

Guadalajara, Jalisco. Resolución del Comité de Transparencia de la Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, correspondiente al 13 de julio de dos mil veintitrés.

ANTECEDENTES:

I. Solicitud de información. El 05 de julio de dos mil veintitrés, se recibió a través del correo electrónico ut@itei.org.mx, la solicitud de información tramitada bajo el número de expediente **UT-202/2023**, requiriendo:

«A quien corresponda.

Solicito por favor me sea enviada, a esta cuenta de correo electrónico, una copia de video en resolución 480p de las cámaras de vigilancia de las instalaciones del ITEI, que se encuentran en Av. Vallarta 1312, esq. Emerson en la colonia Americana, que tengan ángulo de grabación del área de recepción del instituto el día 4 de julio del presente año con horario de las 17:00 a las 19:00 horas. (es decir esas dos horas). Muchas gracias.»

II. Requerimiento de información. Por correo electrónico de 05 de julio del dos mil veintitrés, la Coordinadora de la Unidad de Transparencia del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, solicitó a la Coordinación General de Planeación y Proyectos Estratégicos que se pronunciara sobre la existencia de la información solicitada y, en su caso, su clasificación.

III. Presentación de informe. Por medio del Memorándum CGPPE 086/2023, de fecha 07 de julio del dos mil veintitrés, la Coordinación General de Planeación y Proyectos Estratégicos señaló lo siguiente:

«(...)

Referente a las videograbaciones de seguridad de este Instituto, solicito se someta a análisis del Comité de Transparencia de este Instituto, la clasificación de la información como confidencial y reservada, toda vez que contienen datos personales o identificables de personas físicas ajenas a la Institución, además de vulnerar la seguridad estructural del Instituto. Por otra parte, la Coordinación de Informática y Sistemas no cuenta con las herramientas necesarias que den certeza y seguridad de no revertir la difuminación de rostros o imágenes,

Así mismo, la finalidad el aviso de privacidad para el sistema de video vigilancia del Instituto, informa que solo es para fines de seguridad.

Av. Vallarta 1312, Col. Americana C.P.44160, Guadalajara, Jalisco, México • Tel. (33) 3630 5745

Se adjunta al presente, (03 tres) discos compactos con videograbaciones de la cámara de recepción, cámara de entrada a recepción y cámara secuencia 05, así como un documento de los riesgos sobre la entrega de la información recolectada por las cámaras de seguridad del Instituto (prueba de daño)»

CONSIDERANDO:

I. Competencia. El Comité de Transparencia de la Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco es competente para conocer y resolver la presente clasificación de información, en términos de los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos, 44, fracciones I, II y III, de la Ley General de Transparencia y; las fracciones I, II y III del artículo 30 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

II. Análisis de la solicitud. El solicitante pide una copia de video en resolución 480p de las cámaras de vigilancia de las instalaciones del ITEI. Como se advierte en los antecedentes, la Coordinación General de Planeación y Proyectos Estratégicos señaló que contienen datos personales o identificables de personas físicas ajenas a la Institución, además de vulnerar la seguridad estructural del Instituto. Para efecto de analizar el pronunciamiento de la instancia vinculada, se tiene presente que este Comité al resolver las clasificaciones de información CT-ITEI/003/2023, sostuvo que el derecho de acceso a la información encuentra cimiento en el artículo 6°, apartado A, de la Constitución Política de los Estados Unidos Mexicanos, por el cual todo acto de autoridad (todo acto de gobierno) es de interés general y, por ende, es susceptible de ser conocido por todas las personas.

Sin embargo, lo señalado en el párrafo anterior, tiene como excepción aquella que sea temporalmente reservada o aquellos datos personales considerados como información confidencial, en los términos establecidos por el legislador federal o local.

En desarrollo de ese extremo de excepcionalidad, el artículo 113 de la Ley General de Transparencia, 17 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, así como el Décimo Séptimo al Trigésimo séptimo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, establecen un catálogo genérico de supuestos bajo los cuales debe reservarse la información.

