SISTEMA DE GESTIÓN DE SEGURIDAD DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO ELECTORAL DEL ESTADO DE MÉXICO

PROCEDIMIENTO DE ANÁLISIS DE RIESGOS Y BRECHA

ÍNDICE

1. Términos y definiciones

Activos: Serán considerados activos los datos personales a los que el Instituto Electoral del Estado de México en ejercicio de sus atribuciones da tratamiento, ejemplo, datos de identificación, patrimoniales, académicos, laborales, etc.

También serán activos aquellos elementos valiosos y necesarios que contribuyan para que el Instituto Electoral del Estado de México proteja, conserve los datos personales y cumpla con las obligaciones en la materia, ejemplo, archivero y llave donde se resguardan los datos personales.

Administrador (a): Titular de área o en su caso, encargado (a) de despacho u oficina que decide sobre el tratamiento, que tiene bajo su responsabilidad Sistemas y/o Bases de Datos Personales y que también tiene el carácter de responsable del riesgo.

Alta Dirección: Comité de Transparencia del Instituto Electoral del Estado de México.

Amenaza: Causa potencial de un percance no deseado que puede dar origen a incidentes o violaciones a la seguridad de los datos personales.

Análisis de brecha: Análisis comparativo de las medidas de seguridad existentes contra las faltantes.

Análisis de riesgos: Proceso que permite realizar la evaluación y gestión de riesgos, así como implementar las medidas de seguridad necesarias para proteger los activos.

Áreas: Direcciones y Unidades Administrativas del Instituto Electoral del Estado de México que en cumplimiento de sus atribuciones administran Sistemas y/o Bases de Datos Personales o establecen comunicaciones internas de datos personales.

Base de Datos: Conjunto de archivos, registros, ficheros, condicionados a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento, organización y acceso.

Categoría de datos personales: Clasificación de datos personales que se realiza conforme a su propia naturaleza, por ejemplo, el nombre de una persona es un dato de identificación.

Comunicación interna: Comunicación de datos personales que se realiza entre las áreas del Instituto Electoral del Estado de México para el cumplimiento de sus funciones.

Confidencialidad: Implica que la información no se ponga a disposición, ni sea revelada a individuos, entidades o procesos no autorizados, aún después de cumplida su finalidad.

Datos personales: Cualquier información personal concerniente a una persona identificada o identificable, establecida en cualquier formato o modalidad, y que esté almacenada en los Sistemas y/o Bases de Datos.

Destinatario (a): Persona a quien el Instituto Electoral del Estado de México transfiere datos personales para el cumplimiento de sus atribuciones.

Disponibilidad: Implica que los activos sean accesibles y utilizables para las personas o entidades autorizadas, cuando éstas así lo requieran.

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad adoptadas por el IEEM para garantizar la confidencialidad, integridad y disponibilidad de la información contenida en los Sistemas y/o Bases de Datos Personales.

Encargado (a): Persona que trata datos personales a nombre y por cuenta del Instituto Electoral del Estado de México.

Escenario de riesgo: Descripción de una amenaza que deriva de una vulnerabilidad determinada o un conjunto de vulnerabilidades que ponen en riesgo los activos.

Evaluación del riesgo: Es el procedimiento de identificación, análisis, valoración, tratamiento, seguimiento y revisión del riesgo.

IEEM: Instituto Electoral del Estado de México.

Impacto: Medida del grado de daño sobre el activo derivado de la materialización de una amenaza.

Impacto legal: Es el efecto negativo que implica un incumplimiento legal.

Impacto financiero: Es el efecto negativo que implica la pérdida o daño de recursos financieros, materiales, humanos y tecnológicos.

Incidentes. Hechos o eventos inesperados en el que una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades y que compromete o puede comprometer la seguridad de los datos personales contenidos en Sistemas y/o Bases de Datos Personales.

Integridad: Implica no alterar los activos de manera no autorizada, así como salvaguardar su exactitud y estado completo.

Medidas de seguridad: Acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger a los activos.

Nivel de seguridad: Nivel asignado conforme a la categoría a la que pertenecen los datos personales a los que se da tratamiento, el cual puede ser básico, medio o alto.

Probabilidad: Posibilidad de que se materialice una amenaza originando incidentes o violaciones a la seguridad de los datos personales.

Plan de trabajo: Plan para la implementación de las medidas de seguridad faltantes, así como de las medidas para el cumplimiento de las políticas de gestión y tratamiento de datos personales.

Plan de tratamiento de riesgos: Plan en el que se establece y justifican las estrategias que se seleccionan para tratar los riesgos.

Responsable del activo: Persona o personas que tienen a su cargo y/o resguardo uno o más activos.

Responsable en materia de seguridad: Servidoras y servidores públicos (as) electorales que tienen como función principal atender y vigilar el cumplimiento de las medidas de seguridad establecidas por quienes funjan como administradores, además de las previstas en el artículo 96 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.

Riesgo: Es la probabilidad o posibilidad de que un evento desfavorable ocurra. Tiene un impacto negativo si se materializa.

Riesgo potencial: Valoración de riesgo obtenida cuando se realizan por primera vez los análisis de riesgos.

Riesgo residual: Es el riesgo remanente que se obtiene después de calcular el riesgo potencial y hasta que se alcanza un nivel aceptable de riesgo.

Severidad del impacto: Es la evaluación del efecto y consecuencia de que una amenaza se materialice.

Sistema de Datos Personales: Datos personales contenidos en los archivos del Instituto Electoral del Estado de México que pueden comprender el tratamiento de una o diversas bases de datos para el cumplimiento de una o más finalidades.

Sistema de Gestión: Sistema de Gestión de Seguridad de Protección de Datos Personales del Instituto Electoral del Estado de México.

Titular: Persona física a la que pertenecen los datos personales objeto de tratamiento.

Transferencia: Comunicación de datos personales que el Instituto Electoral del Estado de México realiza a personas distintas de la o el titular o encargado (a).

Tratamiento: Obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Usuarias y/o usuarios: Servidoras y servidores públicos autorizados para tratar los datos personales.

Valor inherente: Valor que se encuentra determinado por la categoría a la que pertenecen los datos personales a los que se les da tratamiento.

Valor por tipo de dato: Se encuentra determinado por el valor inherente de los datos personales a los que se da tratamiento y el número de sus titulares.

Valor por tipo de entorno: Valor determinado por el tipo de entorno mediante el cual se puede acceder o hacer uso no autorizado de los datos personales que se tratan.

Violaciones a la seguridad de los datos personales: Hechos o eventos que en cualquier fase del tratamiento afectan directamente a los datos personales contenidos Sistemas y/o Bases de Datos Personales.

De manera enunciativa más no limitativa, conforme al artículo 38 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 52 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, son la pérdida, robo, extravío; copia o destrucción no autorizada; acceso, uso o tratamiento no autorizado; daño, alteración o modificación no autorizada; así como cualquier otra que afecte la confidencialidad, integridad y disponibilidad de los datos personales.

Vulnerabilidad: Debilidad o fallo que podría originar la materialización de una amenaza.

2. Presentación

Los artículos 6, apartado A, fracción II de la Constitución Política de los Estados Unidos Mexicanos, así como 5, fracción II de la Constitución Política del Estado Libre y Soberano de México, señalan que la información que se refiere a la vida privada y los datos personales debe ser protegida.

Por otra parte, el artículo 16 segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos, establece que toda persona tiene derecho a la protección de sus datos personales.

De este modo, el Instituto Electoral del Estado de México, debe realizar diversas acciones con el objeto de proteger los datos personales que con motivo de sus atribuciones da tratamiento y se encuentran almacenados en Sistemas y/o Bases de Datos Personales.

En este sentido, conforme a lo dispuesto en los artículos 31, 34 y 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como 38, 47 y 48 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, es deber de este órgano electoral adoptar, establecer y mantener medidas de seguridad, las cuales deben estar contenidas en un Sistema de Gestión de Protección de Datos y en los documentos de seguridad de los Sistemas y/o Bases de Datos Personales.

Para tal efecto y en observancia a los artículos 33, fracciones IV, V, VI y VII; 35, fracciones III, IV, V, V de la citada Ley General de Protección de Datos Personales, 46 fracciones IV, V, VI y VII; 49, fracción II, incisos d), e), m) y n) de la Ley Protección de Datos Personales del Estado, se deben realizar análisis de riesgos de los activos que son datos personales y se encuentran almacenados en Sistemas y/o Bases de Datos Personales, así como de aquellos que son indispensables para protegerlos y cumplir con las obligaciones en la materia.

