

# BOLETÍN LEGAL Y TRIBUTARIO

No.39

23 de noviembre  
de 2022



**ADICIONAR**  
Asesorías Empresariales Integrales

## En esta emisión trataremos:

**1. Compliance: Principio de  
responsabilidad  
demostrada  
"Accountability" en el  
tratamiento de los datos  
personales**

**2. Imágenes captadas  
en sistemas de  
videovigilancia están  
sujetas al régimen de  
protección de datos  
personales**

# ADICIONAR



1. **Compliance: Principio de responsabilidad demostrada "Accountability" en el tratamiento de los datos personales**

[Consulte aquí la guía de la SIC para la implementación del principio de Accountability.](#)

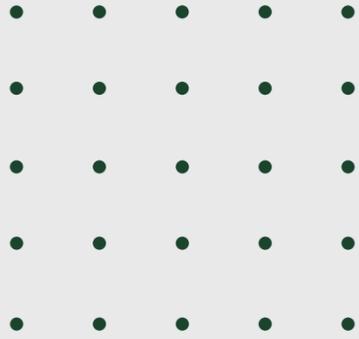


# ¿Que es Compliance?



El termino *Compliance* hace referencia a todo un sistema que propende no solo por el cumplimiento de las leyes y demás normas a las que debe ceñirse una empresa en el marco de las actividades que esta desarrolle, sino que también busca velar por la puesta en practica de principios y valores que estas ejecutan de manera voluntaria, para implementar buenas practicas empresariales.





Una de las principales funciones del *Compliance* consiste en asumir las tareas de prevención, detección y gestión de riesgos.

Algunas de las áreas de especial relevancia que abarca el *Compliance* , son las relacionadas con la prevención del lavado de activos y financiación del terrorismo (LA/FT), el derecho de la competencia, la protección de los derechos de los consumidores, protección de datos personales, entre otras.





# ¿ Como se relaciona el Compliance con la protección de los datos personales ?

El Compliance busca ejecutar y dar cumplimiento a las leyes y demás normas proferidas por la autoridades, entre estas la regulación referente a la protección de los datos personales.

La Ley 1581 de 2012 hace referencia al tratamiento de los datos personales, esta Ley se encarga de reconocer y proteger el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada , por ende, es función del Compliance observar, ejecutar y obedecer este tipo de regulaciones.



# ¿Que es el principio de responsabilidad demostrada o "Accountability" ?



El principio de responsabilidad demostrada (*accountability*) persigue que el cumplimiento de las normas constitucionales y legales sean una realidad verificable.

Ahora bien, el principio de responsabilidad demostrada en el ámbito del tratamiento de datos personales consiste en la implementación de los estándares de protección por parte de los responsables del tratamiento de datos personales, para garantizar a los ciudadanos un manejo idóneo de su información personal, en donde dicha gestión operativa debe de ser verificable.



# Colombia como pionera en regular la Responsabilidad Demostrada



Desde el 2013 Colombia ha sido pionera en regular la responsabilidad demostrada en el tratamiento de los datos personales.

Con la expedición del Decreto 1377 de 2013 se establecieron obligaciones para los responsables del tratamiento de datos personales, tales como, la de 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.

Aquel deber del responsable, se enmarca bajo lo que se ha denominado como el principio de “accountability” o Responsabilidad Demostrada.



# Beneficios que representa implementar la responsabilidad demostrada en el tratamiento de datos personales



Estos son algunos beneficios de implementar el principio de responsabilidad demostrada en el tratamiento de datos personales:

- Genera una mayor protección para los individuos, lo cual se traduce en beneficios para las empresas.
- Para aquellas empresas que se comprometan con la protección de la información personal, existe una verificación por parte de la SIC que le acredita a la empresa la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales, tal como lo señala el artículo 27 del decreto 1377 de 2013.
- Las empresas se encuentran en la capacidad de demostrar el cumplimiento de medidas efectivas tomadas para ejecutar las obligaciones contempladas en la Ley 1581 de 2012 y demás regulaciones en materia de protección de datos.