Junto a la identificación de esos supuestos y con el ánimo de proyectar a cabalidad el principio constitucional que les da sentido, los artículos 103, 104, 108 y 114 la Ley General de Transparencia, 18 y 26 fracción VI de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; así como el Sexto y el Trigésimo tercero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; exigen que en la definición sobre su configuración, además de la realización de un examen casuístico y de justificación fundado y motivado, se desarrolle la aplicación de una prueba de daño; entendido esto como el estándar que implica ponderar la divulgación de la información frente a la actualización de un daño.

Conforme a lo expuesto, toca verificar si es correcta o no la clasificación de temporalmente reservada que sobre la información solicitada hizo la Coordinación General de Planeación y Proyectos Estratégicos, al estimar actualizada la hipótesis contenida en el artículo 113, fracción I, de la Ley General de Transparencia, y 17 fracción I inciso a) y c) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; así como el Décimo octavo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; en virtud de que se encuentra pendiente de resolver el asunto, los cuales establecen:

Artículo 113. Como información reservada podrá clasificarse aquella cuya publicación:

I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;
(...)

Artículo 17. Información reservada- Catálogo

1. Es información reservada:

I. Aquella información pública, cuya difusión:

a) Comprometa la seguridad del Estado o del municipio, la seguridad pública estatal o municipal, o la seguridad e integridad de quienes laboran o hubieren laborado en estas áreas, con excepción de las remuneraciones de dichos servidores públicos;

(...)

c) Ponga en riesgo la vida, seguridad o salud de cualquier persona;

(...)

Décimo octavo. De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada, aquella que comprometa la seguridad pública, al poner en peligro las funciones a cargo de la Federación, la Ciudad de México, los Estados y los

Municipios, tendientes a preservar y resguardar la vida, la salud, la integridad y el ejercicio de los derechos de las personas, así como para el mantenimiento del orden público.

(...)

Asimismo, podrá considerarse como reservada aquella que revele datos que pudieran ser aprovechados para conocer la capacidad de reacción de las instituciones encargadas de la seguridad pública, sus planes, estrategias, tecnología, información, sistemas de comunicaciones.

Sobre el alcance del contenido de ese precepto, a partir de la clasificación de información CT-ITEI/003/2023 este Comité ha sostenido que, en principio, su objeto trasciende al derecho de acceso a la información, toda vez que la información recolectada por las cámaras de seguridad son datos personales y la divulgación de lo captado por las cámaras de seguridad iría en contra de las finalidades establecidas para el sistema de tratamiento de las cámaras de seguridad, de conformidad con lo establecido en el artículo 11 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, toda vez que el tratamiento de las imágenes tiene como finalidad contar con las medidas de seguridad necesarias tanto para el personal del instituto como para los documentos y datos personales recabados por este Órgano Garante y la difusión de dichas imágenes es un tratamiento para una finalidad distinta a la informada por mediante el aviso de privacidad.

De igual forma las grabaciones de las cámaras de seguridad, contienen imágenes que muestra puntos ciegos y vulnerables para efectos de la seguridad estructural y de los datos personales en posesión de este Instituto.

Así, se dijo, cualquier divulgación de las grabaciones de las cámaras de seguridad, es susceptible de reserva, lo cual tendría que ser analizado caso por caso y bajo la aplicación de la prueba de daño.

Como quedó descrito en líneas precedentes, a través del diseño del dispositivo de mérito, se optó por restringir el acceso a la información captada por las cámaras de seguridad de este Instituto, por tanto, dicha información se entenderá válidamente reservada (siempre bajo la valoración del condicionamiento relativo a la demostración de una afectación la seguridad del Instituto, de los datos personales bajo su resguardo y los titulares de los mismos, así como a la específica aplicación de la prueba del daño).

III. Análisis específico de la prueba de daño. En adición hasta lo aquí dicho, se estima que la clasificación antes advertida también se confirma desde la especificidad que en aplicación de la prueba de daño mandatan los artículos 103 y 104, de la Ley General de Transparencia, 17 y 18 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, así como el Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; cuya delimitación, como se verá enseguida, necesariamente debe responder a la propia dimensión del supuesto de reserva con el que se relacione su valoración.

