SDK también estaba compartiendo cierta información técnica a Facebook, incluyendo, el tipo y la versión del sistema operativo, la zona horaria del dispositivo, el sistema operativo del dispositivo, el modelo del dispositivo, el proveedor del servicio de telecomunicaciones o el tamaño de la pantalla.

Zoom inmediatamente procedió a corregir este problema y el 27 de marzo de 2020, Zoom eliminó el SDK de la última versión de las aplicaciones de Zoom. Zoom también pidió a Facebook que borrara cualquier tipo de información que hubiera recibido a través del SDK.

El pronunciamiento de Zoom sobre el tema está disponible en el siguiente enlace: https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/.

Imagen 7: *Respuestas Zoom – documento "20087350--0000200002", obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

El 27 de marzo del 2020, la compañía publica en su blog un artículo titulado "Uso de Zoom del SDK de Facebook en el cliente iOS", en este aseguran haber corregido el SDK para el inicio de sesión. Dado que esta vulnerabilidad se presentó en el mes de marzo, en la actualidad esta autoridad no cuenta con los elementos para realizar una revisión del código de la aplicación.

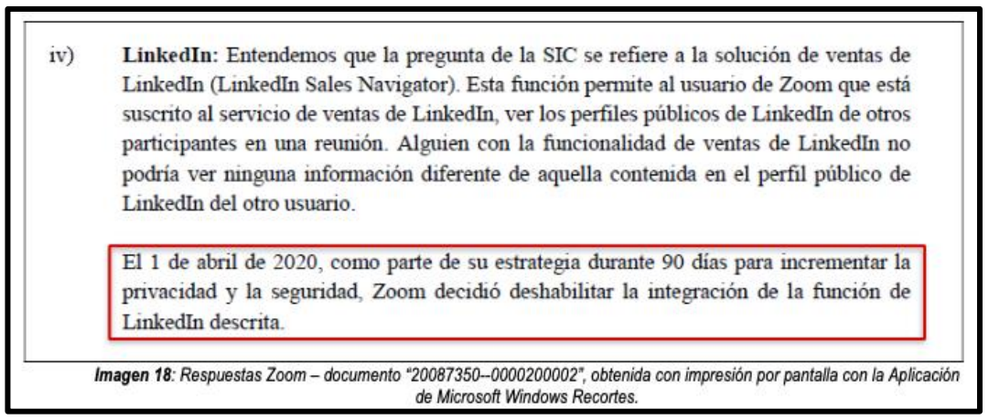
Originalmente implementamos la función "Iniciar sesión con Facebook" utilizando el SDK de Facebook para iOS (Kit de desarrollo de software) para brindarles a nuestros usuarios otra forma conveniente de acceder a nuestra plataforma. Sin embargo, el miércoles 25 de marzo de 2020 nos informaron que el SDK de Facebook estaba recopilando información del dispositivo innecesaria para que brindemos nuestros servicios. La información recopilada por el SDK de Facebook no incluía información y actividades relacionadas con las reuniones, como asistentes, nombres, notas, etc., sino que incluía información sobre dispositivos como el tipo y la versión del sistema operativo móvil, la zona horaria del dispositivo, el sistema operativo del dispositivo, modelo y operador del dispositivo, tamaño de la pantalla, núcleos del procesador y espacio en disco.

La privacidad de nuestros clientes es increíblemente importante para nosotros y, por lo tanto, decidimos eliminar el SDK de Facebook en nuestro cliente iOS y hemos reconfigurado la función para que los usuarios aún puedan iniciar sesión con Facebook a través de su navegador. Los usuarios deberán actualizar a la última versión de nuestra aplicación que ya está disponible a las 2:30 pm hora del Pacífico el viernes 27 de marzo de 2020, para que estos cambios se apliquen, y les recomendamos encarecidamente que lo hagan.

