"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario del Perú: 200 años de independencia"

OPINIÓN CONSULTIVA Nº 02-2021-JUS/DGTAIPD

ASUNTO : Tratamiento de datos a través de cámaras de videovigilancia en espacios de trabajo compartidos (cowork).

REFERENCIA : Hoja de Trámite Nro. 23434-2020MSC

FECHA : Miraflores, 12 de febrero de 2021

I. ANTECEDENTES

1. Mediante el documento de la referencia, se consulta a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante DGTAIPD), lo siguiente:

   a. Dado que actualmente las empresas optan por operar en oficinas de espacios compartidos (cowork) ¿puede reconocerse al responsable del sistema de vigilancia como el titular del banco de datos personales del establecimiento?

   b. De ser afirmativa la respuesta ¿ello significaría que las empresas que operan en los espacios del establecimiento no tendrían la obligación de contar con bancos de datos de videovigilancia inscritos ante la Autoridad Nacional de Protección de Datos Personales, ya que no calificarían como titulares del banco de datos personales?

   c. Con relación a la eventual transferencia de las grabaciones de videovigilancia por parte de las empresas que operan estos sistemas a las empresas que trabajan en el establecimiento, en caso de producirse faltas laborales o irregularidades en materia de seguridad patrimonial ¿Ello convertiría a las empresas en encargadas y/o responsables del tratamiento de dichos datos personales?

   d. ¿Las empresas que califiquen como encargadas y/o responsables del tratamiento de datos personales relacionados a la videovigilancia deberán cumplir con todas las obligaciones de la Ley y su Reglamento? ¿O es que, en atención al tipo de datos personales específicos materia de tratamiento, se tendrá en consideración obligaciones distintas?

e. ¿Con respecto a la hoja Informativa esta deberá indicar que los datos personales de videovigilancia podrán ser transferidos a todas y cada una de las empresas que operan en el establecimiento?

f. En caso de que las empresas del establecimiento sean titulares de los datos personales de videovigilancia ¿Cada empresa deberá cumplir con inscribir el banco de datos de videovigilancia en el Registro de Datos Personales? ¿Cada empresa deberá colocar su cartel informativo de videovigilancia en el establecimiento de espacio compartido? ¿Los espacios compartidos por diferentes empresas podrían tener un cartel informativo de videovigilancia único y consolidado y mantener una hoja informativa por cada empresa?

II. MARCO NORMATIVO DE ACTUACIÓN

2. La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la "DGTAIPD") es la encargada de ejercer la Autoridad Nacional de Transparencia y Acceso a la Información Pública (ANTAI)[1] y la Autoridad Nacional de Protección de Datos Personales (en adelante, la "ANPD")[2].

3. Entre sus funciones se encuentra absolver las consultas que las entidades o las personas jurídicas o naturales le formulen respecto a la aplicación de las normas de transparencia y acceso a la información pública, así como de la normativa sobre protección de datos personales.

4. En esa medida, esta Dirección General emite la presente Opinión Consultiva en el ámbito de la interpretación en abstracto de las normas y no como mandato específico de conducta para un caso en concreto.

5. En ese sentido, este Despacho absolverá la consulta formulada respecto al responsable de datos personales en espacios de trabajo compartidos.

III. ANÁLISIS

A. Sobre el titular del banco de datos personales o responsable del tratamiento en los espacios de trabajo compartidos (cowork) que cuenten con sistemas de videovigilancia

6. La Ley Nº 29733, Ley de Protección de Datos Personales (LPDP), desarrolla el derecho fundamental reconocido en el artículo 2, numeral 6, de la Constitución Política del Perú, que señala que toda persona tiene derecho a "que los servicios

---

1 Decreto Legislativo N° 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de gestión de intereses (publicado el 07 de enero de 2017; Decreto Supremo N° 013-2017-JUS, que aprueba el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos (publicado el 22 de junio de 2017); y Decreto Supremo N° 019-2017-JUS, que aprueba el Reglamento del Decreto Legislativo N° 1353 (publicado el 15 de setiembre de 2017).