PRUEBA DE DAÑO			
DOCUMENTO RESERVADO			
Grabaciones de las cámaras de seguridad instalada en el área de recepción del Instituto			
Fecha de la clasificación	Día 07	Mes 07	Año 2023
Sujeto Obligado	Instituto de Transparencia Información Pública y Protección de Datos Personales del Estado de Jalisco		
Unidad Administrativa interna que generó la información	Coordinación General de Planeación y Proyectos Estratégicos		
Plazo de Reserva	5 años		
Información confidencial	Indefinidamente		
Fecha de inicio del plazo de reserva	07	07	2023
Datos de Unidad Interna Responsable			
Área	Responsable		Cargo
Coordinación General de Planeación y Proyectos Estratégicos	Hilda Nayeli López Preciado		Coordinadora General de Planeación y Proyectos Estratégicos
Domicilio	Teléfono		Correo Electrónico
Avenida Ignacio L. Vallarta 1312, Colonia Americana, Guadalajara, Jalisco	33 36305745		nayeli.lopez@itei.org.mx
En su caso las partes del documento que se consideran reservadas			
202/2023 Grabación de la cámara de seguridad instalada en el área de recepción del Instituto del martes 04 de julio del año 2023			
Prueba de Daño			
Artículo 18 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios			
I. La información solicitada se encuentra prevista en alguna de las hipótesis de reserva que establece la ley;			
II. La divulgación de dicha información atente efectivamente el interés público protegido por la ley, representando un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad estatal;			
III. El daño o el riesgo de perjuicio que se produciría con la revelación de la información supera el interés público general de conocer la información de referencia; y			

IV. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.
La información solicitada se encuentra prevista en alguna de las hipótesis de reserva que establece la ley
Artículo 17, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios señala la posibilidad de comprometer la seguridad e integridad de quienes laboran o hubieren laborado en estas áreas, toda vez, que se puede vulnerar la seguridad estructural del Instituto, mostrando los puntos ciegos de las cámaras de seguridad.
La divulgación de dicha información atente efectivamente el interés público protegido por la ley, representando un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad estatal
La información recolectada por las cámaras de seguridad son datos personales por lo que en dicho sistema de tratamiento se deben observar los principios y deberes estipulados en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.
Implicaciones de la entrega de la información son respecto al principio de finalidad:
a) La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios establece en su artículo 11, que todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, explícitas, lícitas y legítimas. b) El tratamiento de las imágenes tiene como finalidad contar con las medidas de seguridad necesarias tanto para el personal del instituto como para los documentos y datos personales recabados por este Órgano Garante. c) Por lo anterior transferir las imágenes es un tratamiento para una finalidad distinta a la informada por mediante el aviso de privacidad.
La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios establece en su artículo 11, numeral dos señala que. El responsable podrá tratar datos personales para finalidades distintas a aquellas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular.
En este caso transferir las imágenes es un tratamiento para una finalidad distinta a la informada por mediante el aviso de privacidad para la que el Instituto tiene una atribución conferida por la Ley.
Por lo tanto, se requiere medie el consentimiento del titular para entregar los datos personales consistentes en las imágenes.
El daño o el riesgo de perjuicio que se produciría con la revelación de la información supera el interés público general de conocer la información de referencia
Posibilidad de la entrega de una versión pública (desenfocar rostros)
Para poder entregar un documento que contenga datos personales, es posible realizar una versión pública que para el caso consiste en desenfocar de cuerpo completo a las personas por lo siguiente:
a) La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios establece en su artículo 3, fracción IX, señala que es un dato personal cualquier información concerniente a una persona física identificada o identificable y se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. b) En las grabaciones además del rostro se recaba información como, complexión física, manera de caminar, forma de vestir, lugares por los que se circula, género, horarios y asistencias que permiten la determinación de la identidad de manera indirecta. c) Por lo tanto, la información debe difuminarse toda la imagen y no sólo los rostros.
Ahora bien, de acuerdo a la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus

Municipios una versión pública es documento o expediente en el que se da acceso a información eliminando u omitiendo las partes o secciones clasificadas, de conformidad con la Ley General.

