

Tercera Sesión Ordinaria
31 de marzo de 2026

Acuerdo de la Junta Administrativa, por el que se aprueba el Plan de Continuidad del Sistema Electrónico por Internet (SEI), perteneciente al Sistema de Gestión de Calidad Electoral del Instituto Electoral de la Ciudad de México.

A n t e c e d e n t e s

- I. El 31 de enero de 2014, en uso de las facultades que le otorga la Constitución Política de los Estados Unidos Mexicanos (Constitución Federal), el Presidente de la República promulgó la reforma constitucional en materia político-electoral, logrando una reestructuración y redistribución de funciones entre los Organismos Públicos Electorales de las entidades federativas y el Instituto Nacional Electoral (INE), al homologar los estándares con los que se organizan los procesos electorales federales y locales, garantizando así la calidad en la democracia electoral, cuyo Decreto fue publicado en el Diario Oficial de la Federación (DOF), el 10 de febrero de 2014.
- II. El 23 de mayo de 2014, se publicaron en el DOF los correspondientes Decretos por los que se expidieron la Ley General de Partidos Políticos (Ley de Partidos), y la Ley General de Instituciones y Procedimientos Electorales (Ley General), asimismo, se reformaron y adicionaron diversas disposiciones de la Ley General del Sistema de Medios de Impugnación en materia electoral, así como de la Ley Orgánica del Poder Judicial de la Federación.
- III. El 29 de enero de 2016, se publicó en el DOF el Decreto por el que se declararon reformadas y derogadas diversas disposiciones de la Constitución Federal; en materia política de la Ciudad de México, en cuyo artículo Décimo Cuarto transitorio se previó que a partir de su entrada en vigor (al día siguiente de su publicación), todas las referencias que en la Constitución Federal y demás ordenamientos jurídicos que se hagan al Distrito Federal, deberán entenderse referidas a la Ciudad de México.
- IV. El 18 de julio de 2016, se expidió la Ley General de Responsabilidades Administrativas, cuya última reforma fue publicada en el DOF el 15 de diciembre de 2025.

- V. El 14 de octubre de 2016, mediante Acuerdos JA123-16 y JA124-16, la Junta Administrativa del otrora Instituto Electoral del Distrito Federal (Junta), aprobó respectivamente, la Guía Técnica para la Elaboración de Documentos Internos (Guía Técnica), así como el Procedimiento para el control de la información documentada del Sistema de Gestión de Calidad Electoral (Procedimiento), (anteriormente denominado Procedimiento de control de documentos y registros del Sistema de Gestión Electoral), cuya última actualización, fue la aprobada por la Junta el 27 de febrero de 2026, mediante Acuerdo IECM-JA026-26.
- VI. El 5 de febrero de 2017, se publicó en la Gaceta Oficial de la Ciudad de México (Gaceta Oficial), la Constitución Política de la Ciudad de México (Constitución Local), cuya última reforma fue publicada en la Gaceta Oficial el 24 de diciembre de 2025.
- VII. El 7 de junio de 2017 se publicó en la Gaceta Oficial, el Decreto por el cual se abrogó el Código de Instituciones y Procedimientos Electorales del Distrito Federal y se expide el Código de Instituciones y Procedimientos Electorales de la Ciudad de México (Código), en el cual se estableció el cambio de denominación del Instituto Electoral del Distrito Federal por el de Instituto Electoral de la Ciudad de México (Instituto Electoral); asimismo, el 21 de junio del mismo año, se publicó en la Gaceta Oficial, una nota aclaratoria al citado Decreto, el cual ha tenido diversas modificaciones, siendo la última el 23 de diciembre de 2024.
- VIII. El 4 de agosto de 2017, el Consejo General aprobó mediante Acuerdos IECM/ACU-CG-016/2017 e IECM/ACU-CG-022/2017, respectivamente, el Reglamento Interior del Instituto Electoral de la Ciudad de México (Reglamento Interior), el Reglamento de Funcionamiento de la Junta Administrativa (Reglamento de la Junta), así como el Reglamento en Materia de Relaciones Laborales del Instituto Electoral de la Ciudad de México (Reglamento de Relaciones Laborales), con motivo de la expedición y entrada en vigor del Código.
- IX. El 31 de diciembre de 2018, se publicó en la Gaceta Oficial, el Decreto por el que se expide la Ley de Austeridad, Transparencia en Remuneraciones, Prestaciones y Ejercicio de Recursos de la Ciudad de México (Ley de Austeridad), cuya última versión fue la publicada en la Gaceta Oficial el 27 de agosto de 2025.

- X. El 22 de octubre de 2021, la Unidad Técnica de Servicios Informáticos, emitió el Plan de Continuidad del Sistema Electrónico por Internet (SEI), perteneciente al Sistema de Gestión de Calidad Electoral, el cual proporciona un panorama general del escenario, de las estrategias, acciones propuestas, recursos y requerimientos necesarios para establecer las operaciones del sistema en el menor tiempo posible.
- XI. El 1 de septiembre de 2022, en cumplimiento a lo determinado en el Decreto de Reforma al Código (del 26 de mayo de 2022), mediante Acuerdo IECM/ACU-CG-050/2022, el Consejo General, aprobó la estructura orgánica y funcional y ordenó realizar las acciones correspondientes para su implementación.
- XII. El 24 de agosto de 2023, mediante Acuerdo IECM/ACU-CG-070/2023, el Consejo General aprobó las reformas y adiciones al Reglamento Interior y al Reglamento de Sesiones del Consejo General y Comisiones del Instituto Electoral.
- XIII. El 15 de septiembre de 2024, se publicó en el DOF, el Decreto por el que se reformaron, adicionaron y derogaron diversas disposiciones de la Constitución Federal, en materia de reforma del Poder Judicial.
- XIV. El 30 de septiembre de 2024, la Junta mediante Acuerdo IECM-JA104-24, aprobó la modificación al Reglamento de Relaciones Laborales, y fue publicado en la Gaceta Oficial el 17 de octubre de 2024.
- XV. El 14 de octubre de 2024, se publicó en el DOF, el Decreto por el que se reformaron y adicionaron diversas disposiciones de la Ley General, en materia de elección de personas juzgadoras del Poder Judicial de la Federación.
- XVI. El 23 de diciembre de 2024 se publicó en la Gaceta Oficial, el Decreto por el que se reformaron, adicionaron y derogaron diversas disposiciones de la Constitución Local, Código y Ley Procesal, en materia de reforma al Poder Judicial de la Ciudad de México, en el cual, se establecieron diversas disposiciones en materia de elección popular para sus integrantes.

- XVII. El 14 de marzo de 2025, mediante Acuerdos IECM-JA039-25 e IECM-JA040-25, la Junta aprobó respectivamente, la actualización del Manual de Contabilidad Gubernamental (Manual de Contabilidad), y los Lineamientos Generales para la Supervisión, Seguimiento y Evaluación del Cumplimiento del Plan General de Desarrollo (Lineamientos), ambos de este Instituto Electoral.
- XVIII. El 14 de agosto de 2025, la Junta mediante Acuerdos IECM-JA110-25 e IECM-JA112-25, aprobó respectivamente, el Manual de Planeación del Instituto Electoral, para el ejercicio fiscal 2026, (Manual de Planeación 2026), así como la propuesta de tabuladores y remuneraciones aplicables al personal en activo, así como tabuladores y remuneraciones aplicables al personal de nuevo ingreso del Instituto Electoral, para el ejercicio fiscal 2026.
- XIX. El 12 de septiembre de 2025, la Junta mediante Acuerdo IECM-JA125-25, aprobó los Programas Institucionales para el ejercicio fiscal 2026, conforme a lo establecido en el artículo 83, fracción II del Código, así como los Programas Específicos de conformidad con lo establecido en el Manual de Planeación 2026.
- XX. El 30 de septiembre de 2025, mediante Acuerdo IECM-JA130-25, la Junta aprobó la Apertura Programática Presupuestal de Instituto Electoral, para el ejercicio fiscal 2026.
- XXI. El 28 de octubre de 2025, la Junta mediante Acuerdo IECM-JA136-25, aprobó remitir al Máximo Órgano de Dirección el Anteproyecto de Acuerdo del Consejo General, por el que se aprobaron los proyectos de Programa Operativo Anual y de Presupuesto de Egresos del Instituto Electoral para el ejercicio fiscal 2026.
- XXII. El 30 de octubre de 2025, mediante Acuerdo IECM/ACU-CG-104/2025, el Consejo General aprobó los proyectos del Programa Operativo Anual y Presupuesto de Egresos del Instituto, para el ejercicio fiscal 2026, que suma la cantidad de \$1,873,697,234.00 (mil ochocientos setenta y tres millones seiscientos noventa y siete mil doscientos treinta y cuatro pesos 00/100 M.N.).
- XXIII. El 19 de diciembre de 2025, se publicó en la Gaceta Oficial No. 1762 Tomo I, el Decreto por el que se expide el Presupuesto de Egresos de la Ciudad de México para el ejercicio

fiscal 2026, mediante el cual se asigna un presupuesto para el Instituto Electoral por la cantidad de \$1,590,000,000.00 (mil quinientos noventa millones 00/100 M.N.).

- XXIV. El 14 de enero de 2026, mediante Acuerdos IECM-JA004-26 e IECM-JA005-26, la Junta aprobó respectivamente, remitir al Máximo Órgano de Dirección el “Proyecto de Acuerdo de la Junta Administrativa por el que se aprueba remitir al Máximo Órgano de Dirección el *“Proyecto de Acuerdo del Consejo General del Instituto Electoral de la Ciudad de México, por el que se aprueba el ajuste al Programa Operativo Anual y de Presupuesto de Egresos del Instituto Electoral de la Ciudad de México para el ejercicio fiscal 2026, con base en las asignaciones autorizadas por el Congreso de la Ciudad de México, para el ejercicio fiscal 2026”*, y el *“Proyecto de Acuerdo por el que se aprueba el ajuste a los tabuladores y remuneraciones aplicables al personal en activo, así como los tabuladores y remuneraciones aplicables al personal de nuevo ingreso del Instituto Electoral de la Ciudad de México, para el ejercicio fiscal 2026”*.”
- XXV. El 15 de enero de 2026, mediante Acuerdo IECM/ACU-CG-011/2026, el Consejo General aprobó el Plan General de Desarrollo del Instituto Electoral para el periodo 2026-2029 (PGD), que presentó la Comisión Provisional encargada de elaborar la propuesta del PGD Institucional para el periodo 2026-2029, en cumplimiento al Acuerdo IECM/ACU-CG-041/2025.
- XXVI. En la misma fecha, mediante Acuerdo IECM/ACU-CG-012/2026, el Consejo General aprobó el ajuste al Programa Operativo Anual y Presupuesto de Egresos del Instituto Electoral de la Ciudad de México para el ejercicio fiscal 2026, con base en las asignaciones autorizadas por el Congreso de la Ciudad de México, para el ejercicio fiscal 2026, que asciende a la cantidad de \$1,590,000,000.00 (mil quinientos noventa millones de pesos 00/100 M.N.).
- XXVII. El 30 de enero de 2026, mediante Acuerdo IECM-JA012-26, la Junta aprobó las Normas de Racionalidad, Austeridad y Disciplina Presupuestal del Instituto Electoral, para el ejercicio fiscal 2026.
- XXVIII. El 25 de febrero de 2026, la Junta mediante Acuerdo IECM-JA021-26, aprobó el ajuste a los Programas Institucionales para el ejercicio fiscal 2026, conforme a lo establecido en el

artículo 83, fracción II del Código, así como los Programas Específicos de conformidad con lo establecido en el Manual de Planeación 2026, derivado de la entrada en vigor del PGD 2026-2029.

Considerandos

1. Que conforme a lo previsto en el artículo 37, fracción II y 81 primer párrafo del Código, el Instituto Electoral tiene en su estructura orgánica una Junta, la cual es el órgano encargado de velar por el buen desempeño y funcionamiento administrativo de los órganos del Instituto Electoral, así como de supervisar la administración de los recursos humanos, financieros y materiales.
2. Que el artículo 83, fracción I del Código, establece que la Junta tiene la atribución de aprobar los criterios generales y los procedimientos necesarios para la elaboración de los Programas Institucionales del Instituto Electoral, a propuesta de la Secretaría Administrativa.
3. Que el artículo 83, fracción XI del Código establece que la Junta tiene la atribución de emitir los lineamientos y procedimientos técnico-administrativos que se requieran para el eficiente despacho de los asuntos encomendados a cada órgano o unidad del Instituto Electoral, con base en la propuesta que le presente el área competente.
4. Que el artículo 83, fracción XX, inciso c) del Código, dispone que es atribución de la Junta, aprobar a propuesta de la Secretaría Administrativa, la aplicación de mecanismos y procedimientos de planeación operativa institucional.
5. Que de acuerdo con el artículo 87, párrafo primero del Código, la Secretaría Administrativa es el órgano ejecutivo encargado de la administración de los recursos financieros, humanos y materiales del Instituto Electoral.
6. Que el artículo 88, fracciones IV y VII, inciso a) del Código, señala que son atribuciones de la persona Titular de la Secretaría Administrativa, entre otras, aplicar las políticas, normas y procedimientos para la administración de los recursos financieros, humanos y materiales, y de control patrimonial del Instituto Electoral, así como proponer a la Junta para su

aprobación los proyectos de Procedimientos administrativos referentes a recursos financieros, humanos y materiales, servicios generales y control patrimonial.

7. Que en el apartado 6, denominado “Políticas de Operación” numeral 6.1 denominado “Generales”, del Procedimiento para el control de la información documentada del Sistema de Gestión de Calidad Electoral (Procedimiento), se establece lo siguiente:

- a) La documentación de los procesos del Sistema de Gestión de Calidad Electoral (SGCE), puede mantenerse en medio impreso o electrónico.
- b) Los documentos (incluye formatos o anexos) controlados por el SGCE serán las versiones disponibles en el repositorio documental del SGCE.
- c) La documentación de los procesos del SGCE, se documenta en idioma español.
- d) Los manuales, procedimientos, instructivos de trabajo, guías, planes, entre otros deben incluir a pie de página la leyenda “La versión vigente de este documento se encuentra en el repositorio del SGCE”.
- e) Los formatos deberán llevar, como mínimo, el número de revisión y fecha de revisión con la finalidad de tener la trazabilidad de los cambios.
- f) Los anexos que deriven de los documentos dentro del alcance del SGCE podrán llevar el número de revisión y fecha de revisión, en caso de que se considere necesario.
- g) En caso de realizar cambios en los formatos, sin que estos afecten al procedimiento, no es necesario volver a aprobar el documento por el órgano colegiado, la actualización del formato en el repositorio documental deberá solicitarse a la Jefatura de Departamento de Control de Documentos y Registro adscrita a la Subdirección de Gestión de Calidad, a través del formato SA/SGC/FR/02 (Formato de solicitud de movimientos en el repositorio del SGCE) para la actualización adjuntando el documento.
- h) Los registros generados por sistemas informáticos, así como aquellos que por la naturaleza de su contenido sea especial, no necesariamente contarán con todos los elementos de control que establece la Guía para crear y actualizar la información documentada, pudiéndose excluir en su emisión el código, la revisión, número de revisión y documento de referencia, sin embargo, para el control de estos se deberán incluir en la lista maestra y por tanto contarán con un identificador

único (código) y número de revisión correspondiente, por ejemplo: constancias de capacitación, gafetes de identificación, nombramientos.

- i) Mantener las evidencias documentadas (registros) de la siguiente manera:
 - J Legibles.
 - J Fácilmente identificables.
 - J Recuperables.
 - J Asegurar la disposición final de los registros.
- j) De las directrices marcadas en el presente procedimiento, quedan exentos los documentos regulados por el Comité Técnico Interno de Administración de Documentos (COTECIAD).
- k) Todo documento que pase a aprobación de un Órgano Colegiado (Comisiones temporales, Comités, entre otros, que impacten al SGCE o a los servicios prestados por el IECM) que le corresponda, tendrá que alinearse al SGCE y los documentos y formatos serán controlados de acuerdo con el presente procedimiento.
- l) Previo a solicitar la aprobación de la información documentada al Órgano Colegiado que corresponde (por ejemplo: Junta Administrativa) se debe enviar a la Subdirección de Gestión de Calidad para revisar que los documentos cuenten con los requisitos mínimos de la estructura documental vigente, así como la asignación de código y su registro en la lista maestra de información documentada, en caso de ser necesario, el tiempo máximo de revisión será de dos a cinco días hábiles.
- m) Una vez aprobados los documentos por el órgano colegiado que corresponda, se deberá solicitar la actualización del documento al repositorio del SGCE.
- n) La socialización y las evidencias de esta se podrán remitir a la Subdirección de Gestión de Calidad por conducto de la Jefatura de Departamento de Control de Documentos y Registro, de manera posterior a la actualización del repositorio, ya que es de suma importancia contar con la evidencia de que los cambios de la información documentada han sido comunicados a todas las personas involucradas en el proceso.
- o) Los responsables de proceso deberán mantener la información documentada vigente, actualizada y correctamente registrada en el repositorio oficial del SGCE,

asegurando que únicamente se usen versiones autorizadas con el fin de prevenir riesgos operativos, uso inadecuado de documentos y cualquier incumplimiento normativo; asimismo, deberán revisar periódicamente la información bajo su control y gestionar de manera oportuna cualquier actualización conforme a los lineamientos establecidos en el sistema de gestión.