***Imagen 8:** Blog de Zoom -https://blog.zoom.us/zoom-use-of-facebook-sdk-in-ios-client/, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

Acceso a los perfiles de LinkedIn

El acceso a los perfiles de la red social LinkedIn a través de la aplicación Zoom se realizaba gracias a la solución de ventas de esta red social, denominada "*LinkedIn Sales Navigator*". Lo anterior, lo expresa Zoom en el documento "20087350--0000200002" en la página 5, numeral iv), en los siguientes términos:



iv) **LinkedIn:** Entendemos que la pregunta de la SIC se refiere a la solución de ventas de LinkedIn (LinkedIn Sales Navigator). Esta función permite al usuario de Zoom que está suscrito al servicio de ventas de LinkedIn, ver los perfiles públicos de LinkedIn de otros participantes en una reunión. Alguien con la funcionalidad de ventas de LinkedIn no podría ver ninguna información diferente de aquella contenida en el perfil público de LinkedIn del otro usuario.

El 1 de abril de 2020, como parte de su estrategia durante 90 días para incrementar la privacidad y la seguridad, Zoom decidió deshabilitar la integración de la función de LinkedIn descrita.

***Imagen 18**: Respuestas Zoom – documento "20087350--0000200002", obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

En relación con lo anterior, el diario "*The New York Times*" en su artículo titulado "*Una función sobre Zoom mostraba en secreto los datos de los perfiles de LinkedIn de las personas*" evidenciaba como luego de un análisis realizado por el periódico se encontró que en las pruebas realizadas "*descubrieron que incluso cuando un periodista se registraba en una reunión de Zoom con seudónimos ("Anónimo" y "No estoy aquí**"), la herramienta de extracción de datos podía relacionarlo instantáneamente con su perfil de LinkedIn. Al hacerlo, Zoom reveló el nombre real del reportero a otro usuario, anulando sus esfuerzos por mantenerlo en privado***"[18]. (Destacamos).

Actualmente no se encuentra disponible la aplicación "*Reuniones de vídeo de LinkedIn*" relacionadas con la red social. Entonces, no es posible recrear esta vulnerabilidad.

IX. Actuaciones y decisiones de autoridades extranjeras en relación con el Tratamiento de Datos Personales por parte de ZOOM VIDEO COMMUNICATIONS, INC.

El 9 de noviembre de 2020 la COMISIÓN FEDERAL DE COMERCIO DE LOS ESTADOS UNIDOS DE AMÉRICA ("The Federal Trade Commission") publicó un acuerdo resolutorio[19] (*Agreement Containing Consent Order*) en el que establece que Zoom debe proteger de mejor manera la información personal. La autoridad sostuvo que Zoom incumplió la obligación de proteger la información de los usuarios de diversas maneras[20]:

- **Zoom dijo que proporcionó codificación punto a punto** — una manera de proteger las comunicaciones para que únicamente las vean el emisor y el receptor — **para las reuniones de Zoom. No lo hizo**.
- **Zoom dijo que protegió las reuniones con un nivel de codificación más alto del que realmente ofreció**.
- Zoom les dijo a los usuarios que grabaron una reunión que, una vez terminada, se guardaría una grabación segura y codificada de esa reunión. En realidad, **Zoom guardó grabaciones**

[18] Consultado en: https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html
[19] File Nº 1923167 Agreement Containing Consent Order. In the Matter of ZOOM VIDEO COMMUNICATIONS, INC., a corporation, d/b/a ZOOM en: https://www.ftc.gov/system/files/documents/cases/1923167zoomacco2.pdf.
[20] Ibídem.

sin codificar en sus servidores hasta por 60 días antes de pasarlas a su nube de almacenamiento segura.

- **Zoom instaló un software, llamado ZoomOpener, en las computadoras Mac de los usuarios. Este programa eludió una función de seguridad del navegador Safari** y puso en riesgo a los usuarios — por ejemplo, podría haber permitido que extraños espiaran a los usuarios a través de las cámaras web de las computadoras. O los piratas informáticos podrían haber explotado la vulnerabilidad para descargar programas maliciosos en las computadoras de los usuarios y tomar el control de sus dispositivos. **Si los usuarios eliminaban la aplicación de Zoom, el programa ZoomOpener permanecía instalado, al igual que estas vulnerabilidades de seguridad**. Zoom podía volver a instalar la aplicación sin el permiso del usuario y sin informárselo.
- Zoom no les contó la historia completa del programa ZoomOpener a los usuarios. **Zoom dijo que el software era una corrección de fallo, pero no les dijo a los usuarios que instalaría un servidor web que circunvalaría una salvaguarda de privacidad y seguridad, o que el software permanecería instalado en sus computadoras incluso después de haber eliminado Zoom**.

