Plan de Continuidad del Sistema Electrónico por Internet

(SEI)

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

1. Contenido del documento

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.

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, *Business Impact Analysis*), 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, *Business Continuity Plan*).
BCM	Gestión de Continuidad del Negocio (por sus siglas en inglés, *Business Continuity Management*).
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. 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, *Disaster Recovery Plan*, 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 “*Minimum Acceptable Recovery Configuration*”. 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.).

Término	Descripción
RPO	Punto de Recuperación Objetivo (por sus siglas en inglés, *Recovery Point Objetive*), 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, *Recovery Point Objetive*), 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.
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

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.

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.- Falla de la función de servicio al cliente (Help Desk) - Componente CAT dentro del SEI

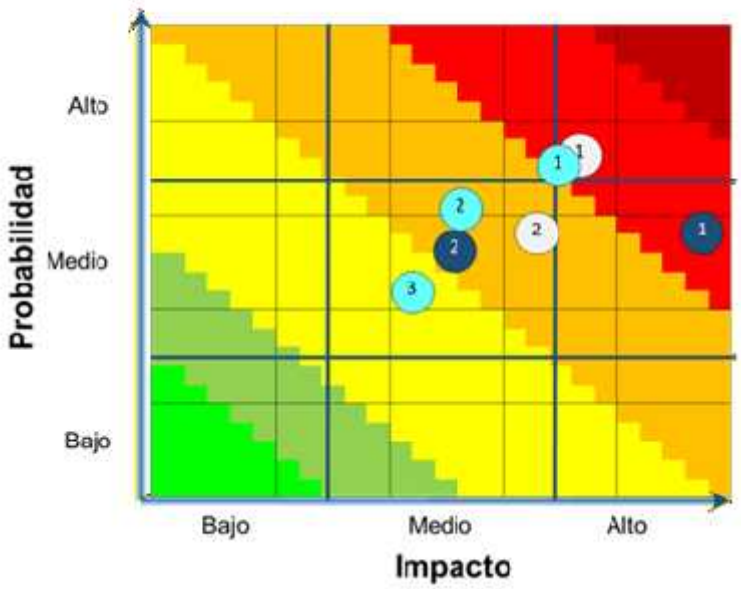
2.- Inefectiva selección de proveedor, evaluación y prácticas de Benchmarking

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



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 alterno 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 alterno, 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.

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: ➢ 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: ➢ 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. (Comunicaciones).	Consola de los equipos CISCO (red y telefonía).
	Correo electrónico.
	PRTG.
	Software de la consola de la red inalámbrica – ARUBA.
Desarrollo de Sistemas Informáticos.	Servicio de mensajes.
	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.

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.
	Software de la consola de la red inalámbrica – ARUBA.
Desarrollo de Sistemas Informáticos.	Servicio de mensajes.
	Correo electrónico.
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Seguridad).	Portal Radware.
	Correo electrónico.
	IPS.
	Forcerpoint.
	Mesa de Ayuda.
Mantenimiento Preventivo a Infraestructura de Cómputo, Comunicaciones, Seguridad y Centro de Cómputo (Centro de Cómputo).	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 alterno, 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? **(Si/No)**	Periodicidad del respaldo actual	RTO	RPO
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 Departamento de Redes y Comunicaciones	Si	Última versión	0 – 4 horas	No Aplica
	Inventario de direcciones IP	Electrónico	NAS	UTSI-Jefatura de Departamento de Redes y Comunicaciones	Si	Última versión	0 – 4 horas	1 día

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? **(Si/No)**	Periodicidad del respaldo actual	RTO	RPO
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? **(Si/No)**	Periodicidad del respaldo actual	RTO	RPO
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

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? **(Si/No)**	Periodicidad del respaldo actual	RTO	RPO
	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.

