Sesión: Décimo Primera Sesión Extraordinaria.
Fecha: 07 de julio de 2022.

INSTITUTO ELECTORAL DEL ESTADO DE MÉXICO
COMITÉ DE TRANSPARENCIA
ACUERDO N°. IEEM/CT/45/2022

DE CLASIFICACIÓN DE INFORMACIÓN COMO CONFIDENCIAL, PARA OTORGAR RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN PÚBLICA 00200/IEEM/IP/2022 Y ACUMULADA

El Comité de Transparencia del Instituto Electoral del Estado de México emite el presente Acuerdo, con base en lo siguiente:

GLOSARIO

Constitución Federal. Constitución Política de los Estados Unidos Mexicanos.

Constitución Local. Constitución Política del Estado Libre y Soberano de México.

IEEM. Instituto Electoral del Estado de México.

Ley General de Datos. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Ley General de Transparencia. Ley General de Transparencia y Acceso a la Información Pública.

Ley de Protección de Datos del Estado. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.

Ley de Transparencia del Estado. Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

Lineamientos de Clasificación. Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

SAIMEX. Sistema de Acceso a la Información Mexiquense.

ANTECEDENTES

1. En fecha veintiocho de junio de dos mil veintidós, se tuvieron por recibidas, vía SAIMEX, las solicitudes de acceso a la información pública registradas con los números de folio **00200/IEEM/IP/2022 y 00201/IEEM/IP/2022,** mediante las cuales se expresó lo siguiente:

   "SOLICITO - Las bases de datos actualizadas, su documento de seguridad, sus avisos de privacidad y los sistemas de Gestión.

   SOLICITO - Las bases de datos actualizadas, su documento de seguridad, sus avisos de privacidad y los sistemas de Gestión." (sic).

2. Las solicitudes fueron turnadas para su análisis y trámite, a la Áreas Administrativas del IEEM, toda vez que la información obra en sus archivos.

3. En ese sentido, las Áreas del IEEM, con excepción de la Dirección Jurídico Consultiva, ya que no administra Sistemas de Datos Personales, a fin de dar respuesta a la solicitud de información, solicitaron poner a consideración del Comité de Transparencia, como información confidencial, los documentos de seguridad de los Sistemas de Datos Personales que administran. Dichas áreas lo plantearon en los términos siguientes:

IEEM
Instituto Electoral del Estado de México

SECRETARÍA EJECUTIVA

SOLICITUD DE CLASIFICACIÓN DE INFORMACIÓN

Toluca, México a 30 de junio de 2022:

Con fundamento en lo establecido en el artículo 59, fracción V, 122 y 132, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, se solicita atentamente a la Unidad de Transparencia, someter a consideración del Comité de Transparencia, la aprobación de clasificación de la información/documentación solicitada, de conformidad con lo siguiente:

Área solicitante: Secretaria Ejecutiva
Número de folio de la solicitud: 00200/IEEM/IP/2022 y acumulada
Modalidad de entrega solicitada: Vía SAIMEX
Fecha de respuesta:

Solicitud:	"SOLICITO – Las bases de datos actualizadas, su documento seguridad, sus avisos de privacidad y los sistemas de Gestión." (sic)
Documentos que dan respuesta a la solicitud:	Documento de Seguridad que administra la Secretaria Ejecutiva del Sistema de Datos Personales denominado ***Integración de Propuestas para la Designación de Titulares de las Áreas Ejecutivas de Dirección del Instituto Electoral del Estado de México***.
Partes o secciones clasificadas:	La totalidad del documento de seguridad del Sistema de Datos personales denominado ***Integración de Propuestas para la Designación de Titulares de las Áreas Ejecutivas de Dirección del Instituto Electoral del Estado de México***.
Tipo de clasificación:	Confidencial.
Fundamento	Los artículos 3 fracciones XIV y XX, 31, 32, 35 y 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; y 4 fracciones XVII y XXX, 43, 44, 45, 48 y 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.
Justificación de la clasificación:	El Instituto Electoral del Estado de México, como sujeto obligado, a través de sus áreas y unidades administrativas y con el objeto de garantizar la protección de los datos personales a los que da tratamiento, debe adoptar, establecer y mantener medidas de

IEEM
Instituto Electoral del Estado de México

SECRETARÍA EJECUTIVA

	seguridad administrativas, físicas y técnicas, las cuales deben estar contenidas en el documento seguridad. En ese sentido, toda vez que en dicho documento se establecen las medidas de seguridad implementadas por la Secretaría Ejecutiva en el Sistema de Datos de que se trata, para proteger los datos personales a los que da tratamiento, las cuales son consideradas como confidenciales, en términos del artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios; se solicita su clasificación como información CONFIDENCIAL.
Periodo de reserva	NO APLICA
Justificación del periodo:	NO APLICA

Nota: Esta clasificación cuenta con el visto bueno del titular del área.

Nombre del Servidor Público Habilitado: Dario Llamas Pichardo

SOLICITUD DE CLASIFICACIÓN DE INFORMACIÓN
Toluca, México a 30 de junio de 2022.

Con fundamento en lo establecido en el artículo 59, fracción V, 122 y 132, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, se solicita atentamente a la Unidad de Transparencia, someter a consideración del Comité de Transparencia, la aprobación de la clasificación de la información/documentación solicitada, de conformidad con lo siguiente:
Área solicitante: Unidad de Género y Erradicación de la Violencia
Número de folio de la solicitud: 00200/IEEM/IP/2022 y 00201/IEEM/IP/2022
Modalidad de entrega solicitada: SAIMEX
Fecha de respuesta: de julio de 2022

Solicitud:	"SOLICITO- Las bases de datos actualizadas, su documento de seguridad, sus avisos de privacidad y los sistemas de Gestión" (SIC)
Documentos que dan respuesta a la solicitud:	• Documentos de seguridad de los Sistemas de Datos personales que administra la Unidad de Género y Erradicación de la Violencia.
Partes o secciones clasificadas:	Totalidad de los Documentos de Seguridad de los Sistemas de Datos Personales que administra la Unidad de Género y Erradicación de la Violencia: • Eventos y Convocatorias de la Unidad de Género. • Investigaciones, Estudios y Evaluaciones de la Unidad de Género y Erradicación de la Violencia. • Acciones para el Fortalecimiento de Capacidades de Precandidatas, Candidatas, Candidatos e Integrantes de Partidos Políticos. • Registro de Quejas y Denuncias relacionadas con Violencia de Género y Violencia Laboral. • Red de Mujeres Electas.
Tipo de clasificación:	CONFIDENCIAL
Fundamento	• Artículos 31, 32, 35 y 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. • Artículo 4, fracciones IV y XXX de la Ley de Protección de Datos en Posesión de Sujetos Obligados del Estado de México y Municipios.
Justificación de la clasificación:	El Instituto Electoral del Estado de México como Sujeto Obligado a través de sus áreas y unidades administrativas con el objeto de garantizar la protección de datos personales a los que da tratamiento adopta y establece medidas de seguridad administrativas, físicas y técnicas las cuales deben de estar contenidas en los documentos de seguridad En este sentido, toda vez que dicho documento establece las medidas de seguridad implementadas por la Unidad de Género y Erradicación de la Violencia para proteger los datos personales a los que da tratamiento, las cuales son consideradas como confidenciales de conformidad con el artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, se solicita su clasificación..
Periodo de reserva	N/A
Justificación del periodo:	N/A

Nota: Esta clasificación cuenta con el visto bueno del titular del área.
Nombre del Servidor Público Habilitado: Diego García Vélez.