De igual manera, se debe efectuar análisis de brecha para comparar las medidas de seguridad existentes contra las que falten por implementarse, y así lograr una mejora continua en el tratamiento y la seguridad de los datos personales contenidos en Sistemas y/o Bases de Datos Personales.

Asimismo, este órgano electoral debe elaborar un plan de trabajo en el que se establezcan las medidas de seguridad que falten por implementarse, así como las necesarias para el cumplimiento de las políticas de tratamiento de datos personales.

Por otra parte, las medidas de seguridad deben ser monitoreadas periódicamente junto con las amenazas y vulnerabilidades a las que estén expuestos los activos y una vez realizadas dichas acciones, se deben incluir en los documentos de seguridad de los Sistemas y/o Bases de Datos Personales.

Derivado de ello y a fin de orientar a las áreas que dan tratamiento a datos personales contenidos en Sistemas y/o Bases de Datos Personales para el cumplimiento de los principios, deberes, así como de las obligaciones que derivan de la normatividad en la materia, se expide el Procedimiento de análisis de riesgos y brecha.

3. Alcance

El alcance del presente Procedimiento está orientado a proteger los datos personales que el IEEM, con motivo del ejercicio de sus atribuciones normativas, da tratamiento y se encuentran contenidos en Sistemas y/o Bases de Datos Personales.

4. Objetivos

- Identificar, describir y evaluar los escenarios que podrían poner en riesgo a los datos personales.

- Identificar, describir y evaluar los escenarios que podrían poner en riesgo a los activos que sean necesarios para proteger y conservar los datos personales.

- Realizar análisis de brecha con el objeto de identificar las medidas de seguridad con las que se cuenta, así como para implementar las que sean necesarias para tratar los riesgos y proteger los activos.

5. Marco Legal

- Constitución Política de los Estados Unidos Mexicanos.
- Constitución Política del Estado Libre y Soberano de México.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

6. Referencias normativas en estándares de calidad

- ISO/IEC 27001:2013. Tecnología de la Información-Técnicas de Seguridad-Sistemas de Gestión de Seguridad de la Información-Requerimientos.
- ISO/IEC 27000:2018 Sistemas de Gestión de Seguridad de la Información y vocabulario.
- ISO/IEC 27005. Gestión de riesgos de seguridad de la información.
- ISO 31000:2018. Gestión del Riesgo-Directrices.

7. Otras referencias

- Metodología de Análisis de Riesgo BAA, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- Metodología de análisis de riesgo según ISO 27005:2018 e ISO 31000:2018.
- Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo, emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- Catálogo de medidas de seguridad que los sujetos obligados pueden considerar para la protección y seguridad de los datos personales tratados, del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Puebla.
- Electropedia de IEC: disponible en http://www.electropedia.org.

8. Descripción general del procedimiento de análisis de riesgos y brecha.

a) Alta Dirección.

En el desarrollo del presente procedimiento se contará con una Alta Dirección encargada de coordinar las acciones que resulten necesarias para proteger los datos personales contenidos en Sistemas y/o Bases de Datos Personales.

b) Análisis de riesgos y brecha internos.

Los análisis de riesgos y brecha se deben llevar a cabo de manera sistemática, mediante la realización de reuniones, por Sistema o Base de Datos y tipo de soporte, basándose en la información que proporcione quien funja como administrador (a)[1], su representante, usuario (a), responsable en materia de seguridad, o en su caso, responsable del activo.

Para tal efecto, en los Sistemas y/o Bases de Datos Personales con un nivel de seguridad medio o alto, la o el administrador (a), se apoyará de una o un responsable en materia de seguridad.

En el caso de que los Sistemas y/o Bases de Datos Personales tengan un nivel de seguridad básico, quien funja como administrador (a) se apoyará de una usuaria o un usuario para los efectos señalados en el párrafo que antecede.

En las reuniones de análisis de riesgos y brecha, deberá estar presente una o un representante de la Unidad de Transparencia, la Subdirección de Administración de Documentos y la Unidad de Informática y Estadística.

También podrá asistir quien funja como jefe (a) de la Unidad de Transparencia, y si así lo determina ésta (e), personal de apoyo adscrito a dicha área.

Por otra parte, se podrá nombrar a un (a) representante para que supla a la o el administrador en sus ausencias, el cual deberá tener un nivel de mando medio o superior para la toma de decisiones y fungir como usuario (a).

Excepcionalmente y sólo en caso de que ninguna persona usuaria tenga un nivel de mando medio o superior, se podrá nombrar a una o un usuario (a) con nivel operativo.

[1] La o el administrador (a) podrá realizar requerimientos a quien funja como encargado (a) o con las áreas con las que se establezcan comunicaciones internas en cualquier etapa del procedimiento de análisis de riesgos y brecha.

Al finalizar las reuniones, se elaborarán minutas por duplicado que contendrán como mínimo los datos de tiempo, modo y lugar de los hechos, la firma de quienes estuvieron presentes, la descripción del proceso completo de cada una de las etapas, así como los anexos del presente Procedimiento que sean requisitados.

De este modo, la Unidad de Transparencia le proporcionará a la o el administrador (a) una de las dos minutas junto con sus anexos para su resguardo y con el objeto de que elabore un informe ejecutivo que deberá enviar por escrito a dicha Unidad para que esta a su vez se lo remita a la Alta Dirección.

La Unidad de Transparencia resguardará la otra de las dos minutas que se elaboren al finalizar las reuniones sin anexos y cuando derivado de sus atribuciones requiera consultarlos, podrá solicitárselo a quienes funjan como administradores (as).

Excepcionalmente, cuando la o el administrador (a) no asista a las reuniones, las minutas no contendrán los anexos que se hayan requisitado y su representante se los deberá remitir para que realice la revisión y validación correspondiente.

Una vez que la o el administrador (a) valide y firme los anexos, se le informará a la Unidad de Transparencia y se elaborará una minuta en la que se incorporarán.

Si derivado de la revisión se realizan ajustes a los anexos, se le deberá informar por oficio a la Unidad de Transparencia, con el objeto de que se programen las reuniones necesarias para que se efectúen las verificaciones correspondientes.

Cuando se lleven a cabo las verificaciones, se adjuntarán a la minuta los anexos que de origen se elaboraron, así como a los que se les hicieron los ajustes.

c) Análisis de riesgos y brecha cuando se realicen comunicaciones internas.

En caso de que derivado de las atribuciones de las áreas resulte necesario realizar comunicaciones internas con otras áreas, quien funja como administrador (a) les informará que los datos personales forman parte de Sistemas y/o Bases de Datos Personales.

De esta manera, las áreas con las que se realicen comunicaciones internas, deberán ejecutar las acciones necesarias para proteger los datos personales a los que tengan acceso y evitar que se materialicen amenazas que den origen a incidentes y violaciones a la seguridad de los datos personales.

De este modo, los riesgos que se identifiquen en los análisis de riesgos y brecha, podrán ser transferidos en parte a las áreas con las que se realicen comunicaciones internas.

d) Análisis de riesgos y brecha cuando se cuente con encargado (a).

El Instituto Electoral del Estado de México, a través de la o el administrador (a) de los Sistemas y Bases de Datos Personales, le especificará a quien funja como encargado (a) las condiciones sobre las cuales se realizará el tratamiento de los datos personales, el nivel de protección requerido y la implementación de las medidas de seguridad, no obstante, la o el encargado (a) será responsable de realizar internamente sus análisis de riesgos y brecha y lo deberá informar periódicamente a la o el administrador (a).

e) Análisis de riesgos y brecha cuando se realicen transferencias.

Además de las y los administradores (as), quienes funjan como destinatarios (as) son responsables de realizar en el ámbito de su competencia los análisis de riesgos y brecha de los datos personales que se les transfieran, para así protegerlos y garantizar su confidencialidad.