13. Premisas

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

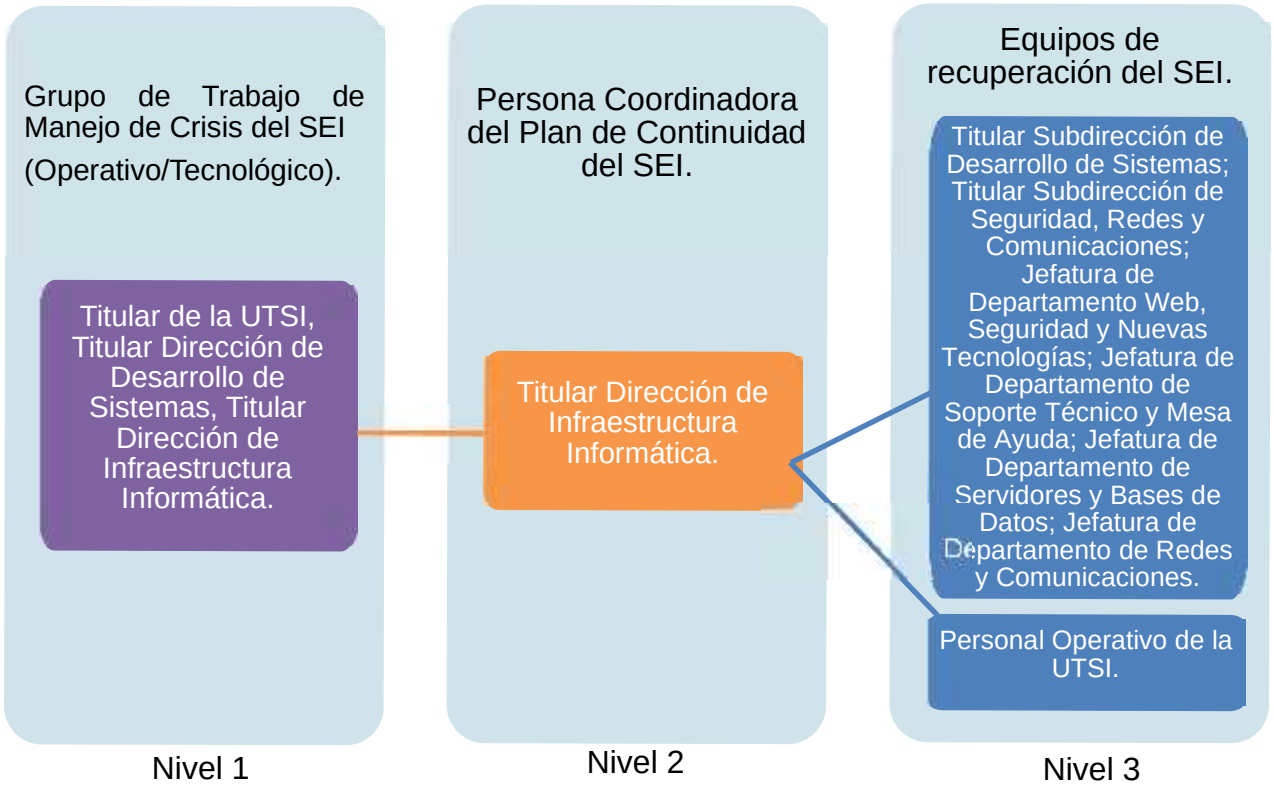
- Existe suficiente personal calificado y disponible para atender las responsabilidades de recuperación de los servicios críticos, es decir, se cuenta con el personal crítico que se encargará de la recuperación de la operación.

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

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

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	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

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.catañeda@iecm.mx
Teléfono trabajo	54833800 Ext. 4605

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 lo 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 cuentan 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 cuentan 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

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	

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:

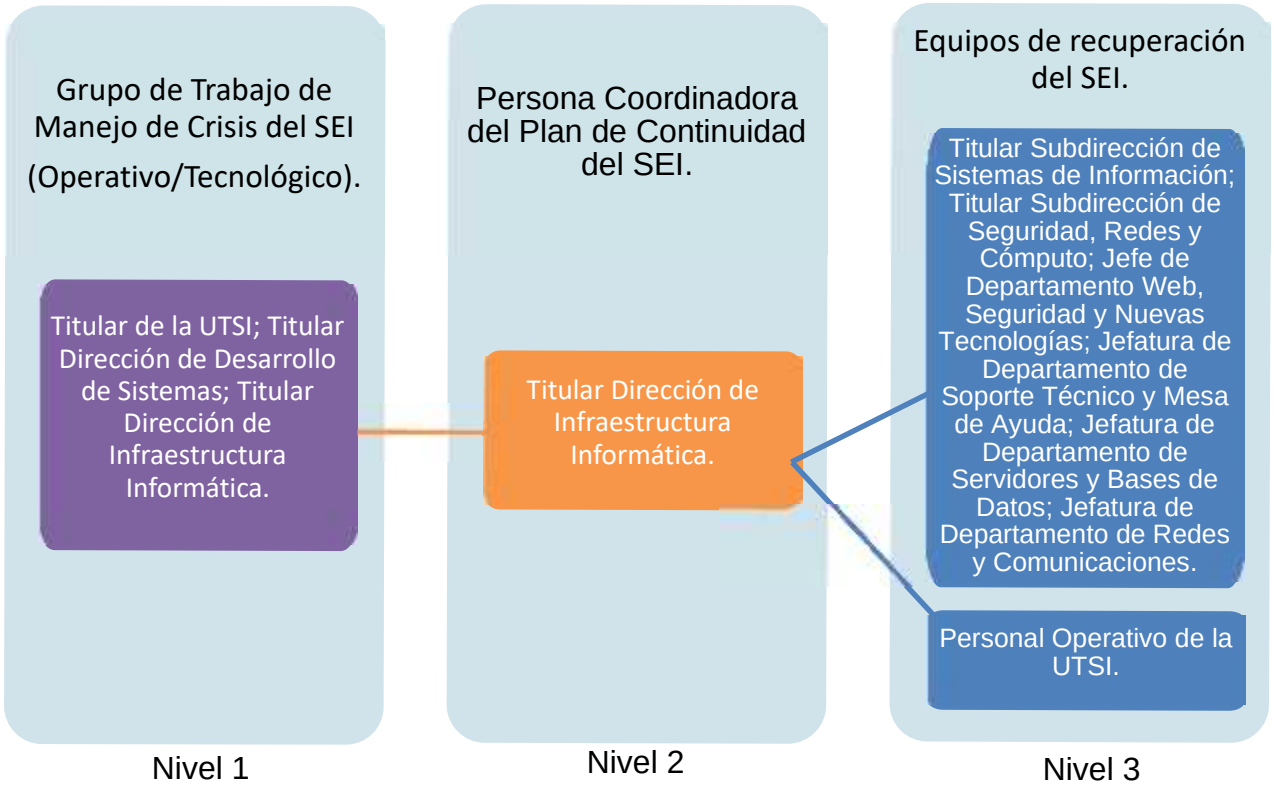
- Minimizar las consecuencias de la interrupción del SEI.
- Garantizar la continuidad operativa y tecnológica del SEI.

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
Nivel 1	Grupo de Trabajo de Manejo de Crisis del SEI.	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. En general, el Grupo de Trabajo de Manejo de Crisis sólo se involucrará en eventos significativos con el potencial de: • Amenazar la integridad física y la seguridad de los empleados del IECM. • No disponibilidad de los servicios tecnológicos que soportan el SEI. Algunas responsabilidades de los miembros del Grupo de Trabajo son: • 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.
Nivel 2	Persona que Coordina el Plan de Continuidad del SEI.	Responsable de coordinar a los equipos de recuperación tecnológica en caso de declararse una contingencia. Algunas responsabilidades del nivel son: • 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
		) 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: 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. 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

Nivel	Puesto	Descripción
		de manera semestral de manera inicial o en su caso de manera anual.
Nivel 3	Responsable del Servicio	Su responsabilidad es la recuperación del servicio de su atribución, asimismo deberá: • 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	Personal que labora directamente para la recuperación del servicio, entre sus responsabilidades están: • 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

<table>
<tr><th>Nivel</th><th>Personal</th></tr>
<tr><td>Nivel 1</td><td>
Grupo de Trabajo de Manejo Crisis

Tecnológico
<table>
<tr><th>Nombre</th><th>Puesto</th></tr>
<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>
</table>
</td></tr>
<tr><td>Nivel 2</td><td>Coordinadora del Plan de Continuidad:

Estefanía Mena Ibarra, Titular de la Unidad Técnica de Servicios Informáticos</td></tr>
<tr><td>Nivel 3</td><td>
Responsable de los servicios críticos:
<table>
<tr><th>Proceso</th><th>Responsable</th></tr>
<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>
</table>
</td></tr>
</table>

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:

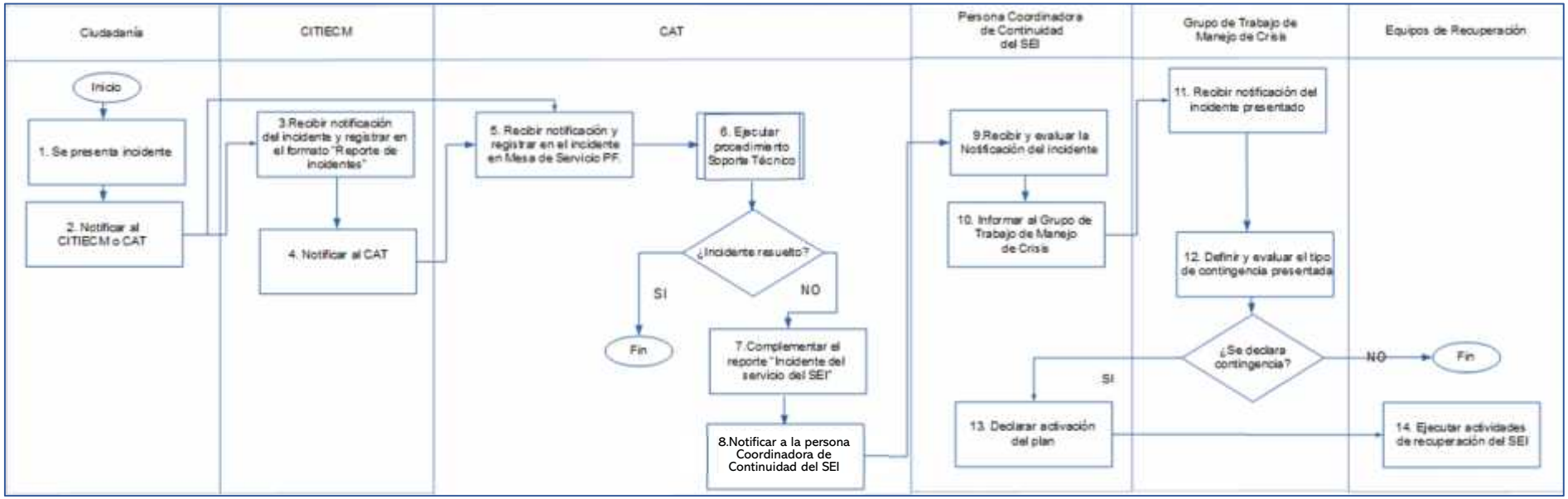
- ISO 22301:2019 de Seguridad y resiliencia de Sistemas de gestión de continuidad de negocio.
- ISO 54001:2019 Sistemas de gestión de calidad-Requisitos específicos para la aplicación de la Norma ISO 9001:2015 a organizaciones electorales en todos los niveles de gobierno.

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	Notificar el incidente presentado ya sea a través del CITIECM o del CAT. • 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). Registrar en el formato para el reporte “Incidente del SEI”, indicando: • 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	Complementar el reporte “Incidente del servicio del SEI”, indicando: • 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.

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: • 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: • 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

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

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

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

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, *Business Impact Analysis*), 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 (*Business Continuity Plan*, 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 "*Minimum Acceptable Recovery Configuration*". 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, *Recovery Point Objetive*), 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, *Recovery Time Objetive*), 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.

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).

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:**	⟩ 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:**	⟩ 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:	⟩ Intentar de nuevo usar la aplicación del Sistema Electrónico por Internet.
4. Falla de la tableta provocada por el ciudadano:	⟩ 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:**	⟩ Consultar con otro personal de soporte del IECM el uso del SEI en la tableta. ⟩ Solicitar apoyo al Centro de Atención Telefónica.

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

1. Robo o extravío de la tableta:	⁾ Informar a la dirección distrital. ⁾ Realizar acciones legales. ⁾ Reportar el incidente. ⁾ Registra el incidente. ⁾ Consultar existencias de tableta para su sustitución.

