TRIBUNAL CONSTITUCIONAL

N° 21 -2016-DIGA/TC

Lima, 31 de marzo de 2016

VISTOS

El Informe N.° 079-2015-OTI/TC, N.° 018-2016-OTI/TC y N.° 034-2016-OTI/TC, de la Oficina de Tecnologías de la Información, del 14 de diciembre de 2015 y15 de febrero y 17 de marzo de 2016 de 16 de febrero de 2016, respectivamente; los Informes N.° 003-2016-OPD/2016 de 19 de enero de 2016 y N.° 005-2016-OPD/TC de 16 de febrero de 2016, expedidos por la Oficina de Planeamiento y Desarrollo, y los proveídos de la Dirección General de Administración, de fecha 8 de enero, 16 de febrero y 21 marzo de 2016; y,

CONSIDERANDO

Que, la Oficina de Tecnologías de la Información ha presentado los proyectos de Directiva sobre "Normas para el Uso del Correo Electrónico en el Tribunal Constitucional" y "Normas que regulan el uso de las tecnologías de la Información y Comunicaciones en el Tribunal Constitucional";

Que, la directiva "Normas para el Uso del Correo Electrónico en el Tribunal Constitucional" tiene por finalidad normar los procedimientos para una gestión eficiente de los servicios de correo electrónico en el Tribunal Constitucional;

Que, por su parte, las "Normas que regulan el uso de las tecnologías de la Información y Comunicaciones en el Tribunal Constitucional", pretenden normar el uso de las tecnologías de Información y Comunicaciones (TIC) en el Tribunal Constitucional;

Que, asimismo, ha preparado la "Política de utilización del Sistema de Video Vigilancia", la misma que tiene el objetivo de garantizar la protección y seguridad de su personal, visitantes, edificaciones, bienes materiales e información;

Que, los referidos proyectos, ha merecido la conformidad de ésta Dirección General de Administración;

En uso de las facultades conferidas por el Reglamento de Organización y Funciones.

SE RESUELVE

ARTÍCULO PRIMERO.- Aprobar las siguientes Directivas:

- Directiva N.° 001-2016-DIGA/TC "Normas para el Uso del Correo Electrónico en el Tribunal Constitucional"; y,
- Directiva N.° 002-2016-DIGA/TC "Normas que regulan el uso de las tecnologías de la Información y Comunicaciones en el Tribunal Constitucional".

El texto de las directivas, forman parte integrante de la presente resolución como anexos 01 y 02.

ARTÍCULO SEGUNDO.- Déjese sin efecto la Directiva N.° 002-2005 "Normas para el Uso del Servicio del Correo Electrónico en el TC", aprobada mediante Resolución Administrativa N° 016-2005-P/TC.

ARTÍCULO TERCERO.- Aprobar la "Política de utilización del Sistema de Video Vigilancia", que como anexo 03 forma parte de la presente resolución.

TRIBUNAL CONSTITUCIONAL

N° 21 -2016-DIGA/TC

Lima, 31 de marzo de 2016

ARTÍCULO CUARTO.- Comunicar la presente resolución a la Secretaría General, a las Oficinas de Gestión y Desarrollo Humano, Tecnologías de la Información, Planeamiento y Desarrollo, y al Órgano de Control Institucional, para su conocimiento y fines de ley.

ARTÍCULO QUINTO.- Encargar a la Jefatura de la Oficina de Tecnologías de la Información, el cumplimiento y difusión de las directivas y la política aprobadas por la presente.

Regístrese y comuníquese.

JOSÉ LUIS ZAVALETA PINEDO
Director General de Administración
TRIBUNAL CONSTITUCIONAL

Tribunal Constitucional

POLÍTICA DE UTILIZACION DEL SISTEMA DE VIDEO VIGILANCIA

Contenido

Política de utilización del sistema de video vigilancia del Tribunal Constitucional

I. OBJETIVO

Garantizar la protección y seguridad de su personal, visitantes, edificaciones, bienes materiales e información.

El sistema de video vigilancia contribuye a evitar, disuadir, gestionar y, cuando es necesario, investigar incidentes relativos a la seguridad y la protección de datos, así como posibles amenazas o intrusiones físicas, incluido el acceso no autorizado a zonas restringidas como el centro de datos y otros.