8. Que el apartado 6.2 denominado “Creación de la Información documentada”, del Procedimiento, perteneciente al SGCE, establece que la información debe elaborarse conforme a los lineamientos establecidos en la Guía para crear y actualizar la información documentada con código SA/SGC/GI/01.
9. Que el apartado 6.3 denominado “Aprobación de la Información documentada”, del Procedimiento, perteneciente al SGCE, establece que la información deberá realizarse de acuerdo con el tipo de documento:

Tipo de documento	Responsable de la aprobación	Identificador de aprobación
<input checked="" type="checkbox"/> Manual de Calidad.	Dirección de Planeación y Recursos Financieros.	Firma autógrafa o electrónica de la persona responsable del área.
<input checked="" type="checkbox"/> Procedimientos. <input checked="" type="checkbox"/> Instructivos. <input checked="" type="checkbox"/> Manuales. <input checked="" type="checkbox"/> Estrategias. <input checked="" type="checkbox"/> Lineamientos. <input checked="" type="checkbox"/> Guías. <input checked="" type="checkbox"/> Planes.	Órgano colegiado (Junta Administrativa, Consejo General, Comisiones).	Número de Acuerdo con el que fue aprobado por el órgano colegiado Ejemplo: IECM-JAXX-AA
<input checked="" type="checkbox"/> Fichas de proceso. <input checked="" type="checkbox"/> Declaraciones de cumplimiento normativo. <input checked="" type="checkbox"/> Matriz de Gestión de Riesgo.	Persona titular del área.	Firma autógrafa o electrónica de la persona responsable del área.

10. Que el apartado 6.4 denominado “Actualización de la información documentada”, del Procedimiento, perteneciente al SGCE, establece que la revisión y/o actualización de la información documentada, deberá realizarse cuando se presente alguno de los siguientes supuestos:

- a) Cambios a la estructura orgánica que implique ajustes en la ejecución del proceso.
- b) Cuando se hayan presentado cambios en los procedimientos, derivados de la mejora de estos (nombre o codificación).
- c) Cuando existan cambios en la normatividad aplicable al proceso que implique adecuaciones o supresiones de estos.
- d) Cuando el área, después de los ejercicios de auditoría externa o interna, determine la necesidad de documentar o fortalecer alguna actividad del proceso, según las observaciones o hallazgos detectados en dichos ejercicios.
- e) La documentación que se refiere a los procesos electorales y mecanismos de participación ciudadana se **revisará al inicio de cada proceso** para asegurar la pertinencia de estos.
- f) Las modificaciones a la información documentada deberán impactar en una nueva versión del documento, la cual debe ser notificada por el responsable del área o enlace de calidad a la Jefatura de Departamento de Control de Documentos y Registro para la actualización del documento en el repositorio documental del SGCE, así como en la lista maestra de información documentada y la identificación del documento obsoleto, en este caso se procederá conforme al numeral 6.9 de la sección altas, actualizaciones y/o bajas del repositorio documental del SGCE.
- g) Con el fin de conservar el histórico de los cambios que ha sufrido un documento o formato, se deberá llevar el control de los cambios (número de revisión), como lo indica la *Guía para crear y actualizar la información documentada SA/SGC/GI/01*.

11. Que derivado de la Auditoría Interna de Calidad 2025 y, en particular, de los hallazgos identificados, se implementó la acción correctiva correspondiente a la oportunidad de mejora con folio AC-31-2005, relativa al proceso de Gestión de Tecnologías de la Información, consistente en la actualización del Plan de Continuidad del Sistema de Emisión

de la Opinión (SEI), integrante del Sistema de Gestión de Calidad Electoral, considerando los nuevos escenarios tecnológicos y operativos.

12. Que mediante oficio IECM/UTSI/104/2026 de fecha 17 de marzo de 2026, la Unidad Técnica de Servicios informáticos, sometió a consideración de la Junta para su análisis, discusión y, en su caso aprobación, el Plan de Continuidad del Sistema Electrónico por Internet (SEI) perteneciente al Sistema de Gestión de Calidad Electoral del Instituto Electoral de la Ciudad de México.
13. Que la aprobación del Plan de Continuidad del Sistema Electrónico por internet SEI, con código UTSI/PL/01, deriva de la actualización de los componentes y datos de los responsables de grupos de trabajo del SEI 2026.

El Plan de Continuidad, está diseñado bajo la norma ISO 22301:2019 para permitir al Instituto Electoral de la Ciudad de México, definir las acciones a tomar en caso de que se presente una determinada contingencia o desastre, que inhabilite la disponibilidad del Sistema Electrónico por Internet SEI, cuando se presente un ejercicio de participación ciudadana.

Adicionalmente, está estructurado para lograr los siguientes objetivos:

-)] Proveer un enfoque organizado para el manejo de las actividades de respuesta y recuperación luego de un incidente no planeado o de una interrupción prolongada del Sistema Electrónico por Internet.
 -)] Ofrecer respuestas oportunas y apropiadas, reduciendo así los impactos operativos, imagen y económicos que puede traer una interrupción del Sistema Electrónico.
14. Que el documento señalado en el considerando 12, fue elaborado dentro del marco de la Política de Gestión de Calidad, en observancia de la Guía Técnica para la Elaboración de Documentos Internos del Instituto Electoral y de conformidad con la normativa vigente y con los fines, obligaciones y compromisos establecidos en el Código.

Por lo expuesto y fundado, la Junta de conformidad en lo dispuesto por el artículo 83 fracción XI del Código, emite el siguiente:

A c u e r d o
IECM-JA042-26

PRIMERO. Se aprueba el Plan de Continuidad del Sistema Electrónico por Internet (SEI), perteneciente al Sistema de Gestión de Calidad Electoral, del Instituto Electoral de la Ciudad de México, identificado con el código UTSI/PL/01, de conformidad con el documento Anexo, el cual forma parte integral del presente Acuerdo.

SEGUNDO. El presente Acuerdo y su Anexo, entrarán en vigor al momento de su aprobación.

TERCERO. Se instruye a la Secretaría Administrativa para que mediante Circular haga del conocimiento de todo el personal del Instituto Electoral, el ajuste del documento mencionado en el punto de Acuerdo **PRIMERO**.

CUARTO. Se instruye a la Unidad Técnica de Servicios Informáticos para que elabore una infografía clara, de fácil lectura y comprensión, dirigida tanto a las áreas del Instituto Electoral como a la ciudadanía usuaria del SEI, a efecto de facilitar su adecuada difusión y entendimiento.

QUINTO. Publíquese el presente Acuerdo y su Anexo, en los estrados de las oficinas centrales, en los estrados electrónicos y para mayor difusión, en los estrados de las oficinas de las treinta y tres Direcciones Distritales de este Instituto Electoral.

SEXTO. Publíquese el presente Acuerdo y su Anexo, en la página de Internet www.iecm.mx; realícense las adecuaciones procedentes en virtud de la determinación asumida por la Junta Administrativa en el apartado de Transparencia de la citada página electrónica.

Así lo aprobaron por unanimidad de votos la y los integrantes de la Junta Administrativa del Instituto Electoral de la Ciudad de México, en sesión ordinaria de fecha treinta y uno de marzo de dos mil veintiséis, firmando al calce la Presidenta y el Secretario de la Junta, de conformidad con lo dispuesto por los artículos 82 del Código de Instituciones y Procedimientos Electorales de la



**JUNTA ADMINISTRATIVA
ACUERDO IECM-JA042-26**

Ciudad de México, 9, fracción XI, 10, fracción X, y 27 del Reglamento de Funcionamiento de la Junta Administrativa.

**LA PRESIDENTA DE LA JUNTA
ADMINISTRATIVA**

**EL SECRETARIO DE LA JUNTA
ADMINISTRATIVA**

MTRA. PATRICIA AVENDAÑO DURÁN

LIC. CÉSAR ALBERTO HOYO RODRÍGUEZ



Plan de Continuidad SEI

IECM-JA042-26

Código: UTSI/PL/01

Página 1 de 68

Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

Plan de Continuidad del Sistema Electrónico por Internet (SEI)

Proyecto:
ALINEACIÓN DEL PLAN DE CONTINUIDAD DEL SISTEMA
ELECTRÓNICO POR INTERNET



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 2 de 68
Revisión: 01

Fecha de revisión: 12/03/26
Fecha de emisión: 22/10/21

1. Contenido del documento

1.	Contenido del documento.....	2
2.	Introducción	3
3.	Definiciones	4
4.	Metodología	6
5.	Objetivos del Plan.....	8
6.	Alcance	9
7.	Riesgos.....	10
8.	Escenarios	11
9.	Recursos mínimos necesarios (MARC)	12
10.	Tiempo Objetivo de Recuperación (RTO, Recovery Time Objective) por aplicativo	14
11.	Punto Objetivo de Recuperación (RPO, Recovery Point Objective) por aplicativo	15
12.	Registros vitales	16
13.	Premisas.....	20
14.	Grupo de Trabajo de Manejo de Crisis (Modelo de Gobierno, Roles y Responsabilidades)	21
15.	Plan de comunicaciones, alerta y declaración de la contingencia (Criterios de activación / Procedimiento de respuesta a incidentes, advertencia y comunicación)	22
16.	Comunicación con las partes interesadas	23
17.	Procedimientos de Recuperación de operaciones (Plan de Continuidad del Negocio, BCP)	28
18.	Procedimientos de Plan de Recuperación ante Desastres (<i>Disaster Recovery Plan</i> , DRP).....	29
19.	Elaboró, Revisó y Aprobó.....	30
	ANEXO 1. Grupos de Trabajo de Manejo de Crisis del SEI.	31
	ANEXO 2. Plan de Comunicación.....	38
	ANEXO 3. Plan de Continuidad de Negocio SEI-BCP.	47
	ANEXO 4. Plan de recuperación ante Desastres SEI - DRP.....	60

Control de Cambios

Revisión	Fecha	Descripción
01	12/03/26	Se actualizan componentes y datos de los responsables de grupos de trabajo del SEI 2026
00	22/10/21	Emisión del documento.



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 3 de 68
Revisión: 01

Fecha de revisión: 12/03/26
Fecha de emisión: 22/10/21

2. Introducción

El Plan de Continuidad del Sistema Electrónico por Internet (SEI), se encuentra diseñado para proporcionar una respuesta inmediata y permitir el proceso de recuperación del aplicativo ante una situación de contingencia ocasionado por cualquier tipo de motivo.

El presente Plan de Continuidad del SEI, proporciona un panorama general del escenario, las estrategias, acciones propuestas, recursos y requerimientos necesarios para restablecer las operaciones del sistema en el menor tiempo posible.

3. Definiciones

Término	Descripción
Análisis de Impacto al Negocio (BIA)	Análisis de Impacto al Negocio, (BIA, <i>Business Impact Analysis</i>), tiene como objetivo identificar los procesos críticos del negocio, así como posibles impactos en caso de no estar disponible el servicio analizado.
Análisis del riesgo	Procedimiento que se debe llevar a cabo para identificar los elementos o los factores que tienen la posibilidad de generar riesgos (u oportunidades) que afecten en forma negativa (o positiva) la operación de la organización y con ello comprender su naturaleza y su nivel de riesgo.
BCP	Plan de Continuidad del Negocio (por sus siglas en inglés, <i>Business Continuity Plan</i>).
BCM	Gestión de Continuidad del Negocio (por sus siglas en inglés, <i>Business Continuity Management</i>).
CAT	Centro de Atención Telefónica.
CITIECM	Centro de Información Telefónica del Instituto Electoral de la Ciudad de México, 01 800 433 32 22.
Contingencia / Desastre	Se entiende como un evento repentino, no planeado, que ocasiona la "inhabilidad de un servicio o proceso o parte de ella", para ejecutar sus procesos críticos por un periodo determinado que resulta en daño o pérdida a un nivel inaceptable.
Contingencia / Desastre	Desde el punto de vista de Tecnología de Información, se define como un evento repentino no planeado que ocasiona la "no disponibilidad" de los servicios informáticos por un periodo tal que, para restablecer estos servicios, es necesario utilizar facilidades alternas de cómputo y telecomunicaciones en otra localidad en caso de ser necesario.
DRP	Plan de Recuperación ante Desastres (por sus siglas en inglés, <i>Disaster Recovery Plan</i> , DRP).
IECM	Instituto Electoral de la Ciudad de México.
Impacto	Conjunto de los efectos que un suceso o un hecho producen en su entorno físico o social.
MARC	Acrónimo de " <i>Minimum Acceptable Recovery Configuration</i> ". Es la Configuración de Recuperación Mínima Aceptable y comprende los elementos humanos, técnicos y materiales que se requieren como mínimo para recuperar los servicios de cómputo y telecomunicaciones que soportan las funciones críticas de operación de la Institución.
Procesos críticos	Son aquellos procesos que por su alta prioridad es indispensable su recuperación en el menor tiempo posible. Ante una contingencia, los procesos críticos no pueden postergar su operación por un tiempo prolongado ya que se pondría en riesgo la integridad de los servicios de la Institución.
Registro vital	Es aquella documentación que contiene información esencial para continuar con la operación ante una interrupción. Pueden estar en formato electrónico, generados por medios electrónicos (computadoras, CD's, microfichas, etc.), así como medios físicos (formas especiales, reportes, material de referencia, etc.).



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 5 de 68
Revisión: 01

Fecha de revisión: 12/03/26
Fecha de emisión: 22/10/21

Término	Descripción
RPO	<p>Punto de Recuperación Objetivo (por sus siglas en inglés, <i>Recovery Point Objective</i>), es el punto en el tiempo (anterior a la contingencia) en el cual, se pueden recuperar los datos. Por ejemplo, realizar respaldos cada 4 horas (RPO=4).</p> <p>*Esta medida de tiempo es independiente del RTO.</p>
RTO	<p>Tiempo de Recuperación Objetivo (por sus siglas en inglés, <i>Recovery Point Objective</i>), es el tiempo requerido para recuperar servicios definidos como críticos. Este tiempo es medido desde el momento de la contingencia hasta el reinicio de las operaciones. Por ejemplo, un proceso crítico no puede tolerar interrupciones mayores a 1 día (RTO=1 día).</p> <p>*Esta medida de tiempo es independiente del RPO.</p>
SEI	Sistema Electrónico por Internet.

4. Metodología

El presente documento se encuentra basado en los lineamientos expresados en las Normas:

-) ISO 22301:2019 de Seguridad y resiliencia de Sistemas de gestión de continuidad de negocio.
-) ISO/TS 54001:2019 Sistemas de gestión de calidad-Requisitos específicos para la aplicación de la Norma ISO 9001:2015 a organizaciones electorales en todos los niveles de gobierno.

Garantizando el pleno cumplimiento de la normatividad en la materia aplicable al Instituto Electoral de la Ciudad de México.

Con base en la metodología del Instituto Internacional de Recuperación de desastres (DRII, por sus siglas en inglés), se desarrolla el presente documento alineado con los requerimientos establecidos dentro de la norma ISO 22301:2019. A continuación, se indica la metodología:



Metodología para el Desarrollo del plan de continuidad

El ciclo de vida del BCM, se encuentra comprendida en 4 fases principales:



Ciclo de vida del BCM



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 7 de 68

Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

El estudio se desarrolló tomando como base la información obtenida de las siguientes fuentes:

-) Información documentada requerida previo inicio del estudio.
-) Información obtenida por el Análisis de Riesgos y de Impacto al Negocio.
-) Información obtenida de la Estrategia de Recuperación.
-) Sesiones de trabajo realizadas con personal crítico responsable del SEI.

Toda la información recabada, fue analizada con el fin de estructurar el presente informe.



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 8 de 68
Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

5. Objetivos del Plan

El presente Plan de Continuidad de Negocio, está diseñado bajo las normas ISO 22301:2019 y ISO/TS 54001:2019 para permitir al Instituto Electoral de la Ciudad de México (IECM), definir las acciones a tomar en caso de que se presente una determinada contingencia o desastre que inhabilite la disponibilidad del SEI, cuando se presente un ejercicio de participación ciudadana.

Adicionalmente, está estructurado para lograr los siguientes objetivos:

-) Proveer un enfoque organizado para el manejo de las actividades de respuesta y recuperación luego de un incidente no planeado o de una interrupción prolongada del Sistema Electrónico por Internet.
-) Ofrecer respuestas oportunas y apropiadas, reduciendo así los impactos operativos, imagen y económicos que puede traer una interrupción del Sistema Electrónico por Internet.

6. Alcance

Realizar la alineación operativa y metodológica del Plan de Continuidad del Sistema Electrónico por Internet, a la norma ISO 22301:2019 de Seguridad y resiliencia de Sistemas de gestión de continuidad de negocio y a la norma ISO/TS 54001:2019 del Sistema de Gestión de Calidad Electoral (SGCE), garantizando el pleno cumplimiento con la normatividad en la materia aplicable al Instituto Electoral de la Ciudad de México.