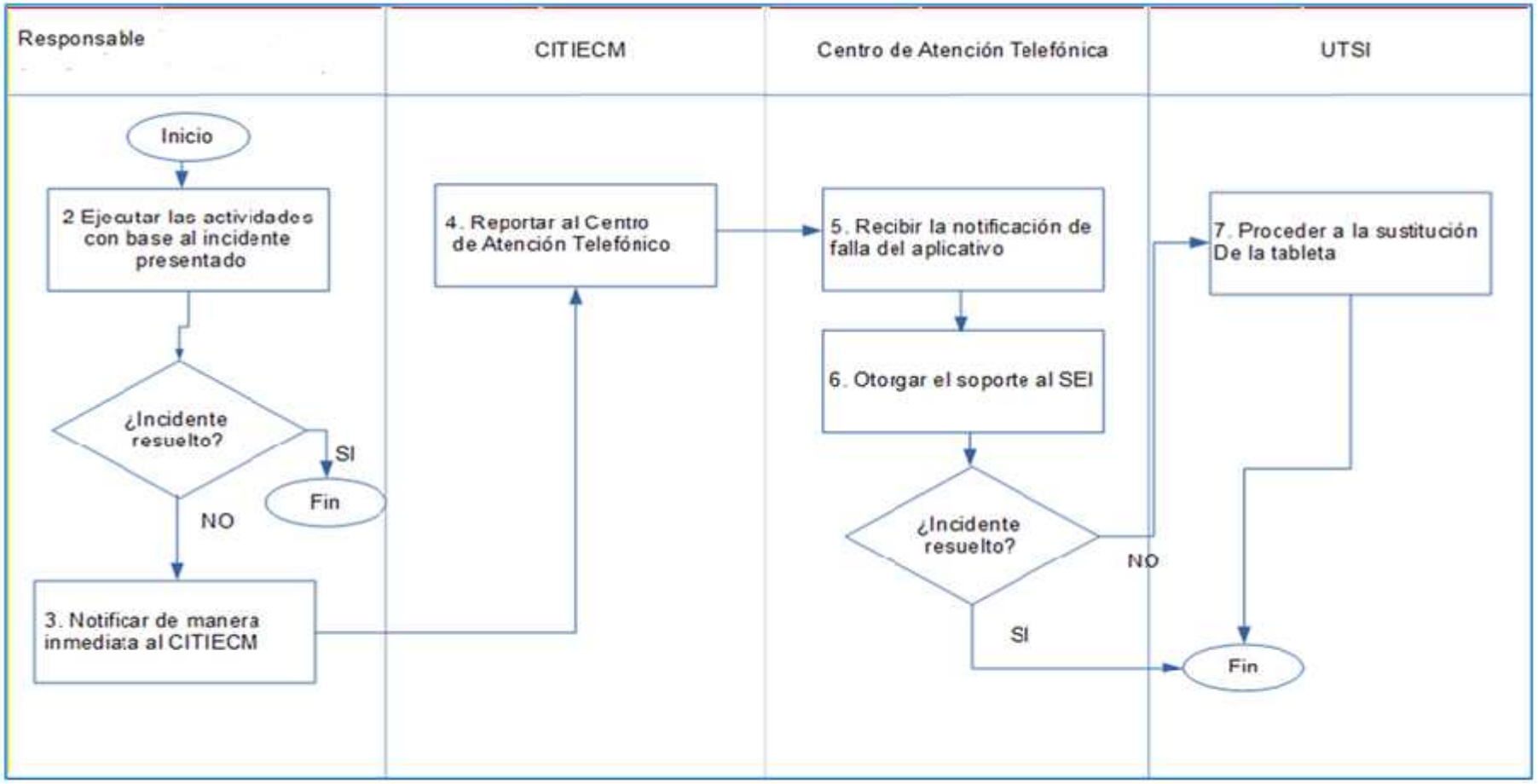
c. Contingencia natural

1. Tormenta eléctrica / Inundación:	⁾ 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	⁾ 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.