Entonces, al igual que esta autoridad, la Comisión Federal de Comercio de los Estados Unidos de América encontró vulnerabilidades en las medidas de seguridad implementadas por Zoom.

X. El principio de Responsabilidad Demostrada respecto de las medidas de seguridad.

La regulación colombiana le exige a todos los Responsables del Tratamiento, incluyendo a ZOOM VIDEO COMMUNICATIONS, INC, cumplir el principio de Responsabilidad Demostrada respecto de las medidas de seguridad para realizar el Tratamiento de Datos personales. En efecto, los artículos 2.2.2.25.6.1 y 2.2.2.25.6.2 del Decreto Único Reglamentario 1074 de 2015 afirman 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, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso.*
>
> ***En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta 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 capítulo.*
>
> *2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.*

3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento.

La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente capítulo".

La regulación colombiana le impone a los Responsables y Encargados del Tratamiento, **la responsabilidad de garantizar la eficacia de los derechos del Titular del dato, la cual no puede ser simbólica, ni limitarse únicamente a la formalidad**. Por el contrario, debe ser real y demostrable. Al respecto, nuestra jurisprudencia ha determinado que "*existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante*"[21].

Adicionalmente, es importante resaltar que los Responsables o Encargados del Tratamiento de los datos, no se convierten en dueños de los mismos como consecuencia del almacenamiento en sus bases o archivos. En efecto, al ejercer únicamente la mera tenencia de la información, solo tienen a su cargo el deber de administrarla de manera correcta, apropiada y acertada. Por consiguiente, **si los sujetos mencionados actúan con negligencia o dolo, la consecuencia directa sería la afectación de los derechos humanos y fundamentales de los titulares de los datos**.

Por su parte, el artículo 2.2.2.25.6.1. *-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*". Así, resulta imposible ignorar la forma en que el Responsable y Encargado del Tratamiento deben probar el poner en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación. Es decir, se reivindica que un Responsable y Encargado no puede utilizar cualquier tipo de políticas o herramientas para dicho efecto, sino solo aquellas que tengan como propósito lograr que los postulados legales sean realidades verificables, y no solo se limiten a creaciones teóricas e intelectuales.

El artículo 2.2.2.25.6.2. *-Políticas Internas Efectivas-*, exige que los Responsables del Tratamiento de Datos personales implementen medidas efectivas y apropiadas que garanticen, entre otras, lo siguiente: "(…) *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*[22]*(accountability)*". El término "***accountability***"[23], a pesar de tener diferentes significados, ha sido entendido en el campo de la protección de datos como el modo en que una organización debe cumplir (en la práctica) las regulaciones sobre el tema, y la manera en que debe demostrar que lo puesto en práctica es útil, pertinente y eficiente.

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

1. Diseñar y activar un programa integral de gestión de datos (en adelante PIGDP). Esto, exige compromisos y acciones concretas de los directivos de la organización. Igualmente requiere la implementación de controles de diversa naturaleza;
2. Desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP; y
3. Demostrar el debido cumplimiento de la regulación sobre tratamiento de datos personales.

El Principio de Responsabilidad Demostrada *–accountability-* demanda implementar acciones de diversa naturaleza[24] para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El mismo, exige que los Responsables y Encargados del Tratamiento adopten medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia.

Dichas acciones o medidas, deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los datos personales.

---

[21] Cfr. Corte Constitucional, sentencia T-227 de 2003.
[22] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf
[23] Cfr. Grupo de trabajo de protección de datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 8.
[24] Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humana y de gestión. Asimismo involucran procesos y procedimientos con características propias en atención al objetivo que persiguen.