II. BASE LEGAL

2.1. Ley N° 28301, Ley Orgánica del Tribunal Constitucional.

2.2. Ley N° 27933, Ley del Sistema Nacional de Seguridad Ciudadana.

2.3. Ley N° 29733 – Ley Protección de Datos Personales

2.4. Decreto Legislativo N° 1218 que regula el uso de las cámaras de video vigilancia.

2.5. Resolución Administrativa N° 145-2010-P/TC, que aprueba el Reglamento de Organización y Funciones del Tribunal Constitucional.

III. DISPOSICIONES GENERALES

La presente política describe el sistema de video vigilancia del Tribunal Constitucional y de las garantías que éste ha establecido para proteger los datos personales, la intimidad y otros derechos fundamentales e intereses legítimos de las personas filmadas por las cámaras.

El Tribunal Constitucional opera sus sistemas de video vigilancia de conformidad con las disposiciones expresadas en la Ley N° 27933, Ley del Sistema Nacional de Seguridad Ciudadana.

El contenido de esta política de video vigilancia tiene vigencia en las diferentes sedes del Tribunal Constitucional.

La política de utilización de los sistemas de video vigilancia del TC no se aplica a la grabación o retransmisión de las audiencias públicas contempladas en la normatividad vigente.

IV. DISPOSICIONES ESPECÍFICAS

4.1. Definiciones

a. Cámara o videocámara.- Medio técnico análogo, digital, óptico o electrónico, fijo o móvil, que permita captar o grabar imágenes, videos o audios.

b. Distancia focal.- Es la distancia entre el centro óptico de la lente y el foco (o punto focal). Los objetivos de las cámaras tienen una distancia focal fija o variable, dependiendo del tipo de objetivo. Al variar la distancia focal se consigue un menor o mayor acercamiento, es lo que comúnmente se denomina zoom.

c. DVR o Digital Video Recorder: Centraliza el control de salida análoga de las cámaras que le envían una señal de video que digitaliza.

d. NVR o Network Video Recorder: Centraliza el control de salida digital y la grabación de todas las cámaras conectadas mediante IP. Con éste sistema las imágenes llegan procesadas al grabador. Esta tecnología ofrece una mayor calidad, con menos ruido y mayor resolución.

e. NDVR o Network Digital Video Recorder: Se trata de un videograbador híbrido, ya que combina ambas tecnologías (NVR y DVR). Se incluye en entornos donde se cuenta con instalaciones analógicas y protocolos IP.

f. Video vigilancia.- Sistema de monitoreo y captación de imágenes, videos o audios de lugares, personas u objetos.

4.2. Aspectos técnicos del sistema

4.2.1. De los requisitos mínimos de las cámaras

Los siguientes son los requisitos mínimos que deben cumplir las cámaras de video grabación, que se adquieran a partir de la entrada en vigencia de la presente política:

a. Permitir actualizaciones del software que el fabricante pueda publicar para la mejora de las prestaciones de la cámara.

b. Poseer una interface web que permita a través de un dispositivo (computador, laptop, tableta, teléfono móvil etc.) equipado con un navegador de internet, realizar su configuración, programación y administración con claves de seguridad.

c. Incorporar funcionalidades que permitan detectar manipulaciones u afectaciones al campo visual de la cámara y capacidad de detección de movimiento adaptativo en la escena. Estas funcionalidades deben ejecutarse, en lo posible, en la misma cámara y no sobre servidor.

d. Deben ser de arquitectura abierta, lo que asegura la compatibilidad con otras cámaras IP, codificadores y grabadoras de video digitales de cualquier fabricante.

e. Contar con iluminación infrarroja mínimo en formato H.264.

f. Soportar temperaturas de operación hasta 45°C.

4.2.2. De la instalación de las cámaras

Con la finalidad que los archivos de video capturados por las cámaras de vigilancia sean de buena calidad permitiendo contar con imágenes faciales aptas para análisis de reconocimiento facial, es importante seguir las siguientes consideraciones:

a. Deberán instalarse, en cuanto las facilidades lo permitan, a una distancia no mayor a 20 metros del punto objetivo y a una altura no mayor a 6 metros de altura (ver fig.1), con un ángulo de visión prácticamente plano. Esto a fin de capturar imágenes faciales con no menos de 50 pixeles como mínimo entre los ojos.