IEEM
Instituto Electoral del Estado de México

DIRECCIÓN DE
PARTICIPACIÓN CIUDADANA

SOLICITUD DE CLASIFICACIÓN DE INFORMACIÓN
Toluca, México a 30 de junio de 2022.

Con fundamento en lo establecido en el artículo 59, fracción V, 122 y 132, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, se solicita atentamente a la Unidad de Transparencia, someter a consideración del Comité de Transparencia, la aprobación de la clasificación de la información/documentación solicitada, de conformidad con lo siguiente:

Área solicitante: Dirección de Participación Ciudadana
Número de folio de la solicitud: 00200/IEEM/IP/2022 y 00201/IEEM/IP/2022
Modalidad de entrega solicitada: SAIMEX
Fecha de respuesta: de julio de 2022

Solicitud:	"SOLICITO- Las bases de datos actualizadas, su documento de seguridad, sus avisos de privacidad y los sistemas de Gestión" (SIC)
Documentos que dan respuesta a la solicitud:	• Documentos de seguridad de los Sistemas de Datos personales que administra la Dirección de Participación Ciudadana
Partes o secciones clasificadas:	Totalidad de los Documentos de Seguridad de los Sistemas de Datos Personales que administra la Dirección de Participación Ciudadana: • Actividades de promoción para la inscripción en la lista nominal de residentes en el extranjero y del voto. • Congreso Estatal de Participación Ciudadana. • Participantes de las carreras deportivas por la democracia. • Eventos realizados por la Dirección de Participación Ciudadana derivados de la Estrategia Nacional de Cultura Cívica 2017-2023 (ENCCIVICA) y del Servicio Electoral Nacional. • Concursos Organizados por la Dirección de Participación Ciudadana.
Tipo de clasificación:	CONFIDENCIAL
Fundamento	• Artículos 31, 32, 35 y 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. • Artículo 4, fracciones IV y XXX de la Ley de Protección de Datos en Posesión de Sujetos Obligados del Estado de México y Municipios.
Justificación de la clasificación:	El Instituto Electoral del Estado de México como Sujeto Obligado a través de sus áreas y unidades administrativas con el objeto de garantizar la protección de datos personales a los que da tratamiento adopta y establece medidas de seguridad administrativas, físicas y técnicas las cuales deben de estar contenidas en los documentos de seguridad En este sentido, toda vez que dicho documento establece las medidas de seguridad implementadas por la Dirección de Participación Ciudadana para proteger los datos personales a los que da tratamiento, las cuales son consideradas como confidenciales de conformidad con el artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, se solicita su clasificación..
Periodo de reserva	N/A
Justificación del periodo:	N/A

Nota: Esta clasificación cuenta con el visto bueno del titular del área.
Nombre del Servidor Público Habilitado: Victor Gabriel Ortiz González
Nombre del titular del área: Liliana Martínez Garnica.

Toluca de Lerdo, México; a 01 de julio de 2022

SOLICITUD DE CLASIFICACIÓN DE INFORMACIÓN:

Con fundamento en lo establecido en los artículos 59, fracción V, 122 y 132, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, se solicita atentamente a la Unidad de Transparencia, someter a consideración del Comité de Transparencia, la aprobación de la clasificación de la información/documentación, de conformidad con lo siguiente:

Área solicitante: Unidad Técnica para la Administración de Personal Electoral.

Número de folio de solicitud: 00200/IEEM/IP/2022 y acumulada.

Modalidad de entrega solicitada: Vía SAIMEX.

Fecha de respuesta:

Solicitud:	**Folio de la solicitud: 00200/IEEM/IP/2022 y acumulada.** *"SOLICITO – Las bases de datos actualizadas, su documento de seguridad, sus avisos de privacidad y los sistemas de Gestión."* (sic).
Documentos que dan respuesta a la solicitud:	Documentos de Seguridad de los Sistemas de Datos Personales que administra esta Unidad: Archivo de Vocales y Listas de Reserva, Registro de Aspirantes al Servicio Electoral Profesional, Registro Único de Servidores Electorales Profesionales y Personal de apoyo para el registro de candidaturas en proceso electoral.
Partes o secciones clasificadas:	En su totalidad, los Documentos de Seguridad de los Sistemas de Datos Personales que administra esta Unidad: Archivo de Vocales y Listas de Reserva, Registro de Aspirantes al Servicio Electoral Profesional, Registro Único de Servidores Electorales Profesionales y Personal de apoyo para el registro de candidaturas en proceso electoral.
Tipo de clasificación:	Confidencial.
Fundamento	Artículos 3, fracciones XIV y XX; 31, 32, 35 y 42 de Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Artículos 4, fracciones XVIII y XXX; 43, 44, 45, 48 y 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.

Justificación de la clasificación:	El Instituto Electoral del Estado de México como sujeto obligado, a través de las áreas y/o unidades administrativas, con el objeto de garantizar los datos personales a los que da tratamiento debe adoptar, establecer y mantener medidas de seguridad administrativas, físicas y técnicas, las cuales deben estar contenidas en el documento de seguridad. En este sentido, toda vez que en dicho documento se establecen las medidas de seguridad implementadas por la Unidad Técnica para la Administración de Personal Electoral para proteger los datos personales que trata, las cuales son consideradas confidenciales en términos del artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, se solicita su clasificación como confidencial.
Periodo de reserva	No aplica.
Justificación del periodo:	No aplica.

Nombre del Servidor Público Habilitado: Christopher Alexis Morán Sánchez.

Subjefe de Desarrollo, Evaluación y Atención al SPEN de la Unidad Técnica: José Rivera Flores.

IEEM
Instituto Electoral del Estado de México

UNIDAD DE
INFORMÁTICA Y ESTADÍSTICA

SOLICITUD DE CLASIFICACIÓN DE INFORMACIÓN
Toluca, México a 1 de julio de 2022.

Con fundamento en lo establecido en el artículo 59, fracción V, 122 y 132, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, se solicita atentamente a la Unidad de Transparencia, someter a consideración del Comité de Transparencia, la aprobación de la clasificación de la información/documentación solicitada, de conformidad con lo siguiente:

Área solicitante: Unidad de Informática y Estadística
Número de folio de la solicitud: 00200/IEEM/IP/2022 y 00201/IEEM/IP/2022
Modalidad de entrega solicitada: Vía SAIMEX
Fecha de respuesta:

Solicitud:	**"SOLICITO - Las bases de datos actualizadas, su documento de seguridad, sus avisos de privacidad y los sistemas de Gestión." (Sic)**
Documentos que dan respuesta a la solicitud:	Documentos de seguridad de los Sistemas de datos personales que administra la Unidad de Informática y Estadística
Partes o secciones clasificadas:	En su totalidad los documentos de seguridad de los Sistemas de datos personales "SISTEMA DE DATOS REGISTRO DE PERSONAL ASPIRANTE A INTEGRAR LA PLANTILLA DEL PREP, INTEGRACIÓN DE PROPUESTAS PARA LA DESIGNACIÓN DE INTEGRANTES DEL COMITÉ TÉCNICO ASESOR DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES DEL INSTITUTO ELECTORAL DEL ESTADO DE MÉXICO" y "REGISTRO DE PERSONAL ASPIRANTE A INTEGRAR LA PLANTILLA DEL PREP 2018"
Tipo de clasificación:	Confidencial
Fundamento	Artículo 3 fracciones XIV y XX, 31, 32, 35 y 42 de la Ley General de Proteccion de Datos Personales en Posesiòn de Sujetos Obligados. Articulos 4, fracciones XVIII y XXX, 43, 44, 45, 48 y 49 de la Ley de Protección de Datos Personales en Posesiòn de Sujetos Obligados del Estado de Mèxico y Municipios.