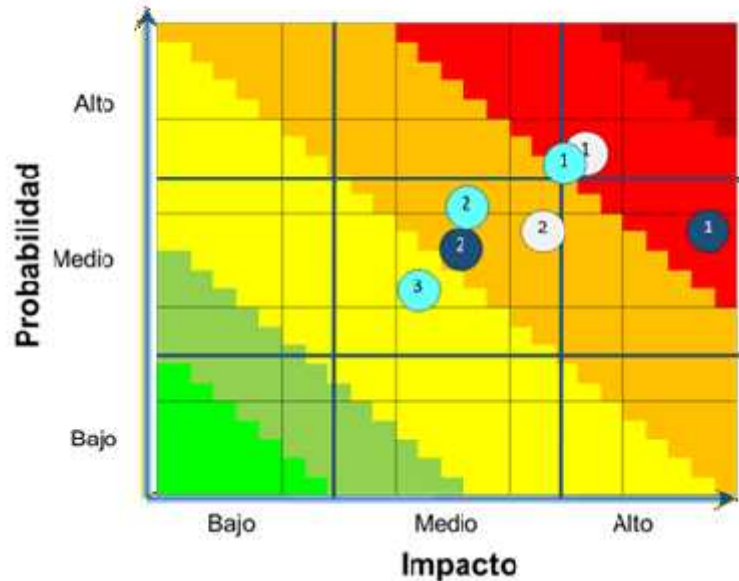
Los procesos analizados que soportan al Sistema Electrónico por Internet (SEI), fueron los siguientes:

Área	Proceso	RTO	RPO	Criticidad
Dirección de Apoyo a Órganos Desconcentrados (DAOD).	Archivo y apoyo logístico para oficinas centrales y órganos desconcentrados.	30 min.	No Aplica.	Muy Alta.
Dirección Ejecutiva de Organización Electoral y Geoestadística (DEOEyG).	Fichas de proceso-Procesos de Participación Ciudadana (Logística consultiva / electiva).	30 min.	No Aplica.	Muy Alta.
Dirección Ejecutiva de Participación Ciudadana y Capacitación.	Registro de Candidaturas para integrar las Comisiones de Participación Comunitaria (COPACO).	5 min.	No Aplica.	Muy Alta.
Unidad Técnica de Servicios Informáticos (UTSI).	Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad).	0 – 2 horas.	Última versión.	Alta.
	Asignación, préstamo o devolución de bienes informáticos.	0 – 4 horas.	0 – 4 horas.	Alta.
	Soporte Técnico.	0 – 4 horas.	0 – 4 horas.	Alta.
	Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Centro de Cómputo).	0 – 4 horas.	0 – 4 horas.	Alta.
	Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Comunicaciones).	0 – 4 horas.	24 horas.	Alta.
	Desarrollo de Sistemas Informáticos.	0 – 4 horas.	Última versión.	Alta.
	Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Bienes informáticos).	> 2 semanas.	No aplica.	Baja.
	Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Redes, CCTV y equipos CISCO).	> 2 semanas.	No aplica.	Baja.

7. Riesgos

Con base al Análisis de Riesgos realizado se identificaron los siguientes escenarios, los cuales tienen un mayor riesgo de probabilidad que causen una indisponibilidad del SEI:

- Tecnológicos** ●
- 1.- Operación deficiente por obsolescencia tecnológica
 - 2.- Falta de pruebas en las diferentes plataformas o equipos tecnológicos que soportan el SEI
- Operativos** ●
- 1.- Falta de la función de servicio al cliente (Help Desk) - Componente CAT dentro del SEI
 - 2.- Inefectiva selección de proveedor, evaluación y prácticas de Benchmarking
 - 3.- Falta de capacitación del personal
- Políticos** ●
- 1.- Cambios en la operación del SEI por modificaciones regulatorias y/o legales
 - 2.- Cambios Regulatorios y/o Legales





Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 11 de 68

Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

8. Escenarios

Como buena práctica, este análisis se desarrolló considerando el **peor escenario**.

Escenario:

“Una indisponibilidad del Sistema Electrónico por Internet (SEI), ocasionado por una falla tecnológica de cualquier motivo, que impida el ejercicio de participación ciudadana de manera electrónica efectuado en un solo día, afectando la credibilidad e imagen del Instituto Electoral de la Ciudad de México (IECM).”

Resumen:

-) Indisponibilidad del SEI ocasionada por cualquier motivo.

9. Recursos mínimos necesarios (MARC)

La siguiente tabla muestra los recursos mínimos que se requerirían tener en un sitio alternativo a lo largo del tiempo en caso de no poder ingresar a la instalación, para operar los servicios más críticos que soportan al SEI. Estos recursos se muestran de manera consolidada, es decir, se sumaron los requerimientos que fueron especificados en cada servicio y se muestran los totales en cada una de las ventanas de tiempo.

Recursos	Recurso	4 horas	1 día	3 días	1 semana	>2 semanas	Total
Personal y Área de Trabajo.	Personal mínimo.	34	0	0	0	0	34
	Laptop / PC.	21	0	0	0	0	21
Telecomunicaciones.	Telefonía.	1	0	0	0	0	1
	Internet.	23	0	0	0	0	23
	VPN.	23	0	0	0	0	23

Resumen de los lugares de trabajo mínimos requeridos en un sitio alternativo, para soportar el SEI.

Si se llegara a presentar un evento de contingencia que interrumpa la disponibilidad del SEI se necesitaría contar de manera inmediata con 102 recursos de los diferentes servicios (lugares de trabajo, laptops, teléfono, accesos a internet y vpn), y se estaría trabajando de forma remota en sede alterna o desde las casas del personal:

-) 34 lugares de trabajo de ser el caso.
-) 21 laptops.
-) 1 teléfono.
-) 23 accesos a internet.
-) 23 VPN.



**Plan de Continuidad
SEI**

IECM-JA042-26
Código: UTSI/PL/01

Página 13 de 68
Revisión: 01

Fecha de revisión: 12/03/26
Fecha de emisión: 22/10/21

A continuación, se indica los recursos humanos por servicio y los proveedores en caso de ser necesarios.

Proceso	Recursos / Proveedores
Asignación, préstamo o devolución de bienes informáticos.	8 personas.
Soporte Técnico.	6 personas de manera remota.
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Comunicaciones).	6 personas.
Desarrollo de Sistemas Informáticos.	5 personas de manera remota.
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad).	3 personas. Se requiere el apoyo de los siguientes proveedores principalmente: <ul style="list-style-type: none"> ➤ Onlinet: Nube Radware. ➤ Scitum – Telmex: Tráfico seguro. ➤ Scitum: Sistema de prevención de intruso. ➤ Onlinet: Filtrado web. ➤ Microsoft: nube Azure. ➤ Layercode Consulting & Services: Servicios especializado de la arquitectura de SEI en la nube Azure.
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad).	3 personas.
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Centro de Cómputo).	3 personas. Se requiere el apoyo de los siguientes proveedores principalmente: <ul style="list-style-type: none"> ➤ Microsoft. ➤ Lenovo. ➤ Dell. ➤ Almacenamiento. ➤ VMware. ➤ Red Hat.

10. Tiempo Objetivo de Recuperación (RTO, Recovery Time Objective) por aplicativo

Con base en los impactos dimensionados anteriormente, ante un evento de desastre, se determinó el máximo tiempo tolerable de recuperación (RTO – *Recovery Time Objective*, por sus siglas en inglés) para cada herramienta utilizada por los servicios críticos que soportan el SEI y con esto minimizar los impactos considerables en caso de una contingencia mayor que pueda poner en riesgo la operación del aplicativo.

0 – 2 horas	
Proceso	Herramienta
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad).	Portal Radware.
	Correo electrónico.
	IPS.
	Forcerpoint.

0 – 4 horas	
Proceso	Herramienta
Asignación, préstamo o devolución de bienes informáticos.	Control de inventario (Excel).
Soporte Técnico.	System Center Service Manager (SCSM).
	Control del requerimiento de usuarios.
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo.	Consola de los equipos CISCO (red y telefonía).
	Correo electrónico.
	PRTG.
(Comunicaciones).	Software de la consola de la red inalámbrica – ARUBA.
	Servicio de mensajes.
Desarrollo de Sistemas Informáticos.	Correo electrónico.
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad).	Mesa de ayuda.
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Centro de Cómputo).	Monitoreo – SEI.
	PRTG.
	Correo electrónico.

Muestra la prioridad de recuperación de las herramientas a lo largo del tiempo.



**Plan de Continuidad
SEI**

IECM-JA042-26
Código: UTSI/PL/01

Página 15 de 68
Revisión: 01

Fecha de revisión: 12/03/26
Fecha de emisión: 22/10/21

11. Punto Objetivo de Recuperación (RPO, Recovery Point Objective) por aplicativo

En la siguiente tabla se muestra la máxima pérdida de transacciones (RPO) que se puede soportar en caso de una contingencia mayor, es decir en una contingencia las herramientas deben contar con la información respaldada con base en cada ventana de tiempo como se indica a continuación.

0 – 4 horas	
Proceso	Herramienta
Asignación, préstamo o devolución de bienes informáticos.	Control de inventario (Excel).

Funcional	
Proceso	Herramienta
Soporte Técnico.	System Center Service Manager (SCSM).
	Control del requerimiento de usuarios.
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Comunicaciones).	Consola de los equipos CISCO (red y telefonía).
	Correo electrónico.
	PRTG.
Desarrollo de Sistemas Informáticos.	Software de la consola de la red inalámbrica – ARUBA.
	Servicio de mensajes.
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad).	Correo electrónico.
	Portal Radware.
	IPS.
	Forcerpoint.
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Centro de Cómputo).	Mesa de Ayuda.
	Monitoreo – SEI.
	PRTG.
	Correo electrónico.

Muestra el RPO que la Administración requiere por aplicación

12. Registros vitales

Los registros vitales contienen información esencial para continuar con la operación ante una interrupción y pueden existir de manera electrónica, papel, etc. Se requiere tener respaldo, en un sitio alternativo, de los registros vitales identificados para que los servicios críticos que soportan el SEI puedan continuar operando de manera alterna en caso de que ocurra una contingencia que inhabilite el aplicativo, de ahí que deben contar con un servidor de archivos que contenga los registros vitales que se identificaron a lo largo de este estudio.

Proceso	Nombre del Registro	Tipo (físico/electrónico)	Ubicación de la información (computadora del responsable, carpeta compartida / Física (oficina, archivero)	Responsable de la información	¿Se realiza respaldo?	Periodicidad del respaldo actual	RTO	RPO
					(Si/No)			
Asignación, préstamo o devolución de bienes informáticos	Control de inventarios	Electrónico	Laptop del responsable / Repositorio de información institucional	UTSI-Asignación, préstamo o devolución de bienes informáticos	Si	Diaria	Inmediata	No Aplica
	Formatos firmados de recibo de bienes	Físico / Electrónico	Laptop del responsable / Repositorio de información institucional / Archivero en la oficina	UTSI-Asignación, préstamo o devolución de bienes informáticos	Si	Diaria	Inmediata	No Aplica
Soporte Técnico	Guiones y procedimientos generados elección y consulta	Electrónico	Sharepoint / Sistema Gestión de Documentos / Correo electrónico	DEOEyG DEPCyC	Si	Estos guiones se elaboran cuando se presenta un ejercicio del proceso electoral y consultivo	Inmediata	No Aplica
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Comunicaciones)	Diagrama de red	Electrónico	NAS	UTSI-Jefatura de Departament o de Redes y Comunicaciones	Si	Última versión	0 – 4 horas	No Aplica
	Inventario de direcciones IP	Electrónico	NAS	UTSI-Jefatura de Departament o de Redes y Comunicaciones	Si	Última versión	0 – 4 horas	1 día



Plan de Continuidad SEI

IECM-JA042-26

Código: UTSI/PL/01

Página 17 de 68

Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

Proceso	Nombre del Registro	Tipo (físico/electrónico)	Ubicación de la información (computadora del responsable, carpeta compartida / Física (oficina, archivero)	Responsable de la información	¿Se realiza respaldo?	Periodicidad del respaldo actual	RTO	RPO
					(Si/No)			
Desarrollo de Sistemas Informáticos	Credenciales de acceso	Electrónico	NUBE	UTSI- Dirección de Desarrollo de Sistemas	Si	Última versión	0 – 4 horas	Última versión
	Manuales de uso	Electrónico	NUBE	UTSI- Dirección de Desarrollo de Sistemas	SI	Última versión	0 – 4 horas	Última versión
	Contratos de servicio	Electrónico	NUBE	UTSI- Dirección de Desarrollo de Sistemas	Si	Actuales	0 – 4 horas	Actuales
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad)	Manuales de operación	Electrónico	Laptop	UTSI- Jefatura de Web, Seguridad y Nuevas Tecnologías	No	Mensual	0 – 2 horas	Última actualización
	Memorias técnicas	Físico / Electrónico	Laptop / Archivero en la oficina	UTSI- Jefatura de Web, Seguridad y Nuevas Tecnologías	No	Última versión	0 – 2 horas	Última actualización
	Lista de proveedores	Electrónico	Laptop	UTSI- Jefatura de Web, Seguridad y Nuevas Tecnologías	Si	Última versión	0 – 2 horas	Última actualización

Proceso	Nombre del Registro	Tipo (físico/electrónico)	Ubicación de la información (computadora del responsable, carpeta compartida / Física (oficina, archivero)	Responsable de la información	¿Se realiza respaldo?	Periodicidad del respaldo actual	RTO	RPO
					(Si/No)			
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Centro de Cómputo)	Inventario de equipos	Electrónico	Nube / Laptop	UTSI-Subdirección de Seguridad, Redes y Cómputo	Si	Mensual	0 – 4 horas	0 – 4 horas
	Diagramas de conectividad de los servidores	Electrónico	Nube / Laptop	UTSI-Subdirección de Seguridad, Redes y Cómputo	Si	Última versión	0 – 4 horas	0 – 4 horas
	Análisis de los servicios	Electrónico	Nube / Laptop	UTSI-Subdirección de Seguridad, Redes y Cómputo	Si	Última versión	0 – 4 horas	0 – 4 horas
	Servidores, BD, Webserver, datos.	Electrónico	Nube / Laptop	UTSI-Subdirección de Seguridad, Redes y Cómputo	Si	Varían día, mes y por temporada	0 – 4 horas	0 – 4 horas
	Cronograma de mantenimiento	Electrónico	Laptop	UTSI-Subdirección de Seguridad, Redes y Cómputo	Si	Última versión	1 semana	1 semana
	Arquitectura del SEI	Electrónico	Físico / electrónico (Correo electrónico)	UTSI-Subdirección de Seguridad, Redes y Cómputo	Si	Última versión	0 – 4 horas	0 – 4 horas



Plan de Continuidad SEI

IECM-JA042-26

Código: UTSI/PL/01

Página 19 de 68

Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

Proceso	Nombre del Registro	Tipo (físico/electrónico)	Ubicación de la información (computadora del responsable, carpeta compartida / Física (oficina, archivero)	Responsable de la información	¿Se realiza respaldo?	Periodicidad del respaldo actual	RTO	RPO
					(Si/No)			
	Inventario de aplicaciones	Electrónico	Nube / Laptop	UTSI-Subdirección de Seguridad, Redes y Cómputo	Si	Mensual / Última versión	0 – 4 horas	0 – 4 horas

Registros vitales identificados por servicio.



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 20 de 68
Revisión: 01

Fecha de revisión: 12/03/26
Fecha de emisión: 22/10/21

13. Premisas

Este Plan de Continuidad para el Sistema Electrónico por Internet, se fundamenta sobre las siguientes premisas básicas:

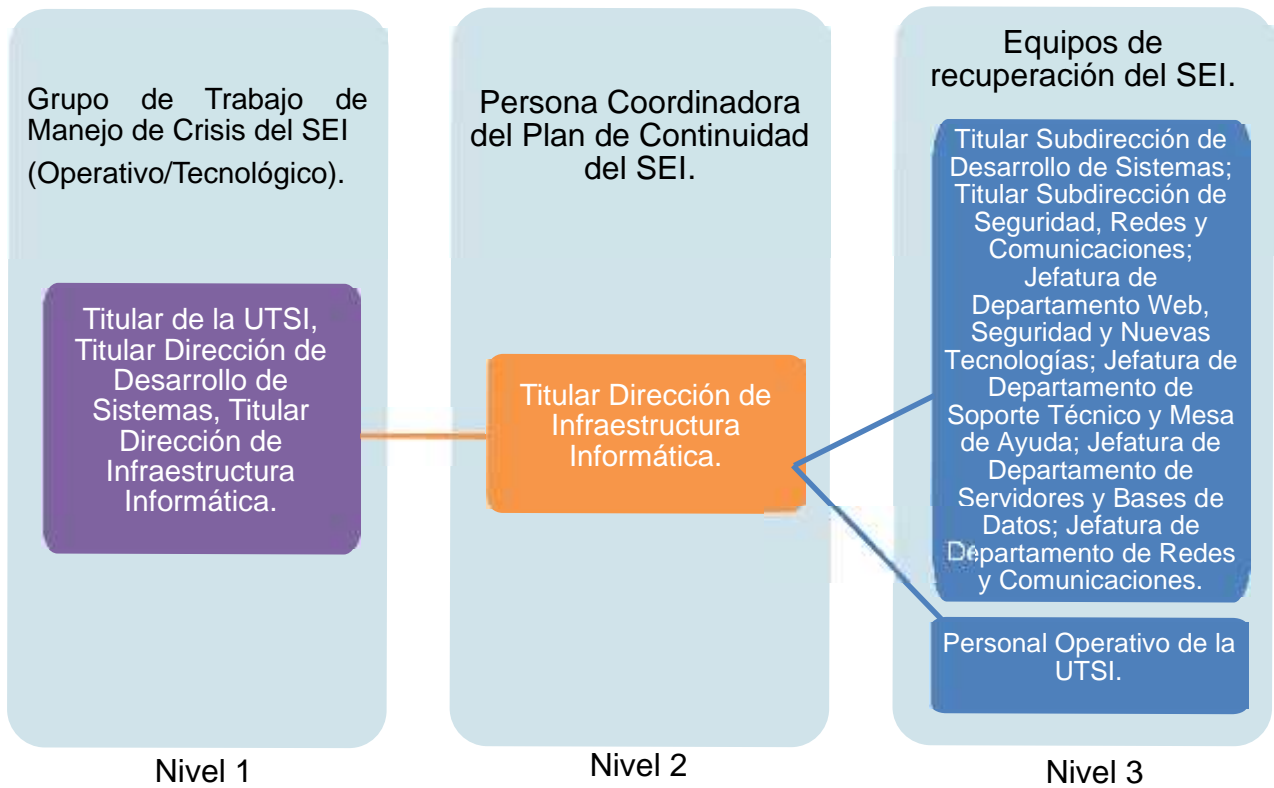
-) Existe suficiente personal calificado y disponible para atender las responsabilidades de recuperación de los servicios críticos, es decir, se cuenta con el personal crítico que se encargará de la recuperación de la operación.