8.1 Roles y responsabilidades.

ROLES	RESPONSABILIDADES COMUNES
Administrador (a)	a) Asistir a las reuniones de análisis de riesgos y brecha.
Representante de la o el administrador	

ROLES	RESPONSABILIDADES COMUNES
Responsable en materia de seguridad de Sistemas y/o Bases de Datos Personales con nivel medio o alto. **Usuario o usuaria de Sistemas y/o Bases de Datos Personales con nivel de seguridad básico.**	Quien funja como representante, sólo asistirá en suplencia de la o el administrador (a). b) Proporcionar la información que se requiera para realizar los análisis de riesgos y brecha. c) Firmar las minutas y los anexos de las reuniones a las que asistan. d) Identificar los activos, su ubicación y a quienes funjan como responsables de los activos. e) Calcular el impacto legal y financiero (valoración de los activos). f) Calcular el valor inherente, por tipo de dato y tipo de entorno (valoración de los activos). g) Identificar las amenazas que podrían materializarse y las causas que podrían generarlas. h) Calcular la probabilidad u ocurrencia de que se materialice una amenaza. j) Calcular la severidad del impacto. k) Calcular el riesgo potencial. l) Identificar los niveles de riesgo. m) Identificar las medidas de seguridad implementadas y faltantes. n) Evaluar la efectividad de las medidas de seguridad.

ROLES	RESPONSABILIDADES COMUNES
	ñ) Revisar el funcionamiento y el estado en el que se encuentran las medidas de seguridad. o) Calcular el riesgo residual.
Representante de la Subdirección de Administración de Documentos	a) Asistir a las reuniones de análisis de riesgos y brecha.
Representante de la Unidad de Informática y Estadística	b) Firmar las minutas de las reuniones a las que asistan.
Representante de la Unidad de Transparencia	c) Emitir opiniones y brindar asesorías en el ámbito de sus atribuciones, a quienes funjan como administradores (as), responsables en materia de seguridad o usuarios (as).

ROLES	RESPONSABILIDADES ESPECÍFICAS
Comité de Transparencia (Alta Dirección)	a) Coordinar acciones para garantizar la protección de los datos personales que con motivo del ejercicio de las atribuciones normativas del IEEM, se da tratamiento y se encuentran contenidos en Sistemas y/o Bases de Datos Personales. b) Aprobar los documentos de seguridad y sus actualizaciones.
Unidad de Transparencia	a) Programar reuniones para realizar análisis de riesgos y brecha.

ROLES	RESPONSABILIDADES ESPECÍFICAS
	b) Programar reuniones para la verificación de los ajustes realizados a los anexos que remita el representante a la o el administrador (a). c) Elaborar por duplicado minutas cuando: - Concluyan las reuniones de análisis de riesgos y brecha. - Quien funja como responsable en materia de seguridad o usuario (o) le entregue los anexos que haya validado y firmado quien funja como administrador (a). - La Unidad de Transparencia proporcione el ID, la clase y tipo de activo a quien funja como administrador (a) y se concluya el anexo 1. d) Proporcionar a las o los administradores (as) una de las dos minutas junto con los anexos originales firmados, si es que en las reuniones fueron requisitados. e) Resguardar las minutas restantes sin anexos que se elaboren al finalizar las reuniones. f) Acceder a los anexos de las minutas con previa autorización de las o los administradores (as) cuando derivado de sus atribuciones sea necesario consultarlos. g) Adicionar a los referentes 1, 2 o 3 los activos, las amenazas, causas o medidas

ROLES	RESPONSABILIDADES ESPECÍFICAS
	de seguridad que las áreas identifiquen y no se encuentren incorporadas. h) Determinar la categoría a la que pertenecen los datos personales que no se encuentren en el referente 1. i) Realizar la incorporación de los datos personales que no se encuentren en el anexo 1 a la tabla de "valor inherente" del numeral 10.3, inciso b) del presente Procedimiento. j) Asignar y proporcionar por oficio, tarjeta o correo electrónico a la o el administrador (a) el ID, la clase y tipo asignado a los activos que se identifiquen e incorporen al referente 1. k) Informar a quien funja como administrador (a) sobre la categoría a la que pertenezcan los datos personales que no se encuentren en el referente 1.
Administrador (a)	a) Designar por oficio, tarjeta o correo electrónico a una persona que funja como responsable en materia de seguridad o usuaria (o), a efecto de que: - La (o) apoye en las reuniones de análisis de riesgos y brecha. b) Designar por oficio, tarjeta o correo electrónico a una o un representante para que la o lo supla en sus ausencias cuando

ROLES	RESPONSABILIDADES ESPECÍFICAS
	se efectúen las reuniones de análisis de riesgos y brecha. c) Realizar los requerimientos que considere necesarios a quien funja como encargado (a) o a las áreas con las que se realizan comunicaciones internas durante el desarrollo de los análisis de riesgos y brecha. d) Revisar y en su caso, validar los anexos que le remita su representante. e) Informar por oficio a la Unidad de Transparencia cuando valide y firme los anexos en caso de no haber asistido a la reunión de análisis de riesgos. f) Informar por oficio a la Unidad de Transparencia si se realizan ajustes a los anexos que le remita su representante. g) Autorizar el acceso a la Unidad de Transparencia de los anexos de las minutas que resguarde quien funja como responsable en materia de seguridad o usuario (a). h) Cuando se realicen comunicaciones internas, informar por escrito que los datos personales se encuentran contenidos en Sistemas y/o Bases de Datos Personales. i) Informar a quien funja como encargado (a) respecto al tratamiento de los datos personales, el nivel de protección requerido

ROLES	RESPONSABILIDADES ESPECÍFICAS
	y la implementación de medidas de seguridad. j) Informar por oficio a la Unidad de Transparencia sobre los activos, las amenazas, causas o medidas de seguridad que no se encuentren en los referentes 1, 2 o 3. k) Informar por oficio a la Unidad de Transparencia sobre los activos que se pierdan, modifiquen, eliminen, incorporen o deterioren para que se agenden nuevas reuniones de análisis de riesgos y brecha. l) Mantener actualizados los inventarios de activos. m) Seleccionar y justificar la elección de las estrategias que se implementen para el tratamiento de riesgos (plan de tratamiento de riesgos). n) En el caso de que haya aceptado el riesgo, deberá informar por oficio a la Unidad de Transparencia cuando cuente con los recursos necesarios para implementar medidas de seguridad correspondientes, a efecto de que se agenden las reuniones respectivas para realizar los análisis de riesgos y brecha. ñ) Ejecutar las acciones para tratar los riesgos. o) Notificar por oficio, tarjeta o correo electrónico a quien funja como encargado,

ROLES	RESPONSABILIDADES ESPECÍFICAS
	así como a las áreas o terceros que tienen acceso a los datos personales (a) cuando se seleccione como estrategia “transmitir el riesgo”. p) Informar por oficio, tarjeta o correo electrónico a la o el destinatario (a) sobre su responsabilidad en la protección de los datos personales que le sean transferidos. q) Implementar las acciones que deriven del Plan de tratamiento de riesgos y el análisis de brecha. r) Seleccionar y justificar la elección de las medidas de seguridad que se vayan a implementar para el tratamiento de riesgos, las actividades, los recursos involucrados, periodos de ejecución (plan de trabajo). s) Realizar gestiones por oficio, tarjeta o correo electrónico para la implementación, incorporación o actualización de las medidas de seguridad, aún y cuando se acepte el riesgo. t) Atender y vigilar el funcionamiento y cumplimiento de las medidas de seguridad. u) Actualizar los documentos de seguridad de los Sistemas y/o Bases de Datos Personales que administre. v) Monitorear y revisar los activos, las medidas de seguridad así como las amenazas y vulnerabilidades a las que estén expuestos los activos.

ROLES	RESPONSABILIDADES ESPECÍFICAS
	Para tal efecto, podrá apoyarse de quien funja como responsable en materia de seguridad, usuario (a) o responsable del activo. w) Fungir como responsable del riesgo. x) Elaborar y remitir por oficio a la Unidad de Transparencia el informe ejecutivo de los análisis de riesgos y brecha. En caso de que se apoye de quien funja como responsable en materia de seguridad o usuario (a), deberá revisar el informe ejecutivo y remitirlo a la Unidad de Transparencia.
Representante de la o el administrador	a) Suplir a la o el administrador (a) en sus ausencias. b) Remitir a quien funja como administrador (a) para su revisión y en su caso, validación, los anexos del presente Procedimiento que se requisiten en las reuniones a las que asista.
Responsable del activo	a) Asistir a las reuniones en las que se realice el análisis de riesgos y brecha de los activos que se encuentran a su resguardo. b) Proporcionar la información que se requiera para realizar los análisis de riesgos y brecha de los activos que se encuentran en su resguardo.