Elaboró: Lic. Alfredo Burgos Cohl
ACUERDO No. IEEM/CT/45/2022

IEEM
Instituto Electoral del Estado de México

UNIDAD DE
INFORMÁTICA Y ESTADÍSTICA

Justificación de la clasificación:	El IEEM como Sujeto Obligado, a traves de sus àreas y/o Unidades administrativas, con el objeto de garantizar la proteccion de los datos personales a los que da tratamiento, debe adoptar, establecer y mantener medidas de seguridad administrativas, fisicas y tecnicas, las cuales se encuentran contenidas en los documentos de seguridad. En este sentido, toda vez que en dicho documento se establecen las medidas de seguridad implementadas por la Unidad de Informática y Estadística para proteger los datos personales que trata, las cuales son consideradas como confidenciales en terminos del articulo 43 de la Ley de Proteccion de Datos Personales en Posesiòn de Sujetos Obligados del Estado de Mèxico y Municipios, se solicita su clasificacion como informacion confidencial.
Periodo de reserva	NA
Justificación del periodo:	NA

Nota: Esta clasificación cuenta con el visto bueno del Subjefe de Informática y Estadística e Infraestructura de la UIE

Nombre del servidor Público Habilitado: Mtra. Ana Angélica López Valdés

Nombre del Subjefe de Informática y Estadística e Infraestructura de la UIE: Mtro. Juan Carlos Baca Belmontes

SOLICITUD DE CLASIFICACIÓN DE INFORMACIÓN
Toluca, México a 4 de julio de 2022:

Con fundamento en lo establecido en el artículo 59, fracción V, 122 y 132, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, se solicita atentamente a la Unidad de Transparencia, someter a consideración del Comité de Transparencia, la aprobación de la clasificación de la información/documentación solicitada, de conformidad con lo siguiente:

Área solicitante: Dirección de Administración
Número de folio de la solicitud: 00200/IEEM/IP/2022 y 00201/IEEM/IP/2022
Modalidad de entrega solicitada: Vía SAIMEX
Fecha de respuesta:

Solicitud:	"SOLICITO - Las bases de datos actualizadas, su documento de seguridad, sus avisos de privacidad y los sistemas de Gestión." (Sic)
Documentos que dan respuesta a la solicitud:	Documento de seguridad de los Sistemas de Datos Personales que administra la Dirección de Administración: • Cámaras de Seguridad del Órgano Central. • Expedientes de Servidores (as) Públicos (as) Electorales y Prestadores (as) de Servicios Profesionales. • Registro de Proveedores y Prestadores de Servicios del Instituto Electoral del Estado de México. • Registro de Visitantes al Edificio Sede del Instituto Electoral del estado de México. • Registro y Control de Asistencia. • Búsqueda de Inmuebles para Órganos Desconcentrados en Procesos Electorales.
Partes o secciones clasificadas:	En su totalidad, el Documento de Seguridad de los Sistemas de Datos Personales que Administra la Dirección de Administración.
Tipo de clasificación:	Confidencial
Fundamento	Artículos 3 fracciones XIV y XX, 31, 32, 35 y 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 4 fracciones XVIII y XXX, 43, 44, 45, 48 y 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.
Justificación de la clasificación:	El Instituto Electoral del Estado de México como sujeto obligado, a través de sus áreas y con el objeto de garantizar la protección de los datos personales a los que da tratamiento, debe adoptar, establecer y mantener medidas de seguridad administrativas, físicas y técnicas que deben estar contenidas en el documento de seguridad. En tal virtud y toda vez que en el documento se establecen las medidas de seguridad implementadas por la Dirección de Administración para proteger los datos personales que trata y que en términos del artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, son confidenciales, se solicita su clasificación.
Periodo de reserva	NA
Justificación del periodo:	NA

Nota: Esta clasificación cuenta con el visto bueno del titular del área.
Nombre del Servidor Público Habilitado: Aranzazú Rodríguez Rivera
Nombre del titular del área: José Mondragón Pedrero

IEEM
Instituto Electoral del Estado de México

CENTRO DE
FORMACIÓN Y
DOCUMENTACIÓN ELECTORAL

SOLICITUD DE CLASIFICACIÓN DE INFORMACIÓN

Toluca, México, 4 de julio de 2022

Con fundamento en lo establecido en el artículo 59, fracción V, 122 y 132, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, se solicita atentamente a la Unidad de Transparencia, someter a consideración del Comité de Transparencia, la aprobación de la clasificación de la información/documentación solicitada, de conformidad con lo siguiente:

Área solicitante: Centro de Formación y Documentación Electoral.
Número de folio de la solicitud: 00200/IEEM/IP/2022 y 00201/IEEM/IP/2022.
Modalidad de entrega solicitada: Vía Saimex.
Fecha de respuesta:

Solicitud	"SOLICITO – Las bases de datos actualizadas, su documento de seguridad, sus avisos de privacidad y los sistemas de Gestión." *(Sic)*
Documentos que dan respuesta a la solicitud	Documentos de seguridad de los sistemas de datos personales administrados por el CFDE.
Partes o secciones clasificadas	Documentos de seguridad de los sistemas de datos personales administrados por el CFDE en su totalidad: 1. Usuarios de la Biblioteca del IEEM. 2. Estudios de Posgrado y seguimiento a egresados. 3. Eventos académicos y de actualización. 4. De la *Revista del Instituto Electoral del Estado de México. Apuntes Electorales*. 5. Atención a la percepción del usuario. 6. Certámenes de investigación.
Tipo de clasificación	Confidencial.
Fundamento	Artículos 3, fracciones XIV y XX, 31, 32, 35 y 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 4, fracción XVIII y fracción XXX; y 43, 44, 45, 48 y 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.
Justificación de la clasificación	El IEEM como sujeto obligado, a través de sus áreas o unidades administrativas, con el objeto de garantizar la protección de los datos personales a los que da tratamiento, debe atender, dotar, establecer y mantener medidas de seguridad administrativas, físicas y técnicas, las cuales deben estar contenidas en los documentos de seguridad.

2

	En este sentido, toda vez que en dicho documento se establecen las medidas de seguridad implementadas por el CFDE para proteger los datos personales que trata y que en términos de artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios son confidenciales, se solicita respetuosamente la clasificación total de los documentos de seguridad de los sistemas de datos personales que administra: 1. Usuarios de la Biblioteca del IEEM. 2. Estudios de Posgrado y seguimiento a egresados. 3. Eventos académicos y de actualización. 4. De la *Revista del Instituto Electoral del Estado de México. Apuntes Electorales.* 5. Atención a la percepción del usuario. 6. Certámenes de investigación.
Periodo de reserva	No aplica.
Justificación del periodo	No aplica.

Nota: Esta clasificación cuenta con el visto bueno del titular del área.

Nombre de la servidora pública habilitada: Marisol Aguilar Hernández.
Nombre del titular del área: Mtra. Fatima Pichardo Mendoza.

3

IEEM
Instituto Electoral del Estado de México

DIRECCIÓN DE
ORGANIZACIÓN

SOLICITUD DE CLASIFICACIÓN DE INFORMACIÓN

Toluca, México a 4 de julio de 2022.