Las premisas secundarias son las siguientes:

-) Se ha efectuado una revisión por los responsables del Plan, se ha actualizado y de manera regular se revisan las actividades y procedimientos a fin de asegurar su objetividad y validez.
-) Los recursos identificados como "Configuración Mínima Aceptable de Recuperación" (*Minimum Acceptable Recovery Configuration*, "MARC") por cada servicio, estarán disponibles para llevar a cabo los procedimientos de recuperación.
-) Una vez definida la estrategia de recuperación, se deberá poner a prueba la ejecución del plan para asegurar la funcionalidad de los procedimientos documentados.

14. Grupo de Trabajo de Manejo de Crisis (Modelo de Gobierno, Roles y Responsabilidades)

La estructura para el grupo de trabajo de manejo de crisis del “SEI” está compuesta por tres niveles, con la finalidad de que los diferentes eventos que se presenten sean escalados para ser atendidos por el nivel que le corresponde. A continuación, se presenta la estructura que conforma el Plan del Grupo de Manejo de Crisis.



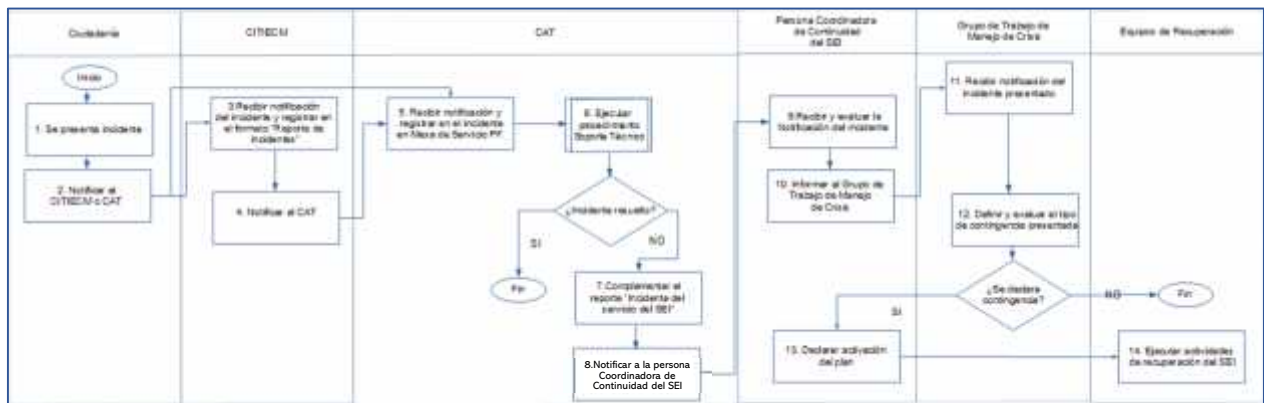
Estructura para el manejo de crisis.

ANEXO 1. Grupos de trabajo de manejo de crisis.

15. Plan de comunicaciones, alerta y declaración de la contingencia (Criterios de activación / Procedimiento de respuesta a incidentes, advertencia y comunicación)

El proceso de notificación, escalamiento y declaración de contingencia es de suma importancia para la continuidad del Sistema Electrónico por Internet (SEI).

A continuación, se muestra el diagrama:



Gráfica Procedimiento de notificación de contingencia del SEI.

ANEXO 2. Plan de Comunicación.

16. Comunicación con las partes interesadas

A continuación, se muestra el árbol de llamadas por Niveles.

Grupo de Trabajo de Manejo de Crisis Tecnológico

Titular

Nombre	María Yolanda Nigo González
Puesto	Directora de Desarrollo de Sistemas
Correo electrónico	yolanda.nigo@iecm.mx
Teléfono trabajo	54833800 Ext. 4618

Suplente

Nombre	Ana Angelica Gonzalez Oliva
Puesto	Directora de Infraestructura Informática
Correo electrónico	ana.gonzalez@iecm.mx
Teléfono trabajo	54833800 Ext. 3819

Titular

Nombre	Ana Angelica Gonzalez Oliva
Puesto	Directora de Infraestructura Informática
Correo electrónico	ana.gonzalez@iecm.mx
Teléfono trabajo	54833800 Ext. 3819

Suplente

Nombre	María Yolanda Nigo González
Puesto	Directora de Desarrollo de Sistemas
Correo electrónico	yolanda.nigo@iecm.mx
Teléfono trabajo	54833800 Ext. 4618

Titular

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext.4605

Suplente

Nombre	Paula Robles Mass Tapia
Puesto	Subdirectora de Sistemas de Información
Correo electrónico	paula.roblesmass@iecm.mx
Teléfono trabajo	54833800 Ext. 4617

Titular

Nombre	Paula Robles Mass Tapia
Puesto	Subdirectora de Sistemas de Información
Correo electrónico	paula.roblesmass@iecm.mx
Teléfono trabajo	54833800 Ext. 4617

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext.4605



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página **24** de **68**
Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

Persona Coordinadora del Plan de Continuidad

Titular

Nombre	Estefanía Mena Ibarra
Puesto	Titular de la Unidad Técnica de Servicios Informáticos
Correo electrónico	estefania.mena@iecm.mx
Teléfono trabajo	54833800 Ext. 4622

Suplente

Nombre	Ana Angelica González Oliva
Puesto	Directora de Infraestructura Informática
Correo electrónico	ana.gonzalez@iecm.mx
Teléfono trabajo	54833800 Ext. 3819



Plan de Continuidad SEI

IECM-JA042-26

Código: UTSI/PL/01

Página 25 de 68

Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

Equipos de recuperación

Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad).

Titular

Nombre	Miguel Angel Garcia Morales
Puesto	Jefe de Departamento Web, Seguridad y Nuevas Tecnologías
Correo electrónico	miguel.garcia@iecm.mx
Teléfono trabajo	54833800 Ext. 4683

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext. 4605

Asignación, préstamo o devolución de bienes informáticos

Titular

Nombre	Alejandro Magaña Reyes
Puesto	Jefe de Departamento de Soporte Técnico y Mesa de Ayuda
Correo electrónico	alejandra.magana@iecm.mx
Teléfono trabajo	54833800 Ext. 4690

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext.4605

Soporte Técnico

Titular

Nombre	Alejandro Magaña Reyes
Puesto	Jefe de Departamento de Soporte Técnico y Mesa de Ayuda
Correo electrónico	alejandra.magana@iecm.mx
Teléfono trabajo	54833800 Ext. 4690

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext.4605



**Plan de Continuidad
SEI**

IECM-JA042-26

Código: UTSI/PL/01

Página 26 de 68

Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Bienes informáticos).

Titular

Nombre	Alejandro Magaña Reyes
Puesto	Jefe de Departamento de Soporte Técnico y Mesa de Ayuda
Correo electrónico	alejandro.magana@iecm.mx
Teléfono trabajo	54833800 Ext. 4690

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext.4605

Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Centro de Cómputo).

Titular

Nombre	Victor Hugo Oropeza Cadena
Puesto	Jefe de Departamento de Servidores y Bases de Datos
Correo electrónico	victor.oropeza@iecm.mx
Teléfono trabajo	54833800 Ext. 4681

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext.4605

Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Comunicaciones).

Titular

Nombre	Marco Tulio Conde Cruz
Puesto	Jefe de Departamento de Redes y Comunicaciones
Correo electrónico	marcotulio.conde@iecm.mx
Teléfono trabajo	54833800 Ext.4694

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.cataneda@iecm.mx
Teléfono trabajo	54833800 Ext. 4605



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 27 de 68
Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Redes, CCTV y equipos CISCO).

Titular

Nombre	Marco Tulio Conde Cruz
Puesto	Jefe de Departamento de Redes y Comunicaciones
Correo electrónico	marcotulio.conde@iecm.mx
Teléfono trabajo	54833800 Ext.4694

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.cataneda@iecm.mx
Teléfono trabajo	54833800 Ext. 4605

Desarrollo de Sistemas Informáticos.

Titular

Nombre	Paula Robles Mass Tapia
Puesto	Subdirectora de Sistemas de Información
Correo electrónico	paula.roblesmass@iecm.mx
Teléfono trabajo	54833800 Ext. 4617

Suplente

Nombre	María Yolanda Nigo González
Puesto	Directora de Desarrollo de Sistemas
Correo electrónico	yolanda.nigo@iecm.mx
Teléfono trabajo	54833800 Ext. 4618

17. Procedimientos de Recuperación de operaciones (Plan de Continuidad del Negocio, BCP)

Los siguientes procedimientos de recuperación y retorno para el Sistema Electrónico por Internet (SEI) se encuentran basados en la evaluación de riesgos realizada de manera previa, tomando en cuenta los impactos y tiempos críticos definidos en el Análisis de Impacto al Negocio desarrollado.

Los riesgos operativos más viables son:

Riesgo	Escenario
Falla de la función de servicio al cliente (Help Desk) - Componente CAT dentro del SEI Módulo.	La función de servicio al cliente no se encuentra habilitada, lo cual impacta en los servicios proporcionados por el instituto o en la indisponibilidad del SEI en caso de presentarse alguna falla. (módulo).
La aplicación SEI no puede identificar la credencial para votar en el momento en que el ciudadano quiere ejercer su derecho.	El aplicativo podría presentar problemas cuando requiera identificar la credencial para votar.
Inefectiva selección de proveedor, evaluación y prácticas de Benchmarking.	La falta de un proceso para administrar la calidad del proveedor podría ocasionar problemas en los servicios proporcionados por el instituto o en el proveedor contratado para el SEI.
Falta de capacitación del personal.	Una falta de capacitación del personal responsable y de apoyo para la ciudadanía para ejercer su derecho, podría ocasionar que el SEI no sea usado de manera correcta o en su caso se lleve mayor tiempo del estimado.

Así mismo se toman en cuenta otro tipo de escenario con menor probabilidad de ocurrencia, los cuales son:

-) Falla o pérdida de dispositivo móvil.
-) Contingencias naturales y/o sociales que pudieran interrumpir su operación normal.
-) Contingencia natural que impida la disponibilidad del Centro de Cómputo.
-) Contingencia social que impida la disponibilidad del Centro de Cómputo.
-) Falla en los dispositivos de votación destinados para el Voto vía electrónica (voto offline) que impida la continuidad operativa.
-) Robo o extravío de los dispositivos de votación de Voto vía electrónica (voto offline).

ANEXO 3. Plan de Continuidad de Negocio SEI-BCP.

18. Procedimientos de Plan de Recuperación ante Desastres (*Disaster Recovery Plan, DRP*)

Los siguientes procedimientos de recuperación y retorno para el Sistema Electrónico por Internet (SEI) se encuentran basados en la evaluación de riesgos realizada de manera previa, tomando en cuenta los impactos y tiempos críticos definidos en el Análisis de Impacto al Negocio desarrollado.

Los riesgos operativos más viables son:

Riesgo	Escenario
Operación deficiente por obsolescencia tecnológica.	Tecnología obsoleta provocaría una “no disponibilidad” de los servicios tecnológicos, por falta de mantenimiento, falta de actualizaciones, etc.
Falta de pruebas en las diferentes plataformas o equipos tecnológicos que soportan el SEI con el fin de validar la funcionalidad correcta del aplicativo (Android, IOS).	Una falta de pruebas en las diferentes plataformas y equipos podría ocasionar una “no disponibilidad” del SEI.

Así mismo se toman en cuenta otro tipo de escenario con menor probabilidad de ocurrencia, los cuales son:

-) Falla o pérdida de dispositivo móvil.
-) Contingencias naturales y/o sociales que pudieran interrumpir su operación normal.
-) Contingencia natural que impida la disponibilidad del Centro de Cómputo.
-) Contingencia social que impida la disponibilidad del Centro de Cómputo.
-) Caídas regionales de centros de datos o interrupciones en servicios críticos en la nube de Azure.
-) Falla en los dispositivos de votación para personas en estado de postración y prisión preventiva para el Voto vía electrónica (Voto-offline) que impida la continuidad operativa.
-) Robo o extravío de los dispositivos de votación para personas en estado de postración y prisión preventiva para el Voto vía electrónica (Voto-offline).

Por lo que se debe de consultar al Plan de Recuperación en caso de Desastres del SEI:

ANEXO 4. Plan de Recuperación ante Desastres SEI - DRP



Plan de Continuidad SEI

IECM-JA042-26

Código: UTSI/PL/01

Página 30 de 68

Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

19. Elaboró, Revisó y Aprobó

Elaboró

Nombre	Puesto	Fecha	Firma
Ana Angelica González Oliva	Directora de Infraestructura Informática	12/03/2026	

Revisó

Nombre	Puesto	Fecha	Firma
Estefanía Mena Ibarra	Titular de la Unidad Técnica de Servicios Informáticos	13/03/2026	
Javier Castañeda López	Subdirector de Seguridad, Redes y Cómputo	13/03/2026	
Maria Yolanda Nigó González	Directora de Desarrollo de Sistemas	13/03/2026	
Miguel Angel García Morales	Jefe de Departamento Web, Seguridad y Nuevas Tecnologías	13/03/2026	
Paula Robles Mass Tapia	Subdirectora de Sistemas de Información	13/03/2026	

Aprobó

Nombre	Puesto	Fecha	Firma
Estefanía Mena Ibarra	Titular de la Unidad Técnica de Servicios Informáticos	16/03/2026	
Maria Yolanda Nigó González	Directora de Desarrollo de Sistemas	16/03/2026	
Javier Castañeda López	Subdirector de Seguridad, Redes y Cómputo	16/03/2026	
Miguel Angel García Morales	Jefe de Departamento Web, Seguridad y Nuevas Tecnologías	16/03/2026	
Paula Robles Mass Tapia	Subdirectora de Sistemas de Información	16/03/2026	



Plan de Continuidad SEI

IECM-JA042-26

Código: UTSI/PL/01

Página 31 de 68

Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

ANEXO 1. Grupos de Trabajo de Manejo de Crisis del SEI.

El Plan de Continuidad del SEI permitirá establecer la manera cómo se debe notificar y activar dicho plan ante una contingencia de cualquier tipo, ya sea operativa o tecnológica, que ocasione una “no disponibilidad” del Sistema Electrónico por Internet (SEI).

La coordinación de los recursos y procedimientos permitirá manejar las situaciones de crisis de mejor manera, disminuyendo el impacto que pudiera ocasionar, lo cual permitirá un Manejo de Crisis adecuado.

Objetivo:

El Instituto Electoral de la Ciudad de México busca estar preparada adecuadamente para el manejo de una crisis durante la operación del SEI con el fin de:

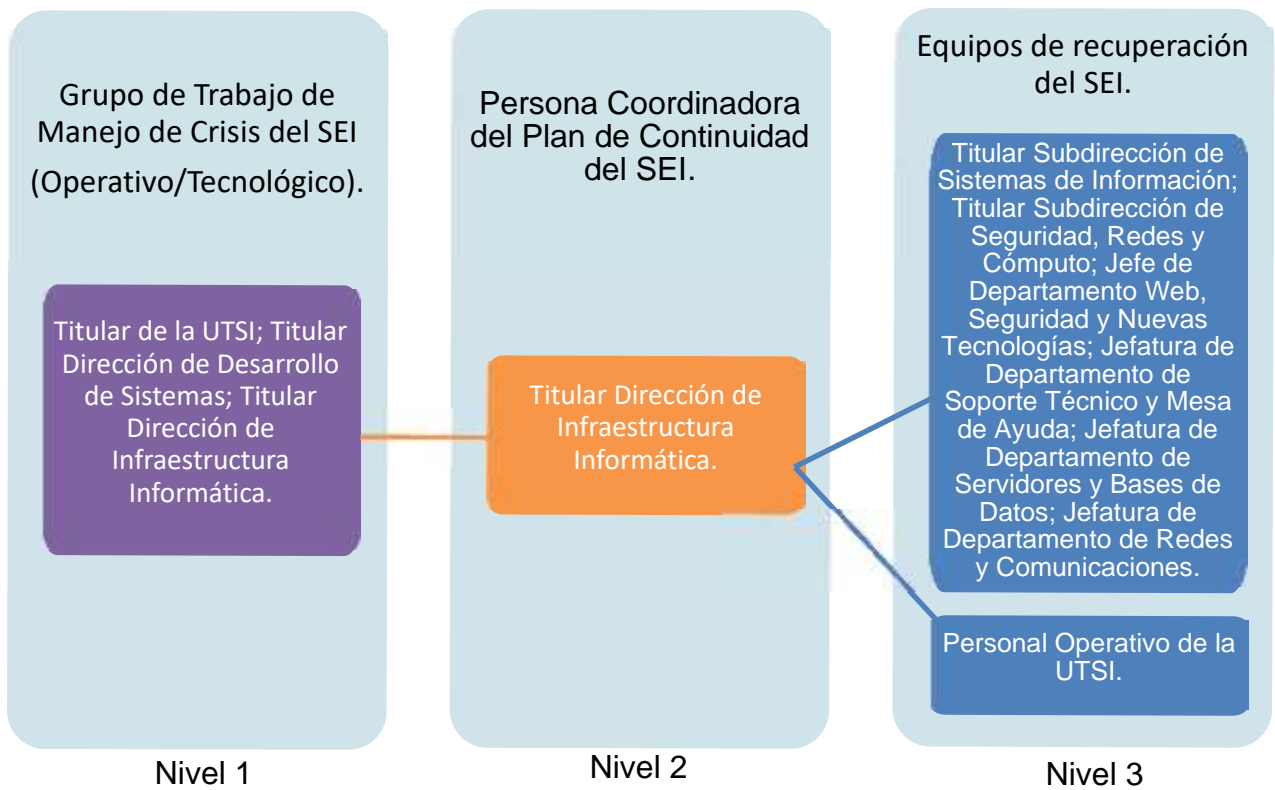
-) Minimizar las consecuencias de la interrupción del SEI.
-) Garantizar la continuidad operativa y tecnológica del SEI.