ROLES	RESPONSABILIDADES ESPECÍFICAS
	c) Podrá emitir opiniones cuando se realicen los análisis de riesgos y brecha de los activos que se encuentren en su resguardo. d) Firmar las minutas y los anexos de las reuniones a las que asistan e) Informar por escrito a la o el administrador (a) cuando haya una pérdida, robo, daño, deterioro o modificación de los activos que se encuentran a su resguardo, con el objeto de que se le dé aviso a la Unidad de Transparencia y se programen reuniones para la realización de nuevos análisis de riesgos y brecha. f) Podrá apoyar en la identificación de las medidas de seguridad implementadas y por implementar de los activos que se encuentran en su resguardo. Nota: La o el responsable del activo, podrá fungir también como administrador (a), responsable en materia de seguridad, del riesgo, usuario (a) o representante del administrador (a). Asimismo, podrá tener tal carácter alguna persona distinta a las señaladas en el párrafo anterior que tenga a su resguardo uno o más activos. g) Monitorear y revisar los activos, las medidas de seguridad, así como las amenazas y vulnerabilidades a las que

ROLES	RESPONSABILIDADES ESPECÍFICAS
	estén expuestos los activos que se encuentran a su resguardo.
Responsable en materia de seguridad de Sistemas y/o Bases de Datos Personales con nivel medio o alto.	a) Apoyar a la o el administrador (a) en las reuniones de análisis de riesgos y brecha. b) Resguardar las minutas que se generen en cada una de las reuniones de los análisis de riesgos y brecha junto con sus anexos. c) Requisitar los anexos del presente Procedimiento. d) Incorporar al listado de activos el ID, la clase y tipo de activo cuando éstos no se encuentren en el referente 1. e) Proporcionar a la Unidad de Transparencia los anexos validados y firmados por quien funja como administrador (a) para que los incorpore a las minutas. f) Proponer a la o el administrador estrategias para el tratamiento de riesgos. g) Ejecutar las acciones para tratar los riesgos h) Proponer a la o el administrador (a) las medidas de seguridad que se vayan a implementar para el tratamiento de riesgos, las actividades, los recursos involucrados, periodos de ejecución.

ROLES	RESPONSABILIDADES ESPECÍFICAS
	i) Apoyar a quien funja como administrador (a) en la atención y vigilancia del cumplimiento a las medidas de seguridad. j) Monitorear y revisar los activos, las medidas de seguridad, así como las amenazas y vulnerabilidades a las que estén expuestos los activos. k) Apoyar a quien funja como administrador (a) a elaborar el informe ejecutivo de los análisis de riesgos y brecha.
Usuario o usuaria de Sistemas y/o Bases de Datos Personales con nivel de seguridad básico.	a) Apoyar a la o el administrador (a) en las reuniones de análisis de riesgos y brecha. b) Resguardar las minutas que se generen en cada una de las reuniones de los análisis de riesgos y brecha junto con sus anexos. c) Requisitar los anexos del presente Procedimiento d) Incorporar al listado de activos el ID, la clase y tipo de activo cuando éstos no se encuentren en el referente 1. e) Proporcionar a la Unidad de Transparencia los anexos validados y firmados por quien funja como administrador (a) para que los incorpore a las minutas. f) Proponer a la o el administrador estrategias para el tratamiento de riesgos.

ROLES	RESPONSABILIDADES ESPECÍFICAS
	g) Ejecutar las acciones para tratar los riesgos h) Proponer a la o el administrador (a) las medidas de seguridad que se vayan a implementar para el tratamiento de riesgos, las actividades, los recursos involucrados, periodos de ejecución. i) Apoyar a quien funja como administrador (a) en la atención y vigilancia del cumplimiento a las medidas de seguridad. j) Monitorear y revisar los activos, las medidas de seguridad, así como las amenazas y vulnerabilidades a las que estén expuestos los activos. k) Apoyar a quien funja como administrador (a) a elaborar el informe ejecutivo de los análisis de riesgos y brecha.
Encargado (a)	a) Atender los requerimientos que le realicen quienes funjan como administradores (as), durante el desarrollo de los análisis de riesgos y brecha. b) Proteger los datos personales a los que da tratamiento, conforme a lo instruido por quien funja como administrador (a). c) Realizar internamente los análisis de riesgos y brecha de los activos a los que den tratamiento en nombre y a cuenta del Instituto Electoral del Estado de México.

ROLES	RESPONSABILIDADES ESPECÍFICAS
	d) Las demás que le confiera la normatividad aplicable.
Destinatario (a)	a) Proteger los datos personales que se le transfieran, en términos de la normatividad aplicable. b) Realizar en el ámbito de su competencia los análisis de riesgos y brecha. c) Las demás que le confiera la normatividad aplicable.
Áreas con las que se establecen comunicaciones internas.	a) Proteger los datos personales a los que tengan acceso. b) Atender los requerimientos que le realicen quienes funjan como administradores (as), durante el desarrollo de los análisis de riesgos y brecha. c) Proteger los datos personales a los que en ejercicio de sus atribuciones accedan.
Jefe (a) de la Unidad de Transparencia	a) Podrá asistir a las reuniones de análisis de riesgos y brecha. b) Firmar las minutas de las reuniones a las que asista. c) Designar por oficio, tarjeta o correo electrónico al personal de apoyo de la Unidad de Transparencia que asista a las reuniones de análisis de riesgos y brecha, si así lo determina.

ROLES	RESPONSABILIDADES ESPECÍFICAS
	d) Remitir por escrito a la Alta Dirección el "Informe de análisis de riesgos y de brecha" de las áreas administradoras de Sistemas y/o Bases de Datos Personales.
Personal de apoyo adscrito a la Unidad de Transparencia	a) Asistir a las reuniones de análisis de riesgos y brecha si así lo determina la o el Jefe (a) de la Unidad de Transparencia. b) Auxiliar a la o el representante de la Unidad de Transparencia en las reuniones de análisis de riesgos y brecha. c) Firmar las minutas de las reuniones a las que asista.

9. Etapas del análisis de riesgos y brecha.

9.1 Identificación de los activos.

La identificación de activos se realizará tomando en consideración el referente 1 del presente Procedimiento, así como la clase y tipo de activo.

Clase	Tipo
Primarios	• Datos personales. • Actividades y procedimientos.

Clase	Tipo
Secundarios	• Personas. • Hardware. • Software. • Redes. • Información. • Inmuebles. • Equipamiento auxiliar. • Mobiliario. • Servicios internos y externos.

Los activos identificados se registrarán en el listado establecido en el anexo 1 del presente Procedimiento.

Si los activos no se encuentran en el referente 1, no se adjuntará el “listado de activos” (anexo 1) a la minuta y quien funja como administrador (a), informará dicha circunstancia a la Unidad de Transparencia.

La Unidad de Transparencia realizará las gestiones correspondientes y le proporcionará a quien funja como administrador (a) el ID, la clase y el tipo de activo.

Cuando se identifiquen activos que son datos personales y no se encuentren en el referente 1, la Unidad de Transparencia también asignará la categoría a la que éstos pertenezcan para que posteriormente se realice su valoración.

Una vez que se le proporcionen dichos datos a quien funja como administrador (a), éstos se deberán adicionar al “listado de activos” y se elaborará otra minuta en la que se incorpore el anexo correspondiente.

9.2 Inventarios de activos

Identificados los activos, se elaborará un inventario por Sistema o Base de Datos Personales y tipo de soporte, conforme al anexo 2, el cual contendrá por lo menos lo siguiente:

- Nombre y tipo de soporte del Sistema o Base de Datos Personales al que están relacionados los activos.
- Área.
- ID, clase, tipo y nombre de activo.
- Ubicación.
- Nombre, cargo y firma de quien funja como administrador (a)/ responsable del riesgo.
- Nombre, cargo y firma de quien funja como representante si es que suple a la o el administrador (a).
- Nombre, cargo y firma de la o el responsable en materia de seguridad, cuando los Sistemas o Bases de Datos Personales sean de nivel medio o alto.
- Nombre, cargo y firma de la o el usuario (a), si los Sistemas o Bases de Datos Personales son de nivel básico.
- Nombre, cargo y firma de las o los responsables del activo.