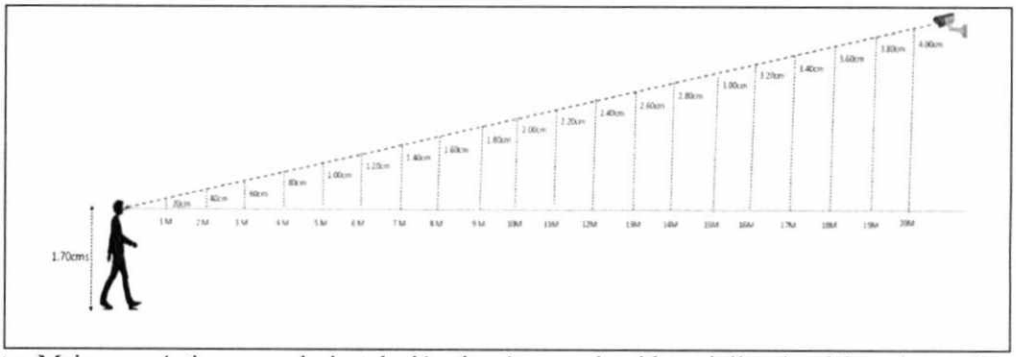
b. Verificar que la posición de la cámara sea estable y no haya vibraciones luego de la instalación (evitar instalar la cámara cerca de ascensores, motores, aires acondicionados, etc.).

c. Verificar cuanto menos una vez al día que la red y energía eléctrica funcionen adecuadamente,

d. Asegurar que la longitud focal sea la requerida considerando el área de captura y el ángulo de la cámara, para ello debe elegir un lente con la distancia focal requerida a fin de obtener imágenes de calidad que puedan ser posteriormente analizadas.

e. La(s) cámara(s) no deben tener obstáculos visibles en el área de captura, para ello de hace necesario verificar que la ubicación regular de personas/objetos no se ubiquen frente a la cámara bloqueando el área de captura.

Fig.1: Cuadro de distancias y altura máxima para instalación de cámaras



Fuente: Mejores prácticas para la instalación de cámaras de video vigilancia elaborado por la PNP.

Previo a la instalación de las cámaras es importante:

a. Identificar el número de cámaras que serán necesarias para cubrir el área de captura; si es un área de captura ancha puede requerir varias cámaras, si es un área de captura estrecha una sola cámara.

b. Verificar la Iluminación (de preferencia solar en el día y buena iluminación artificial durante la noche).

4.3. Zonas bajo video vigilancia

La localización de las cámaras está basada en los riesgos e impacto que generaría la ocurrencia de algún siniestro que atente contra la protección y seguridad del personal, visitantes, edificaciones, bienes materiales y datos, garantizando que las cámaras solo enfoquen lugares pertinentes, tanto dentro como fuera de la institución.

Las cámaras de video vigilancia operan de manera permanente conectadas a un equipo de grabación digital. Las videocámaras están instaladas en los locales del Tribunal Constitucional, y comprenden zonas como entradas principales, patios, corredores y ambientes interiores de las edificaciones.

El TC no vigila zonas en las que las expectativas de intimidad son mayores, como es al interior de las oficinas. Excepcionalmente, y por necesidades de seguridad debidamente justificadas, podrán instalarse cámaras en dichas zonas con la autorización previa de la Dirección General de Administración. En este caso se colocará un letrero que señalice su ubicación en los locales en que se encuentren instaladas.

Excepcionalmente y por necesidad de seguridad debidamente justificada, podrán utilizarse cámaras encubiertas cuando sea indispensable a efectos de prevención, investigación, detección y represión de infracciones de naturaleza penal. Su utilización estará sujeta a la aprobación previa de la Dirección General de Administración en el marco de una investigación de seguridad oficial ordenada por el Secretario General. La utilización de cámaras encubiertas será siempre proporcional a la gravedad de la presunta infracción y se hará de conformidad con la Normatividad vigente referida a la protección de Datos Personales. Cada caso en que se utilicen cámaras encubiertas se documentará en detalle, especificándose los siguientes elementos:

- un fin claramente identificado que no pueda alcanzarse por ningún otro método alternativo de investigación que suponga una menor intrusión en la intimidad;

- una evaluación del impacto para la zona vigilada por las videocámaras encubiertas y los individuos que puedan resultar afectados;

- un periodo de tiempo estrictamente limitado;

- emplazamientos estrictamente limitados;

- destinatarios estrictamente limitados y claramente identificados;
- borrado inmediato de las imágenes en cuanto ya no sean necesarias a los fines de la investigación.