Alcance:

Realizar la alineación operativa y metodológica del Plan de Continuidad del Sistema Electrónico por Internet, a la norma ISO 22301:2019 de Seguridad y resiliencia de Sistemas de gestión de continuidad de negocio y la norma ISO/TS 54001:2019 del Sistema de Gestión de Calidad Electoral (SGCE), garantizando asimismo el pleno cumplimiento con la normatividad en la materia aplicable al Instituto Electoral de la Ciudad de México.

Estructura del Manejo de Crisis:

A continuación, se indica el modelo de gobierno para el Grupo de Trabajo de Manejo de Crisis del SEI, la cual se encuentra compuesta por tres niveles:



Estructura para el manejo de crisis.

Roles y responsabilidades:

Nivel	Puesto	Descripción
<p>Nivel 1</p>	<p>Grupo de Trabajo de Manejo de Crisis del SEI.</p>	<p>Equipo de respuesta al más alto nivel jerárquico, en el que participan la persona titular de la UTSI, así como las personas titulares de las dos direcciones de la Unidad. Provee la supervisión y la toma de decisiones estratégicas para eventos que han escalado al nivel de una crisis y requieren una toma de decisiones más allá del alcance del Coordinador del Plan de Continuidad del SEI.</p> <p>En general, el Grupo de Trabajo de Manejo de Crisis sólo se involucrará en eventos significativos con el potencial de:</p> <ul style="list-style-type: none">) Amenazar la integridad física y la seguridad de los empleados del IECM.) No disponibilidad de los servicios tecnológicos que soportan el SEI. <p>Algunas responsabilidades de los miembros del Grupo de Trabajo son:</p> <ul style="list-style-type: none">) Autorizar de manera inmediata la solicitud, ante la Secretaría Administrativa, de compra de recursos requeridos para la atención de la contingencia tecnológica y/u operativa.) Designar y/o autorizar recursos (humanos, tecnológicos, financieros) para responder ante la crisis tecnológica y/u operativa.) Supervisar la implementación y el desarrollo de las estrategias para controlar la crisis.
<p>Nivel 2</p>	<p>Persona que Coordina el Plan de Continuidad del SEI.</p>	<p>Responsable de coordinar a los equipos de recuperación tecnológica en caso de declararse una contingencia.</p> <p>Algunas responsabilidades del nivel son:</p> <ul style="list-style-type: none">) Es la persona responsable de declarar la activación del plan de continuidad, con autorización del Grupo de Trabajo de Manejo de Crisis del SEI.

Nivel	Puesto	Descripción
		<ul style="list-style-type: none">) Evaluar el impacto y coordinar las actividades de atención a la crisis.) Validar las estrategias de respuesta ante la contingencia.) Tomar las decisiones de cómo actuar durante una crisis.) Asegurar que las actividades de respuesta se realicen de acuerdo con lo establecido.) Asegurar que las instalaciones afectadas y las instalaciones alternas tengan los mejores recursos disponibles (tecnología, personal, equipos, Etc.).) Servir como centro de recepción de información proveniente del personal operativo.) Mantener la comunicación y proveer de información al Grupo de Trabajo de Manejo de Crisis del SEI para la toma de decisiones.) Mantener actualizados los planes de continuidad de manera periódica, los cuales incluyen: <ul style="list-style-type: none"> o Análisis de Impacto al Negocio. o Evaluación de Riesgos. o Diseño y selección de la estrategia. o Plan de Continuidad del SEI. o Plan de Continuidad del Negocio (BCP). o Plan de Recuperación en Caso de Desastres (DRP). o Árbol de Llamadas. o Procedimientos de recuperación y retorno. o Ejecución de las pruebas. o Planes de mejora. <p>Nota: La actualización de los planes se deberá de realizar ante un cambio en los servicios y/o procesos, cambio de personal y/o proveedores, cambio en la infraestructura tecnológica que soporta el SEI. Se recomienda realizarlo</p>

Nivel	Puesto	Descripción
		de manera semestral de manera inicial o en su caso de manera anual.
Nivel 3	Responsable del Servicio	<p>Su responsabilidad es la recuperación del servicio de su atribución, asimismo deberá:</p> <ul style="list-style-type: none">) Evaluar la situación de contingencia presentada.) Notificar estatus del servicio a ser recuperado a la persona Coordinadora del Plan de Continuidad del SEI.) Notificar incidentes, problemas o situaciones que se presenten para la recuperación del servicio a la persona Coordinadora del Plan de Continuidad del SEI.) Asegurar que las actividades de respuesta a su cargo se realicen de acuerdo con lo establecido.
	Personal operativo de sistemas	<p>Personal que labora directamente para la recuperación del servicio, entre sus responsabilidades están:</p> <ul style="list-style-type: none">) Evaluar la situación de contingencia presentada.) Notificar estatus del servicio a ser recuperado a la persona superior jerárquica.) Notificar incidentes, problemas o situaciones que se presenten para la recuperación del servicio a la persona superior jerárquica.) Ejecutar los procesos de recuperación definidos.

Integrantes

Nivel	Personal										
Nivel 1	Grupo de Trabajo de Manejo Crisis										
	Tecnológico										
	<table border="1"> <thead> <tr> <th>Nombre</th> <th>Puesto</th> </tr> </thead> <tbody> <tr> <td>María Yolanda Nigo González</td> <td>Directora de Desarrollo de Sistemas</td> </tr> <tr> <td>Ana Angelica González Oliva</td> <td>Directora de Infraestructura Informática</td> </tr> <tr> <td>Javier Castañeda López</td> <td>Subdirector de Seguridad, Redes y Cómputo</td> </tr> <tr> <td>Paula Robles Mass Tapia</td> <td>Subdirectora de Sistemas de Información</td> </tr> </tbody> </table>	Nombre	Puesto	María Yolanda Nigo González	Directora de Desarrollo de Sistemas	Ana Angelica González Oliva	Directora de Infraestructura Informática	Javier Castañeda López	Subdirector de Seguridad, Redes y Cómputo	Paula Robles Mass Tapia	Subdirectora de Sistemas de Información
	Nombre	Puesto									
	María Yolanda Nigo González	Directora de Desarrollo de Sistemas									
Ana Angelica González Oliva	Directora de Infraestructura Informática										
Javier Castañeda López	Subdirector de Seguridad, Redes y Cómputo										
Paula Robles Mass Tapia	Subdirectora de Sistemas de Información										
Nivel 2	Coordinadora del Plan de Continuidad: Estefanía Mena Ibarra, Titular de la Unidad Técnica de Servicios Informáticos										
Nivel 3	Responsable de los servicios críticos:										
	<table border="1"> <thead> <tr> <th>Proceso</th> <th>Responsable</th> </tr> </thead> <tbody> <tr> <td>Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad)</td> <td>Miguel Angel García Morales Jefe de Departamento Web, Seguridad y Nuevas Tecnologías</td> </tr> <tr> <td>Asignación, préstamo o devolución de bienes informáticos</td> <td>Alejandro Magaña Reyes Jefe de Departamento de Soporte Técnico y Mesa de Ayuda</td> </tr> <tr> <td>Soporte Técnico</td> <td>Alejandro Magaña Reyes Jefe de Departamento de Soporte Técnico y Mesa de Ayuda</td> </tr> <tr> <td>Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Centro de Cómputo)</td> <td>Victor Hugo Oropeza Cadena Jefe de Departamento de Servidores y Bases de Datos</td> </tr> </tbody> </table>	Proceso	Responsable	Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad)	Miguel Angel García Morales Jefe de Departamento Web, Seguridad y Nuevas Tecnologías	Asignación, préstamo o devolución de bienes informáticos	Alejandro Magaña Reyes Jefe de Departamento de Soporte Técnico y Mesa de Ayuda	Soporte Técnico	Alejandro Magaña Reyes Jefe de Departamento de Soporte Técnico y Mesa de Ayuda	Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Centro de Cómputo)	Victor Hugo Oropeza Cadena Jefe de Departamento de Servidores y Bases de Datos
	Proceso	Responsable									
	Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad)	Miguel Angel García Morales Jefe de Departamento Web, Seguridad y Nuevas Tecnologías									
	Asignación, préstamo o devolución de bienes informáticos	Alejandro Magaña Reyes Jefe de Departamento de Soporte Técnico y Mesa de Ayuda									
Soporte Técnico	Alejandro Magaña Reyes Jefe de Departamento de Soporte Técnico y Mesa de Ayuda										
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Centro de Cómputo)	Victor Hugo Oropeza Cadena Jefe de Departamento de Servidores y Bases de Datos										



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 37 de 68
Revisión: 01

Fecha de revisión: 12/03/26

Fecha de emisión: 22/10/21

Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Comunicaciones)	Marco Tulio Conde Cruz Jefe de Departamento de Redes y Comunicaciones
Desarrollo de Sistemas Informáticos	Paula Robles Mass Tapia Subdirectora de Sistemas de Información
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Bienes informáticos)	Alejandro Magaña Reyes Jefe de Departamento de Soporte Técnico y Mesa de Ayuda
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Redes, CCTV y equipos CISCO)	Marco Tulio Conde Cruz Jefe de Departamento de Redes y Comunicaciones

ANEXO 2. Plan de Comunicación.

Objetivo:

Contar con un plan de comunicaciones en caso de presentarse una indisponibilidad del Sistema Electrónico por Internet (SEI) que afecte el ejercicio de participación ciudadana.

Alcance:

Realizar la alineación operativa y metodológica del Plan de Continuidad del Sistema Electrónico por Internet, a la norma ISO 22301:2019 de Seguridad y resiliencia de Sistemas de gestión de continuidad de negocio y la norma ISO/TS 54001:2019 del Sistema de Gestión de Calidad Electoral (SGCE), garantizando el pleno cumplimiento con la normatividad en la materia aplicable al Instituto Electoral de la Ciudad de México.

Marco normativo:

El presente documento se encuentra basado en los lineamientos expresados en la Norma:

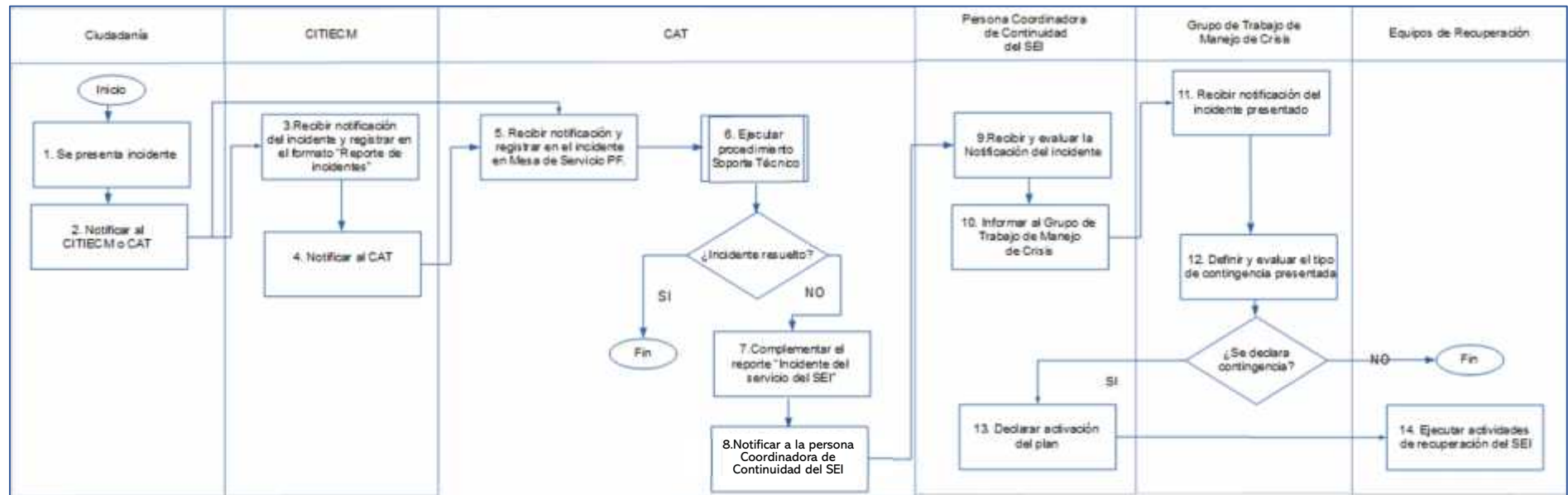
-) ISO 22301:2019 de Seguridad y resiliencia de Sistemas de gestión de continuidad de negocio.
-) ISO 54001:2019 Sistemas de gestión de calidad-Requisitos específicos para la aplicación de la Norma ISO 9001:2015 a organizaciones electorales en todos los niveles de gobierno.

Asimismo, en la declaración de cumplimiento normativo de la Unidad Técnica de Servicios Informáticos, se señala la normatividad vigente aplicable.

Diagrama de flujo

El plan de comunicaciones cuenta con el siguiente proceso de notificación, escalamiento y declaración de contingencia es de suma importancia para la continuidad del Sistema Electrónico por Internet (SEI).

A continuación, se muestra el diagrama:



Actividades

Número	Actividad	Unidad Responsable	Documento Empleado
1	Se presenta incidente en el SEI.		N/A
2	<p>Notificar el incidente presentado ya sea a través del CITIECM o del CAT.</p> <ul style="list-style-type: none">) CITIECM: 800 433 3222 (territorio nacional, por cobrar).) (+ 52) 55 2652 1175 (desde el extranjero, local por cobrar).) CAT: (+ 52) 55 5483 3875 (local, por cobrar). <p>Registrar en el formato para el reporte "Incidente del SEI", indicando:</p> <ul style="list-style-type: none">) Hora.) Tipo de Problema.) Nombre de la persona que reporta. 	Ciudadanía	Formato para Reporte Incidente del SEI.
3	Recibir notificación del incidente presentado, vía correo electrónico o vía telefónica del incidente presentado en el SEI.	CITIECM	N/A
4	Notificar al CAT.	CITIECM	N/A
5	Recibir y registrar el incidente en Mesa de servicio PF.	CAT	N/A
6	Ejecutar procedimiento de Soporte Técnico.	CAT	N/A
	¿Incidente resuelto? SI: FIN DE PROCEDIMIENTO. NO: Continúa en actividad 7.	CAT	N/A
7	<p>Complementar el reporte "Incidente del servicio del SEI", indicando:</p> <ul style="list-style-type: none">) Hora.) Tipo de incidente presentado.) Actividades realizadas.) Áreas involucradas.) Problemas presentados. 	CAT	Formato para Reporte Incidente del SEI.
8	Notificar a la persona Coordinadora del Plan de Continuidad del SEI, el incidente presentado, enviando el reporte documentado, vía correo electrónico o vía telefónica.	CAT	Formato para Reporte Incidente del SEI.