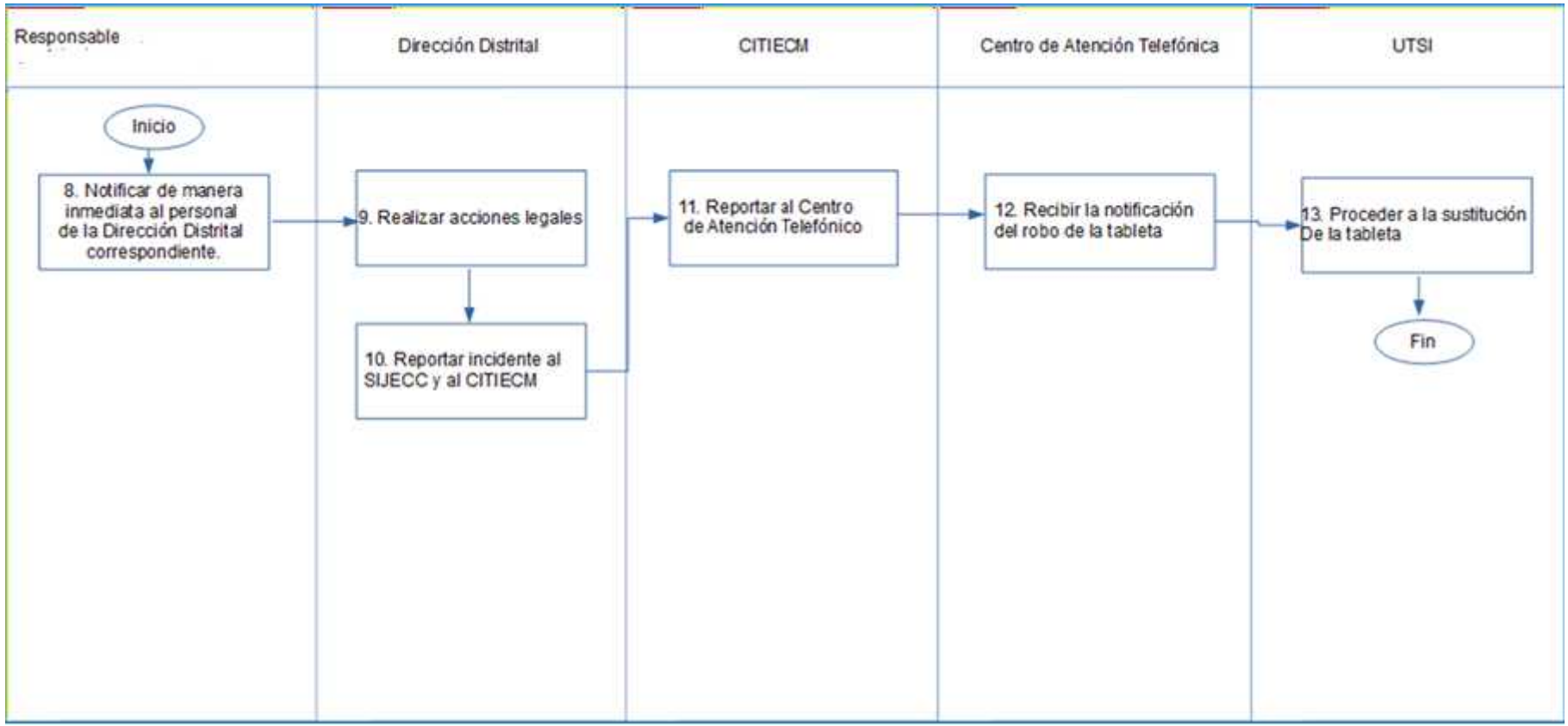
Diagrama de flujo

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:

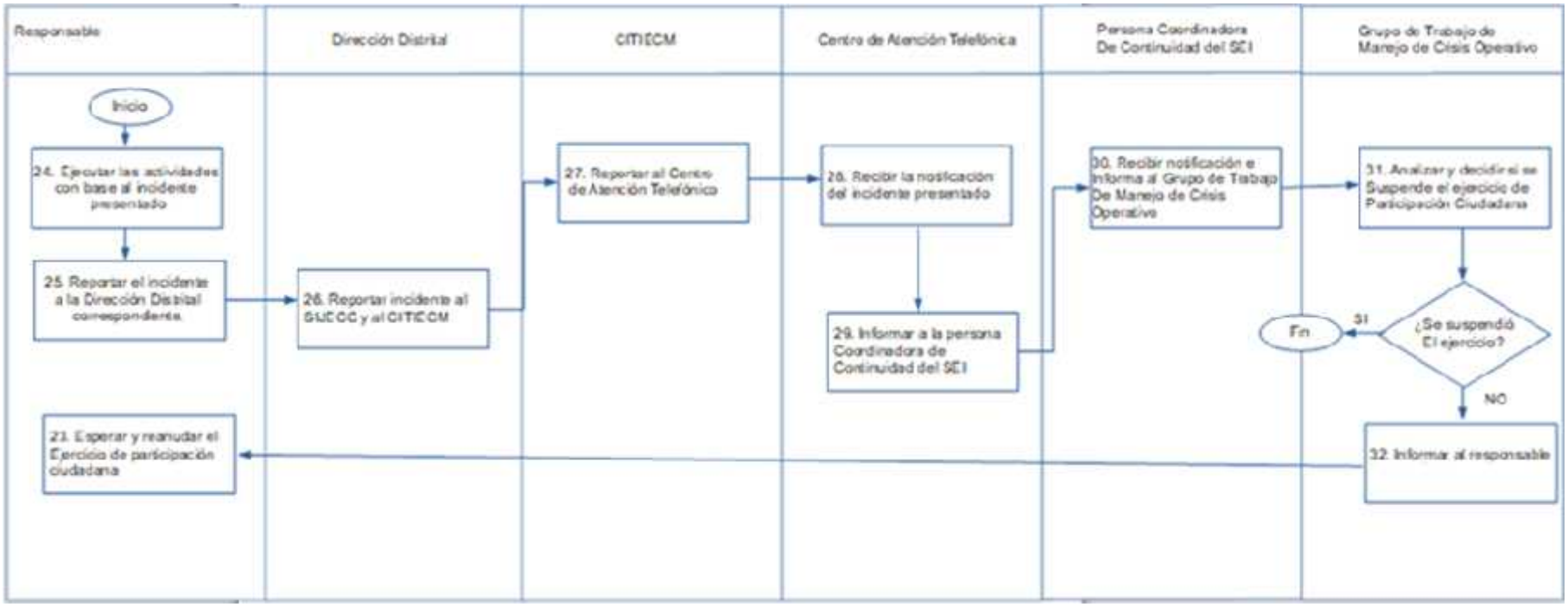
a. Falla de la tableta en donde reside el aplicativo SEI.



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



c. Contingencia natural.



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

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

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.

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			

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 cuentan 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.

- 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.