ADICIONAR



**2. Imágenes captadas en sistemas de videovigilancia están sujetas al régimen de protección de datos personales**

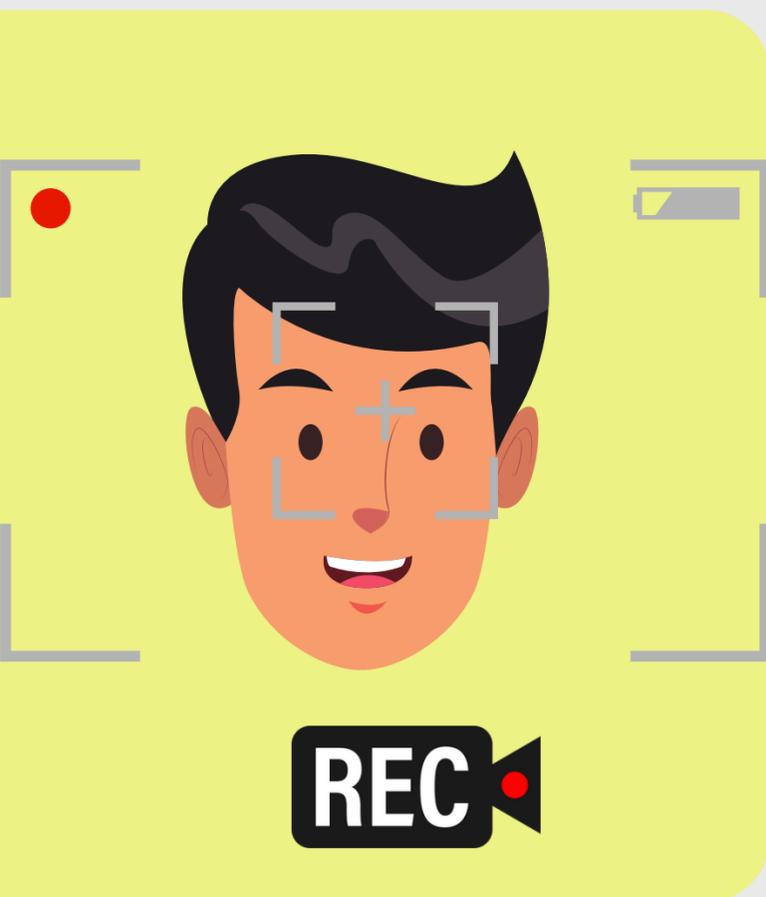
[Consulte aquí la guía de vigilancia de la SIC](#)





# Imágenes captadas en sistemas de videovigilancia están sujetas al régimen de protección de datos personales

La Superintendencia de Industria y Comercio, precisó que las grabaciones o imágenes que estén vinculadas con una o varias personas determinadas o determinables encuadran dentro del concepto de dato personal y por tanto están sujetas al régimen de protección de datos personales (Ley 1581 del 2012)



Dicho tratamiento, recordó la entidad, solo puede realizarse cuando exista la autorización previa e informada del titular, la cual podrá manifestarse por escrito, de forma oral o mediante conductas inequívocas que se entiendan como una manifestación de otorgamiento de la autorización.