**Plan de Continuidad
SEI**

IECM-JA042-26
Código: UTSI/PL/01

Página 41 de 68
Revisión: 01

Fecha de revisión: 13/03/26
Fecha de emisión: 22/10/21

Número	Actividad	Unidad Responsable	Documento Empleado
9	Recibir notificación y evaluar la situación en conjunto con el personal del IECM con la información recabada del incidente presentado.	Persona Coordinadora del Plan de Continuidad del SEI.	N/A
10	Informar al Grupo de Trabajo de Manejo de Crisis el tipo de incidente presentado.	Persona Coordinadora del Plan de Continuidad del SEI.	N/A
11	Recibir notificación del incidente presentado en el SEI, con toda la información disponible para su análisis.	Grupo de Trabajo de Manejo de Crisis.	Formato para Reporte Incidente del SEI.
12	Definir y evaluar de manera expedita la situación presentada con el fin de tomar la decisión más efectiva ante la situación presentada. Tomar la decisión de activar el plan de continuidad con base en: <ul style="list-style-type: none">) Tiempo transcurrido desde el incidente.) Impactos ocasionados. 	Grupo de Trabajo de Manejo de Crisis.	N/A
	¿Se declara contingencia? NO: Fin de procedimiento. SI: Continúa en actividad 13.		
13	Declarar activación del plan con base al incidente presentado.	Persona Coordinadora del Plan de Continuidad del SEI.	Procedimientos de recuperación en caso de desastres (DRP).
14	Ejecutar actividades de recuperación para el SEI.	Equipos de Recuperación del IECM.	N/A
16	Elaborar reporte final indicando: <ul style="list-style-type: none">) Hora de inicio.) Hora de finalización.) Actividades realizadas.) Área que participaron.) Proveedores que participaron (Si aplica).) Compra o renta de recursos requeridos.) Plan de mejora. 	Persona Coordinadora del Plan de Continuidad del SEI.	Reporte final de incidente.
FIN DE PROCEDIMIENTO			

Comunicación con las partes interesadas

A continuación, se muestra el árbol de llamadas por Niveles:

Grupo de Trabajo de Manejo de Crisis Tecnológico

Titular

Nombre	María Yolanda Nigo González
Puesto	Directora de Desarrollo de Sistemas
Correo electrónico	yolanda.nigo@iecm.mx
Teléfono trabajo	54833800 Ext. 4618

Suplente

Nombre	Ana Angelica González Oliva
Puesto	Directora de Infraestructura Informática
Correo electrónico	ana.gonzalez@iecm.mx
Teléfono trabajo	54833800 Ext. 3819

Titular

Nombre	Ana Angelica González Oliva
Puesto	Directora de Infraestructura Informática
Correo electrónico	ana.gonzalez@iecm.mx
Teléfono trabajo	54833800 Ext. 3819

Suplente

Nombre	María Yolanda Nigo González
Puesto	Directora de Desarrollo de Sistemas
Correo electrónico	yolanda.nigo@iecm.mx
Teléfono trabajo	54833800 Ext. 4618

Titular

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext.4605

Suplente

Nombre	Paula Robles Mass Tapia
Puesto	Subdirectora de Sistemas de Información
Correo electrónico	paula.roblesmass@iecm.mx
Teléfono trabajo	54833800 Ext. 4617

Titular

Nombre	Paula Robles Mass Tapia
Puesto	Subdirectora de Sistemas de Información
Correo electrónico	paula.roblesmass@iecm.mx
Teléfono trabajo	54833800 Ext. 4617

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext.3605



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 43 de 68

Revisión: 01

Fecha de revisión: 13/03/26

Fecha de emisión: 22/10/21

Persona Coordinadora del Plan de Continuidad

Titular

Nombre	Estefanía Mena Ibarra
Puesto	Titular de la Unidad Técnica de Servicios Informáticos
Correo electrónico	estefania.mena@iecm.mx
Teléfono trabajo	54833800 Ext. 4622

Suplente

Nombre	Ana Angelica González Oliva
Puesto	Directora de Infraestructura Informática
Correo electrónico	ana.gonzalez@iecm.mx
Teléfono trabajo	54833800 Ext. 3819



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 44 de 68

Revisión: 01

Fecha de revisión: 13/03/26

Fecha de emisión: 22/10/21

Equipos de recuperación

Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad).

Titular

Nombre	Miguel Angel García Morales
Puesto	Jefe de Departamento Web, Seguridad y Nuevas Tecnologías
Correo electrónico	miguel.garcia@iecm.mx
Teléfono trabajo	54833800 Ext. 4683

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext. 4605

Asignación, préstamo o devolución de bienes informáticos

Titular

Nombre	Alejandro Magaña Reyes
Puesto	Jefe de Departamento de Soporte Técnico y Mesa de Ayuda
Correo electrónico	alejandro.magana@iecm.mx
Teléfono trabajo	54833800 Ext. 4690

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext.4605

Soporte Técnico

Titular

Nombre	Alejandro Magaña Reyes
Puesto	Jefe de Departamento de Soporte Técnico y Mesa de Ayuda
Correo electrónico	alejandro.magana@iecm.mx
Teléfono trabajo	54833800 Ext. 4690

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext.4605



**Plan de Continuidad
SEI**

IECM-JA042-26
Código: UTSI/PL/01

Página 45 de 68
Revisión: 01

Fecha de revisión: 13/03/26
Fecha de emisión: 22/10/21

Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Bienes informáticos).

Titular

Nombre	Alejandro Magaña Reyes
Puesto	Jefe de Departamento de Soporte Técnico y Mesa de Ayuda
Correo electrónico	alejandro.magana@iecm.mx
Teléfono trabajo	54833800 Ext. 4690

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext.4605

Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Centro de Cómputo).

Titular

Nombre	Victor Hugo Oropeza Cadena
Puesto	Jefe de Departamento de Servidores y Bases de Datos
Correo electrónico	victor.oropeza@iecm.mx
Teléfono trabajo	54833800 Ext. 4681

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext.4605

Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Comunicaciones).

Titular

Nombre	Marco Tulio Conde Cruz
Puesto	Jefe de Departamento de Redes y Comunicaciones
Correo electrónico	marcotulio.conde@iecm.mx
Teléfono trabajo	54833800 Ext.4694

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	javier.castaneda@iecm.mx
Teléfono trabajo	54833800 Ext. 4605



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 46 de 68

Revisión: 01

Fecha de revisión: 13/03/26

Fecha de emisión: 22/10/21

Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Redes, CCTV y equipos CISCO).

Titular

Nombre	Marco Tulio Conde Cruz
Puesto	Jefe de Departamento de Redes y Comunicaciones
Correo electrónico	marcotulio.conde@iecm.mx
Teléfono trabajo	54833800 Ext.4694

Suplente

Nombre	Javier Castañeda López
Puesto	Subdirector de Seguridad, Redes y Cómputo
Correo electrónico	alejandro.magana@iecm.mx
Teléfono trabajo	54833800 Ext. 4605

Desarrollo de Sistemas Informáticos

Titular

Nombre	Paula Robles Mass Tapia
Puesto	Subdirectora de Sistemas de Información
Correo electrónico	paula.roblesmass@iecm.mx
Teléfono trabajo	54833800 Ext. 4617

Suplente

Nombre	María Yolanda Nigo González
Puesto	Directora de Desarrollo de Sistemas
Correo electrónico	yolanda.nigo@iecm.mx
Teléfono trabajo	54833800 Ext. 4618

ANEXO 3. Plan de Continuidad de Negocio SEI-BCP.

Objetivo

Contar con un procedimiento de recuperación operativa en caso de presentarse una indisponibilidad del Sistema Electrónico por Internet (SEI) durante los procesos de participación ciudadana.

Alcance

Realizar la alineación operativa y metodológica del Plan de Continuidad del Sistema Electrónico por Internet (SEI), a la norma ISO 22301:2019 de Seguridad y resiliencia de Sistemas de gestión de continuidad de negocio y a la norma ISO/TS 54001:2019 del Sistema de Gestión de Calidad Electoral (SGCE), garantizando el pleno cumplimiento con la normatividad en materia aplicable al Instituto Electoral de la Ciudad de México.

Marco normativo

El presente documento se encuentra basado en los lineamientos expresados en la Norma:

-) ISO 22301:2019 de Seguridad y resiliencia de Sistemas de gestión de continuidad de negocio.
-) ISO 54001:2019 Sistemas de gestión de calidad-Requisitos específicos para la aplicación de la Norma ISO 9001:2015 a organizaciones electorales en todos los niveles de gobierno.

Asimismo, en la declaración de cumplimiento normativo de la Unidad Técnica de Servicios Informáticos, se señala la normatividad vigente aplicable.

Definiciones

Término	Descripción
Análisis de Impacto al Negocio (BIA)	Análisis de Impacto al Negocio, (BIA, <i>Business Impact Analysis</i>), tiene como objetivo identificar los procesos críticos del negocio, así como posibles impactos en caso de no estar disponible el servicio analizado.
Análisis del riesgo	Procedimiento que se debe llevar a cabo para identificar los elementos o los factores que tienen la posibilidad de generar riesgos (u oportunidades) que afecten en forma negativa (o positiva) la operación de la organización y con ello comprender su naturaleza y su nivel de riesgo.
BCP	Plan de Continuidad del Negocio (<i>Business Continuity Plan</i> , BCP).
Desastre	Se entiende como un evento repentino, no planeado, que ocasiona la “inhabilidad de un servicio o proceso o parte de ella”, para ejecutar sus procesos críticos por un periodo determinado que resulta en daño o pérdida a un nivel inaceptable. Desde el punto de vista de Tecnología de Información, se define como un evento repentino no planeado que ocasiona la “no disponibilidad” de los servicios informáticos por un periodo tal que, para restablecer estos servicios, es necesario utilizar facilidades alternas de cómputo y telecomunicaciones en otra localidad en caso de ser necesario.
Impacto	Conjunto de los efectos que un suceso o un hecho producen en su entorno físico o social.
MARC	Acrónimo de “ <i>Minimum Acceptable Recovery Configuration</i> ”. Es la Configuración de Recuperación Mínima Aceptable y comprende los elementos humanos, técnicos y materiales que se requieren como mínimo para recuperar los servicios de cómputo y telecomunicaciones que soportan las funciones críticas de operación de la Institución.
Procesos críticos	Son aquellos procesos que por su alta prioridad es indispensable su recuperación en el menor tiempo posible. Ante una contingencia, los procesos críticos no pueden postergar su operación por un tiempo prolongado ya que se pondría en riesgo la integridad de los servicios de la Institución.
Registro vital	Es aquella documentación que contiene información esencial para continuar con la operación ante una interrupción. Pueden estar en formato electrónico, generados por medios electrónicos (computadoras, CD’s, microfichas, etc.), así como medios físicos (formas especiales, reportes, material de referencia, etc.).
RPO	Punto de Recuperación Objetivo (por sus siglas en inglés, <i>Recovery Point Objective</i>), es el punto en el tiempo (anterior a la contingencia) en el cual, se pueden recuperar los datos. Por ejemplo, realizar respaldos cada 4 horas (RPO=4). *Esta medida de tiempo es independiente del RTO.
RTO	Tiempo de Recuperación Objetivo (por sus siglas en inglés, <i>Recovery Time Objective</i>), es el tiempo requerido para recuperar servicios definidos como críticos. Este tiempo es medido desde el momento de la contingencia hasta el reinicio de las operaciones. Por ejemplo, un proceso crítico no puede tolerar interrupciones mayores a 1 día (RTO=1 día). *Esta medida de tiempo es independiente del RPO.



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 49 de 68
Revisión: 01

Fecha de revisión: 13/03/26
Fecha de emisión: 22/10/21

Políticas de operación

De acuerdo con la Evaluación de Riesgos y el Análisis de Impacto al Negocio, se describen los riesgos operativos detectados y viables para el Sistema Electrónico por Internet (SEI).

Riesgo	Escenario
Falla de la función de servicio al usuario (Help Desk) - Componente CAT dentro del SEI Módulo.	La función de servicio al usuario no se encuentra habilitada, lo cual impacta en los servicios proporcionados por el instituto o en la indisponibilidad del SEI en caso de presentarse alguna falla. (módulo).
La aplicación SEI no puede identificar la credencial para votar en el momento en que el ciudadano quiere ejercer su derecho.	El aplicativo podría presentar problemas cuando requiera identificar la credencial para votar.
Inefectiva selección de proveedor, evaluación y prácticas de Benchmarking.	La falta de un proceso para administrar la calidad del proveedor podría ocasionar problemas en los servicios proporcionados por el instituto o en el proveedor contratado para el SEI.
Falta de capacitación del personal.	Una falta de capacitación del personal responsable y de apoyo para la ciudadanía para ejercer su derecho, podría ocasionar que el SEI no sea usado de manera correcta o en su caso se lleve mayor tiempo del estimado.

También han de tomarse en cuenta otros tipos de escenarios con una menor probabilidad de ocurrencia, entre los cuales están los siguientes:

-) Falla o pérdida de dispositivo móvil.
-) Contingencias naturales y/o sociales que pudieran interrumpir su operación normal.
-) Falla en los dispositivos de votación ubicados en el voto vía electrónica (voto offline) que impida la continuidad operativa.
-) Robo o extravío de los dispositivos de votación ubicados en el voto vía electrónica (voto offline).



Plan de Continuidad SEI

IECM-JA042-26
Código: UTSI/PL/01

Página 50 de 68
Revisión: 01

Fecha de revisión: 13/03/26
Fecha de emisión: 22/10/21

Tipo de incidentes

A continuación, se describen los tipos de incidentes operativos que podrían presentarse durante la ejecución del SEI en voto vía electrónica, así como una serie de actividades que deberán realizarse con base al incidente presentado.

a. Falla de la tableta en donde reside el aplicativo SEI.

Tipo de incidentes	Actividades
1. No enciende la tableta:	<ul style="list-style-type: none">) Conectar el dispositivo a la batería externa.) Esperar 5 minutos a que el dispositivo inicie operación.) Ingresar de nuevo a la aplicación del Sistema Electrónico por Internet.) Retirar la batería externa hasta que el dispositivo reporte 100% la carga.
2. No funciona el SEI:	<ul style="list-style-type: none">) Mantener oprimidos: el botón superior de apagado + el botón frontal de inicio de la tableta.) Soltar los botones hasta que aparezca el icono de una manzana.) Esperar a que el equipo inicie operación.) Ingresar de nuevo a la aplicación del Sistema Electrónico por Internet.
3. Sin conexión a Internet:	<ul style="list-style-type: none">) Intentar de nuevo usar la aplicación del Sistema Electrónico por Internet.
4. Falla de la tableta provocada por el ciudadano:	<ul style="list-style-type: none">) Revisar el estado de la tableta.) Mantener oprimidos: el botón superior de apagado + el botón frontal de inicio de la tableta.) Soltar los botones hasta que aparezca el icono de una manzana.) Esperar a que el equipo inicie operación.) Ingresar de nuevo a la aplicación del Sistema Electrónico por Internet.
5. Falla del soporte por parte del personal del IECM para el uso de la tableta:	<ul style="list-style-type: none">) Consultar con otro personal de soporte del IECM el uso del SEI en la tableta.) Solicitar apoyo al Centro de Atención Telefónica.



**Plan de Continuidad
SEI**

IECM-JA042-26

Código: UTSI/PL/01

Página 51 de 68

Revisión: 01

Fecha de revisión: 13/03/26

Fecha de emisión: 22/10/21

b. Robo o extravío de tableta en donde reside el aplicativo SEI

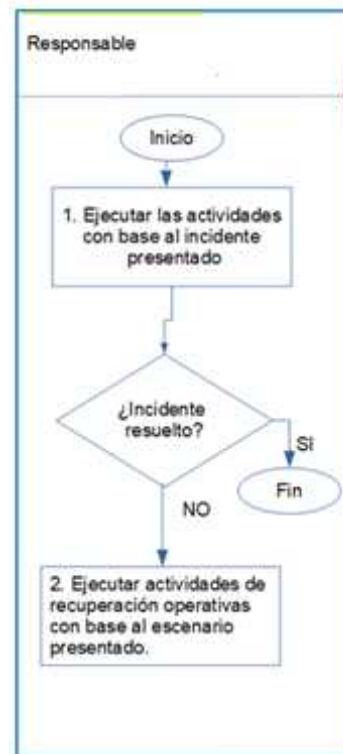
1. Robo o extravío de la tableta:	<ul style="list-style-type: none">) Informar a la dirección distrital.) Realizar acciones legales.) Reportar el incidente.) Registra el incidente.) Consultar existencias de tableta para su sustitución.
--	---

c. Contingencia natural

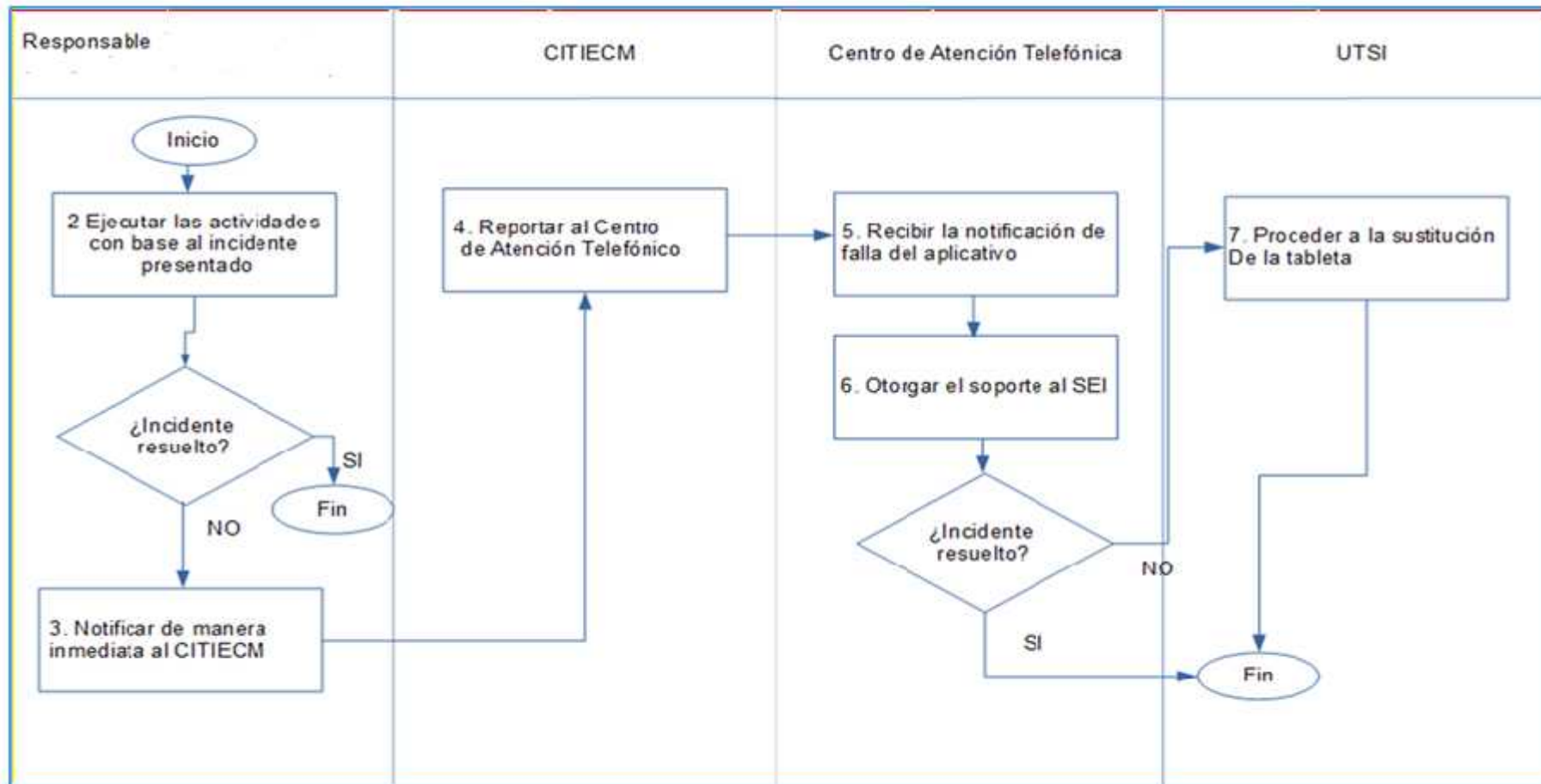
1. Tormenta eléctrica / Inundación:	<ul style="list-style-type: none">) Revisar y en su caso proteger a las tabletas en donde reside el SEI de posibles afectaciones por la lluvia o agua acumulada.) Informar a la dirección distrital.) Si se considera necesario, suspender temporalmente la recepción de los votos y las opiniones, e informar de la suspensión, a quienes estén esperando para emitir su voto y sus opiniones.
2. Sismo	<ul style="list-style-type: none">) Revisar que las instalaciones y equipos se encuentren en buen estado.) Validar que las tabletas cuenten con el servicio de internet para la funcionalidad del SEI.) Informar a la dirección distrital.) Si se considera necesario, suspender temporalmente la recepción de los votos y las opiniones, e informar de la suspensión, a quienes estén esperando para emitir su voto y sus opiniones.