Con fundamento en lo establecido en el artículo 59, fracción V, 122 y 132, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, se solicita atentamente a la Unidad de Transparencia, someter a consideración del Comité de Transparencia, la aprobación de la clasificación de la información/documentación solicitada, de conformidad con lo siguiente:

Área solicitante: Dirección de Organización
Número de folio de la solicitud: 00200/IEEM/IP/2022 y acumulada
Modalidad de entrega solicitada: SAIMEX
Fecha de respuesta: 02/AGOSTO/2022

Solicitud:	***"SOLICITO – ... su documento de seguridad,..."* (SIC)**
Documentos que dan respuesta a la solicitud:	Documentos de Seguridad de los Sistema de Datos Personales que administra la Dirección de Organización: • "Integración de las propuestas y designación de consejeras y consejeros electorales en órganos desconcentrados en procesos electorales" • "Expedientes de observadores electorales durante los procesos electorales locales" • "Observadores electorales 2011 y 2012"
Partes o secciones clasificadas:	• En su totalidad los Documentos de Seguridad de los Sistema de Datos Personales que administra la Dirección de Organización.
Tipo de clasificación:	Confidencial.
Fundamento:	• Artículo 3, fracciones XIV y XX, 31, 32, 35 y 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. • Artículo 4, fracción XVIII y XXX, 43, 44, 45, 48 y 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.
Justificación de la clasificación:	El IEEM, a través de sus áreas y/o unidades administrativas, con el objeto de garantizar la protección de los datos personales a los que da tratamiento, debe adoptar, establecer y mantener medidas de seguridad administrativas, físicas y técnicas, las cuales deben de estar contenidas en los Documentos de Seguridad. En este sentido, toda vez que en dicho Documento se establecen las medidas de seguridad implementadas por la Dirección de Organización para proteger los datos personales que trata, y éstas son consideradas como confidenciales en términos del artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, se solicita la clasificación de los Documentos de Seguridad de los Sistema de Datos Personales previamente descritos, como información confidencial.

Página 1

Periodo de reserva	No aplica.
Justificación del periodo	No aplica.

Nota: Esta clasificación cuenta con el visto bueno del titular del área.

Nombre del Servidor Público Habilitado: Lic. Octavio Tonathiu Morales Peña
Nombre del titular del área: Lic. Víctor Hugo Cintora Vilchis

Página 2

SOLICITUD DE CLASIFICACIÓN DE INFORMACIÓN

Toluca, México a 04 de julio de 2022

Con fundamento en lo establecido en el artículo 59, fracción V, 122 y 132, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, se solicita atentamente a la Unidad de Transparencia, someter a consideración del Comité de Transparencia, la aprobación de la clasificación de la información/documentación solicitada, de conformidad con lo siguiente:

Área solicitante: Dirección de Partidos Políticos
Número de folio de la solicitud: 00200/IEEM/IP/2022 y acumulada 00201/IEEM/IP/2022
Modalidad de entrega solicitada: SAIMEX

Solicitud:	**SOLICITO - Las bases de datos actualizadas, su documento de seguridad, sus avisos de privacidad y los sistemas de Gestión**
Documentos que dan respuesta a la solicitud:	Documentos de Seguridad de los Sistemas de Datos Personales que administra la Dirección de Partidos Políticos.
Partes o secciones clasificadas:	En su totalidad los Documentos de Seguridad de los Sistemas de Datos Personales siguientes: ✓ Registro de los Representantes de los Partidos Políticos y Candidatos Independientes ante los Consejos: General, Distritales y Municipal. ✓ Padrón de Afiliados de organizaciones de ciudadanos que pretenden constituir un Partido Político Local. ✓ Registro de Candidaturas a cargos de elección popular en el Estado de México. ✓ Expedientes de Aspirantes a Candidatos Independientes. ✓ Cédula de Respaldo Ciudadano, Aspirante a Candidato (a) Independiente. ✓ Expedientes de aspirantes a Monitoristas para los Procesos Electorales Locales. ✓ Cursos de la Dirección de Partidos Políticos. ✓ Eventos de la Dirección de Partidos Políticos.
Tipo de clasificación:	Confidencial.
Fundamento	Artículo 3, fracciones XIV y XX, 31, 32, 35 y 42 de la ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; Artículo 4 fracciones XVIII y XXX, 43, 44, 45, 48 y 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.
Justificación de la clasificación:	El Instituto Electoral del Estado de México como sujeto obligado, a través de sus áreas y/o unidades administrativas,

	con el objeto de garantizar la protección de datos personales a los que da tratamiento, debe adoptar, establecer y mantener medidas de seguridad administrativas, físicas y técnicas, las cuales deben estar contenidas en los documentos de seguridad. En este sentido, toda vez que en dichos documentos se establecen las medidas de seguridad implementadas por la Dirección de Partidos Políticos para proteger los datos personales que trata, las cuales son consideradas como confidenciales en términos del artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, se solicita su clasificación como información confidencial.
Periodo de reserva	No aplica.
Justificación del periodo:	No aplica.

Nombre del Servidor Público Habilitado: Karim Segura Hernández
Nombre del Titular del Área: Lic. Osvaldo Tercero Gómez Guerrero

IEEM
Instituto Electoral del Estado de México

CONTRALORÍA GENERAL

SOLICITUD DE CLASIFICACIÓN DE INFORMACIÓN

Toluca, México a 01 de julio de 2022

Con fundamento en lo establecido en los artículos 59, fracción V, 122 y 132, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, y 49 fracción I de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, se solicita atentamente a la Unidad de Transparencia, someter a consideración del Comité de Transparencia, la aprobación de la clasificación de la información/documentación solicitada, de conformidad con lo siguiente:

Área solicitante: Contraloría General
Número de folio de la solicitud: 00200/IEEM/IP/2022 y 00201/IEEM/IP/2022
Modalidad de entrega solicitada: Saimex
Fecha de respuesta: 18 de julio de 2022

Solicitud:	00200/IEEM/IP/2022 y 00201/IEEM/IP/2022
Documentos que dan respuesta a la solicitud:	Documento de Seguridad de los Sistemas de Datos Personales que administra la Contraloría General.
Partes o secciones clasificadas:	En su totalidad el Documento de Seguridad de los Sistemas de Datos Personales: Sistema de Manifestación de Bienes y Declaración de Intereses; Sistema de Captación de Quejas y Denuncias y Sistema y Libro de Gobierno de la Contraloría General, que administra la Contraloría General.
Tipo de clasificación:	Confidencial
Fundamento	Artículos 3 fracciones XIV y XX, 31, 32, 35 y 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 4 fracciones XVIII y XXX, 43, 44, 45, 48 y 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.
Justificación de la clasificación:	El Instituto Electoral del Estado de México, a través de sus áreas y/o unidades administrativas con el objeto de garantizar la protección de datos personales a los que da tratamiento, debe optar, establecer y mantener medidas de seguridad administrativas, físicas y técnicas, las cuales deben estar contenidas en el Documento de Seguridad. En este sentido, toda vez que en dichos documentos se encuentran establecidas las medidas de seguridad implementadas por la Contraloría General para proteger los datos personales a los que da tratamiento, y al existir disposición legal expresa que establece que por la naturaleza de la información, las medidas de seguridad que se adopten serán consideradas confidenciales conforme al artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, se solicita su clasificación como información confidencial.
Periodo de reserva	N/A
Justificación del periodo:	N/A

Nota: Esta clasificación cuenta con el visto bueno del titular del área.

