

## ACTA DE LA TERCERA SESIÓN ORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL DISTRITO FEDERAL

Ciudad de México, a veintiocho de junio de dos mil dieciséis, siendo las diecisiete horas con diez minutos, se reunió en la Sala de Plenos del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, el Comité de Transparencia para celebrar la Tercera Sesión Ordinaria, encontrándose presentes los siguientes:

1. Rodrigo Montoya Castillo, Presidente del Comité.
2. Ana Lía de Fátima García García Secretaria Ejecutiva.
3. Carla Patricia Rivas García, Responsable de la Unidad de Transparencia.
4. Jorge Oropeza Rodríguez, Subdirector de Servicios Legales y Representante de la Dirección Jurídica y Desarrollo Normativo.
5. César Iván Rodríguez Sánchez, Contralor.
6. Armando Manuel González Campuzano, Director de Administración y Finanzas.
7. Ana María Cervantes Jasso, Directora de Datos Personales.

**I. Lista de asistencia y verificación del quórum.** Una vez que quedó comprobada la asistencia de los integrantes del Comité de Transparencia, su Presidente declaró la existencia de quórum legal para sesionar.

**II. Lectura y, en su caso, aprobación del orden del día.** Acto seguido, el Presidente del Comité de Transparencia sometió a consideración de sus integrantes, el siguiente Orden del Día:

1. Lista de Asistencia y verificación del quórum.
2. Aprobación del orden del día.
3. Presentación, análisis y, en su caso, aprobación de la clasificación recaída a la solicitud de información con folio 3100000102516, con su respectiva respuesta por parte de la Dirección de Administración y Finanzas.

#### 4. Asuntos Generales.

Por Unanimidad: Se aprobó el Orden del Día.

III. Análisis, y en su caso, aprobación de las clasificaciones recaídas a las solicitudes de información con folios 3100000102516, con su respectiva respuesta por parte de la Dirección de Administración y Finanzas.

### ANTECEDENTES

La Unidad de Transparencia, recibió la solicitud de información con folio 3100000102516, misma que fue turnada a la Dirección de Administración y Finanzas. En la solicitud de referencia, se requirió:

*"1.- SOLICITO LA VERSIÓN PÚBLICA DEL DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES QUE CONTEGA LA INFORMACIÓN RELATIVA A LOS TRABAJADORES DEL INSTITUTO, LOS PROGRAMAS DE CAPACITACIÓN DE DICHO PERSONAL, LOS PRESTADORES DE SERVICIO SOCIAL DEL INSTITUTO ASI COMO*

*2.-EL FORMATO A TRAVÉS DEL CUAL RECABAN LA INFORMACIÓN DE DICHO SISTEMA"*

En tal virtud, el Director de Administración y Finanzas, presentó la siguiente argumentación para responder al solicitante:

*"...  
Por lo que respecta al primer punto de la presente solicitud, referente a "SOLICITO LA VERSION PUBLICA DEL DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES QUE CONTENGA INFORMACION RELATIVA A LOS TRABAJADORES DEL INSTITUTO, LOS PROGRAMAS DE CAPACITACION DE DICHO PERSONAL, LOS PRESTADORES DE SERVICIO SOCIAL DEL INSTITUTO" le notifico que pongo a su disposición el Documento de Seguridad del Sistema de Datos Personales de los Recursos Humanos, el cual integra los datos del personal de estructura y honorarios, así como a los prestadores de servicio social con los que cuenta el Instituto, se precisa, que este documento se entrega en versión pública, debido a que contiene información de*

acceso restringido, en su modalidad de confidencial, que debe ser resguardada, como son los siguientes datos:

1. Mapa de ubicación topográfica de los archivos del Sistema de Datos Personales de los Recursos Humanos
2. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales
3. Medidas normas procedimientos y criterios enfocados a garantizar el nivel de seguridad alto
4. Procedimiento para la realización de copias de respaldo y recuperación de los datos para los sistemas de datos personales automatizados
5. Procedimientos de notificación gestión y respuesta ante incidencias
6. Procedimientos para la realización de auditorías, en su caso
7. Número de inventario de los archiveros donde se resguarda
8. Número de local
9. Número de inventario de los equipos de cómputo donde se resguarda

Estos datos tienen el carácter de confidencial debido a que contienen las **medidas de seguridad técnica y organizativa** que garantizan la confidencialidad e integridad del sistema de datos personales del Área de Recursos Humanos, además preservan el pleno ejercicio de los derechos tutelados, frente a la alteración, pérdida, transmisión y acceso no autorizado, lo anterior, de conformidad a lo establecido en el los artículos 5to, decimo párrafo, 8 fracción VIII, 14 inciso A) fracción II, y B) fracción I, inciso (b y 15 de la Ley de Protección de Datos Personales del Distrito Federal.