Así mismo la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios establece en su artículo 3, fracción XXXIV señala que la supresión es la baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Por lo tanto, en la elaboración de la versión pública se están suprimiendo datos personales y debe observarse lo señalado en la normativa relativa a la protección de datos personales.

Ahora bien el artículo 23, de los Lineamientos para el Debido Tratamiento que Deberán Observar los Sujetos Obligados del Estado de Jalisco, señala que la supresión de los datos personales el responsable deberá establecer políticas, métodos y técnicas orientadas a la supresión definitiva de éstos, de tal manera que la probabilidad de recuperarlos sea mínima.

Para lograr un difuminado, pixelado o borrado de los rostros que garantice que mediante aplicaciones sencillas de instalar en cualquier dispositivo no se recupere la información requiere la obtención de software especializados con los que al día de hoy no cuenta el Instituto.

Por lo tanto, al día de hoy, no se garantiza que la probabilidad de recuperar los datos personales sea mínima.

Implicaciones de la entrega de la Información a seguridad de los datos personales.

Para determinar las medidas de seguridad necesarias para garantizar la confidencialidad e integridad de los datos personales, durante el año 2018 se realizó un análisis de riesgo bajo la metodología BAA del INAI.

De acuerdo a la metodología antes señalada "un acercamiento para evaluar las medidas de seguridad necesarias para proteger los activos de información es a través del análisis de riesgo, de modo que se pueda determinar cuál riesgo es más importante mitigar o cuáles activos se encuentran más expuestos".

En dicha metodología de análisis de riesgo se toman tres variables:

- 1) Beneficio para el atacante. Aquellos datos personales que representen mayor beneficio tienen más probabilidad de ser atacados (por ejemplo, beneficio económico por venderlos o usarlos).
- 2) Accesibilidad para el atacante. Aquellos datos personales que sean de fácil acceso tienen mayor probabilidad de ser atacados (por ejemplo, miles de personas pueden acceder a la vez a una base de datos a través de un sitio web, pero sólo unas cuantas lo podrían hacer a un archivero).
- 3) Anonimidad del atacante. Aquellos datos personales cuyo acceso represente mayor anonimidad tienen más probabilidad de ser atacados (por ejemplo, internet es un medio más anónimo que presentarse físicamente a las instalaciones de una empresa).

Lo anterior implica que mediante la obtención de las imágenes solicitadas, más el acceso a la versión pública del documento de seguridad, y el acceso a información estadística que el instituto está obligado a publicar o que se pueda pedir por acceso a la información, se pueda realizar un análisis de riesgo y se pueda determinar cuáles son los datos personales más expuestos.

Lo anterior se afirma por las siguientes consideraciones:

Beneficio del atacante

De acuerdo a la metodología de análisis de riesgo implementada por este instituto, el beneficio del atacante deriva en el nivel de riesgo por tipo de dato, determinado por el riesgo inherente del dato y el volumen de titulares de las que se tratan datos.

El riesgo inherente se determina por el tipo de datos que se trata; los datos personales relativos a la información bancaria tienen mayor riesgo inherente que los nombres o correos electrónicos. En este sentido los tipos de datos que se tratan son públicos porque deben ser informados mediante el aviso de privacidad y se encuentran en la parte pública del documento de seguridad.

El segundo elemento para determinar el beneficio del atacante, el volumen de titulares, o es información fundamental o de libre acceso. Ejemplo: la cantidad de personal adscrito al instituto es pública, así como lo datos que se obtienen de ellos por lo que determinar el beneficio del atacante a sistema de tratamiento de recursos humanos es sencillo.

Accesibilidad del atacante

Accesibilidad, es el factor que determina el nivel de riesgo por tipo de acceso, es decir, el número de accesos potenciales a los datos.

Se realiza determinando la cantidad de accesos potenciales a los datos personales que se pretende proteger, es decir, definiendo cuántas personas tienen la posibilidad de acceder a la información en un intervalo de tiempo, por ejemplo, durante 24 horas. Para este parámetro, entre mayor sea la accesibilidad, mayor riesgo existe para la información. Mediante las imágenes que muestran archiveros y circulación de personal por el Instituto, así la información sobre el soporte en el que se encuentran los datos personales estipulado en la parte pública del documento de seguridad se puede determinar la cantidad de accesos potenciales, así como los momentos en que menos seguridad contienen.