# Imágenes captadas en sistemas de videovigilancia están sujetas al régimen de protección de datos personales

REC



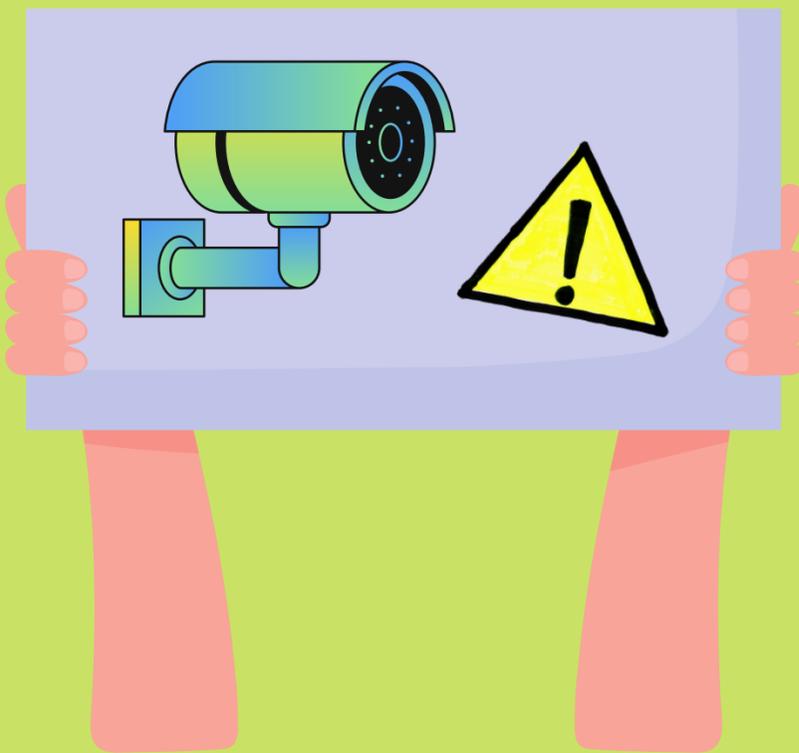
En el caso de la autorización para el tratamiento de datos personales a través de cámaras se pueden utilizar señales o avisos distintivos en las zonas de videovigilancia, principalmente en el ingreso, los lugares que están siendo vigilados y monitoreados como las porterías, ascensores, garajes y todos los demás sitios en donde se utilicen cámaras o mecanismos de vigilancia. Incluso, se pueden emplear anuncios de audio. Los avisos deben ser visibles y legibles.



# Contenido de los avisos de privacidad en los sistemas de vigilancia

En la Guía de Protección de Datos Personales en Sistemas de Videovigilancia proferida por la autoridad de datos personales, la SIC recordó que los avisos deben como mínimo, cumplir con el contenido de un aviso de privacidad:

- Incluir información sobre quién es el responsable del tratamiento y sus datos de contacto.
- Indicar el tratamiento que se dará a los datos y la finalidad del mismo.
- Incluir los derechos de los titulares.
- Indicar dónde está publicada la política de tratamiento de la información.