Sin ser óbice de lo anterior, dicha clasificación se despliega en el recurso de revisión RR.SIP.1364/2013, donde se tuvo a bien hacer los siguientes señalamientos:

“El quince de agosto de dos mil trece, a través del sistema electrónico “INFOMEX”, mediante la solicitud de información con folio 031400011213, el particular requirió **en medio electrónico gratuito**:

“Quiero saber si en cumplimiento a las disposiciones normativas ya publicaron en gaceta oficial el aviso de los sistemas de protección de datos personales, en cuyo caso quiero me informen la fecha de publicación, y me den acceso a la **versión pública de los documentos de seguridad** que hayan implementado para cada uno de sus sistemas registrados.” (sic)

Respuesta del Ente Obligado:

Después de ser analizada la naturaleza jurídica del documento de seguridad se le informó al ahora recurrente de manera puntual y concordante, que el “documento de su interés se define como el instrumento que establece las medidas de seguridad y procedimientos administrativos, físicos y técnicos de seguridad aplicables a los sistemas de datos

*personales, necesarios para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos contenidos en los sistemas". Por lo anterior, se le dio a conocer cada uno de los Sistemas de Datos Personales del Ente Obligado, señalando que cada uno cuenta con su respectivo documento de seguridad, dando cumplimiento a la obligación prevista en el artículo 14, B Niveles de seguridad, fracciones I, II y III de la Ley de Protección de Datos Personales para el Distrito Federal.*

*De igual forma, se hizo de conocimiento al particular que si bien se trataba de un documento generado por el Ente Obligado en cumplimiento a un mandato de ley, no era susceptible la publicidad de éste, toda vez que contenía las medidas de seguridad estratégicas aplicables a cada Sistema de Datos Personales, mismas que deberían ser salvaguardadas ya que darlas a conocer podría afectar el adecuado tratamiento de los datos personales contenidos en los Sistemas del Ente Obligado, además de causar daño a la esfera jurídica de terceros, y que por su propia naturaleza no son susceptibles de ser transmitidos salvo con fines de auditoría.*

*Resolución del Recurso de Revisión RR.SIP.1364/2013*

*Por lo anterior, para garantizar el principio de seguridad, los Entes Públicos deben de elaborar el documento de seguridad en que se establezca de manera clara y específica la forma en que los datos personales serán tratados, para que sólo los que estén autorizados por una disposición legal puedan llevar a cabo su tratamiento.*

*Ahora bien, una vez analizada la naturaleza jurídica de la información solicitada, y con el objeto de determinar si es procedente la entrega en versión pública de la misma, a través del oficio INFODF/DJDN/SP/1716/2013 del veintidós de octubre de dos mil trece, se solicitó a la Dirección de Datos Personales de este Instituto para que en relación a la solicitud de acceso a la información pública con folio 0314000111213:*

*"...Informe si en su criterio, es factible elaborarse una versión pública de los documentos de seguridad de los Sistemas de Datos Personales que generan los Entes Públicos.*

*a) En caso afirmativo, indique cuáles secciones del documento de seguridad deberían ser protegidas y no hacerse públicas, así como los fundamentos y razones técnicas que sustenten sus consideraciones.*

*b) En caso negativo, señale de manera fundada y motivada por qué no sería posible entregar una versión pública de los referidos documentos de seguridad." (sic)*

*En virtud de lo anterior, el veintinueve de octubre de dos mil trece la Directora de Datos Personales de este Instituto mediante el oficio INFODF/DDP/315/2013, dio respuesta a lo requerido en el oficio antes descrito, señalando las siguientes conclusiones:*