9.3 Valoración de los activos

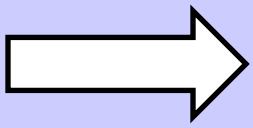
Se deberán valorar cada uno de los activos y serán registrados en el anexo número 3, conforme a los siguientes criterios:

a) Criterios de valoración de los activos que no son datos personales

- **Impacto legal y financiero**

Se deberá determinar el impacto legal y financiero que provocaría la pérdida de integridad, confidencialidad y disponibilidad generada por la falta, daño, alteración, extravío, destrucción, uso o acceso no autorizado a los activos.

Los valores se asignarán por cada activo conforme a las siguientes tablas:

<table>
<tr><th colspan="5">IMPACTO LEGAL</th></tr>
<tr><td>INTEGRIDAD (I)</td><td>1</td><td rowspan="6">  </td><td>INCUMPLIMIENTO A LOS DEBERES (ID)</td><td>1</td></tr>
<tr><td>CONFIDENCIALIDAD (C)</td><td>2</td><td>INCUMPLIMIENTO A LAS MEDIDAS DE SEGURIDAD (IMS)</td><td>1</td></tr>
<tr><td>DISPONIBILIDAD (D)</td><td>3</td><td>INCUMPLIMIENTO A LOS PRINCIPIOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES (IP)</td><td>1</td></tr>
<tr><td colspan="2" rowspan="3">En primer lugar, se deberá analizar si la falta, daño, alteración, extravío, destrucción, uso o acceso no autorizado podría provocar la pérdida de integridad, confidencialidad o disponibilidad de los activos.

Posteriormente, se deberá asignar el valor de 1 si se pierde la confidencialidad, 2 si se pierde la integridad y 3 si se pierde la disponibilidad del activo.

Cuando algún supuesto no aplique, se deberá asignar un valor de cero.

De este modo, si por ejemplo, se perdiera la integridad y disponibilidad de los activos, se deberán asignar los siguientes valores:

<table><tr><td>INTEGRIDAD (I)</td><td>1</td></tr><tr><td>CONFIDENCIALIDAD (C)</td><td>0</td></tr><tr><td>DISPONIBILIDAD (D)</td><td>3</td></tr></table></td><td>VIOLACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES (VS)</td><td>1</td></tr>
<tr><td colspan="2">En segundo lugar, si se produce la pérdida de integridad, confidencialidad o disponibilidad de los activos, se deberá determinar si ello podría conllevar o contribuir a la materialización de violaciones a la seguridad de los datos personales o a que se incumplan los deberes, principios en materia de protección de datos personales, así como las medidas de seguridad que se encuentren previstas en las Leyes General y Estatal de Protección de Datos Personales en Posesión de Sujetos Obligados.

Posteriormente, se deberá asignar el valor de 1 a los supuestos señalados en la presente tabla, si es que aplican.

Cuando algún supuesto no aplique, se deberá asignar un valor de cero.

De este modo, si por ejemplo, se perdiera la confidencialidad del activo y ésta pudiera generar algún incumplimiento a los deberes y a las medidas de seguridad, se deberán asignar los siguientes valores:</td></tr>
</table>

		INCUMPLIMIENTO A LOS DEBERES (ID) 1 **INCUMPLIMIENTO A LAS MEDIDAS DE SEGURIDAD (IMS)** 1 **INCUMPLIMIENTO A LOS PRINCIPIOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES (IP)** 0 **VIOLACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES (VS)** 0

Para calcular el impacto legal (IL) se sumarán los siguientes valores:

Integridad (I) + Confidencialidad (C) + Disponibilidad (D) + Incumplimiento a los deberes (ID) + Incumplimiento a las Medidas de Seguridad (IMS) + Incumplimiento a los principios en materia de protección de datos personales (IP) + Violaciones a la seguridad de los datos personales (VS).

IL= I+C+D+ID+IMS+IP+VS

IMPACTO FINANCIERO				
INTEGRIDAD (I)	1		**RECURSOS HUMANO (RH)**	1
CONFIDENCIALIDAD (C)	2		**RECURSOS MATERIALES (RM)**	1
DISPONIBILIDAD (D)	3		**RECURSOS FINANCIEROS (RF)**	1
En primer lugar, se deberá analizar si la falta, daño, alteración, extravío, destrucción, uso o acceso no autorizado podría provocar la pérdida de integridad, confidencialidad o disponibilidad de los activos. Posteriormente, se deberá asignar el valor de 1 si se pierde la confidencialidad, 2 si se pierde la integridad y 3 si se pierde la disponibilidad del activo. Cuando algún supuesto no aplique, se deberá asignar un valor de cero.			**RECURSOS TECNOLÓGICOS (RT)**	1
			En segundo lugar, si se produce la pérdida de integridad, confidencialidad o disponibilidad de los activos, se deberá determinar si ello podría conllevar o contribuir al daño de recursos humanos, materiales, financieros o tecnológicos. Posteriormente, se deberá asignar el valor de 1 a los supuestos señalados en la presente tabla, si es que aplican.	

<table>
<tr>
<td>De este modo, si por ejemplo, se perdiera la integridad y disponibilidad de los activos, se deberán asignar los siguientes valores:

<table><tr><td>INTEGRIDAD (I)</td><td>1</td></tr><tr><td>CONFIDENCIALIDAD (C)</td><td>0</td></tr><tr><td>DISPONIBILIDAD (D)</td><td>3</td></tr></table></td>
<td></td>
<td>Cuando algún supuesto no aplique, se deberá asignar un valor de cero.

De este modo, si por ejemplo, se perdiera la disponibilidad del activo y ésta pudiera generar algún daño a los recursos humanos y materiales con los que se cuenta, se deberán asignar los siguientes valores:
<table><tr><td>RECURSOS HUMANOS (RH)</td><td>1</td></tr><tr><td>RECURSOS MATERIALES (RM)</td><td>1</td></tr><tr><td>RECURSOS FINANCIEROS (RF)</td><td>0</td></tr><tr><td>RECURSOS TECNOLÓGICOS (RT)</td><td>0</td></tr></table></td>
</tr>
</table>

Para calcular el impacto financiero (IF) se sumarán los siguientes valores:

Integridad (I) + Confidencialidad (C) + Disponibilidad (D) + Recursos Humanos (RH) + Recursos Materiales (RM) + Recursos Financieros (RF) + Recursos Tecnológicos (RT).

IF= I+C+D+RH+ RM+ RF+ RT

En el caso de que los activos no tengan algún impacto legal o financiero, se les asignará un valor de 0 (IL=0 o IF=0)

b) Criterios de valoración de los activos que son datos personales.

- **Valor inherente.**

Se deberá identificar el valor inherente, tomando en consideración la categoría a la que pertenecen los datos personales, conforme a la siguiente tabla:

Valor inherente	Nombre del activo
Bajo	* Datos de identificación.

Medio	* Datos patrimoniales. * Datos sobre juicios, medios de impugnación y procedimientos tramitados por autoridades administrativas, jurisdiccionales o judiciales. * Datos académicos. * Datos laborales, entre otros.
Alto	* Datos personales sensibles que forman parte de la esfera más íntima de su titular cuya utilización indebida podría dar origen a discriminación, conllevarlo a un riesgo grave o revelar aspectos como: - Origen racial o étnico. - Estado de salud física o mental. - Información vinculada con el estado de salud. - Información genética. - Creencias religiosas, filosóficas y morales. - Opiniones políticas. - Preferencia sexual. * Datos de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad de conformidad con las leyes civiles. * Datos biométricos.
Los datos personales señalados en la presente tabla se enuncian de manera no limitativa. Cuando las áreas identifiquen datos personales que no se encuentren en esta tabla, deberán informarlo a la Unidad de Transparencia para que ésta a su vez, determine la categoría a la que pertenecen. También incorporará los datos personales a la presente tabla y realizará la actualización de la misma.	

En caso de que las áreas recaben datos personales que pertenezcan a diversas categorías, el valor inherente que se asignará será el que tenga un mayor nivel.

En este sentido, si, por ejemplo, se recaban datos personales de identificación y patrimoniales, el valor inherente deberá ser medio.

- **Valor por tipo de dato.**

Se deberá identificar el valor inherente, así como el número de titulares por Sistema o Base de Datos Personales y asignar un valor conforme a lo establecido en la siguiente tabla:

VALOR INHERENTE				VALOR POR TIPO DE DATO
NÚMERO DE TITULARES	Bajo	Medio	Alto	
	1 en adelante	1-5,000	1-500	2
	No aplica	5,001-50,000	501-5,000	4
	No aplica	50,001-95,000	5,001-50,000	6
	No aplica	95,001 en adelante	50,001-95,000	8
	No aplica	No aplica	95,001 en adelante	10

De esta manera, si, por ejemplo, el valor inherente es medio y se cuenta con un registro de 5,500 titulares, se deberá asignar un valor de 4.