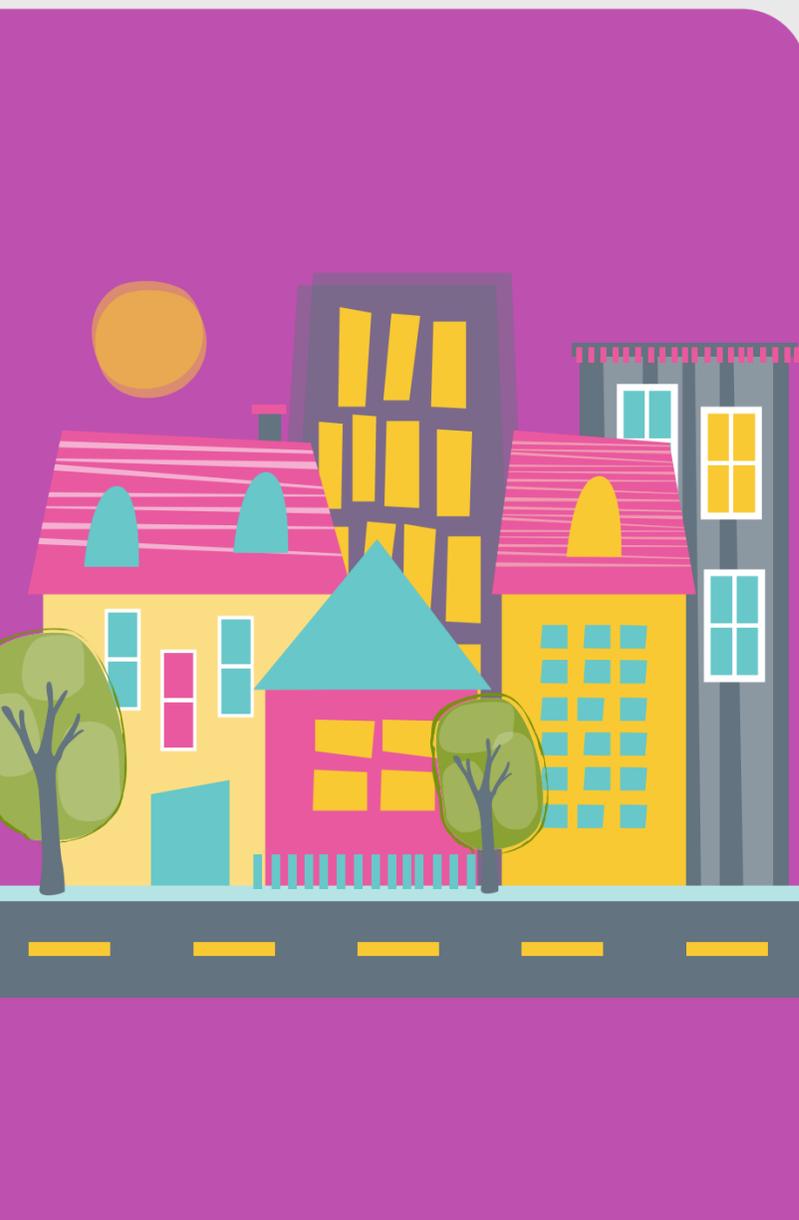


# Sobre los sistemas de vigilancia con acceso a las vías públicas:

El Estado se encuentra legitimado para operar sistemas de vigilancia mediante cámaras con acceso a las vías públicas, con el fin de garantizar la seguridad de las personas y los bienes, excluyendo de este ejercicio a los particulares, sin embargo, algunos sistemas de vigilancia privados eventualmente pueden tomar imágenes de la vía pública con la finalidad de garantizar la seguridad en los entornos privados. Un ejemplo de lo anterior son las imágenes tomadas en puntos de acceso como porterías

La recolección de estas imágenes por parte de particulares debe tener como único propósito el fin legítimo perseguido, el cual es garantizar la seguridad.

En todo caso el Titular de los datos personales también se encuentra facultado para solicitar la supresión de sus imágenes en la medida que no exista un deber legal o contractual que impida tal supresión





# Tratamientos personales de niños, niñas y adolescentes en sistemas de vigilancia.

Según la Guía de Protección de Datos Personales en Sistemas de Videovigilancia proferida por la SIC, el tratamiento de las imágenes de los niños, niñas y adolescentes solo se podrá realizar cuando: Responda y respete su interés superior y se asegure el respeto de sus derechos fundamentales.

Los Responsables y Encargados que utilicen sistemas de vigilancia que involucren el Tratamiento de imágenes de niños, niñas y/o adolescentes deben observar las siguientes reglas:

- Contar con la autorización de los padres o representantes legales de los menores.
- Informar a los padres o representantes legales acerca de la finalidad y el Tratamiento al cual serán sometidos los datos personales de los menores.





## Tratamientos personales de niños, niñas y adolescentes en sistemas de vigilancia.

- Limitar la recolección y demás Tratamiento de las imágenes, de acuerdo con lo que resulte proporcional y adecuado en consideración a la finalidad previamente informada.
- Garantizar la seguridad y reserva de los datos personales de los menores.
- Restringir el acceso y la circulación de las imágenes, conforme a lo establecido en la ley.





# Recomendaciones generales sobre el tratamiento personales en sistemas de vigilancia.

Dentro de la Guía de Protección de Datos Personales en Sistemas de Videovigilancia proferida por la SIC se emiten las siguientes recomendaciones relacionadas con el tratamiento de datos personales en los sistemas de vigilancia:

- Las bases de datos con fines de videovigilancia deben inscribirse en el Registro Nacional de Bases de Datos RNBD.
- Antes de implementar un sistema de vigilancia tenga en cuenta las disposiciones contenidas en el Régimen General de Protección de Datos Personales.
- Implemente medidas de seguridad y confidencialidad para el Tratamiento de la información recolectada.





# Recomendaciones generales sobre el tratamiento personales en sistemas de vigilancia.

- Evalúe el impacto que un SV puede tener respecto de la intimidad y la protección de los datos personales de los Titulares.
- Obtenga la autorización o consentimiento del Titular de los datos personales para el Tratamiento de los mismos, adoptando los mecanismos necesarios para dar cumplimiento a lo establecido en el Régimen General de Protección de Datos Personales.



## Si necesita asesoría no dude en contactarnos .



[contacto@adicionar.com.co](mailto:contacto@adicionar.com.co)



315 344 4539 - 301 399 6268



Carrera 9 No 72-81 - Oficina 206



<https://adicionar.com.co/>



<https://www.linkedin.com/company/79936824/admin/>