*"...*

## CONCLUSIONES

- *De conformidad con lo que establece el artículo 13 de la Ley de Protección de Datos Personales para el Distrito Federal, el documento de seguridad es el instrumento que establece las medidas y procedimientos administrativos, físicos y técnicos de seguridad aplicables a los sistemas de datos personales necesarios para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos contenidos en dichos sistemas.*
- *Asimismo el documento de seguridad es de observancia obligatoria para todos los servidores públicos del ente público, así como para toda aquella persona que debido a la prestación de un servicio tenga acceso a los sistemas de datos personales, no así para personas que no estén facultadas para tratar los datos personales del sistema que corresponda.*
- *En atención a lo dispuesto en el artículo 15 de la Ley de Protección de Datos Personales para el Distrito Federal, el documento de seguridad es definido como confidencial, sin embargo en atención que se pretende acceder a la información mediante una solicitud de información pública es importante señalar que el referido documento de seguridad no encuadra en los supuestos jurídicos contemplados en el artículo 38 de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.*
- *En consecuencia, el Ente recurrido actuó de manera correcta al reservar el documento de seguridad bajo las causales del artículo 37, fracciones XII y XIV de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, ya que el hecho de que un tercero conozca la información contenida en el documento de seguridad, puede generar una ventaja personal y propiciar un acceso no autorizado a la información de carácter personal que se trata en los sistemas de datos personales, lo cual podría vulnerar el principio de confidencialidad previsto en la Ley de Protección de Datos Personales para el Distrito Federal, que garantiza que exclusivamente aquellos que cuenten con la atribución legal accedan a la información contenida en el sistema de datos personales de que se trate.*

*Por lo que se refiere a dar a conocer las medidas de seguridad adoptadas en el sistema de datos personales que corresponda, generaría una vulneración al principio de seguridad previsto en la Ley de Protección de Datos Personales para el Distrito Federal, además de poner en riesgo las instalaciones estratégicas del Ente Obligado.*

- *Al ser información que no encuadra como de acceso restringido en su modalidad de confidencial en términos de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, **sí podría ser susceptible de darse a conocer parte del documento de seguridad, como lo es el nombre del sistema; cargo y adscripción del responsable; ámbito de aplicación; estructura y descripción del sistema de datos personales; y especificación detallada de la categoría de datos personales contenidos en el sistema, ya que se trata de información de carácter público, y que incluso está a***

disposición de los particulares en el Registro Electrónico de Sistemas de Datos Personales en su sección de Consulta Pública.

- Sin embargo, la información referente al **ámbito de aplicación espacial y de contenidos, funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales; medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido por el artículo 14 de la Ley y los presentes Lineamientos; procedimientos de notificación, gestión y respuesta de incidencias; procedimientos para la realización de copias de respaldo y recuperación de los datos, para los sistemas de datos personales automatizados; y procedimientos para la realización de auditorías, en su caso; es jurídicamente imposible darla a conocer**, en aras de proteger la confidencialidad, integridad y disponibilidad del tratamiento de los datos personales contenidos en el sistema de datos personales del que se trate..." (sic)

De lo transcrito, se concluye que la información solicitada no encuadra en su totalidad como información de acceso restringido en términos de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, por lo que sí podría ser susceptible de darse a conocer parte del documento de seguridad.

Por otra parte, y considerando el principio de máxima publicidad de la información, así como lo señalado por la Dirección de Datos Personales de este Instituto, se puede observar que hay partes del documento de seguridad que podrían ser susceptibles de darse a conocer, como lo son:

- 1) Nombre del Sistema.
- 2) Cargo y adscripción del responsable.
- 3) *Ámbito de aplicación, sólo lo que respecta al Sistema de Datos Personales que es aplicable, tipo de tratamientos de los datos, nivel de seguridad aplicable y personal autorizado para dar tratamiento a los datos.*
- 4) Estructura y descripción del Sistema de Datos Personales.
- 5) Especificación detallada de la categoría de datos personales contenidos en el sistema.