- **Valor por tipo de entorno.**

Se deberá identificar el tipo de entorno mediante el cual se accede a los activos que son datos personales y asignar un valor de acuerdo a lo siguiente:

ENTORNO	VALOR POR TIPO DE ENTORNO
Físico	2
Red interna	4
Red inalámbrica	6
Red de terceros	8
Internet	10

En este sentido, si por ejemplo, el entorno por el cual se accede a los activos es físico, el valor debe ser 2.

En el caso de que se acceda a los activos desde diversos entornos, se deberá considerar al de mayor valor.

9.4 Identificación de las amenazas y sus causas.

Se deberán identificar por cada activo las amenazas que podrían generarles algún daño, así como las causas que las originen, tomando en consideración el referente 2.

Para tal efecto, se elaborará un listado en el que se registrarán las amenazas y causas por cada activo en términos de lo establecido en el anexo 4.

Si las amenazas o las causas que se identifiquen no se encuentran en el referente 2, se informará dicha circunstancia a la Unidad de Transparencia para que realice la incorporación respectiva.

9.5 Probabilidad u Ocurrencia

Para calcular la probabilidad u ocurrencia de que se materialice una amenaza en un escenario de riesgos, se realizarán los siguientes pasos:

1. Por cada uno de los activos se asignará un valor a los criterios que se señalan enseguida:

CRITERIO: PERSONAL AUTORIZADO (PA)

UNA PERSONA DEL ÁREA	DOS O MÁS PERSONAS DE LA MISMA ÁREA	UNA PERSONA ADSCRITA A ÁREAS DIFERENTES A LA QUE ADMINISTRA EL SITEMA O BASE DE DATOS PERSONALES	DOS O MÁS PERSONAS ADSCRITAS A ÁREAS DIFERENTES A LA QUE ADMINISTRA EL SISTEMA O BASE DE DATOS PERSONALES	PERSONAS EXTERNAS AL IEEM
1	2	3	4	5

En este apartado se deberá asignar un valor atendiendo al número de personas que se encuentran autorizadas para acceder, consultar, registrar, modificar, o actualizar el activo. En este sentido, si por ejemplo, 3 personas de una misma área tienen acceso al activo, se deberá asignar el número 2.				

CRITERIO: INTERÉS EN EL ACTIVO (IA)

NULO INTERÉS	POCO INTERÉS	INTERÉS REGULAR	INTERÉS RELEVANTE	INTERÉS DE ALTA RELEVANCIA
1	2	3	4	5
			* Cuando los activos sean datos personales, únicamente se podrán asignar los valores de 4 y 5, derivado de su propia naturaleza. * En el caso de que se trate de datos personales sensibles, el valor que se asignará será de 5.	
En este apartado se deberá asignar un valor atendiendo a la importancia que tiene el activo. De este modo, si por ejemplo, el activo es de interés relevante, se deberá asignar el número 4.				

CRITERIO: PROTECCIÓN FÍSICA O ELECTRÓNICA DEL ACTIVO (PFE)

CUENTA CON MÁS DE UNA MEDIDA DE SEGURIDAD Y ÉSTAS SE MONITOREAN PERIÓDICAMENTE.	CUENTA CON MÁS DE UNA MEDIDA DE SEGURIDAD	CUENTA SÓLO CON UNA MEDIDA DE SEGURIDAD Y ÉSTA SE MONITOREA PERIÓDICAMENTE.	CUENTA SÓLO CON UNA MEDIDA DE SEGURIDAD	NO CUENTA CON MEDIDAS DE SEGURIDAD
1	2	3	4	5
En este apartado se deberá asignar un valor atendiendo al nivel de protección con el que cuenta el activo. En este sentido, si el activo sólo tiene una medida de seguridad, se deberá asignar un valor de 4, no obstante, si no se cuenta con medidas de seguridad, se deberá asignar un valor de 5.				

CRITERIO: FRECUENCIA DE LA OCURRENCIA (FO)

IMPROBABLE (varios años)	RARA VEZ (anualmente)	POCO PROBABLE (mensualmente)	PROBABLE (semanalmente)	MUY PROBABLE (diariamente)
1	2	3	4	5

En este apartado se deberá asignar un valor atendiendo a la probabilidad de que una amenaza se materialice.
En este sentido, si hay probabilidad de que una amenaza se materialice en varios años, se deberá seleccionar "improbable".
Si es probable que la amenaza se materialice anualmente, se deberá seleccionar "rara vez".
Si es probable que la amenaza se materialice mensualmente, se deberá seleccionar "poco probable".
Si es probable que la amenaza se materialice semanalmente, se deberá seleccionar "probable".
Si es probable que la amenaza se materialice diariamente, se deberá seleccionar "muy probable".

2. Una vez determinados los valores anteriores, se deberá sumar el valor asignado al criterio de personal autorizado (PA) + el valor del interés del activo (IA) + el valor de protección física o electrónica del activo (PFE) + el valor de la frecuencia de ocurrencia (FO) y dividir entre 4, conforme a la siguiente fórmula:

Probabilidad u ocurrencia (PO)= (PA + IA +PFE + FO) ÷ 4

El valor de la probabilidad u ocurrencia podrá ser cualitativo y cuantitativo, conforme a la tabla que se muestra a continuación:

Probabilidad u ocurrencia (PO)	
Valor cuantitativo	**Valor cualitativo**
01 ≥ ≤ 2	Muy bajo
2 > ≤ 3	Bajo

3 > ≤ 4	Medio
4 > ≤ 5	Alto
Significado de los símbolos: ≥ igual o mayor ≤ igual o menor > mayor que	

3. Los valores asignados a cada uno de los criterios, así como el valor total de la probabilidad u ocurrencia, se deberán registrar en los formatos de cálculo de riesgo potencial (anexos 5 y 6), así como de riesgo residual (7 y 8).

9.6 Severidad del impacto (SI)

Se deberá calcular la severidad del impacto por cada activo y los valores se registrarán en los formatos de cálculo de riesgo potencial (anexos 5 y 6), así como de riesgo residual (7 y 8), conforme a lo siguiente:

a) Severidad del impacto de los activos que no son datos personales

Para obtener la severidad del impacto (SI) de los activos que no son datos personales, se debe realizar lo siguiente:

> Sumar el valor del impacto legal (IL) + el valor del impacto financiero (IF) y dividir entre 4, conforme a la fórmula que se señala enseguida:

$$\mathbf{SI=}\ IL+IF \div 4$$

b) Severidad del impacto de los activos que son datos personales

Para obtener la severidad del impacto (SI) de los activos que son datos personales, se debe realizar lo siguiente:

> Sumar el valor por tipo de dato (VTD) + el valor por tipo de entorno (VTE) y dividir entre 4, conforme a la fórmula siguiente:

SI= VTD+ VTE ÷ 4

9.7 Riesgo potencial (RP)

Obtenida la probabilidad u ocurrencia de la amenaza, así como la severidad del impacto, se deberá realizar el cálculo del riesgo potencial y registrarlo en el anexo 5 o 6, dependiendo si los activos son o no datos personales.

Para determinar el valor del riesgo potencial, se deberá realizar lo siguiente:

Sumar el valor de la probabilidad u ocurrencia (PO) + severidad del impacto (SI) y dividir entre 2, como se establece en la siguiente fórmula:

RP = PO+SI÷2

Cuando se calcule el riesgo residual, se deberá anotar el valor total del riesgo potencial en los anexos 7 y 8 del presente Procedimiento, según corresponda.

9.8 Niveles de riesgo

a) Identificación de los niveles de riesgo

Los niveles de riesgo se encuentran determinados por el resultado total del riesgo potencial, conforme a la siguiente tabla:

Nivel de riesgo (NR)	
Valor cuantitativo	**Valor cualitativo**
0 > ≤ 1	Muy bajo
1 > ≤ 2	Bajo
2 **>** **≤** 3	Medio
3 **>** **≤** 4	Alto

4 > ≤ 5	Muy alto
Significado de los símbolos: ≥ igual o mayor ≤ igual o menor > mayor que	

De esta manera, si por ejemplo, el resultado del riesgo potencial es igual a 1, el nivel de riesgo será muy bajo.

b) Registro de los niveles de riesgo.