Nombre del Servidor Público Habilitado: Lic. Daniela Sánchez Priego
Nombre del titular del área: Mtro. Jesús Antonio Tobías Cruz

SOLICITUD DE CLASIFICACIÓN DE INFORMACIÓN

Toluca, México, a 30 de junio de 2022

Con fundamento en lo establecido en el artículo 59, fracción V, 122 y 132, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, se solicita atentamente a la Unidad de Transparencia, someter a consideración del Comité de Transparencia, la aprobación de la clasificación de la información/documentación solicitada, de conformidad con lo siguiente:

Área solicitante: Unidad de Transparencia
Número de folio de la solicitud: 00200/IEEM/IP/2022 y 00201/IEEM/IP/2022
Modalidad de entrega solicitada: SAIMEX

Solicitud:	"SOLICITO - Las bases de datos actualizadas, su documento de seguridad, sus avisos de privacidad y los sistemas de Gestión." (Sic)
Documentos que dan respuesta a la solicitud:	Documento de seguridad del sistema de datos personales denominado "Atención y trámite de solicitudes en el ejercicio del derecho a la protección de datos personales", que administra la Unidad de Transparencia.
Partes o secciones clasificadas:	En su totalidad el documento de seguridad del sistema de datos personales denominado "Atención y trámite de solicitudes en el ejercicio del derecho a la protección de datos personales", que administra la Unidad de Transparencia.
Tipo de clasificación:	Confidencial
Fundamento	Artículos 3, fracciones XIV y XX, 31, 32, 35, y 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Artículos 4, fracciones XVIII y XXX, 43, 44, 45, 48 y 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.
Justificación de la clasificación:	El Instituto Electoral del Estado de México como Sujeto Obligado a través de sus áreas y/o unidades administrativas, con el objeto de garantizar la protección de datos personales a los que da tratamiento, debe adoptar, establecer las medidas de seguridad administrativas, físicas y técnicas, las cuales deben estar contenidas en los documentos de seguridad. En este sentido, toda vez que en dicho documento se establecen las medidas de seguridad implementadas por la Unidad de Transparencia para proteger los datos personales que trata, las

	cuales por disposición expresa del artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios son confidenciales, se solicita su clasificación.
Periodo de reserva	No aplica
Justificación del periodo:	No aplica

Nota: Esta clasificación cuenta con el visto bueno del titular del área.

Nombre del Servidor Público Habilitado: Juan Carlos Hernández Ortiz
Nombre del titular del área: Lilibeth Álvarez Rodríguez

En esta virtud, con base en las solicitudes de clasificación enviadas por las áreas responsables, se procede al análisis de los documentos referidos, a efecto de determinar si deben ser clasificados como confidenciales.

CONSIDERACIONES

I. Competencia

Este Comité de Transparencia es competente para confirmar, modificar o revocar la clasificación de información como confidencial, de conformidad con el artículo 49, fracciones II y VIII de la Ley de Transparencia del Estado.

Asimismo, es competente para supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad, de conformidad con el artículo 94, fracción V de la Ley de Protección de Datos del Estado.

II. Fundamento

a) En el artículo 6, apartado A), fracciones I y II, de la Constitución Federal, se establece que toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y solo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes; por lo que en la interpretación de este derecho deberá prevalecer el principio de máxima publicidad, y que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes de la materia.

Asimismo, en el artículo 16, párrafos primero y segundo del citado ordenamiento, se prevé que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento, aunado a que toda persona tiene derecho a la protección de sus datos personales.

b) En los artículos 3, fracciones IX y XIV, 4, 16, 17, 18, 35, 36 y 84 de la Ley General de Datos se dispone que:

Datos personales: son cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

- La Ley es aplicable a cualquier tratamiento de datos personales que obre en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación.
- El responsable del tratamiento de datos personales deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.
- El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.
- Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.
- De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente: **I.** El inventario de datos personales y de los sistemas de tratamiento; **II.** Las funciones y obligaciones de las personas que traten datos personales; **III.** El análisis de riesgos; **IV.** El análisis de brecha; **V.** El plan de trabajo; **VI.** Los mecanismos de monitoreo y revisión de las medidas de seguridad, y **VII.** El programa general de capacitación.
- El responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos: **I.** Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo; **II.** Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; **III.** Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y **IV.** Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

c) En el artículo 100 de la Ley General de Transparencia se prevé que la clasificación es el proceso mediante el cual el Sujeto Obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, y que los titulares de las áreas de los Sujetos Obligados serán los responsables de clasificar la información.

El citado ordenamiento también estipula, en su artículo 116, párrafo primero, que se considera información confidencial la que contenga datos personales concernientes a una persona identificada o identificable.

d) Los Lineamientos de Clasificación establecen, de manera específica, en el numeral Trigésimo octavo, fracción I, que es considerada información confidencial los datos personales en términos de la legislación aplicable, esto es,

la Ley General de Datos y la Ley de Protección de Datos del Estado.

e) La Constitución Local dispone, en el artículo 5, fracciones I y II, que: "Toda la información en posesión de cualquier autoridad, entidad, órgano y organismos de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos estatales y municipales, así como del gobierno y de la administración pública municipal y sus organismos descentralizados, asimismo, de cualquier persona física, jurídica colectiva o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones previstas en la Constitución Política de los Estados Unidos Mexicanos de interés público y seguridad, en los términos que fijen las leyes.

La información referente a la intimidad de la vida privada y la imagen de las personas será protegida a través de un marco jurídico rígido de tratamiento y manejo de datos personales, con las excepciones que establezca la ley reglamentaria." (sic).

f) La Ley de Protección de Datos del Estado ordena, en los artículos 4, fracciones XI y XVIII, 5, 15, 22, párrafo primero, 25, 40, 48, 49, 50 y 94, fracción V lo siguiente:

Datos personales: Es la información concerniente a una persona física o jurídica colectiva identificada o identificable, establecida en cualquier formato o modalidad, y que esté almacenada en los sistemas y bases de datos; se considerará que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier documento informativo físico o electrónico.

Documento de seguridad: al instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de la información contenida en los sistemas y bases de datos personales.

- La Ley será aplicable a cualquier tratamiento de datos personales en posesión de Sujetos Obligados.

- Los responsables en el tratamiento de datos personales observarán los principios de calidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad y responsabilidad.

- Particularmente, el principio de finalidad refiere que todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la

normatividad aplicable les confiera.

- Por lo que respecta al principio de licitud, este refiere que el tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

- Finalmente, el deber de confidencialidad consiste en que la información no se pondrá a disposición ni se revelará a individuos, entidades o procesos no autorizados.

- Los sujetos obligados elaborarán y aprobarán un documento que contenga las medidas de seguridad aplicables a las bases y sistemas de datos personales, tomando en cuenta los estándares internacionales de seguridad, la presente Ley, así como los lineamientos que se expidan. El documento de seguridad será de observancia obligatoria para los responsables, encargados y demás personas que realizan algún tipo de tratamiento a los datos personales. A elección del sujeto obligado, éste podrá ser único e incluir todos los sistemas y bases de datos personales que posea, por unidad administrativa en que se incluyan los sistemas y bases de datos personales en custodia, individualizado para cada sistema, o mixto.