2 Ley N° 29733, Ley de Protección de Datos Personales, artículo 32.

informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".

7. En ese sentido, establece obligaciones para quienes realizan tratamiento de datos personales[3]: titular del banco de datos, encargado de tratamiento, responsable de tratamiento.

8. Al respecto, de acuerdo con el artículo 2, numeral 17, de la LPDP, el titular del banco de datos personales es aquella persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

9. Por otro lado, el encargado de tratamiento, de acuerdo con el artículo 2, numeral 7, de la LPDP, es aquella persona que realiza el tratamiento de datos personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación.

10. Finalmente, el responsable de tratamiento, de acuerdo con el artículo 2, numeral 14, del Reglamento de la LPDP, aprobado mediante Decreto Supremo Nº 003-2013-JUS, es aquel que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales[4]. Es decir, el responsable de los datos personales define los fines y medios del tratamiento.

11. La captación y grabación de datos personales a través de sistemas de videovigilancia constituyen tratamientos de datos personales[5], por lo que para realizarlos el titular del banco de datos debe cumplir las disposiciones de la LPDP y su reglamento, entre ellas, la obligación de informar lo señalado en el artículo 18

[3] El artículo 2, numeral 19, de la LPDP define al tratamiento de datos personales como cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

[4] La LPDP, artículo 2, numeral 1, define al 1**. Banco de datos personales como "**Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso."

[5] La Directiva Nro. 01-2020-JUS/DGTAIP sobre tratamiento de datos personales mediante sistemas de videovigilancia, aprobada por Resolución Directoral Nro. 02-2020-JUS/DGTAIPD, define el tratamiento de datos personales a través de sistemas de videovigilancia, como "cualquier operación o procedimiento técnico automatizado o no, que permita la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de la imagen o voz captados por medio de un sistema de cámaras fijas o móviles ya sea en tiempo real o en visualización de grabaciones de imágenes, vídeos o audios".

de la LPDP[6] y la de inscribir los bancos de datos personales ante el Registro Nacional de Protección, conforme el artículo 78 del Reglamento de la LPDP.[7]

12. En ese marco, es necesario establecer quién es el titular del banco de datos personales y quién es el encargado de tratamiento en los casos de tratamiento de datos a través de videovigilancia en espacios de *coworking*.

13. Al respecto, el contrato de *coworking*[8] es un acuerdo entre las partes signatarias mediante el cual, una de las partes intervinientes (denominada parte arrendadora/ *coworking*), que es propietaria de la oficina, se obliga a poner a disposición de la otra parte interviniente (parte arrendataria/ *coworker*) el uso y disfrute de uno o varios puestos de trabajo y/u oficinas cerradas en otra. Se trata del arrendamiento de un local de negocio que, según lo que se haya pactado, añade determinadas prestaciones adicionales. Por ello, se puede afirmar que es una mezcla entre un contrato de alquiler de local y un contrato de prestación de servicios, ya que además de la puesta a disposición del uso y disfrute de un puesto de trabajo con acceso a Internet, fax, impresora, salas de reunión, entre otros, regula la prestación de servicios adicionales, como, por ejemplo, servicios de recepción, de atención de llamadas, de recepción de correo y, también, podría incluirse, servicios de seguridad del local a través de sistemas de videovigilancia.

14. Es decir, la arrendadora (*coworking*) arrienda un espacio en su oficina a una persona natural que realiza trabajo independiente o autónomo o a una empresa

---

[6] LPDP
Artículo 18. Derecho de información del titular de datos personales El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del o de los encargados del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello.

Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables.