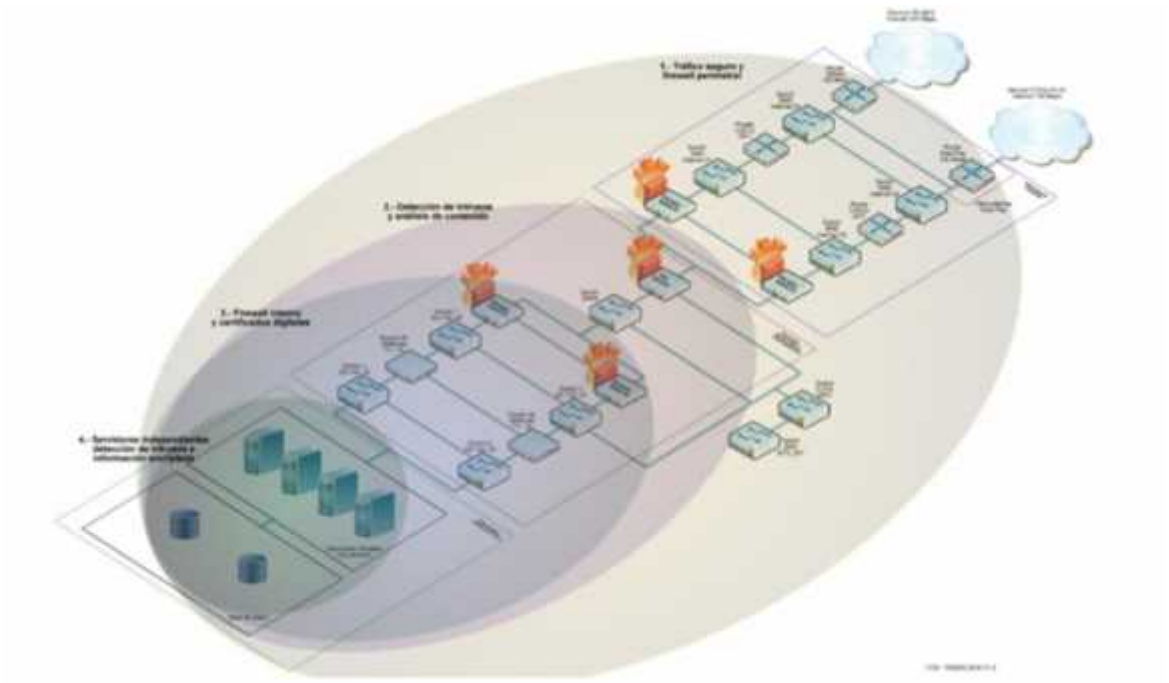
Definiciones

Término	Descripción
Análisis de Impacto al Negocio (BIA)	Análisis de Impacto al Negocio, (BIA, *Business Impact Analysis*), 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 "*Minimum Acceptable Recovery Configuration*". 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, *Recovery Point Objetive*), 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, *Recovery Time Objetive)*, 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:

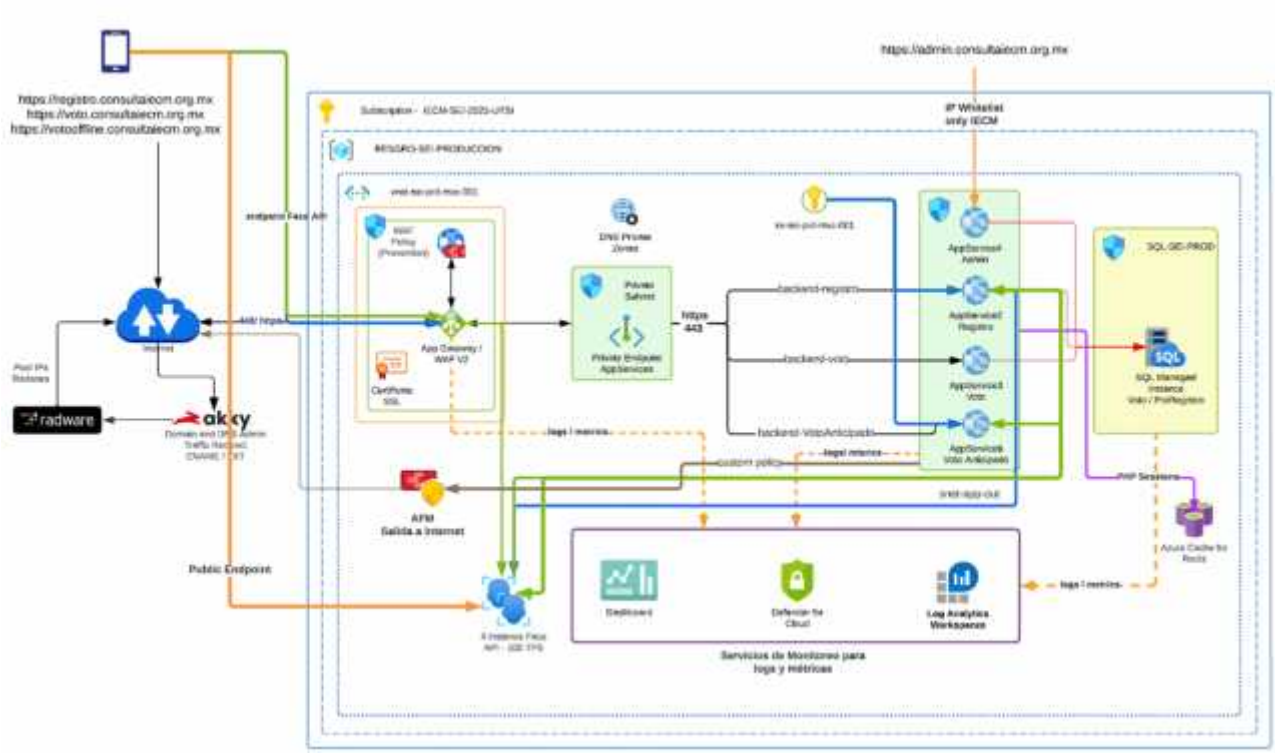
a) Infraestructura en sitio.