Los niveles de riesgo se registrarán en los anexos 5 y 6 (cálculo de riesgo potencial), 7 y 8 (cálculo de riesgo residual), así como 9 (plan de tratamiento de riesgos) y 11 (plan de trabajo) respectivamente.

Los niveles de riesgos pueden cambiar por diversos factores como lo son:

- Incremento o decremento del valor de los activos.
- El surgimiento de nuevas amenazas.
- Cambio en el valor asignado a los criterios para calcular la probabilidad u ocurrencia.
- Deficiencia en las medidas de seguridad implementadas.
- Cambio de procesos o procedimientos internos en el tratamiento de datos personales.
- Entrada en vigor o reformas a la normatividad aplicable en materia de protección de datos personales.

9.9 Selección de estrategia para el tratamiento del riesgo.

Identificados los niveles de riesgo, se deberá elegir una estrategia para su tratamiento conforme a lo siguiente:

a) Aceptar el riesgo

El riesgo podrá aceptarse cuando:

- Los costos para la implementación de las medidas de seguridad sean mayores al valor del activo o a los recursos empleados para evitar, mitigar o transferir el riesgo.
- Los costos no estén contemplados dentro de la programación presupuestal.
- Los activos no sean datos personales.
- El nivel de riesgo sea muy bajo, siempre y cuando los activos no sean necesarios para resguardar o almacenar datos personales que formen parte de Sistemas y Bases de Datos Personales o cuando no se hayan presentado previamente incidentes o violaciones a la seguridad de los datos personales.

En el caso de que posteriormente a la aceptación del riesgo se cuente con los recursos necesarios para la implementación de las medidas de seguridad, se deberá dar aviso a la Unidad de Transparencia a efecto de que se agenden las reuniones necesarias para realizar los análisis de riesgos y brecha correspondientes.

b) Evitar el riesgo

Se podrá evitar el riesgo cuando:

- El riesgo no sea aceptable
- El nivel de riesgo sea bajo, medio o alto.
- Los activos sean datos personales almacenados en Sistemas y/o Bases de Datos Personales.
- Se trate de activos que resulten necesarios para resguardar o almacenar datos personales que formen parte de Sistemas y/o Bases de Datos Personales.
- Se hayan presentado previamente incidentes.

c) Mitigar el riesgo

Se podrá mitigar el riesgo con el objeto de reducir el impacto y los niveles de riesgo cuando:

- El riesgo no sea aceptable
- El nivel de riesgo sea muy alto.
- La probabilidad de que se materialice la amenaza en los activos que sean datos personales almacenados en Sistemas y/o Bases de Datos Personales, sea inminente.

- La probabilidad de que se materialice la amenaza sobre los activos que sean medios para resguardar o almacenar datos personales que formen parte de Sistemas y/o Bases de Datos Personales, sea inminente.
- Se hayan presentado previamente violaciones a la seguridad de los datos personales.

d) Transmitir el riesgo

Se podrá transmitir una parte del riesgo y compartirlo cuando:

- El riesgo no sea aceptable
- El activo esté en una área o lugar distinto al que se encuentra el responsable del activo.
- El Sistema y/o Base de Datos Personales cuente con encargado (a) o destinatario (a).
- Terceros tengan acceso a los datos personales.
- Se realicen comunicaciones internas con las diversas áreas.
- La normatividad en la materia así lo permita.

Las estrategias establecidas en los incisos a, b, c y d, podrán ser actualizadas ante el surgimiento de supuestos distintos a los mencionados.

De esta manera, si surge un supuesto que no esté contemplado en alguna de las presentes estrategias, se deberá dar aviso a la Unidad de Transparencia.

Lo anterior, para que se realice el análisis correspondiente, se haga la incorporación del supuesto a las estrategias señaladas en este apartado y se elabore el plan de tratamiento de riesgos.

9.10 Plan de tratamiento de riesgos.

Seleccionada la estrategia, se deberá elaborar un plan de tratamiento de riesgos conforme al anexo 9, el cual deberá contener como mínimo:

- Nombre y tipo de soporte del Sistema o Base de Datos Personales.

- Área.
- ID del activo.
- Nombre del activo.
- Nivel de riesgo.
- Estrategia seleccionada.
- Justificación de la estrategia seleccionada.

La estrategia que se seleccione también deberá registrarse en el anexo 11 del presente Procedimiento.

9.11 Acciones derivadas de las estrategias para el tratamiento de riesgos.

Cuando se seleccione como estrategia “aceptar el riesgo”, sólo se monitorearán los activos y se realizarán gestiones (trámites o solicitudes) para la implementación, incorporación o actualización de las medidas de seguridad.

En el caso de que la estrategia seleccionada para el tratamiento corresponda a “evitar el riesgo”, se implementarán, incorporarán o actualizarán medidas de seguridad para proteger los activos.

En el caso de que la estrategia seleccionada para el tratamiento corresponda a “mitigar el riesgo”, se implementarán, incorporarán o actualizarán medidas de seguridad de manera inmediata para proteger los activos.

Si se selecciona “transmitir el riesgo”, se deberá notificar a quien se le transfiera en parte el riesgo para que realice las acciones conducentes y se protejan los activos.

9.12 Análisis de brecha

Elaborado el plan de tratamiento de riesgos, se deberán identificar y registrar en el anexo 10, las medidas de seguridad implementadas y faltantes de cada activo, conforme a lo siguiente:

a) Identificación de las medidas de seguridad implementadas.

Se deberán identificar las medidas que se tengan implementadas por cada activo, tomando en consideración el referente 3 del presente Procedimiento.

b) Identificación de medidas de seguridad faltantes.

Se deberán identificar las medidas que falten por implementarse, tomando en consideración el referente 3 del presente Procedimiento.

Si las medidas de seguridad implementadas y faltantes que se identifiquen no se encuentran en el referente 3, se informará dicha circunstancia a la Unidad de Transparencia para que realice la incorporación respectiva.

9.13 Plan de trabajo (medidas de seguridad faltantes).

Para la implementación de las medidas de seguridad faltantes, se elaborará un plan de trabajo que se deberá registrar en el anexo 11 y que contendrá como mínimo:

- ID del activo.
- Nombre del activo.
- Nivel de riesgo.
- Estrategia para el tratamiento del riesgo.
- Medidas de seguridad faltantes.
- Actividades que se llevarán a cabo para implementar las medidas de seguridad faltantes.
- Recursos involucrados.
- Responsables de la implementación.
- Periodo de ejecución.
- Justificación de la implementación.

Cuando se implementen medidas de seguridad para los activos que son datos personales, se debe tomar en consideración lo siguiente:

- El valor inherente.
- La sensibilidad de los datos personales.

- El desarrollo tecnológico (si aplica).
- Las posibles consecuencias de una violación a la seguridad de los datos personales para las y los titulares.
- Las transferencias de datos personales que se realicen (si aplica).
- El número de titulares.
- Las violaciones a la seguridad previas ocurridas en los sistemas de tratamiento (si es que se han presentado).
- El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

9.14 Monitoreo y revisión de las medidas de seguridad.

Implementado el plan de trabajo, se revisará el funcionamiento, así como el estado actual en el que se encuentran las medidas de seguridad implementadas y las que se vayan a implementar por cada activo.

Para tal efecto, se deberá registrar en el anexo 12 lo siguiente:

- ID.
- Nombre del activo.
- Responsable del activo.
- Medidas de seguridad implementadas.
- Estado actual.
- Observaciones y/o comentarios.
- Responsable de la revisión.
- Fecha de la revisión.
- Nivel de efectividad.

El nivel de efectividad de las medidas de seguridad se determinará, conforme a los siguientes criterios:

EFECTIVIDAD		
CRITERIO	**NIVEL**	**PORCENTAJE**
La medida de seguridad no se encuentra en óptimas condiciones y no se han realizado gestiones para mejorarlas.	Muy bajo	20%
La medida de seguridad no está en óptimas condiciones pero se han realizado gestiones para mejorarlas.	Bajo	40%
La medida de seguridad se encuentra en óptimas condiciones.	Medio	60%
La medida de seguridad se encuentra en óptimas condiciones y existe evidencia documental de su cumplimiento.	Alto	80%
La medida de seguridad se encuentra en óptimas condiciones, existe evidencia documental de su cumplimiento y se monitorea periódicamente.	Muy alto	100%

9.15 Documento de seguridad.

Realizadas las etapas anteriores, se deberán actualizar en los documentos de seguridad aprobados por la Alta Dirección, los siguientes apartados:

- Análisis de riesgos.
- Análisis de brecha.
- Medidas de seguridad aplicables a los Sistemas y/o Bases de Datos Personales
- El plan de trabajo.
- Los mecanismos de monitoreo y revisión de las medidas de seguridad.