- El documento de seguridad deberá contener como mínimo lo siguiente: I. Respecto de los sistemas de datos personales: a) El nombre. b) El nombre, cargo y adscripción del administrador de cada sistema y base de datos. c) Las funciones y obligaciones del responsable, encargado o encargados y todas las personas que traten datos personales. d) El folio del registro del sistema y base de datos. e) El inventario o la especificación detallada del tipo de datos personales contenidos. f) La estructura y descripción de los sistemas y bases de datos personales, lo cual consiste en precisar y describir el tipo de soporte, así como las características del lugar donde se resguardan. II. Respecto de las medidas de seguridad implementadas deberá incluir lo siguiente: a) Transferencia y remisiones. b) Resguardo de soportes físicos y electrónicos. c) Bitácoras para accesos, operación cotidiana y violaciones a la seguridad de los datos personales. d) El análisis de riesgos. e) El análisis de brecha. f) Gestión de incidentes. g) Acceso a las instalaciones h) Identificación y autenticación. i) Procedimientos de respaldo y recuperación de datos. j) Plan de contingencia. k) Auditorías. l) Supresión y borrado seguro de datos. m) El plan de trabajo. n) Los mecanismos de monitoreo y revisión de las medidas de seguridad. o) El programa general de capacitación. Revisión y actualización del documento de seguridad.

- El responsable revisará el documento de seguridad de manera periódica y actualizarlo cuando ocurran los eventos siguientes: I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en

un cambio en el nivel de riesgo. II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión. III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida. IV. Implementación de acciones correctivas y preventivas ante una violación de la seguridad de los datos personales.

- El Comité de Transparencia tendrá las atribuciones siguientes: Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.

g) La Ley de Transparencia del Estado prevé en el artículo 3, fracciones IX y XX que:
Un dato personal es la información concerniente a una persona, identificada o identificable, y la información clasificada es aquella considerada por la ley como reservada o confidencial.

III. ACUMULACIÓN DE LAS SOLICITUDES DE INFORMACIÓN

Como ya se señaló, en fecha veintiocho de junio de dos mil veintidós se recibieron vía SAIMEX las solicitudes de acceso a la información pública identificadas con números de folio **00200/IEEM/IP/2022** y **00201/IEEM/IP/2022,** en lo subsecuente solicitudes de información **00200/IEEM/IP/2022 y acumulada.**

Lo anterior, tiene sustento en la resolución relevante ***"Efectos Jurídicos de la acumulación de las solicitudes de información pública"***, dictada por el Pleno del INFOEM, en el recurso de revisión **00091/INFOEM/IP/RR/2013 y acumulados**, aprobado por unanimidad de votos en la Séptima Sesión Ordinaria del día diecinueve de febrero del año dos mil trece, en la cual se señala que la acumulación se entiende como la figura procesal por virtud de la cual existen en dos o más causas, autos o acciones elementos de conexidad o de identidad en las partes, acciones y materia de la litis o controversia. Los principios a los que obedece la acumulación son dos: el de economía procesal y el de evitar que sobre causas conexas o idénticas se pronuncien resoluciones contrarias o contradictorias.

Asimismo, el artículo 18 del Código de Procedimientos Administrativos señala lo siguiente:

> *"Artículo 18.-* ***La autoridad administrativa*** *o el Tribunal* ***acordarán la acumulación de los expedientes*** *del procedimiento y proceso administrativo que ante ellos se sigan, de oficio o a petición de parte,* ***cuando las partes o los actos administrativos sean iguales, se trate de actos conexos o resulte conveniente el trámite unificado de los***

asuntos, para evitar la emisión de resoluciones contradictorias. *La misma regla se aplicará, en lo conducente, para la separación de los expedientes."*

En esta tesitura, se determina que:

- En sentido amplio, las disposiciones contenidas en el Código de Procedimientos Administrativos son aplicables supletoriamente a lo establecido en la Ley de Transparencia del Estado.

- La acumulación de expedientes es viable cuando las partes sean iguales, resulte conveniente el trámite unificado de los asuntos y para evitar la emisión de resoluciones contradictorias.

Aunado a ello, en la resolución recaída al recurso de revisión 01245/INFOEM/IP/RR/2018 y acumulados, la autoridad en consulta determinó que:

- El artículo 18 del mencionado Código dispone la posibilidad para que las autoridades administrativas acumulen los expedientes de los procedimientos, pues la naturaleza de la figura jurídica de acumulación obedece a una cuestión práctica de economía procesal, cuando en dos o más procedimientos administrativos las partes o los actos administrativos son iguales, o se trata de actos conexos o resulta conveniente el trámite unificado de los asuntos.

- Con atención al artículo 165 de la Ley de Transparencia del Estado, que dispone: *Los Sujetos Obligados establecerán la forma y términos en que darán trámite interno a las solicitudes en materia de acceso a la información…"*, y la fracción IV del artículo 53 del mismo ordenamiento, el cual establece que las Unidades de Transparencia realizarán con efectividad los trámites internos necesarios para la atención de las solicitudes de información; debe interpretarse de manera sistemática en el sentido de que es procedente la acumulación de solicitudes de información para su atención. Lo anterior da pauta a que el trámite y determinación final de las solicitudes acumuladas se realicen bajo los principios de economía procesal e invariabilidad para evitar resoluciones contradictorias.

Luego, de todo lo expuesto se colige que la acumulación es el acto procesal llevado a cabo por diversas autoridades, que no afecta los derechos sustantivos del particular, y dicha acumulación procede cuando las partes sean iguales y cuando se trate del mismo solicitante y el mismo Sujeto Obligado.

En efecto, las solicitudes de información que nos ocupan fueron realizadas por el mismo **SOLICITANTE** ante el mismo **SUJETO OBLIGADO**, por lo que resulta conveniente la respuesta conjunta por economía procesal y con el fin de no emitir respuestas contradictorias entre sí.

Asimismo, otros elementos que se toman en consideración para la acumulación de las solicitudes de información es la temporalidad y la temática de estas, ya que las solicitudes fueron presentadas en misma fecha y respecto de la misma información, por lo tanto, el vencimiento del plazo para que este Sujeto Obligado dé respuesta a las solicitudes de información en comento será el mismo día.

Así las cosas, resulta procedente la acumulación de las solicitudes de información antes señaladas, ya que del análisis de las mismas se puede apreciar la conexidad de la información solicitada.

Por lo tanto, la acumulación de las solicitudes de información en estudio para ser atendidas conjuntamente, no transgrede el derecho de acceso a la información pública del solicitante, dada su notoria semejanza, máxime que en la respuesta proporcionada a todas esas solicitudes la información le será proporcionada en su totalidad.

IV. Motivación

De conformidad con lo establecido en el artículo 16 de la Constitución General, todo acto que genere molestia en cualquier persona, emitido por autoridad competente, se debe encontrar fundado y motivado. Sirve de apoyo la siguiente jurisprudencia:

Época: Novena Época
Registro: 203143
Instancia: Tribunales Colegiados de Circuito
Tipo de Tesis: Jurisprudencia
Fuente: Semanario Judicial de la Federación y su Gaceta
Tomo III, Marzo de 1996
Materia(s): Común
Tesis: VI.2o. J/43
Página: 769

"FUNDAMENTACIÓN Y MOTIVACIÓN.

La debida fundamentación y motivación legal, deben entenderse, por lo primero, la cita del precepto legal aplicable al caso, y por lo segundo, las razones, motivos o circunstancias especiales que llevaron a la autoridad a concluir que el caso particular encuadra en el supuesto previsto por la norma legal invocada como fundamento.