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

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

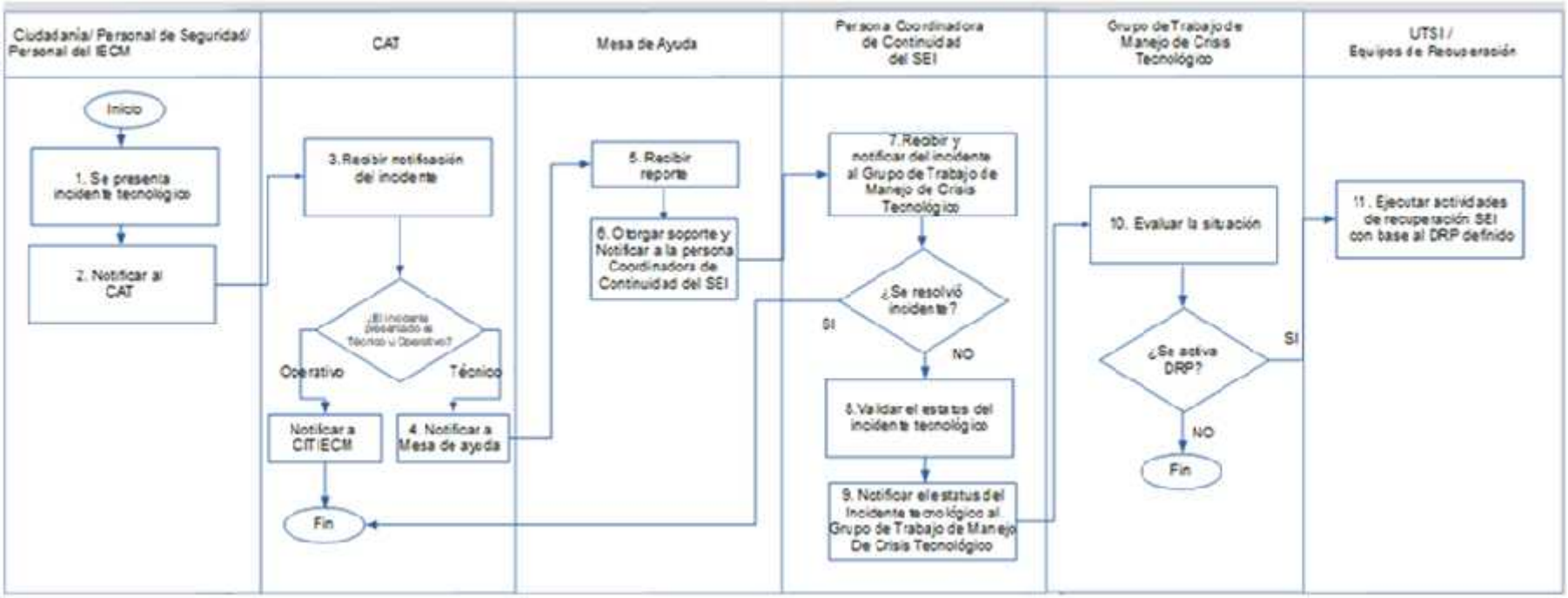
La estrategia de recuperación definida cuenta con los siguientes componentes:

- 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:



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

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			