No obstante, también hay partes del documento de seguridad que es imposible darlas a conocer, como son:

- 1) *Funciones y obligaciones del personal que intervenga en el tratamiento de los Sistemas de Datos Personales.*
- 2) *Medidas, normas, procedimientos y criterios enfocados a garantizar e nivel de seguridad.*

- 3) *Procedimientos de notificación, gestión y respuesta de incidencias.*
- 4) *Procedimientos para la realización de copias de respaldo y recuperación de los datos, para los Sistemas de Datos Personales automatizados.*
- 5) *Procedimientos para la realización de auditorías, en su caso.*

Por lo anterior, se concluye que el Ente Obligado si puede generar una versión pública de los documentos de seguridad y conceder el acceso a la información solicitada por el particular, restringiendo el acceso a la información antes descrita.  
..." (sic)

## ANÁLISIS

El presidente del Comité concedió el uso de la palabra al Licenciado Armando Manuel González Campuzano, Director de Administración y Finanzas, para que expusiera los argumentos en que fundó y motivó la clasificación de la información:

**Armando Manuel González Campuzano**, expuso que pone a disposición el Documento de Seguridad del Sistema de Datos Personales de los Recursos Humanos, el cual integra los datos del personal de estructura y honorarios, así como a los prestadores de servicio social con los que cuenta el Instituto, se precisa, que este documento se entrega en versión pública, debido a que contiene información de acceso restringido, en su modalidad de confidencial, que debe ser resguardada, como son los siguientes datos: Mapa de ubicación topográfica de los archivos del Sistema de Datos Personales de los Recursos Humanos, Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales, Medidas normas procedimientos y criterios enfocados a garantizar el nivel de seguridad alto, Procedimiento para la realización de copias de respaldo y recuperación de los datos para los sistemas de datos personales automatizados, Procedimientos de notificación gestión y respuesta ante incidencias, Procedimientos para la realización de auditorías, en su caso, Número de inventario de los archiveros donde se resguarda, Número de local, Número de inventario de los equipos de cómputo donde se resguarda.

Dichos datos tienen el carácter de confidencial debido a que contienen las **medidas de seguridad técnica y organizativa** que garantizan la confidencialidad e integridad del sistema de datos personales del Área de Recursos Humanos, además preservan el pleno ejercicio de los derechos tutelados, frente a la alteración, pérdida, transmisión y acceso no autorizado, lo anterior, de conformidad a lo establecido en el los artículos 5to, decimo

párrafo, 8 fracción VIII, 14 inciso A) fracción II, y B) fracción I, inciso (b y 15 de la Ley de Protección de Datos Personales del Distrito Federal.

Siendo pertinente citar la resolución al recurso de revisión con número de expediente RR.SIP.1364/2013, donde se señaló que a bien hacer los siguientes señalamientos: *para garantizar el principio de seguridad, los Entes Públicos deben de elaborar el documento de seguridad en que se establezca de manera clara y específica la forma en que los datos personales serán tratados, para que sólo los que estén autorizados por una disposición legal puedan llevar a cabo su tratamiento.*

Siendo que el veintinueve de octubre de dos mil trece la Directora de Datos Personales de este Instituto, señaló a manera de conclusiones que, de conformidad con lo que establece el artículo 13 de la Ley de Protección de Datos Personales para el Distrito Federal, el documento de seguridad es el instrumento que establece las medidas y procedimientos administrativos, físicos y técnicos de seguridad aplicables a los sistemas de datos personales necesarios para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos contenidos en dichos sistemas.

El documento de seguridad es de observancia obligatoria para todos los servidores públicos del ente público, así como para toda aquella persona que debido a la prestación de un servicio tenga acceso a los sistemas de datos personales, no así para personas que no estén facultadas para tratar los datos personales del sistema que corresponda.

En atención a lo dispuesto en el artículo 15 de la Ley de Protección de Datos Personales para el Distrito Federal, el documento de seguridad es definido como confidencial, sin embargo en atención que se pretende acceder a la información mediante una solicitud de información pública es importante señalar que el referido documento de seguridad no encuadra en los supuestos jurídicos contemplados en el artículo 38 de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

En consecuencia, el Ente recurrido actuó de manera correcta al reservar el documento de seguridad bajo las causales del artículo 37, fracciones XII y XIV de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, ya que el hecho de que un tercero conozca la información contenida en el documento de seguridad, puede generar una ventaja personal y propiciar un acceso no autorizado a la información de carácter personal que se trata en los sistemas de datos personales, lo cual podría vulnerar el principio de confidencialidad previsto en la Ley de Protección de Datos Personales para el Distrito Federal, que garantiza que exclusivamente aquellos que cuenten con la atribución legal accedan a la información contenida en el sistema de datos personales de que se trate.