El Principio de Responsabilidad Demostrada demanda menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. Requiere apremiar acciones concretas por parte de las organizaciones para garantizar el debido tratamiento de los datos personales. El éxito del mismo dependerá del compromiso real de todos los miembros de una organización. Especialmente, de los directivos de las organizaciones, pues, sin su apoyo sincero y decidido, cualquier esfuerzo será insuficiente para diseñar, llevar a cabo, revisar, actualizar y/o evaluar los programas de gestión de datos.

Adicionalmente, el reto de las organizaciones frente al Principio de Responsabilidad Demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas. Como se ha manifestado, exige que se demuestre el cumplimiento real y efectivo en la práctica de sus funciones.

En este sentido, desde el año 2006 la Red Iberoamericana de Protección de Datos (RIPD) ha puesto de presente que, "*la autorregulación sólo* [sic] *redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que* ***no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales****"* [25]. (Énfasis añadido).

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

Aunque no es el espacio para explicar cada uno de los aspectos mencionados en la guía[26], es destacable que el Principio de Responsabilidad Demostrada se articula con el concepto de *compliance*, en la medida que este hace referencia a la autogestión o "*conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos*"[27].

La **identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos son elementos cardinales del *compliance* y buena parte de lo que implica el Principio de Responsabilidad Demostrada (*accountability*)**. En la mencionada guía se considera fundamental que las organizaciones desarrollen y ejecuten, entre otros, un "*sistema de administración de riesgos asociados al tratamiento de datos personales*"[28] que les permita "*identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales*"[29].

QUINTO: Sin perjuicio de todo lo anterior, destacamos las siguientes **CONCLUSIONES**:

1. **ZOOM VIDEO COMMUNICATIONS, INC** tienen la obligación de cumplir la legislación Colombiana, así como las órdenes y requerimientos de esta autoridad.
2. La Ley 1581 de 2012 es aplicable a **ZOOM VIDEO COMMUNICATIONS, INC** porque recolectan Datos personales en el territorio de la República de Colombia a través de *cookies* que instala en los equipos o dispositivos de las personas residentes o domiciliadas en Colombia.
3. **ZOOM VIDEO COMMUNICATIONS, INC** trata Datos personales de los usuarios que usaron Zoom para participar en mas de 17 millones de reuniones entre el 1 y el 28 de abril de 2020.
4. 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

---

[25] 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.
[26] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf
[27] Cfr. World Compliance Association (WCA). http://www.worldcomplianceassociation.com/ (última consulta: 6 de noviembre de 2018).
[28] Cfr. Superintendencia de Industria y Comercio (2015) "*Guía para implementación del principio de responsabilidad demostrada (accountability)*", págs 16-18.
[29] *Ibidem*.

evitar situaciones indeseadas que pueden afectar los derechos de los titulares y de los mismos Responsables y Encargados del Tratamiento de los datos.

5. Zoom ha reconocido algunas fallas de seguridad y ha adoptado medidas para subsanarlas. No obstante, según pronunciamiento reciente de la FTC aún subsisten algunas falencias. Dado lo anterior, esta entidad considera necesario emitir órdenes administrativas de carácter preventivo para garantizar el principio y el deber de seguridad.

SEXTO: Que, en virtud de la situación actual, en particular la emergencia sanitaria, se ha restringido el ingreso a las instalaciones de la Superintendencia de Industria y Comercio, en consecuencia, se establecieron las medidas pertinentes para permitir el acceso completo a los expedientes, por lo que la sociedad debe: (i) enviar un correo electrónico a contactenos@sic.gov.co o habeasdata@sic.gov.co, solicitando el acceso al expediente a través de la plataforma servicios en línea, indicando el número de radicado del expediente; (ii) una vez reciba respuesta respecto de la solicitud de acceso, la sociedad debe registrarse en servicios en línea en el enlace https://servicioslinea.sic.gov.co/servilinea/ServiLinea/Portada.php y a través del mismo , luego del registro, puede consultar el expediente digitalmente.