SEGUNDO TRIBUNAL COLEGIADO DEL SEXTO CIRCUITO.

Amparo directo 194/88. Bufete Industrial Construcciones, S.A. de C.V. 28 de junio de 1988. Unanimidad de votos. Ponente: Gustavo Calvillo Rangel. Secretario: Jorge Alberto González

Alvarez.

Revisión fiscal 103/88. Instituto Mexicano del Seguro Social. 18 de octubre de 1988. Unanimidad de votos. Ponente: Arnoldo Nájera Virgen. Secretario: Alejandro Esponda Rincón.

Amparo en revisión 333/88. Adilia Romero. 26 de octubre de 1988. Unanimidad de votos. Ponente: Arnoldo Nájera Virgen. Secretario: Enrique Crispín Campos Ramírez.

Amparo en revisión 597/95. Emilio Maurer Bretón. 15 de noviembre de 1995. Unanimidad de votos. Ponente: Clementina Ramírez Moguel Goyzueta. Secretario: Gonzalo Carrera Molina.

Amparo directo 7/96. Pedro Vicente López Miro. 21 de febrero de 1996. Unanimidad de votos. Ponente: María Eugenia Estela Martínez Cardiel. Secretario: Enrique Baigts Muñoz".

En esa virtud, se analizarán los documentos de seguridad de los sistemas de datos personales administrados por las áreas, para determinar si deben ser clasificados como confidenciales, al tenor de lo siguiente:

La Ley de Protección de Datos Personales del Estado, tiene por objeto establecer las bases, principios y procedimientos para tutelar y garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de los sujetos obligados.

A partir de la publicación de la Ley en comento, el IEEM, por conducto de la Unidad de Transparencia y con la participación de las áreas del IEEM generadoras de la información, se establecieron acciones conducentes con la finalidad de establecer los soportes para la realización de los documentos de seguridad.

Dicho documento permite identificar los datos personales recabados por el IEEM y en consecuencia la creación de los sistemas de tratamiento de datos personales sobre los mismos. De igual manera, contiene información cuyo objeto primordial es la protección y el adecuado tratamiento de los datos personales custodiados por el IEEM.

Los documentos de seguridad tienen por objetivo asegurar la integridad, la confidencialidad y disponibilidad de los datos e información personal que se encuentran en poder del IEEM como sujeto obligado y delimita las obligaciones de los responsables, encargados y usuarios de cada sistema y medidas de seguridad administrativa, física y técnica que deberá implementarse para el correcto manejo de la información que el IEEM posee.

Es de mencionar que el documento de seguridad es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad antes mencionadas que el IEEM ha adaptado, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales en su posesión.

Para tal efecto, resulta importante señalar que los datos personales, son aquella

información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse de manera directa o indirecta a través de información tal como el nombre, su domicilio, número telefónico, número de seguridad social, datos relativos a su patrimonio, características físicas, vida familiar, entre otros.

Asimismo, los datos personales sensibles son aquellos que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, tales como los relativos a su origen étnico o racial, estado de salud, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencias sexuales u otros similares.

Resulta importante señalar lo establecido en el artículo 3, fracción XIV de la Ley General de Transparencia el cual refiere que el documento de seguridad es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Asimismo, la fracción XVIII, del artículo 4 de la Ley de Protección de Datos del Estado refiere lo siguiente:

> *XVIII. Documento de seguridad: al instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de la información contenida en los sistemas y bases de datos personales.*

Ahora bien, en términos de lo señalado por el artículo 48 de la Ley de Protección de Datos del Estado, los sujetos obligados elaborarán y aprobarán un documento que contenga las medidas de seguridad aplicables a las bases y sistemas de datos personales, tomando en cuenta los estándares internacionales de seguridad, la Ley y los lineamientos que se expidan.

En este sentido, el documento de seguridad es de observancia obligatoria para los responsables, encargados y demás personas que realizan algún tipo de tratamiento a los datos personales. A elección del sujeto obligado, éste podrá ser único e incluir todos los sistemas y bases de datos personales que posea, por unidad administrativa en que se incluyan los sistemas y bases de datos personales en custodia, individualizado para cada sistema, o mixto.

Para tal efecto, en artículo 49 de la Ley en consulta señala que el documento de seguridad deberá contener como mínimo lo siguiente:

I. Respecto de los sistemas de datos personales:

a) El nombre.
b) El nombre, cargo y adscripción del administrador de cada sistema y base de datos.
c) Las funciones y obligaciones del responsable, encargado o encargados y todas las personas que traten datos personales.
d) El folio del registro del sistema y base de datos.
e) El inventario o la especificación detallada del tipo de datos personales contenidos.
f) La estructura y descripción de los sistemas y bases de datos personales, lo cual consiste en precisar y describir el tipo de soporte, así como las características del lugar donde se resguardan.

II. Respecto de las medidas de seguridad implementadas deberá incluir lo siguiente:

a) Transferencia y remisiones.
b) Resguardo de soportes físicos y electrónicos.
c) Bitácoras para accesos, operación cotidiana y violaciones a la seguridad de los datos personales.
d) El análisis de riesgos.
e) El análisis de brecha.
f) Gestión de incidentes.
g) Acceso a las instalaciones.
h) Identificación y autenticación.
i) Procedimientos de respaldo y recuperación de datos.
j) Plan de contingencia.
k) Auditorías.
l) Supresión y borrado seguro de datos.
m) El plan de trabajo.
n) Los mecanismos de monitoreo y revisión de las medidas de seguridad.
o) El programa general de capacitación.

De esta manera, el responsable del tratamiento de los datos personales le corresponde revisar el documento de seguridad de manera periódica y actualizarlo cuando ocurran los eventos siguientes:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.

III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.
IV. Implementación de acciones correctivas y preventivas ante una violación de la seguridad de los datos personales.

Es de suma importancia referir que dentro del contenido del documento de seguridad se incluyen las medidas de seguridad, que son todas aquellas medidas que adopta el comité de Transparencia y en su caso, en conjunto con las áreas del IEEM que posee la información para asegurar que la información confidencial y los datos personales son resguardados de manera íntegra, segura y adecuada, ya sea a través de mecanismos administrativos, técnicos y físicos.

Para tal efecto, se cuenta con medidas de seguridad administrativas, físicas y técnicas:

> ***Medidas de seguridad administrativas:*** *a las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, y capacitación del personal, en materia de protección de datos personales.*
>
> ***Medidas de seguridad físicas:*** *a las acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.*
>
> *De manera enunciativa más no limitativa, se considerarán las actividades siguientes:*
>
> *a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.*
> *b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.*
> *c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización.*
> *d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad e integridad.*
>
> ***Medidas de seguridad técnicas:*** *a las acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.*
>
> *De manera enunciativa más no limitativa, se considerarán las actividades siguientes:*
>
> *a) Prevenir que el acceso a los sistemas y bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.*

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Por lo anterior, el responsable adoptará, establecerá, mantendrá y documentará las medidas de seguridad administrativas, físicas y técnicas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, a través de controles y acciones que eviten su daño, alteración, pérdida, destrucción, o el uso, transferencia, acceso o cualquier tratamiento no autorizado o ilícito, de conformidad con lo dispuesto en los lineamientos que al efecto se expidan.

Las medidas de seguridad constituyen mínimos exigibles, por lo que el sujeto obligado adoptará las medidas adicionales que estime necesarias para brindar mayor garantía en la protección y resguardo de los sistemas y bases de datos personales.

De conformidad con el artículo 43 de la Ley de Protección de Datos del Estado, dada la naturaleza de las medidas de seguridad y registro del nivel de seguridad que se adopten, serán consideradas confidenciales.

El responsable y el encargado establecerán medidas para garantizar que cualquier persona que actúe bajo la autoridad de éstos y que tenga acceso a datos personales sólo pueda tratarlos siguiendo las instrucciones del responsable y observando lo previsto en la normatividad aplicable.

Las medidas de seguridad que al efecto se establezcan indicarán el nombre y cargo del administrador o usuaria o usuario, según corresponda.

Por cuanto hace a los tipos y niveles de seguridad, de conformidad con el artículo 44 de la Ley de Protección de Datos Personales del Estado, el responsable adoptará las medidas de seguridad, conforme a lo siguiente:

A. Tipos de seguridad:

I. Física: a la medida orientada a la protección de instalaciones, equipos, soportes, sistemas o bases de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor.

II. Lógica: a las medidas de seguridad administrativas y de protección que permiten la identificación y autenticación de las usuarias y los usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función.

III. De desarrollo y aplicaciones: a las autorizaciones con las que contará la creación o tratamiento de los sistemas o bases de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de las usuarias y usuarios, la separación de entornos, la metodología a seguir, ciclos de vida y gestión, así como las consideraciones especiales respecto de aplicaciones y pruebas.

IV. De cifrado: a la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la seguridad de la información.

V. De comunicaciones y redes: a las medidas de seguridad técnicas, así como restricciones preventivas y de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.

B. Niveles de seguridad:

I. Básico: a las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas y bases de datos personales.

Dichas medidas corresponden a los siguientes aspectos:

a) Documento de seguridad.
b) Funciones y obligaciones del personal que intervenga en el tratamiento de las bases o sistemas de datos personales.
c) Registro de incidencias.
d) Identificación y autenticación.
e) Control de acceso.
f) Gestión de soportes.
g) Copias de respaldo y recuperación.

II. Medio: a la adopción de medidas de seguridad cuya aplicación corresponde a bases o sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los aspectos siguientes:

a) Responsable de seguridad.
b) Auditoría.
c) Control de acceso físico.
d) Pruebas con datos reales.

III. Alto: a las medidas de seguridad aplicables a bases o sistemas de datos concernientes a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad pública, prevención, investigación y persecución de delitos.

En estos casos, además de incorporar las medidas de nivel básico y medio, deberán completar las que se detallan a continuación:

a) Distribución de soportes.
b) Registro de acceso.
c) Telecomunicaciones.

Los diferentes niveles de seguridad son establecidos atendiendo a las características propias de la información.

Por tal motivo y de conformidad con lo anteriormente señalado, para establecer y mantener las medidas de seguridad para la protección de los datos personales en poder del IEEM, los responsables tienen que realizar al menos las siguientes actividades interrelacionadas:

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

III. Elaborar un inventario de datos personales y de las bases y o sistemas de tratamiento.

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulnerabilidades a las que están sujetos los datos personales.

VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

En este sentido, es evidente que la difusión del documento de seguridad en cuestión, en nada contribuye a la transparencia ni a la rendición de cuentas, sino por el contrario su publicación podría actualizar una vulneración a los principios jurídicos tutelados por la Ley de Protección de Datos Personales del Estado, concatenado con la Ley de Transparencia del Estado, al entregar información que debe considerarse como confidencial, por contener información relativa entre otra, a las medidas de seguridad, el análisis de riesgo, el análisis de brecha y los planes de trabajo relativos a los datos personales en poder de este sujeto obligado.

Aunado a lo anterior, se considerarán como violaciones de seguridad, en cualquier fase del tratamiento de datos:

I. La pérdida, robo, extravío.
II. La copia o destrucción no autorizada.
III. El uso o tratamiento no autorizado.
IV. El daño, la alteración o modificación no autorizada.

Los responsables deben establecer medidas de seguridad de nivel alto, para garantizar la integridad, disponibilidad y **confidencialidad de la información**, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción **o el uso, acceso o tratamiento no autorizado.**

Por lo anteriormente expuesto, es de mencionar que los documentos de seguridad registrados y en poder de las áreas del IEEM, contienen disposiciones en materia de protección de datos personales, debido a la existencia de riesgos de los propios sistemas que contienen datos personales recabados por el propio Instituto, por lo que es evidente determinar la clasificación del documento de seguridad como confidencial, pues la vulneración del mismo supondría un agravio en contra de los titulares de los datos personales que resguarda cada área del IEEM, toda vez que la información contenida en los documentos de seguridad de los sistemas de datos personales registrados en el sistema Intranet, administrado por el INFOEM, ya sean físicos o electrónicos, advierte información sensible y de carácter personal, por lo cual, se tiene el imperativo legal de proteger.

Conclusión

Por todo lo anterior, este Comité de Transparencia determina que es procedente la acumulación de las solicitudes de información, en términos de lo anteriormente analizado.

De igual manera, este Comité de Transparencia determina que es procedente la clasificación de los documentos de seguridad de los sistemas de datos personales en poder de las áreas del IEEM registrados en el sistema Intranet del INFOEM, de conformidad con el artículo 43 de la Ley de Protección de Datos Personales del Estado, garantizar la seguridad de los datos de carácter confidencial evitando su alteración o acceso no autorizado.

Por lo expuesto, fundado y motivado, este Comité de Transparencia:

A C U E R D A

PRIMERO. Se aprueba la acumulación de las solicitudes de información pública **00200/IEEM/IP/2022 y acumulada**, por existir conexidad en la materia, sin que ello afecte los derechos sustantivos del particular.

SEGUNDO. Se confirma la clasificación de los documentos de seguridad de los sistemas de datos personales registrados en el sistema Intranet del INFOEM, en poder de las áreas del IEEM como confidencial.

TERCERO. La UT deberá hacer del conocimiento de las áreas del IEEM el presente Acuerdo para que lo incorporen al expediente electrónico en el SAIMEX.

CUARTO. La UT deberá notificar al particular, a través de SAIMEX, el presente Acuerdo junto con la respuesta de las áreas del IEEM.

Así lo determinaron por unanimidad de votos los Integrantes del Comité de Transparencia del Instituto Electoral del Estado de México, de conformidad con las Leyes de Transparencia y Protección de Datos Personales del Estado, en su Décimo Primera Sesión Extraordinaria del día siete de julio de dos mil veintidós, y cierran su actuación firmando al calce para constancia legal.

Dra. Paula Melgarejo Salgado
Consejera Electoral y Presidenta
del Comité de Transparencia
(RÚBRICA)

Elaboró: Lic. Alfredo Burgos Cohl
ACUERDO No. IEEM/CT/45/2022

Lic. Juan José Hernández López
Subdirector de Administración de Documentos e integrante del Comité de Transparencia
(RÚBRICA)

Mtro. Jesús Antonio Tobías Cruz
Contralor General e integrante del Comité de Transparencia
(RÚBRICA)

Mtra. Lilibeth Álvarez Rodríguez
Jefa de la Unidad de Transparencia e integrante del Comité de Transparencia
(RÚBRICA)

Mtra. Mayra Elizabeth López Hernández
Directora Jurídico Consultiva e integrante del Comité de Transparencia
(RÚBRICA)

Lic. Georgette Ruíz Rodríguez
Oficial de Protección de Datos Personales
(RÚBRICA)