En el caso que el titular del banco de datos establezca vinculación con un encargado de tratamiento de manera posterior al consentimiento, el accionar del encargado queda bajo responsabilidad del Titular del Banco de Datos, debiendo establecer un mecanismo de información personalizado para el titular de los datos personales sobre dicho nuevo encargado de tratamiento.

Si con posterioridad al consentimiento se produce la transferencia de datos personales por fusión, adquisición de cartera, o supuestos similares, el nuevo titular del banco de datos debe establecer un mecanismo de información eficaz para el titular de los datos personales sobre dicho nuevo encargado de tratamiento.

[7] **Reglamento de la LPDP**
Artículo 78.- Obligación de inscripción.
Las personas naturales o jurídicas del sector privado o entidades públicas que creen, modifiquen o cancelen bancos de datos personales están obligadas a tramitar la inscripción de estos actos ante el Registro Nacional de Protección de Datos Personales.

[8] Un desarrollo sobre el contrato de coworking: *Vid.* Luis Ángel TRIGUERO MARTÍNEZ, «La influencia del entorno *crowd* sobre las relaciones de trabajo y sus protagonistas: *crowdworking* y *crowdworkers*», *Labour & Law Issues,* Vol. 2, No. 2, 2016, pp. 82 – 108.

(*coworker*) que puede tener una planilla de trabajadores. Dentro de los servicios que presta la empresa de *coworking* puede incluirse, como encargos, una serie de tratamientos de datos personales, como, por ejemplo, servicios de atención de llamadas telefónicas de sus clientes, donde se recoge y almacena nombres, apellidos, datos de contacto, entre otros datos personales.

15. Lo mismo sucede en el caso de que la empresa de coworking le brinde el servicio de seguridad videovigilada a la empresa *coworker*, ello sin perjuicio de que la empresa de coworking encargada de este tratamiento decida, por ejemplo, que tal servicio se implemente y ejecute por una tercera empresa especializada en brindar estos servicios. Esto, atendiendo a lo establecido en los artículos 37 y 38 del Reglamento de la LPDP, que abren la posibilidad de que el tratamiento de los datos personales se realice por un tercero diferente al encargado del tratamiento a través de la suscripción de un contrato o convenio. Este tercero subcontratado asume las mismas obligaciones que se establezcan para el encargado del tratamiento.

16. Cabe aclarar que, en este supuesto, se requiere de manera previa una autorización por parte del titular del banco de datos personales o responsable del tratamiento, es decir, del coworker. Dicha autorización se entenderá también concedida si estaba prevista en el instrumento jurídico mediante el cual se formalizó la relación entre el responsable del tratamiento o titular del banco de datos y el encargado de este. El tratamiento que haga el subcontratista se realiza en nombre y por cuenta del responsable del tratamiento o titular del banco de datos, pero la carga de probar la autorización corresponde al encargado del tratamiento, es decir a la empresa coworking.

17. El contrato de *coworking*, en lo que al derecho de protección de datos se refiere, regula la relación entre el *coworker* y el *coworking* (cuando este último actúa como encargado de tratamiento), por lo que deberá delimitar el ámbito de actuación. En ese sentido, se recomienda que incluya lo siguiente:

    a. El objeto, la duración, la naturaleza, y la finalidad del tratamiento de datos de carácter personal que se tratarán en virtud del encargo.
    b. El tipo de datos personales (por ejemplo, datos básicos identificativos: nombre, apellido, DNI, imagen o voz, estas últimas en el caso de encargo de tratamiento de datos personales a través de servicios de videovigilancia).
    c. Categorías de titulares de datos personales: trabajadores, clientes, proveedores.
    d. Las obligaciones y derechos del titular del banco de datos o responsable de tratamiento (coworker).
    e. Obligaciones del encargado de tratamiento (es decir, el coworking); entre otras:
        - Tratar los datos de carácter personal siguiendo las instrucciones del responsable de tratamiento o titular del banco de datos personales.
        - Garantizar la confidencialidad de las personas autorizadas a tratar los datos, cumpliendo las medidas de seguridad establecidas por la LPDP y su reglamento, así como en otras normas complementarias.