Anonimidad del Atacante

Después de obtener el factor Accesibilidad, se debe identificar qué tan anónimos son los accesos a la información; es decir, el nivel de riesgo por tipo de entorno. Este factor representa el nivel de percepción que se tiene de que un atacante potencial provoque consecuencias negativas para la organización, en caso de acceder o hacer uso no autorizado de los datos personales que se tratan.

En este caso el nivel de anonimidad es el mínimo, empero lo anterior mediante el conjunto de los tres elementos se podría identificar la mayoría de las vulnerabilidades del Instituto.

Por lo anterior se realiza las siguientes dos subsunciones

1. La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, establece en su artículo 30, que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.
2. El análisis de riesgo permite determinar cuál riesgo más importante mitigar o cuáles activos se encuentran más expuestos.

Por lo tanto, proveer la información necesaria para que un tercero ajeno a la Institución realice un análisis de riesgo de la seguridad de los datos personales que posee el ITEI y conozca los activos más expuestos, no permite protegerlos contra

daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Con relación a la videograbación analizada, contiene imágenes que muestra puntos ciegos y vulnerables para efectos de la seguridad estructural, de los ingresos las diversas áreas del Instituto, en ese sentido, su publicación y/o difusión implicaría dar a conocer aspectos sensibles de la Infraestructura de área de ingresos, lo que podría en peligro la seguridad de la institución y personal que en algún momento dado estén en ella.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

La reserva de la información contenida en los videos de seguridad del expediente es total.

En ese sentido, se confirma la reserva temporal por el plazo señalado en la prueba de daño presentada por la Coordinación General de Planeación y Proyectos Estratégicos; es decir, por un periodo de 05 cinco años.

Por lo expuesto y fundado; se,

RESUELVE:

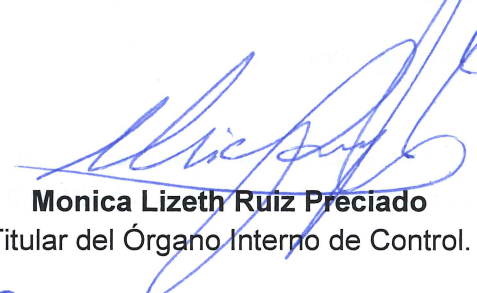
ÚNICO. Se confirma la clasificación de reserva temporal de la información solicitada, acorde con lo señalado en esta resolución.

Notifíquese al solicitante, a la instancia vinculada, así como a la Unidad de Transparencia del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco y, en su oportunidad, archívese como asunto concluido.

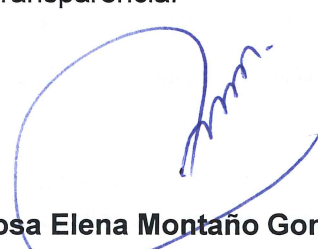
Así, por unanimidad de votos, lo resolvió el Comité de Transparencia del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco y firman el Doctor Salvador Romero Espinosa, Comisionado Presidente y Presidente del Comité de Transparencia; la Licenciada Monica Lizeth Ruiz Preciado, titular del Órgano Interno de Control y, la Maestra Rosa Elena Montaña González, Directora Jurídica y Unidad de Transparencia y Secretaria del Comité de Transparencia; integrantes del Comité,



Salvador Romero Espinosa
Presidente del Comité de Transparencia.



Monica Lizeth Ruiz Preciado
Titular del Órgano Interno de Control.



Rosa Elena Montaña González
Secretaría del Comité de Transparencia

1
REMG/RMQ

¹ La presente hoja de firmas forma parte integral de la Resolución de la Clasificación de Información CT-ITEI/003/2023 aprobada en la Séptima Sesión Ordinaria del Comité de Transparencia del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, celebrada el día 13 de julio del año 2023 dos mil veintitrés. -----