No obstante, en aras de garantizar los derechos de defensa y contradicción de la investigada, en el caso en que la misma considere necesario el acceso físico del expediente, deberá enviar un correo electrónico a la dirección de correo habeasdata@sic.gov.co, solicitando que le asignen una cita para que pueda examinar el expediente, con el número de la referencia, en las instalaciones de la Superintendencia de Industria y Comercio en la ciudad de Bogotá. Lo anterior por cuanto se deben garantizar el ingreso a las instalaciones con las adecuadas medidas de bioseguridad.

SÉPTIMO: Una orden administrativa no es una sanción, sino una medida necesaria para la adecuación de las actividades u operaciones de los Responsables del Tratamiento a las disposiciones de la regulación colombiana sobre protección de Datos personales. Las sanciones por infringir la Ley Estatutaria 1581 de 2012 *-multas, suspensión de actividades, cierre temporal o definitivo-* están previstas en el artículo 23 de dicha norma. Allí se puede constatar que las órdenes no son sanciones.

OCTAVO: Que para garantizar el debido Tratamiento de Datos personales efectuado en el territorio de la República de Colombia es necesario emitir varias órdenes a **ZOOM VIDEO COMMUNICATIONS, INC.**

En mérito de lo expuesto, este Despacho.

RESUELVE

ARTÍCULO PRIMERO. ORDENAR a la sociedad **ZOOM VIDEO COMMUNICATIONS, INC** en adelante **Zoom**, 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:
   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 **Zoom;**
   c) La naturaleza y el ámbito de las actividades de **Zoom;**
   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 y fines del Tratamiento;
   h) Las actualizaciones o cualquier tipo de modificación de la plataforma de **Zoom**, sus productos y cualquier otra forma en que **Zoom** utilice, recopile, comparta o trate los datos recolectados;

i) El acceso a los Datos personales por parte de los empleados, contratistas y en general los colaboradores de **Zoom;**
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 los Titulares.

3) Desarrollar, implementar y mantener un programa de gestión y manejo de incidentes de seguridad en Datos personales, que contemple procedimiento para información sin dilación indebida a esta Superintendencia de Industria y Comercio 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 **Zoom.**

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) **Zoom** 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, certificar a esta entidad 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. La sociedad **ZOOM VIDEO COMMUNICATIONS, INC** deberá cumplir lo ordenado en esta resolución dentro de los cuatro (4) meses siguientes a la ejecutoria del presente acto administrativo y acreditar ante la Dirección de Investigaciones de Protección de Datos Personales de la Superintendencia de Industria y Comercio las medidas y procedimientos adoptados dentro de los cinco (5) días siguientes al vencimiento de dicho término.

PARÁGRAFO PRIMERO. Para demostrar el cumplimiento, la sociedad **ZOOM VIDEO COMMUNICATIONS, INC** deberá 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 deber de seguridad de la Ley Estatutaria 1581 de 2012 respecto de los Datos personales.

PARÁGRAFO SEGUNDO. La entidad o empresa que emita el certificado será seleccionada por **ZOOM VIDEO COMMUNICATIONS, INC,** pero debe ser un tercero cuya gestión esté libre de todo conflicto de interés que le reste independencia y sea ajena a cualquier tipo de subordinación respecto de **ZOOM VIDEO COMMUNICATIONS, INC.**

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. Notificar el contenido de la presente resolución a **ZOOM VIDEO COMMUNICATIONS, INC** informándole 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

Dada en Bogotá, D.C., 23 NOVIEMBRE 2020

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE SALAZAR MUÑOZ

Firmado digitalmente por CARLOS ENRIQUE SALAZAR MUÑOZ
Fecha: 2020.11.23 12:08:47 -05'00'

CARLOS ENRIQUE SALAZAR MUÑOZ

ALC/CEZ

NOTIFICACIÓN:

Sociedad (1):	**ZOOM VIDEO COMMUNICATIONS, INC**
Identificación[30]:	N/A
Correo electrónico:	legal@zoom.us
Dirección:	N/A
Ciudad:	San José (California)
Presidente Jurídico:	Lynn Haaland
Identificación[31]:	SIN IDENTIFICACIÓN

[30] No se cuenta con identificación.
[31] No se cuenta con identificación.