- De decidir subcontratar el encargo, hacerlo atendiendo a lo dispuesto en la LPDP y su reglamento.
- Suprimir o devolver los datos de carácter personal al responsable de tratamiento o titular del banco de datos personales una vez finalizada la prestación de servicios, o incluso, poner a disposición del responsable de tratamiento o titular del banco de datos personales toda la información necesaria para demostrar que el *Coworking* cumple con la normativa de protección de datos.

B. Empresa de *coworker* como titular del banco de datos de seguridad y de control laboral a través de sus sistemas de videovigilancia

18. La empresa de *coworker* renta un espacio en las instalaciones de la empresa coworking, con los servicios propios de este tipo de contrato, para realizar sus actividades comerciales o laborales, y como tal, decide qué personas se dirigen al espacio que ha arrendado.

19. Dicho lo anterior, es claro que en un contrato de *coworking*, en lo que respecta a la videovigilancia de seguridad y control laboral, será la empresa de *coworker* (arrendataria del espacio) la responsable del tratamiento o titular de los bancos de datos personales y, por lo tanto, responsable del cumplimiento de las obligaciones; así, en su calidad de tal, y en virtud de lo dispuesto en la LPDP, su reglamento, y la Directiva Nro. 01-2020-JUS/DGTAIP sobre tratamiento de datos personales mediante sistemas de videovigilancia, aprobada por Resolución Directoral Nro. 02-2020-JUS/DGTAIPD, tiene la obligación de inscribir el banco de datos de videovigilancia en el Registro Nacional de Banco de Datos (numeral 6.9)[9].

20. Por su parte, la empresa de *coworking* (arrendadora del espacio) es la encargada del tratamiento, ya que brinda el servicio a raíz de una relación jurídica determinada; y, como tal, debe cumplir con las obligaciones propias de esta condición, de acuerdo con lo dispuesto en los numerales 6.17 y siguientes de la Directiva Nro. 01-2020-JUS/DGTAIP sobre tratamiento de datos personales mediante sistemas de videovigilancia, aprobada por Resolución Directoral Nro. 02-2020-JUS/DGTAIPD[10].

---

[9] **Registro de banco de datos de videovigilancia**
6.9 La persona natural, jurídica o entidad pública que utilice un sistema de videovigilancia o cualquier dispositivo que permita el tratamiento de datos para dicho fin, debe solicitar la inscripción del banco de datos personales respectivo a la Dirección de Protección de Datos Personales, unidad orgánica de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, encargada de la administración del Registro Nacional de Protección de Datos Personales.
6.10 Los sistemas que no almacenan imágenes, sino que consisten exclusivamente en la reproducción y emisión de imágenes en tiempo real, no son considerados bancos de datos. Sin embargo, esto no los exime del cumplimiento de las demás obligaciones contenidas en la LPDP, su reglamento y la presente directiva, en lo que resulte aplicable.

[10] **Formalidades que debe seguir el encargado del tratamiento**
6.17 Cuando una persona natural, jurídica o entidad pública ha instalado o pretende instalar un sistema de cámaras de videovigilancia, pero encarga a otra la gestión del sistema con utilización de los equipos o

21. Respecto a la obligación de informar sobre las características del tratamiento realizado mediante sistemas de videovigilancia, conforme el artículo 18 de la LPDP, dadas las particularidades del contrato de coworking, la empresa de coworking (arrendadora) será la encargada de tratamiento de la videovigilancia de los distintos *coworkers* o arrendatarios.