4.4. Del uso de las imágenes

a. El sistema de video vigilancia es un sistema convencional. Graba imágenes digitalizadas de determinados movimientos detectados por las cámaras en la zona vigilada, junto con la hora, la fecha y la localización.

b. Todas las cámaras funcionan veinticuatro horas al día, siete días a la semana.

c. Cuando es preciso, la calidad de la imagen permite la identificación de individuos en la zona de cobertura de las cámaras.

d. El TC no utiliza técnicas de video vigilancia inteligentes o de alta tecnología, pero interconecta los sistemas de protección por videocámara que funcionan en sus distintas sedes.

e. El TC utiliza su sistema de video vigilancia únicamente a efectos de protección y seguridad. El sistema contribuye a garantizar la seguridad tanto de los edificios del TC, su personal y visitantes como de los bienes contenidos en sus instalaciones y la información allí almacenada.

   Este sistema es complementario a otros sistemas de seguridad físicos, como vigilancia mediante personal destinado a esa finalidad, sistemas de control de acceso y/o sistemas de detección de intrusiones.

f. El sistema no será usado para ningún otro fin distinto, como por ejemplo vigilar el trabajo de los funcionarios u otros miembros del personal. El sistema podrá ser usado como medio de investigación o como prueba en investigaciones internas o procedimientos disciplinarios cuyo propósito exclusivo sea investigar un incidente de seguridad física o, en casos excepcionales, en el marco de investigaciones penales. Estas se emprenderán siempre por mandato específico y escrito del Secretario General o de la autoridad facultada para proceder con las actividades que involucren el uso del sistema para el fin específico.

g. Utilización de vídeo *ad hoc*. Cuando exista una necesidad de seguridad debidamente justificada de video vigilancia *ad hoc*, las operaciones se planificarán con antelación, se elaborará una evaluación de impacto y se informará al responsable de la administración de los sistema de video vigilancia.

4.5. Del acceso a las imágenes recogidas

a. El acceso a las grabaciones, las imágenes de vídeo y la arquitectura técnica del sistema de video vigilancia en directo estará limitado a un pequeño número de individuos claramente identificables, basándose en el

principio de la necesidad de conocer. El Director General de Administración, mediante documento, especificará el propósito y el alcance de los derechos de acceso para cada individuo autorizado. En particular, delimitará quién tiene derecho a ver las imágenes en tiempo real; ver las grabaciones; copiar, descargar o borrar cualquier grabación.

b. Todo el personal con derechos de acceso, recibirá una formación básica sobre protección de datos y sistemas de video vigilancia. La formación se impartirá a cada nuevo miembro del personal y se realizarán talleres periódicos sobre cuestiones relacionadas con el cumplimiento de las normas de protección de datos y uso de los sistema de video vigilancia al menos una vez cada dos años para todo el personal que disponga de derechos de acceso.

c. Todas las transmisiones y comunicaciones de datos al exterior proporcionadas por la Oficina de Tecnologías de la Información, responsable de la administración de las imágenes y grabaciones de las cámaras de video vigilancia, estarán documentadas y serán sometidas a una evaluación rigurosa sobre la necesidad de dicha transmisión y de la compatibilidad de la finalidad de la transmisión con el propósito de seguridad inicial del tratamiento. El registro de conservación y transmisión de datos podrá ser consultado por los servicios de auditoría interna del TC, o los funcionarios que el Secretario General autorice.

No se dará acceso a los servicios de gestión o de recursos humanos, excepto en el marco de procedimientos disciplinarios entablados directamente a raíz de un incidente de seguridad física.

Podrá permitirse el acceso a la Policía Nacional o Serenazgo, las autoridades judiciales reconocidas, los órganos del Estado de lucha contra el fraude (como la Fiscalía de la Nación o la Contraloría General de la República), u organizaciones internacionales interesadas si es necesario investigar o reprimir infracciones penales.

Cada fallo de seguridad y/o de funcionamiento relacionado con las cámaras quedará consignado en el registro de acontecimientos de las cámaras de video vigilancia y se informará de ello lo antes posible al jefe de la Oficina responsable de la administración de las imágenes y grabaciones de las cámaras de video vigilancia.