Cuando se calcule el riesgo residual, se volverán actualizar los apartados señalados en los documentos de seguridad.

9.16 Riesgo residual.

Una vez que se implementen las medidas de seguridad faltantes, se deberá calcular el riesgo residual por primera vez dentro de un periodo máximo de 12 meses, conforme a lo siguiente:

- **Cálculo de riesgo residual por primera vez.**

a) Se realizarán nuevamente las etapas de los análisis de riesgos y brecha desde la identificación de activos hasta la severidad del impacto.

b) Se sumará el valor de la probabilidad u ocurrencia (PO) + el valor de la severidad del impacto (SI) y se dividirá entre 2 para calcular el índice de riesgo residual (IRR):

$$IRR = PO+SI÷2$$

c) Se restará el riesgo potencial (RP) correspondiente al primer análisis de riesgos y brecha, menos el índice del riesgo residual (IRR):

$$\text{Riesgo residual (RR1)} = RP-IRR^{2}$$

d) Se identificará el nivel de riesgo conforme a lo siguiente:

Nivel de riesgo (NR)	
Valor cuantitativo	**Valor cualitativo**
0 > ≤ 1	Muy bajo
1 > ≤ 2	Bajo

[2] Únicamente se restará el riesgo potencial menos el índice de riesgo residual cuando se calcule el riesgo residual por primera vez.

2 > ≤ 3	Medio
3 > ≤ 4	Alto
4 > ≤ 5	Muy alto
Significado de los símbolos: ≥ igual o mayor ≤ igual o menor > mayor que	

Los niveles de riesgo se encuentran determinados por el resultado total del riesgo residual.

Los valores obtenidos en los incisos b), c) y d), se deberán registrar en los anexos 7 cuando los activos no sean datos personales y 8 en el caso de que si lo sean.

e) Se seleccionará la estrategia para tratar el riesgo, conforme al numeral 9.9 del presente Procedimiento.

f) Se elaborará el plan de tratamiento de riesgos, conforme al numeral 9.10 del presente Procedimiento.

g) Se realizarán las acciones derivadas de las estrategias para el tratamiento de riesgos, conforme al numeral del presente 9.11 Procedimiento.

h) Se realizará el análisis de brecha, conforme al numeral 9.12 del presente Procedimiento.

i) Se elaborará el plan de trabajo, conforme al numeral 9.13 del presente Procedimiento.

j) Se monitorearán y revisarán las medidas de seguridad, conforme al numeral 9.14 del presente Procedimiento.

k) Se actualizarán los documentos de seguridad de los Sistemas y/o Bases de Datos Personales, conforme al numeral 9.15 del presente Procedimiento.

l) Se elaborará el informe ejecutivo, establecido en el numeral 9.17 del presente Procedimiento.

- **Cálculo de riesgo residual para alcanzar un nivel de riesgo aceptable.**

Cuando los activos aún no tengan un nivel de riesgo aceptable (muy bajo), se realizarán de nueva cuenta las etapas establecidas en el inciso **a)** y se calculará el índice de riesgo residual (IRR), hasta que se alcance un nivel aceptable, conforme al inciso **b)** de la primera viñeta del numeral 9.16 del presente Procedimiento (IRR=PO+SI÷2).

De esta manera, se restará el riesgo residual (RR) obtenido en el análisis de riesgos y brecha anterior menos el índice de riesgo residual que se calcule nuevamente, como se muestra enseguida:

Riesgo residual (RR2) = RR1-IRR

Riesgo residual (RR3) = RR2-IRR

Riesgo residual (RR4) = RR3-IRR y así sucesivamente

Dichos valores se deberán registrar en el anexo 7 cuando los activos no sean datos personales y 8 en el caso de que si lo sean.

Finalmente, se deberán efectuar nuevamente las etapas señaladas en los incisos **d)**, **e)**, **f)**, **h), i), j), k) y l)** del numeral 9.16.

En este sentido, si por ejemplo, la segunda vez que se realiza el cálculo del riesgo residual RR2, se obtiene un total de 2, el nivel de riesgo sería bajo y por la tanto, se deben realizar nuevamente las etapas señaladas en la presente viñeta.

Si la tercera vez que se realiza el cálculo del riesgo residual RR3, se obtiene un total de 1, el nivel de riesgo sería muy bajo y ya no se volverían a realizar las etapas señaladas en la presente viñeta, toda vez que se alcanzaría un nivel de riesgo aceptable.

Riesgo residual	**Nivel de riesgo**	
	Valor cuantitativo	**Valor cualitativo**
RR2	2	Bajo

RR3	**1**	**Muy bajo**
Nivel de riesgo aceptable		
* Para una mejor comprensión del ejemplo señalado anteriormente, se insertó la presente tabla.		

9.17 Informe ejecutivo

Se deberá elaborar un informe ejecutivo que contenga por lo menos el resumen de cada una de las etapas del análisis de riesgos y brecha, considerando las minutas instrumentadas para tal efecto.

Una vez que se elabore dicho informe, se deberá enviar por oficio a la Unidad de Transparencia para su remisión a la Alta Dirección.

10. Aplicación, seguimiento y revisión.

Los análisis de riesgos y brecha se realizarán por lo menos cuando:

- Se apruebe la creación o modificación de Sistemas y o Bases de Datos Personales.
- Se apruebe la supresión de datos personales contenidos en Sistemas y o Bases de Datos Personales.
- Se cambien las condiciones de los activos o las personas con acceso autorizado a ellos, independientemente de que se haya aceptado el riesgo.
- Se modifiquen, roben, pierdan, eliminen o incorporen activos.
- Los activos se cambien de lugar.
- Las medidas de seguridad que se implementen, se deterioren, dañen o fallen.

En el caso de que se materialice alguno de los supuestos establecidos en las viñetas 3, 4, 5 y 6, se deberá dar aviso a la Unidad de Transparencia para que se programen nuevas reuniones de análisis de riesgos y brecha.

Por otra parte, a efecto de asegurar un debido tratamiento de los riesgos identificados, así como de reducir los niveles de riesgos hasta un nivel aceptable, se realizarán como mínimo las siguientes acciones:

- Ejecuciones periódicas de los análisis de riesgos y brecha de manera aleatoria.
- Monitoreo y revisión de los activos, medidas de seguridad, así como de las amenazas y vulnerabilidades a las que estén expuestos, independientemente del nivel de riesgo y la estrategia que se seleccione para su tratamiento.

11. Documentos relacionados

- Política de Gestión Datos Personales del IEEM.
- Políticas en materia de protección de datos personales del IEEM.
- Documento de seguridad.

12. Referentes

- Referente 1. Clasificación de activos.
- Referente 2. Amenazas y causas más comunes.
- Referente 3. Listado de medidas de seguridad más comunes.

13. Anexos

- Anexo 1. Listado de activos identificados.
- Anexo 2. Inventario de activos.
- Anexo 3. Listado de valoración de activos.
- Anexo 4. Listado de amenazas y causas.
- Anexo 5. Formato de cálculo de riesgo potencial (activos que no son datos personales).
- Anexo 6. Formato de cálculo de riesgo potencial (activos que son datos personales).
- Anexo 7. Formato de cálculo de riesgo residual (activos que no son datos personales).
- Anexo 8. Formato de cálculo de riesgo residual (activos que son datos personales).
- Anexo 9. Plan de tratamiento de riesgos.
- Anexo 10. Análisis de brecha.
- Anexo 11. Plan de trabajo.

- Anexo 12. Revisión de las medidas de seguridad.

14. CONTROL DE CAMBIOS

Número de revisión	Páginas modificadas	Descripción del cambio	Fecha de modificación
Registrar de manera consecutiva las revisiones al Procedimiento.	Señalar las páginas en las cuales se realizaron las modificaciones.	Especificar de manera concreta las modificaciones realizadas.	Anotar la fecha en que se realiza la modificación.