Por lo que se refiere a dar a conocer las medidas de seguridad adoptadas en el sistema de datos personales que corresponda, generaría una vulneración al principio de seguridad previsto en la Ley de Protección de Datos Personales para el Distrito Federal, además de poner en riesgo las instalaciones estratégicas del Ente Obligado.

Al ser información que no encuadra como de acceso restringido en su modalidad de confidencial en términos de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, **sí podría ser susceptible de darse a conocer parte del documento de seguridad, como lo es el nombre del sistema; cargo y adscripción del responsable; ámbito de aplicación; estructura y descripción del sistema de datos personales; y especificación detallada de la categoría de datos personales contenidos en el sistema, ya que se trata de información de carácter público**, y que incluso está a disposición de los particulares en el Registro Electrónico de Sistemas de Datos Personales en su sección de Consulta Pública.

Sin embargo, la información referente al **ámbito de aplicación espacial y de contenidos, funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales; medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido por el artículo 14 de la Ley y los presentes Lineamientos; procedimientos de notificación, gestión y respuesta de incidencias; procedimientos para la realización de copias de respaldo y recuperación de los datos, para los sistemas de datos personales automatizados; y procedimientos para la realización de auditorías, en su caso; es jurídicamente imposible darla a conocer**, en aras de proteger la confidencialidad, integridad y disponibilidad del tratamiento de los datos personales contenidos en el sistema de datos personales del que se trate..." (sic)

De lo anterior, se concluye que la información solicitada no encuadra en su totalidad como información de acceso restringido en términos de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, por lo que sí podría ser susceptible de darse a conocer parte del documento de seguridad.

Por otra parte, y considerando el principio de máxima publicidad de la información, así como lo señalado por la Dirección de Datos Personales de este Instituto, se puede observar que hay partes del documento de seguridad que podrían ser susceptibles de darse a conocer, como lo son:

- 1) Nombre del Sistema.
- 2) Cargo y adscripción del responsable.

- 3) Ámbito de aplicación, sólo lo que respecta al Sistema de Datos Personales que es aplicable, tipo de tratamientos de los datos, nivel de seguridad aplicable y personal autorizado para dar tratamiento a los datos.
- 4) Estructura y descripción del Sistema de Datos Personales.
- 5) Especificación detallada de la categoría de datos personales contenidos en el sistema.

No obstante, también hay partes del documento de seguridad que es imposible darlas a conocer, como son:

- 1) Funciones y obligaciones del personal que intervenga en el tratamiento de los Sistemas de Datos Personales.
- 2) Medidas, normas, procedimientos y criterios enfocados a garantizar e nivel de seguridad.
- 3) Procedimientos de notificación, gestión y respuesta de incidencias.
- 4) Procedimientos para la realización de copias de respaldo y recuperación de los datos, para los Sistemas de Datos Personales automatizados.
- 5) Procedimientos para la realización de auditorías, en su caso.

Por lo anterior, se concluye que el Ente Obligado si puede generar una versión pública de los documentos de seguridad y conceder el acceso a la información solicitada por el particular, restringiendo el acceso a la información antes descrita.

**César Iván Rodríguez Sánchez**, señaló que a su criterio el documento de seguridad constituía en su totalidad información confidencial.

**Jorge Oropeza Rodriguez**, sugirió fundamentar de manera debida la clasificación presentada por la Dirección de Administración y Finanzas; de igual forma, consideró que se debía entregar versión pública de los documentos requeridos acorde a la versión que se encuentra publicada en el Portal de Internet de este Instituto.

Al no haber más comentarios, el **Presidente del Comité** sometió a votación del Comité de Transparencia, con fundamento en el artículo 90, fracciones II, VIII y XII de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México y el artículo 22 del Reglamento del Instituto de Acceso a la Información

Pública y Protección de Datos Personales del Distrito Federal en materia de Transparencia y Acceso a la Información Pública, la siguiente:

CLASIFICACIÓN DE LA INFORMACIÓN RELATIVA A LA SOLICITUD DE INFORMACIÓN CON FOLIO 3100000102516, PROPUESTA POR LA DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS, CONCEDIÉNDOSE EL ACCESO A UNA VERSIÓN PÚBLICA DEL DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DE LOS RECURSOS HUMANOS DEL INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA DEL DISTRITO FEDERAL.

LA INFORMACIÓN PÚBLICA A LA QUE SE DARÁ ACCESO SERÁ LA SIGUIENTE:

1. NOMBRE DEL SISTEMA
2. FECHA DE ELABORACIÓN
3. FECHA DE ÚLTIMA ACTUALIZACIÓN
4. ELABORÓ
5. APROBÓ
6. GUÍA DE CONTENIDO
7. INTRODUCCIÓN
8. NOMBRE DEL SISTEMA
9. RESPONSABLE DEL SISTEMA
10. ÁMBITO DE APLICACIÓN
11. ÁMBITO ESPACIAL
12. ÁMBITO DE CONTENIDOS
13. NORMATIVIDAD APLICABLE
14. ESTRUCTURA Y DESCRIPCIÓN DEL SISTEMA DE DATOS PERSONALES
15. PROCEDIMIENTO DE LA OBTENCIÓN DE LOS DATOS
16. CESIÓN DE DATOS
17. NIVEL DE SEGURIDAD
18. ESPECIFICACIÓN DETALLADA DE LA CATEGORÍA DE DATOS PERSONALES

AHORA BIEN, SE RESGUARDA LA INFORMACIÓN DE ACCESO RESTRINGIDO EN SU MODALIDAD DE **CONFIDENCIAL** CONSISTENTE EN:

1. MAPA DE UBICACIÓN TOPOGRÁFICA DE LOS ARCHIVOS DEL SISTEMA DE DATOS PERSONALES DE LOS RECURSOS HUMANOS

2. FUNCIONES Y OBLIGACIONES DEL PERSONAL QUE INTERVENGA EN EL TRATAMIENTO DE LOS SISTEMAS DE DATOS PERSONALES
3. MEDIDAS NORMAS PROCEDIMIENTOS Y CRITERIOS ENFOCADOS A GARANTIZAR EL NIVEL DE SEGURIDAD ALTO
4. PROCEDIMIENTO PARA LA REALIZACIÓN DE COPIAS DE RESPALDO Y RECUPERACIÓN DE LOS DATOS PARA LOS SISTEMAS DE DATOS PERSONALES AUTOMATIZADOS
5. PROCEDIMIENTOS DE NOTIFICACIÓN GESTIÓN Y RESPUESTA ANTE INCIDENCIAS
6. PROCEDIMIENTOS PARA LA REALIZACIÓN DE AUDITORÍAS, EN SU CASO
7. NÚMERO DE INVENTARIO DE LOS ARCHIVEROS DONDE SE RESGUARDA
8. NÚMERO DE LOCAL
9. NÚMERO DE INVENTARIO DE LOS EQUIPOS DE CÓMPUTO DONDE SE RESGUARDA

Clasificación que fue aprobada por unanimidad de votos de los integrantes del Comité de Transparencia.

#### IV. Asuntos Generales

En el Orden del Día no se enlistó ningún asunto general.

Por lo tanto, y no habiendo otro asunto que tratar, se dio por concluida la Tercera Sesión Ordinaria del Comité de Transparencia de este Instituto, a las dieciocho horas del veintiocho de junio de dos mil dieciséis. Firman al calce y al margen los que en ella intervinieron.



---

Rodrigo Montoya Castillo  
Presidente del Comité de  
Transparencia



---

Ana Lía de Fátima García García  
Secretaría Ejecutiva

Jorge Oropeza Rodríguez  
Subdirector de Servicios Legales y  
Representante de la Dirección Jurídica  
y Desarrollo Normativo

César Iván Rodríguez Sánchez  
Contralor

Carla Patricia Rivas García  
Responsable de la Unidad de  
Transparencia

Armando Manuel González Campuzano  
Director de Administración y Finanzas

Ana María Cervantes Jasso  
Directora de Datos Personales