4.6. De la protección y salvaguarda de los datos personales

A fin de proteger la seguridad del sistema de video vigilancia, incluidos los datos personales, se han establecido las medidas técnicas y organizativas siguientes:

- Los servidores donde se almacenan las imágenes grabadas estarán emplazados en locales seguros y protegidos por medidas de seguridad físicas; el perímetro lógico de la infraestructura de TI estará protegido por cortafuegos de red; y se reforzará la seguridad de los sistemas informáticos principales donde se almacenen estos datos.

- Las medidas administrativas incluyen la obligación de que todo el personal de planta del TC y/o subcontratado con acceso al sistema (incluido el personal de mantenimiento del equipo y los sistemas) se someta a un control de seguridad individual.

- Todo el personal (externo e interno) firmará acuerdos de no divulgación y de confidencialidad.

- A los usuarios se les garantizarán derechos de acceso exclusivamente a aquellos recursos que sean estrictamente necesarios para desempeñar sus tareas.

- Solo el administrador del sistema, designado por la jefatura de la Oficina de Tecnologías de la Información con el refrendo de la Dirección General de Administración, estará facultado para conceder, modificar o anular los derechos de acceso de cualquier persona. Toda concesión, modificación o anulación de los derechos de acceso se realizará con arreglo a criterios estrictos y con la documentación que sustente esta necesidad.

- El TC llevará una lista actualizada permanentemente de todas las personas que tengan acceso al sistema y en ella se describirán en detalle los derechos de acceso de cada una.

- La Jefatura de la Oficina de Tecnologías de la Información será consultada antes de adquirir o instalar cualquier nuevo sistema de video vigilancia.

a. **Protección de la intimidad.** Para reforzar la protección de la intimidad, el TC ha previsto:

- La difuminación de imágenes (para hacer la imagen total o parcialmente irreconocible, según corresponda),

- La limitación de la duración del almacenamiento de las filmaciones de vídeo, de conformidad con los requisitos de seguridad establecidos en el punto 4.6.

b. **Revisiones periódicas.**

Cada dos años, el TC lleva a cabo una revisión periódica de la evaluación y cumplimiento de la protección de datos recogidos por el sistema de video vigilancia. Durante las revisiones periódicas el TC reevalúa, entre otras cosas,

- Que el sistema siga cumpliendo el objetivo para el que fue creado,

- Existan alternativas adecuadas, y

- Esta política siga ajustándose al Reglamento Interno de Trabajo y la legislación vigente.

4.7. Período de conservación de los datos

Las imágenes se conservarán durante 40 días. Posteriormente, se borrarán de conformidad con el criterio de "primeras imágenes grabadas, primeras borradas". Si se produce un incidente de seguridad, las filmaciones pertinentes podrán ser conservadas durante un período más largo que el normal y cuanto tiempo sea necesario para proseguir con la investigación respectiva. La conservación se documentará rigurosamente y se revisará periódicamente la necesidad de conservar imágenes. El registro de conservación y de transmisión podrá ser consultado por los servicios de auditoría interna del TC y el responsable de la protección de datos.

4.8. De las obligaciones de los responsables

La Oficina de Abastecimiento es la responsable de mantener la operatividad de todas las cámaras instaladas en las sedes del Tribunal Constitucional debiendo cumplir con las siguientes obligaciones:

a. Mantener el normal funcionamiento de los equipos que conforman el sistema de video vigilancia lo que incluye, que estos cuenten con alimentación eléctrica permanente.

b. No manipular, desarmar ni destruir parcial o totalmente los equipos de video vigilancias, ni realizar acciones que impidan la recepción y transmisión de señales desde y/o hacia los mismos.

c. Coordinar la reparación de las cámaras de video vigilancia que presenten falla, avería, desperfecto, desinstalación por causas de mantenimiento o toda aquella circunstancia que impida el funcionamiento normal de los sistemas.