22. En ese sentido, es posible que en la puerta de ingreso al edificio de propiedad de la empresa coworking, donde se encuentran las oficinas o espacios arrendados por las empresas *coworkers*, se coloque un solo cartel informativo, y no un cartel por cada *coworker* o arrendatario. Al respecto, cabe resaltar que dicho cartel debe cumplir con lo dispuesto en el numeral 6.11 de la Directiva antes mencionada[11] y con lo contenido en el numeral 6.12 de esta misma norma[12] referida a las características del informativo adicional del sistema de videovigilancia.

---

acceso a las imágenes o voces, debe de suscribirse un contrato, convenio o documento similar en el que se establezca el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos y categorías de interesados, las obligaciones y derechos que correspondan, así como el destino de los datos al finalizar la prestación.
6.18 El contrato, convenio o documento similar atiende a las circunstancias concretas de la prestación del servicio. El encargado está obligado, en mérito de él, a cumplir con las condiciones técnicas y organizativas necesarias para respetar las obligaciones establecidas en la LPDP; a observar los requisitos legales que lo habilitan para prestar el servicio; a seguir las instrucciones del responsable del tratamiento o del titular del banco de datos; a realizar las acciones necesarias para asistir al responsable o titular del banco de datos en el cumplimiento de su deber de responder frente el ejercicio de los derechos señalados en la LPDP; y, en general, de colaborar en el cumplimiento de las obligaciones del titular del banco de datos.
6.19 El encargado del tratamiento debe garantizar al responsable que el acceso a los datos sólo se realizará por personas debidamente autorizadas debiendo adoptar las medidas de seguridad necesarias para asegurar el adecuado uso del sistema y tratamiento de los datos personales.
6.20 El encargado del tratamiento del sistema de videovigilancia debe notificar, sin dilación, al responsable del tratamiento acerca de la existencia de una violación o brecha de seguridad.
6.21 De acuerdo con lo establecido en el artículo 37 del RLPDP, es posible la subcontratación con terceros, debiendo asumir la persona natural o jurídica subcontratada las mismas obligaciones que se establezcan para el titular del banco de datos, responsable o encargado del tratamiento, según corresponda, de acuerdo con lo establecido en el artículo 38 del RLPDP.

[11] **Características del cartel informativo**
6.11 Cada acceso a la zona videovigilada debe tener un cartel o anuncio visible con fondo amarillo o cualquier otro que contraste con el color de la pared y que lo haga suficientemente visible. Su contenido mínimo debe indicar (Anexo 1):
6.11.1 La identidad y domicilio del titular del banco de datos personales. 6.11.2 Ante quién y cómo se pueden ejercitar los derechos establecidos en la LPDP.
6.11.3 Lugar dónde puede obtener la información contenida en el artículo 18 de la LPDP.
6.11.4 En lo que se refiere a las dimensiones, los elementos gráficos podrán tener, como mínimo, las siguientes: 297 x 210 mm. Cuando el espacio en que se vaya a ubicar el cartel informativo no lo permita, este debe adecuarse al espacio disponible, de tal forma que cumpla su finalidad informativa.

[12] **Características del informativo adicional del sistema de videovigilancia**
6.12 El informativo adicional del sistema de videovigilancia (Anexo 2) debe estar disponible, ya sea a través de medios informáticos, digitalizados o impresos, y debe contener la información requerida para garantizar el derecho reconocido en el artículo 18 de la LPDP:
6.12.1 La identidad y domicilio del titular del banco de datos personales y del encargado del tratamiento, de ser el caso.
6.12.2 La finalidad.
6.12.3 Las transferencias y destinatarios de los datos personales.
6.12.4 El plazo durante el cual se conservarán los datos personales.

23. Cabe aclarar que el control de seguridad en las instalaciones es distinto al control laboral de las actividades realizadas por los trabajadores de las empresas de *coworker*. Al respecto, el control de seguridad se refiere al mantenimiento del orden y la custodia de los bienes e instalaciones de la empresa de *coworking*, de los bienes de las empresas *coworkers* y de las personas que ingresen a las oficinas como, clientes, proveedores, visitantes de las instalaciones, etc. Mientras que la finalidad del control laboral supone la supervisión de las obligaciones laborales de los trabajadores subordinados a la empresa de *coworke*r por parte de esta.

24. Por lo tanto, atendiendo al contexto de la actividad de *coworking* que supone compartir espacios de trabajo entre varias personas naturales o jurídicas, en el caso de que una o varias de las empresas de *coworker* decidan utilizar los sistemas de videovigilancia no sólo para fines de seguridad, sino también para fines laborales, estas deberán informar expresa y específicamente a sus trabajadores, titulares de los datos personales captados a través de sistemas de videovigilancia, que estos serán utilizados también para fines de supervisión y control laboral.

25. Cabe advertir que el control laboral a través de sistemas de videovigilancia sólo será legítimo cuando se realice atendiendo al principio de proporcionalidad, de acuerdo con lo dispuesto en el artículo 7 de la LPDP y el numeral 7.13 y siguientes de la Directiva Nro. 01-2020-JUS/DGTAIP sobre tratamiento de datos personales mediante sistemas de videovigilancia, aprobada por Resolución Directoral Nro. 02-2020-JUS/DGTAIPD[13].

IV. CONCLUSIONES

1. En el caso de contratos de *coworking* es posible que entre sus prestaciones se encuentre el servicio de seguridad o de control laboral a través de sistemas de videovigilancia, en donde la empresa coworker (arrendataria del espacio) es la titular del banco de datos personales o responsable del tratamiento de los datos personales de sus trabajadores y la empresa de coworking (arrendadora del espacio) la encargada de su tratamiento.

6.12.5 El ejercicio de los derechos de información, acceso, cancelación y oposición de los derechos de información, acceso, cancelación y oposición de los datos.

[13] **Principio de proporcionalidad**
7.13 El control laboral a través de sistemas de videovigilancia sólo se realiza cuando sea pertinente, adecuado y no excesivo para el cumplimiento de tal fin.
7.14 Asimismo, la instalación de las cámaras o, en todo caso, su ámbito de captación debe restringirse a los espacios indispensables para satisfacer las finalidades de control laboral.
7.15 En ningún caso se admite la instalación de sistemas de grabación o captación de sonido ni de videovigilancia en los lugares destinados al descanso o esparcimiento de los trabajadores, como vestuarios, servicios higiénicos, comedores o análogos.
7.16 La grabación videovigilada con sonido en el lugar de trabajo sólo se admitirá cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad y finalidad.

2. Ambas empresas deberán cumplir con las obligaciones propias de su condición de titular del banco de datos personales o encargadas del tratamiento de los servicios de seguridad o control laboral, a través de sistemas de videovigilancia establecidas en la LPDP, su reglamento y la Directiva Nro. 01-2020-JUS/DGTAIP sobre tratamiento de datos personales mediante sistemas de videovigilancia, aprobada por Resolución Directoral Nro. 02-2020-JUS/DGTAIPD.

3. En el caso de los contratos de *coworking* adquiere especial atención el deber de informar sobre los posibles controles laborales a través de sistemas de videovigilancia, dado que al compartir un mismo espacio trabajadores de empresas de *coworker* distintas, es posible que no todas tengan previsto, en el encargo de videovigilancia a la empresa de *coworking*, la supervisión de sus trabajadores, por lo que se deberá informar expresa y específicamente a los trabajadores de las empresas que han previsto este tipo de control de la posible supervisión de sus actividades laborales por este medio. Cabe advertir que los controles laborales videovigilados sólo serán legítimos cuando se realicen atendiendo al principio de proporcionalidad.

Aprobado por:	**Aprobado por:**
_____ **Eduardo Luna Cervantes** Director General de la Dirección de Transparencia, Acceso a la Información Pública y Protección de Datos Personales	_____ **María Alejandra González Luna** Directora (e) de la Dirección de Transparencia y Acceso a la Información Pública