Diagrama de flujo

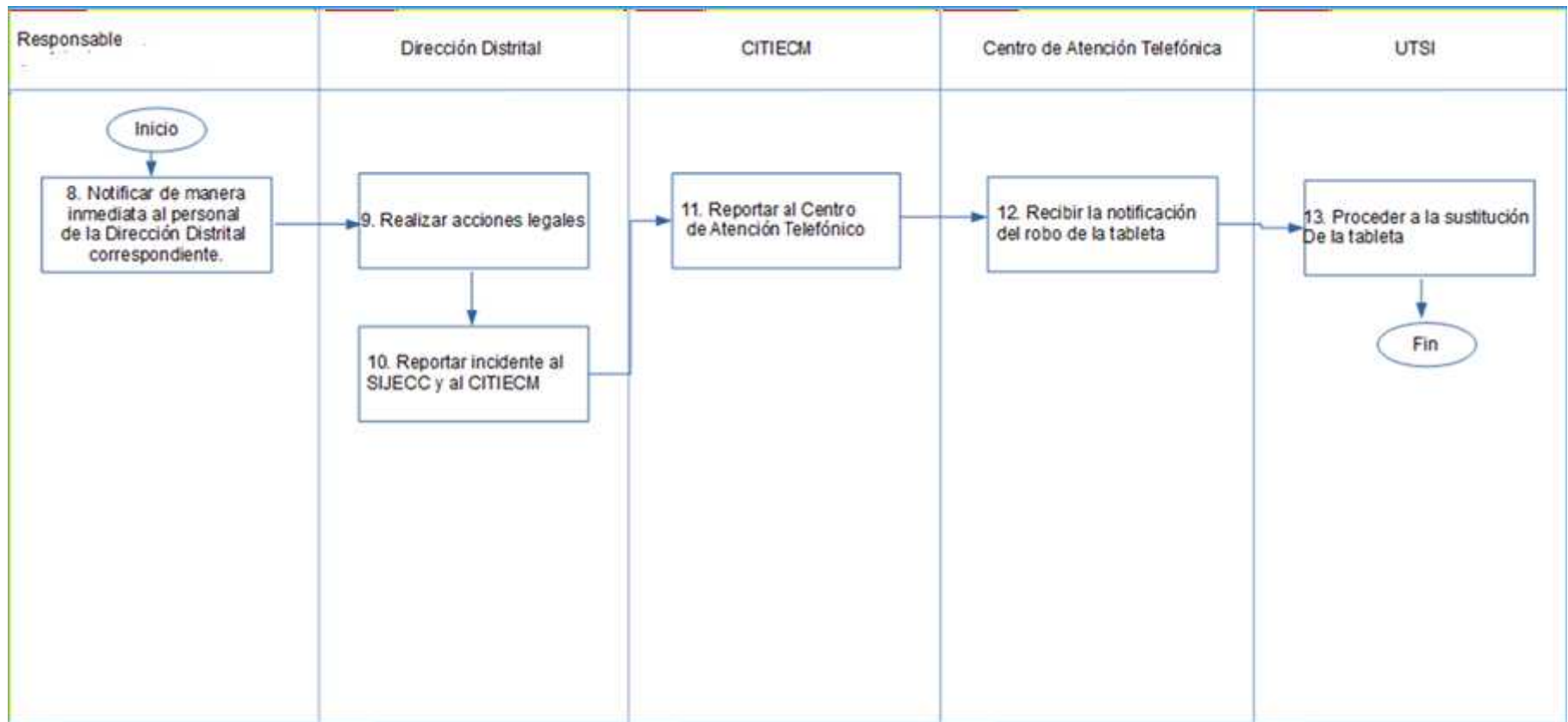
El procedimiento para la recuperación de la operatividad del SEI en caso de presentarse una indisponibilidad de este, se muestra en el siguiente diagrama de manera general:



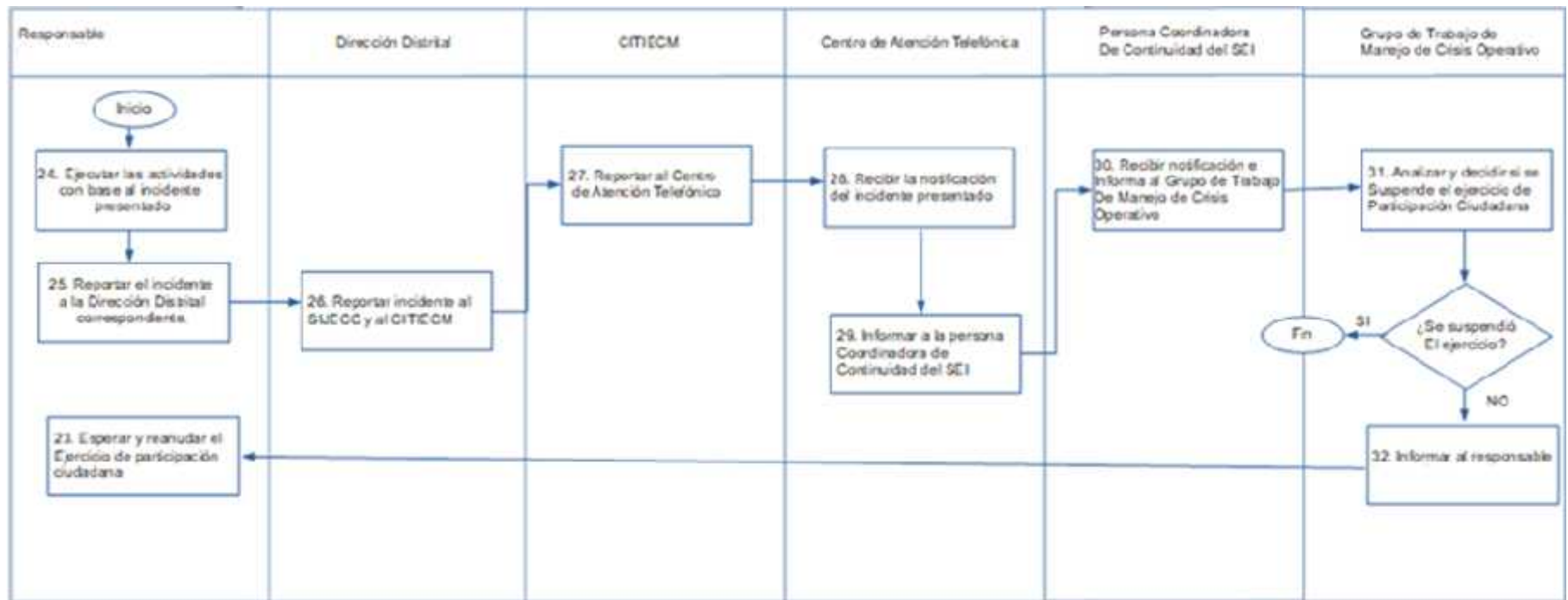
a. Falla de la tableta en donde reside el aplicativo SEI.



b. Robo o extravío de tableta en donde reside el aplicativo SEI.



c. Contingencia natural.





**Procedimiento de
recuperación tecnológica del
SEI - DRP**

IECM- JA042-26

Código: UTSI/PL/01

Página 56 de 68

Revisión: 01

Fecha de revisión: 13/03/26

Fecha de emisión: 22/10/21

Procedimientos de recuperación operativa.

Número	Actividad	Unidad Responsable	Documento Empleado
1	Ejecutar las actividades con base al incidente presentado (consultar el tipo de incidentes que corresponda).	Responsable del Órgano Desconcentrado.	Cuadro de tipo de incidentes. J a) Falla de la tableta en donde reside el aplicativo SEI. J b) Robo o extravío de la tableta. J c) Contingencia natural.
	¿Se solucionó el problema? SI: FIN DE PROCEDIMIENTO NO: Continuar en actividad 2.		
2	Ejecutar actividades de recuperación operativas con base al escenario presentado.	Responsable del Órgano Desconcentrado.	N/A



Procedimiento de
recuperación tecnológica del
SEI - DRP

IECM- JA042-26

Código: UTSI/PL/01

Página 57 de 68

Revisión: 01

Fecha de revisión: 13/03/26

Fecha de emisión: 22/10/21

a. Falla de la tableta en donde reside el aplicativo SEI			
Número	Actividad	Unidad Responsable	Documento Empleado
2	Realizar las acciones pertinentes con base al problema presentado consulta la a) Falla de la tableta en donde reside el aplicativo SEI.	Responsable del Órgano Desconcentrado.	
	¿El incidente fue resuelto? SI: FIN DE PROCEDIMIENTO NO: Continuar en actividad 4.		
3	Notificar de manera inmediata al CITIECM al teléfono 800 433 322.	Responsable del Órgano Desconcentrado.	N/A
4	Reportar al Centro de Atención Telefónico, al número 55843800 extensión 4690 .	CITIECM.	N/A
5	Recibir la notificación de falla del aplicativo SEI.	Centro de Atención Telefónica / UTSI.	N/A
6	Otorgar el soporte al SEI con base a los problemas presentados.	Centro de Atención Telefónica / UTSI.	N/A
	¿El soporte al SEI fue resuelto? Si: FIN DE PROCEDIMIENTO. No: Continua en actividad 7.	Coordinador de Continuidad del SEI.	
7	Proceder a la sustitución de la tableta. FIN DEL PROCEDIMIENTO.	UTSI.	N/A



**Procedimiento de
recuperación tecnológica del
SEI - DRP**

IECM- JA042-26

Código: UTSI/PL/01

Página **58** de **68**

Revisión: 01

Fecha de revisión: 13/03/26

Fecha de emisión: 22/10/21

b. Robo o extravío de tableta en donde reside el aplicativo SEI			
Número	Actividad	Unidad Responsable	Documento Empleado
8	Notificar de manera inmediata al personal de la Dirección Distrital correspondiente de acuerdo a b) Robo o extravío de tableta donde reside el aplicativo SEI.	Responsable del Órgano Desconcentrado.	N/A
9	Realizar las acciones legales a que haya lugar.	Dirección Distrital.	N/A
10	Reportar el incidente a través del SIJECC, e informe de los hechos al CITIECM, al teléfono 800 433 322.	Dirección Distrital.	
11	Reportar al Centro de Atención Telefónico, al número 55843800 extensión 4690 .	CITIECM.	N/A
12	Recibir la notificación de robo de tableta.	Centro de Atención Telefónica / UTSI.	N/A
13	Procederá a la sustitución de la tableta. FIN DEL PROCEDIMIENTO.	UTSI.	N/A

NOTA: Para los escenarios de:

- a. Falla de la tableta en donde reside el aplicativo SEI.
- b. Robo o extravío de tableta en donde reside el aplicativo SEI ubicadas en voto vía electrónica (voto offline).

Se podría operar de la siguiente manera:

En caso de que se sustituya la Tableta y aun así no sea posible continuar con la emisión del sufragio, o bien que ya no existieran Tabletas disponibles para sustitución, se deberá de ejecutar la siguiente acción:

-) Se solicitará al personal de la DEOEyG dispuesto en el centro de distribución más cercano, la documentación y materiales electivos/consultivos necesarios para reanudar y garantizar la emisión del sufragio de manera continua y en su modalidad tradicional.



**Procedimiento de
recuperación tecnológica del
SEI - DRP**

IECM- JA042-26

Código: UTSI/PL/01

Página **59** de **68**

Revisión: 01

Fecha de revisión: 13/03/26

Fecha de emisión: 22/10/21

d. Contingencia natural			
Número	Actividad	Unidad Responsable	Documento Empleado
14	Realizar las acciones pertinentes con base al problema presentado consulta la c) Contingencia natural.	Responsable del Órgano Desconcentrado.	N/A
15	Reportar el incidente a la Dirección Distrital correspondiente.	Responsable del Órgano Desconcentrado.	N/A
16	Reportar el incidente a través del SIJECC, e informe de los hechos al CITIECM al teléfono 800 433 322.	Dirección Distrital.	
17	Reportar al Centro de Atención Telefónico, al número 55843800 extensión 4690 .	CITIECM.	N/A
18	Recibir la notificación del incidente presentado.	Centro de Atención Telefónica / UTSI.	N/A
19	Informar a la persona Coordinadora de Continuidad del SEI.	Centro de Atención Telefónica / UTSI.	
20	Recibir e informar al Grupo de Manejo de Crisis Operativo.	Coordinadora de Continuidad del SEI.	
21	Analizar y decidir si se suspende el ejercicio de participación ciudadana.	Grupo de Manejo de Crisis Operativo.	N/A
	¿Se suspendió el ejercicio de participación ciudadana? SI: FIN DE PROCEDIMIENTO. NO: Informar al responsable de la Mesa Receptora de Votación y Opinión (MRVyO) la espera y reanudación del ejercicio.	Grupo de Manejo de Crisis Operativo.	N/A
22	Esperar y reanudar el ejercicio de participación ciudadana.	Responsable del Órgano Desconcentrado.	N/A
FIN DE PROCEDIMIENTO			



**Procedimiento de
recuperación tecnológica del
SEI - DRP**

IECM- JA042-26

Código: UTSI/PL/01

Página 60 de 68

Revisión: 01

Fecha de revisión: 13/03/26

Fecha de emisión: 22/10/21

ANEXO 4. Plan de recuperación ante Desastres SEI - DRP.

Objetivo

Contar con un procedimiento de recuperación tecnológica en caso de presentarse una indisponibilidad del Sistema Electrónico por Internet (SEI) durante los procesos de participación ciudadana.

Alcance

Realizar la alineación operativa y metodológica del Plan de Continuidad del Sistema Electrónico por Internet a la norma ISO 22301:2019 de Seguridad y resiliencia de Sistemas de gestión de continuidad de negocio y la norma ISO/TS 54001:2019 del Sistema de Gestión de Calidad Electoral (SGCE), garantizando asimismo el pleno cumplimiento con la normatividad en materia aplicable al Instituto Electoral de la Ciudad de México.

Con base a la Evaluación de Riesgos realizada de manera previa y tomando en cuenta los impactos y tiempos críticos definidos en el Análisis de Impacto al Negocio desarrollado.

Los riesgos tecnológicos más viables de presentarse son:

Riesgos	Escenario
Operación deficiente por obsolescencia tecnológica.	Tecnología obsoleta provocaría una “no disponibilidad” de los servicios tecnológicos, por falta de mantenimiento, falta de repuestos, etc.
Falta de pruebas en las diferentes plataformas o equipos tecnológicos que soportan el SEI con el fin de validar la funcionalidad correcta del aplicativo (Android, IOS).	Una falta de pruebas en las diferentes plataformas y equipos podría ocasionar una “no disponibilidad” del SEI.

Así mismo se toman en cuenta otro tipo de escenario con menor probabilidad de ocurrencia, los cuales son:

-) Enlace de comunicaciones con el Servicio de Internet para Oficinas Centrales del IECM (Servicio de internet y Red LAN).
-) Enlace de comunicaciones con el Servicio de Internet para Oficinas Centrales del IECM.
-) Servicio de suministro eléctrico al centro de cómputo del IECM.
-) Suministro de condiciones ambientales estables (Aire Acondicionado).
-) Servicio de seguridad en Internet.



Procedimiento de recuperación tecnológica del SEI - DRP

IECM- JA042-26

Código: UTSI/PL/01

Página 61 de 68

Revisión: 01

Fecha de revisión: 13/03/26

Fecha de emisión: 22/10/21

-) Servicio de seguridad central en servidores.
-) Servicio de Base de datos.
-) Centro de Cómputo del IECM.

Marco normativo

El presente documento se encuentra basado en los lineamientos expresados en la Norma:

-) ISO 22301:2019 de Seguridad y resiliencia de Sistemas de gestión de continuidad de negocio.
-) ISO 54001:2019 Sistemas de gestión de calidad-Requisitos específicos para la aplicación de la Norma ISO 9001:2015 a organizaciones electorales en todos los niveles de gobierno.

Asimismo, en la declaración de cumplimiento normativo de la Unidad Técnica de Servicios Informáticos, se señala la normatividad vigente aplicable.

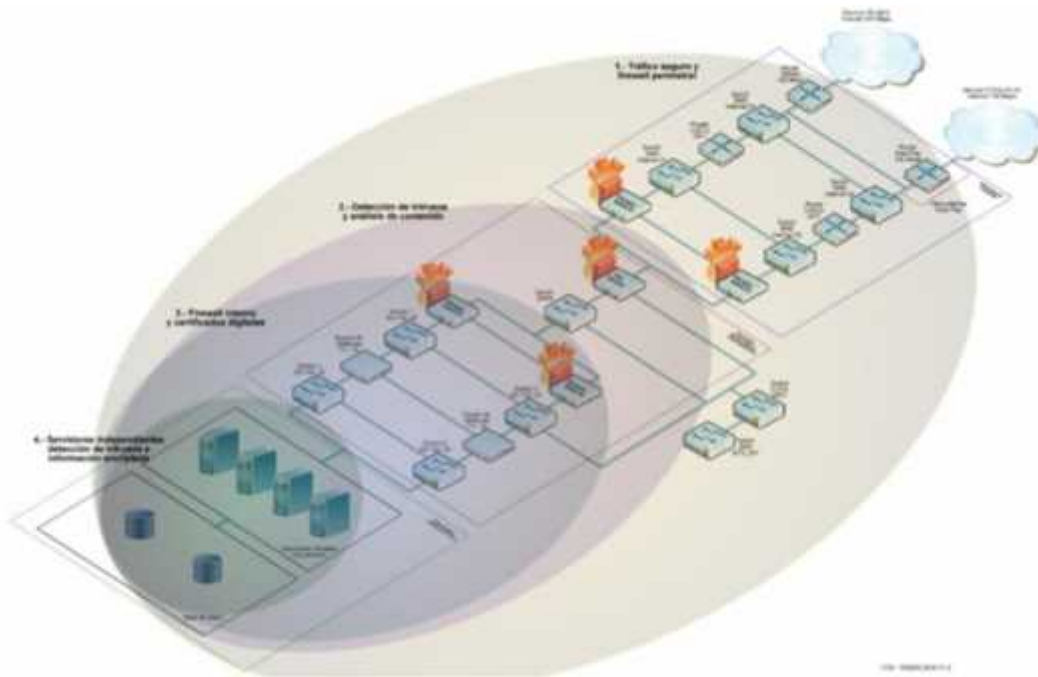
Definiciones

Término	Descripción
Análisis de Impacto al Negocio (BIA)	Análisis de Impacto al Negocio, (BIA, <i>Business Impact Analysis</i>), tiene como objetivo identificar los procesos críticos del negocio, así como posibles impactos en caso de no estar disponible el servicio analizado.
Análisis del riesgo	Procedimiento que se debe llevar a cabo para identificar los elementos o los factores que tienen la posibilidad de generar riesgos (u oportunidades) que afecten en forma negativa (positiva) la operación de la organización y con ello comprender su naturaleza y su nivel de riesgo.
Desastre	Se entiende como un evento repentino, no planeado, que ocasiona la “inhabilidad de un servicio o proceso o parte de ella”, para ejecutar sus procesos críticos por un periodo determinado que resulta en daño o pérdida a un nivel inaceptable. Desde el punto de vista de Tecnología de Información, se define como un evento repentino no planeado que ocasiona la “no disponibilidad” de los servicios informáticos por un periodo tal que, para restablecer estos servicios, es necesario utilizar facilidades alternas de cómputo y telecomunicaciones en otra localidad en caso de ser necesario.
Impacto	Conjunto de los efectos que un suceso o un hecho producen en su entorno físico o social.
MARC	Acrónimo de “ <i>Minimum Acceptable Recovery Configuration</i> ”. Es la Configuración de Recuperación Mínima Aceptable y comprende los elementos humanos, técnicos y materiales que se requieren como mínimo para recuperar los servicios de cómputo y telecomunicaciones que soportan las funciones críticas de operación de la Institución.
Procesos críticos	Son aquellos procesos que por su alta prioridad es indispensable su recuperación en el menor tiempo posible. Ante una contingencia, los procesos críticos no pueden postergar su operación por un tiempo prolongado ya que se pondría en riesgo la integridad de los servicios de la Institución.
Registro vital	Es aquella documentación que contiene información esencial para continuar con la operación ante una interrupción. Pueden estar en formato electrónico, generados por medios electrónicos (computadoras, CD’s, microfichas, etc.), así como medios físicos (formas especiales, reportes, material de referencia, etc.).
RPO	Punto de Recuperación Objetivo (por sus siglas en inglés, <i>Recovery Point Objective</i>), es el punto en el tiempo (anterior a la contingencia) en el cual, se pueden recuperar los datos. Por ejemplo, realizar respaldos cada 4 horas (RPO=4). *Esta medida de tiempo es independiente del RTO.
RTO	Tiempo de Recuperación Objetivo (por sus siglas en inglés, <i>Recovery Time Objective</i>), es el tiempo requerido para recuperar servicios definidos como críticos. Este tiempo es medido desde el momento de la contingencia hasta el reinicio de las operaciones. Por ejemplo, un proceso crítico no puede tolerar interrupciones mayores a 1 día (RTO=1 día). *Esta medida de tiempo es independiente del RPO.

Infraestructura tecnológica del SEI

La Infraestructura que soporta el Voto Electrónico para la operación del SEI se muestra a continuación:

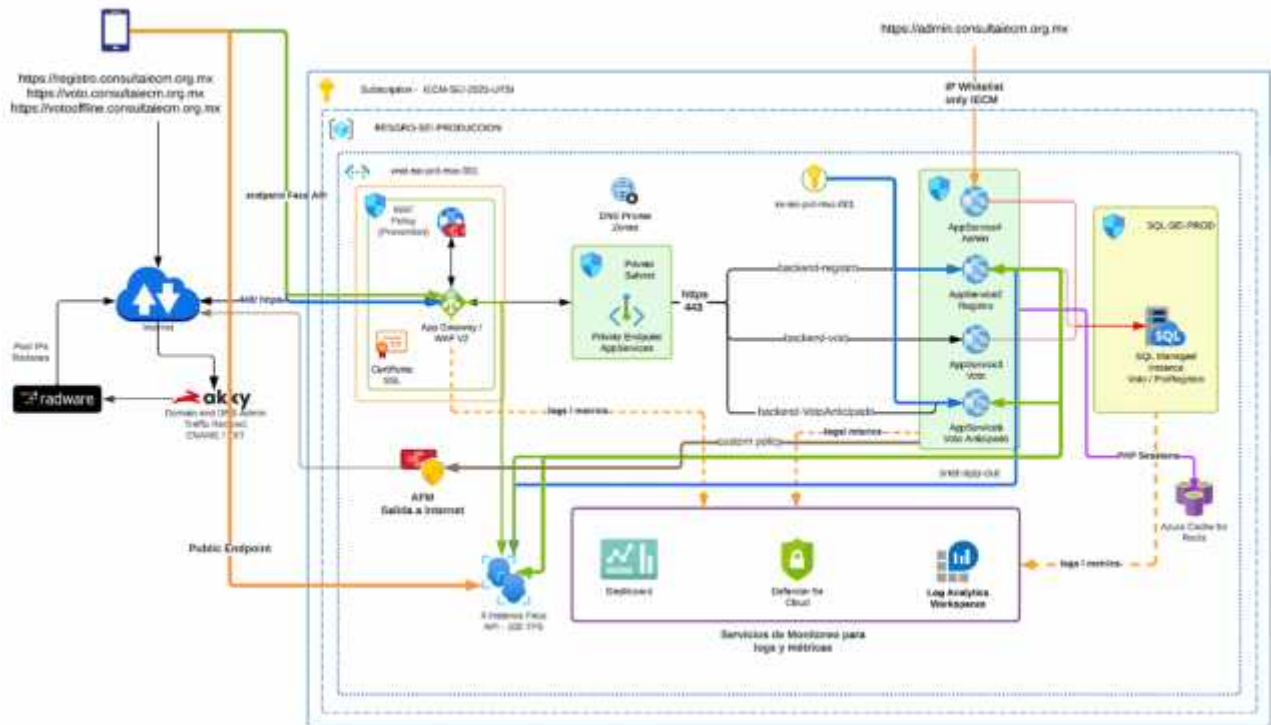
a) Infraestructura en sitio.



Dicha infraestructura está compuesta por diferentes componentes tanto de hardware como de software, los cuales se describen en la siguiente tabla:

Cantidad	Equipo	Marca	Modelo
2	Firewall	CISCO	ASA 5545X
2	Balanceador	F5	BIG-IP-1600
2	Balanceador	F5	BIG-IP-i4600
2	Servidor	Alto Rendimiento	X86
1	Unidad de Almacenamiento	DELL	STORAGE 2540 M2
2	Servidor	Alto Rendimiento	X86
1	Servidor	Alto Rendimiento	X86
2	Switch	CISCO	SG 102-24 24-PORT GIBABITS

b) Arquitectura en la nube.



Dicha arquitectura está compuesta por diferentes componentes, los cuales se describen en la siguiente tabla:

Recurso	Tipo	Estado de HA
WAF	Firewall	Radware
DNS	Dominios	Akky
agtw-sei-prd-mxc-001	Application Gateway	HA habilitado mediante múltiples instancias
api-face-prod-sei2025	Face API	HA nativo del servicio
api2-face-prod-sei2025	Face API	HA nativo del servicio
api3-face-prod-sei2025	Face API	HA nativo del servicio
api4-face-prod-sei2025	Face API	HA nativo del servicio
app-sei-prd-mxc-002	App Service	HA habilitado mediante múltiples instancias
app-sei-prd-mxc-003	App Service	HA habilitado mediante múltiples instancias
app-sei-prd-mxc-006	App Service	HA habilitado mediante múltiples instancias



**Procedimiento de
recuperación tecnológica del
SEI - DRP**

IECM- JA042-26

Código: UTSI/PL/01

Página **65** de **68**

Revisión: 01

Fecha de revisión: 13/03/26

Fecha de emisión: 22/10/21

Recurso	Tipo	Estado de HA
asp-sei-prd-mxc-004	App Service	HA habilitado mediante múltiples instancias
fw-sei-prd-mxc-001	Azure Firewall	HA administrado por Azure con redundancia interna
kv-sei-prd-mxc-001	Key Vault	HA nativo con replicación interna
redis-sei2025	Azure Cache for Redis	HA mediante réplica primaria/secundaria
sqlmi-sei-prd-mxc-001	SQL Managed Instance	HA nativo basado en clúster Always On

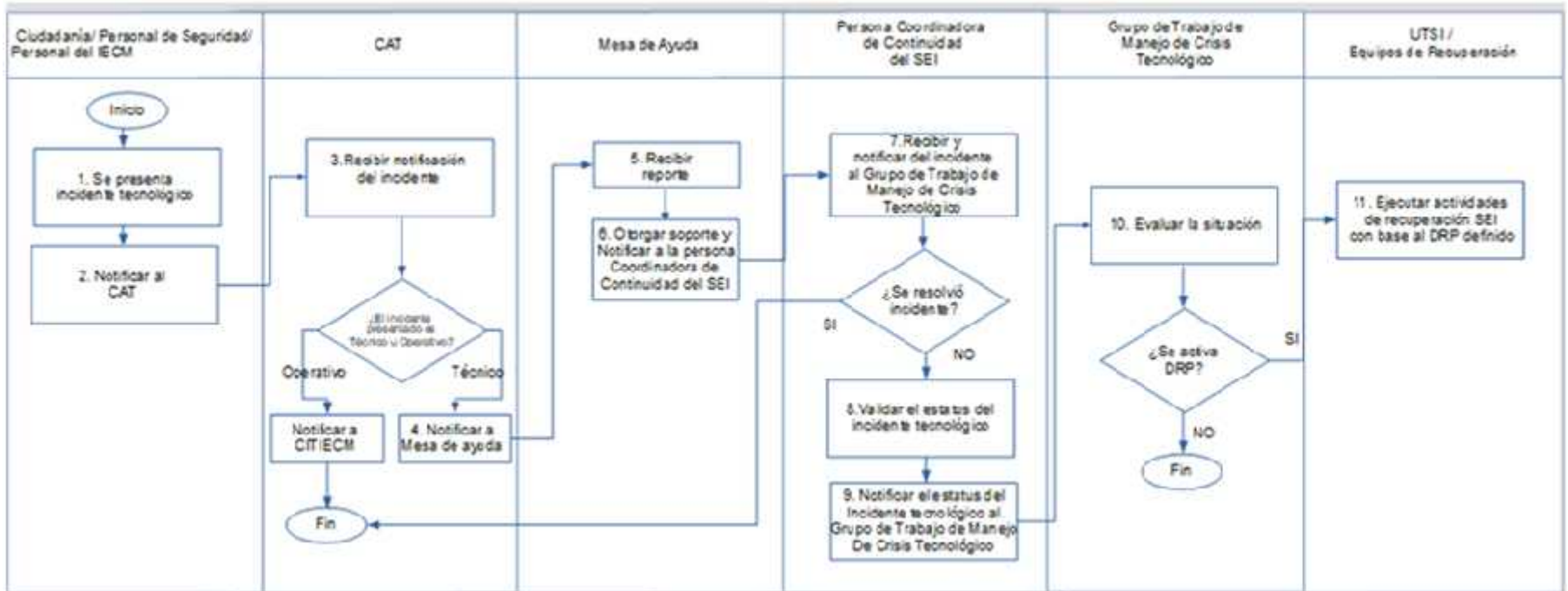
La estrategia de recuperación definida cuenta con los siguientes componentes:

) Máquinas y componentes virtuales en AZURE con HA.

Mediante los componentes de Azure Site Recovery de Microsoft Azure el equipo interno de IECM puede llevar a cabo la conexión de manera interna de sus aplicaciones hacia este servicio y poder ofrecer la recuperación del aplicativo.

Diagrama de flujo

El procedimiento para la recuperación tecnológica del SEI en caso de presentarse una indisponibilidad de este, se muestra en el siguiente diagrama de manera general:





Plan de Continuidad SEI

IECM- JA042-26
Código: UTSI/PL/01

Página 67 de 68
Revisión: 01

Fecha de revisión: 13/03/26
Fecha de emisión: 22/10/21

Procedimientos de recuperación operativa

Número	Actividad	Unidad Responsable	Documento Empleado
1	Se presenta incidente en el Sistema Electrónico por Internet (SEI).	Ciudadanía / personal del IECM.	
2	Notificar al Centro de Atención Telefónica (CAT).	Ciudadanía / personal del IECM.	N/A
3	Recibir el reporte del incidente y clasificarlo como técnico u operativo.) En caso de ser operativo se notificará a CITIECM. Fin de Procedimiento.) En caso de ser tecnológico, continuar en actividad 4.	Centro de Atención Telefónica (CAT).	N/A
4	Notificar a Mesa de Ayuda. el incidente presentado.	Centro de Atención Telefónica (CAT).	N/A
5	Recibir el reporte del incidente tecnológico.	Mesa de Ayuda / UTSI.	N/A
6	Otorgar el soporte requerido y reportar el incidente tecnológico a la persona Coordinadora de Continuidad del SEI.	Mesa de Ayuda / UTSI.	N/A
7	Recibir notificación del reporte de incidente e informar de este al Grupo de Trabajo de Manejo de Crisis del SEI.	Persona Coordinadora de Continuidad del SEI.	N/A
	¿El incidente se resolvió? SI: Fin de procedimiento. NO: Continuar en actividad 8.		
8	Validar el estatus del incidente técnico presentado.	Persona Coordinadora de Continuidad del SEI.	N/A
9	Notificar la continuidad del incidente presentado al Grupo de Trabajo de Manejo de Crisis del SEI.	Persona Coordinadora de Continuidad del SEI.	N/A



**Plan de Continuidad
SEI**

**IECM- JA042-26
Código: UTSI/PL/01**

Página 68 de 68

Revisión: 01

Fecha de revisión: 13/03/26

Fecha de emisión: 22/10/21

Número	Actividad	Unidad Responsable	Documento Empleado
10	Evaluar el estatus del incidente, acciones tomadas, tiempo transcurrido, entre otros. ¿Se activa el DRP? NO: Fin de procedimiento. SI: Continúa en actividad 12.	Grupo de Trabajo de Manejo de Crisis Tecnológico.	N/A
11	Activar y ejecutar actividades de recuperación del SEI con base al DRP desarrollado.	UTSI Equipos de Recuperación.	DRP desarrollado SEI.
FIN DE PROCEDIMIENTO			

HOJA DE FIRMAS