La Oficina de Tecnologías de la Información es la responsable de mantener operativo el sistema de grabación debiendo cumplir con las siguientes obligaciones:

a. Informar inmediatamente y por escrito a la Oficina de Abastecimiento en caso de alguna anomalía en el funcionamiento de las cámaras, ya sea por ausencia de conexión de red, falla eléctrica o falla del equipo, a fin de subsanar o restablecer el servicio, proceder a la reparación del equipo, o adquirir uno nuevo, según fuera el caso.

b. Mantener la operatividad del sistema de grabación asegurando el buen funcionamiento de los equipos NVR/DVR/NDVR instalados en cada una de las sedes del Tribunal Constitucional.

c. Administrar los permisos de acceso a las imágenes captadas por las cámaras de video vigilancia solamente al personal autorizado por la Dirección General de Administración, así como de la cancelación de accesos.

d. Atender solicitudes de video grabación sujetándose a los lineamientos establecidos en la sección 4.5 "Del acceso a las imágenes recogidas".

e. Generar las copias de respaldo por el periodo establecido en la sección 4.7 "Período de conservación de los datos".

4.9. Información al público

a. **Enfoque multinivel** El TC seguirá un enfoque multinivel que comprende los elementos siguientes:

- En cada una de las entradas de las sedes del TC, se colocará un cartel informativo detallado en que se advertirá de la utilización de sistemas de video vigilancia;

- La política de utilización de sistemas de video vigilancia se publicará en la página web del TC para facilitar la consulta de personas que deseen más información sobre éstas prácticas de utilización por parte del TC.

El cartel informativo del TC figura en el **Anexo** adjunto.

b. **Comunicación específica individual.** Sin perjuicio de las normas aplicables a las investigaciones, se deberá remitir una comunicación individual a las personas que hayan sido identificadas por cámara (por ejemplo, por el personal de seguridad en una investigación de seguridad) cuando concurran una o varias de las siguientes circunstancias:

- Su identidad quede consignada en un expediente/un registro,

- La grabación de vídeo se utilice en contra del individuo, se guarde más allá del período de conservación normal o se transfiera fuera de nuestras oficinas, o la identidad del individuo se revele a alguien ajeno a la Institución.

El envío de la comunicación podrá retrasarse si se considera necesario para prevenir, detectar, investigar y reprimir infracciones penales graves.

4.10. Derechos de los interesados

Las personas interesadas tienen el derecho de acceder a los datos personales de naturaleza gráfica que el TC tiene sobre ellos, captados por el sistema de video vigilancia. Cualquier solicitud referente al acceso, rectificación, bloqueo y supresión de los datos personales obtenidos mediante la utilización de cámaras de vídeo deberá remitirse a la Dirección General de Administración.

La Dirección General de Administración (DIGA) enviará al solicitante un acuse de recibo en el plazo de cinco días hábiles a contar desde la fecha de recepción de la solicitud. Cuando sea posible, la persona responsable de la DIGA responderá al fondo de la solicitud en un plazo de 15 días calendario. Si ello no fuera posible, el solicitante será informado de los próximos pasos y de la razón del retraso del plazo mencionado. Incluso en los casos más complejos, la

solicitud deberá responderse o deberá remitirse una respuesta definitiva en la que se argumenten los motivos por qué se rechaza la solicitud en un plazo máximo de tres meses. El responsable de la DIGA hará todo lo posible por responder antes, sobre todo si el solicitante demuestra la urgencia de la solicitud.

Si se solicita específicamente, podrá organizarse un visionado de las imágenes.

En dichos casos, los solicitantes deberán indicar su identidad mediante prueba indubitable (por ejemplo, aportando documentos de identidad cuando asista al visionado), y especificar también la fecha, hora, localización y circunstancias en que fueron filmados por las cámaras. Asimismo deberán presentar una fotografía reciente que permita al personal de seguridad identificarlos a partir de las imágenes revisadas.

En caso de irregularidad o evidente abuso por parte del interesado en el ejercicio de sus derechos, la DIGA podrá consultar al Secretario General y/o al órgano técnico responsable de la administración de los equipos de video vigilancia sobre la solicitud del interesado, quienes decidirán acerca de la admisibilidad de la solicitud y del curso apropiado que debe dársele.

La solicitud para visionar secuencias grabadas podrá rechazarse cuando se aplique a un caso específico, por ejemplo para proteger la investigación de una infracción penal. También podrá ser necesaria una restricción para proteger los derechos y libertades de otras personas.

4.11. Derecho de recurso

Cualquier interesado podrá presentar una reclamación ante el Secretario General si considera que se han violado sus derechos reconocidos en la normatividad vigente como consecuencia del tratamiento de los datos e imágenes recogidas por nuestro sistema de video vigilancia.

Anexo: