DOCUMENTO DE SEGURIDAD DE SISTEMAS Y BASES DE DATOS PERSONALES

Área Responsable: _____

(Se deberá agregar el área administradora de Sistemas y/o Bases de Datos Personales)

Sistemas y/o Bases de Datos Personales administrados por el área: *(En este apartado deberán enlistarse todos los sistemas y/o bases de datos que están en poder del área)* *1._____* *2._____*	
Sujeto Obligado.	Instituto Electoral del Estado de México
Nombre del Administrador. Cargo. Área de adscripción.	*(En este apartado deberá anotarse el nombre del titular del área).* *(En este apartado deberá anotarse el cargo del titular del área).* *(En este apartado deberá anotarse la adscripción del área).*
Funciones y Obligaciones del Responsable (administrador), encargado o encargados y todas las personas que traten datos personales.	*(En este apartado se precisarán, conforme al Código Electoral del Estado de México, el Manual de Organización, el Reglamento Interno del Instituto Electoral del Estado de México y en su caso, la legislación específica aplicable, las funciones y obligaciones que corresponden al administrador, a los encargados, así como a todas las personas que traten datos personales contenidos en los Sistemas y/o Bases de Datos, con un nivel de básico a alto de protección del área o unidad administrativa que corresponda).*
Folio del registro del sistema y base de datos.	*(En este apartado se precisarán el número o números de registro de cédula en el INTRANET del INFOEM por sistema y/o bases de datos en poder del área)*.
El inventario o la especificación detallada del tipo de datos personales contenidos.	*(En este apartado deberán precisarse o enlistarse los datos personales que se encuentran en tratamiento por sistema y/o base de datos).*
La estructura y descripción de los sistemas y bases de datos personales, las cuales consisten en	*(En este apartado deberá precisarse por cada sistema y/o base de datos personales en poder del área si el soporte es en forma física, electrónica o ambas).*

precisar y describir el tipo de soporte, así como las características del lugar donde se resguardan.	*(Se describirá el soporte en el que se encuentran los datos, por ejemplo, para soportes físicos podrían ser entre otros, documentos o expedientes y para soportes electrónicos, hojas de cálculo).*
	(Se deberán precisar por cada uno de los sistemas y/o bases de datos personales las características del lugar donde se resguardan los datos personales dependiendo si se trata de un soporte físico o electrónico).
MEDIDAS DE SEGURIDAD IMPLEMENTADAS	
Transferencia y remisiones.	*(Se deberán precisar por cada uno de los sistemas y/o bases de datos personales las transferencias que en su caso se realicen de los datos personales, así como los destinatarios de los mismos).*
Resguardo de soportes físicos y electrónicos.	*(Se deberán señalar las medidas de seguridad para el resguardo de los soportes físicos y electrónicos de los sistemas y/o bases de datos personales para evitar la alteración, pérdida o accesos no autorizados a los mismos).*
Bitácoras para accesos, operación cotidiana y violaciones a la seguridad de los datos personales.	(*Se deberán especificar todos los elementos que se encuentran contenidos en las bitácoras de acceso, operación cotidiana y violaciones a la seguridad de los datos personales, elaboradas por las áreas. De igual manera se deberá señalar quien es el servidor público(a) responsable de llevar el control de acceso por sistemas y/o bases de datos personales en poder del área).*
El análisis de riesgos.	*(En este apartado el área deberá agregar de manera sintetizada por cada sistema y/o bases de datos personales que obran en su poder, los riesgos detectados respecto a la seguridad de los datos personales y los recursos involucrados en su tratamiento a partir de las medidas de seguridad implementadas).*
El análisis de brecha.	*(En este apartado se deberán anotar de manera sintetizada los resultados del análisis de la comparación realizada por el área de las medidas de seguridad existentes contra las faltantes, de acuerdo con el tipo y nivel de seguridad aplicable a los sistemas y/o bases de datos personales de conformidad con lo establecido en el artículo 44 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios).*
Gestión de incidentes.	*(En este apartado se deberán describir los mecanismos, políticas y controles de seguridad que se deberán tomar en caso de que ocurra un incidente de seguridad. Dicho apartado aplica a los sistemas y/o bases de datos personales con un nivel de básico a alto de protección).*

Acceso a las instalaciones.	*(Se deberá especificar quiénes están expresamente autorizados para ingresar a las instalaciones donde se encuentren los sistemas y/o bases de datos personales, ya sea en soporte físico o electrónico. Este apartado aplica a los sistemas y/o bases de datos personales con un nivel de básico a alto de protección).*
Identificación y autenticación.	*(Se establecerá el procedimiento que permita la correcta identificación y autenticación, de forma inequívoca y personalizada, para ello se deberá agregar una relación actualizada por sistemas y/o bases de datos personales en posesión de los servidores públicos que tengan acceso autorizado conforme a sus facultades, competencias y funciones. Este apartado aplica a los sistemas y/o bases de datos personales con un nivel básico a alto de protección).*
Procedimientos de respaldo y recuperación de datos.	*(Se deberán describir los mecanismos para la realización de copias de respaldo y recuperación de datos personales.* *En caso de que los datos personales se encuentren en soporte físico se procurará que el respaldo se efectúe mediante la digitalización de los documentos.* *Cuando los datos personales se encuentren en soporte electrónico se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida involuntaria o destrucción accidental. Este apartado aplica a los sistemas y/o bases de datos personales con un nivel básico a alto de protección).*
Plan de contingencia.	*(Se deberá agregar la siguiente leyenda:* *"Se establecerá el conjunto de procedimientos alternativos a seguir en caso de que exista una violación a la seguridad de los datos personales, así como las acciones que serán definidas en el plan de contingencia institucional").*
Auditorías.	*(Se deberá agregar la siguiente leyenda en los sistemas y/o bases de datos personales de nivel medio y alto de protección:* *"Las medidas de seguridad implementadas a los sistemas y/o bases de datos personales, se sujetarán a una auditoría*

	por parte de la Contraloría General para verificar el cumplimiento de la ley". *En los sistemas y/o bases de datos personales de nivel básico de protección se deberá agregar la siguiente leyenda: "No aplica").*
Supresión y borrado seguro de datos.	*(Se precisarán por sistema y/o bases de datos personales los mecanismos para la supresión y borrado seguro de los datos personales una vez que se haya cumplido con la finalidad de su utilización.* *Nota: La áreas deberán tomar en consideración si la normatividad en materia electoral prevé reglas específicas para la destrucción de algún tipo de documento que contenga datos personales, ejemplo "listado nominal").*
El plan de trabajo.	*(Se deberá agregar la siguiente leyenda:* *"En caso de violación a la seguridad de los datos personales se aplicarán las acciones preventivas y correctivas a seguir para adecuar las medidas de seguridad y el tratamiento de los datos personales establecidos en el plan de trabajo si fuese el caso, a efecto de evitar que la violación se repita").*
Los mecanismos de monitoreo y revisión de las medidas de seguridad.	*(Se precisarán los mecanismos para monitorear y revisar de manera periódica las medidas de seguridad implementadas por el área, así como las amenazas y vulnerabilidades a las que están sujetos los datos personales contenidos en los sistemas y/o bases de datos personales).*
El programa general de capacitación.	*(Se deberá agregar la siguiente leyenda:* *"El personal será capacitado de manera permanente en coordinación con la Unidad de Transparencia conforme al programa anual de actividades aprobado por el Consejo General del IEEM").*