

PLAN DE SEGURIDAD Y CONTINUIDAD PELE 2021

Programa de Resultados Electorales Preliminares

Contenido

Glosario.....	2
1. Introducción	3
2. Objetivos	3
2.1. Objetivo General	3
2.2. Objetivos Particulares	3
3. Alcance.	4
4. Marco Normativo	4
5. Directrices de Seguridad de la información para el PREP	5
5.1. Análisis de riesgos en materia de seguridad de la información	10
5.2. Implementación de Plan de Tratamiento de Riesgos	12
5.3. Fortalecimiento de las Actividades Operativas	12
5.4. Fortalecimiento de las Infraestructura Tecnológica	12
5.5. Control de Acceso	13
5.6. Monitoreo y Respuesta a Incidentes de Seguridad	13
6. Directrices de Seguridad Operativa del PREP	14
6.1. Factores de Riesgo.	14
6.2. Activos críticos.	14
6.3. Áreas de amenaza.	15
6.4. Identificación de riesgos.....	15
7. Seguridad y riesgos del Sistema Informático PREP	17
8. Implementación del Plan de Tratamiento de Riesgos.....	18
8.1. Fortalecimiento de las actividades operativas del PREP	18
8.2. Fortalecimiento de la Infraestructura Tecnológica	18
8.3. Control de Acceso	20
8.2. Plan de Concientización	20
9. Plan de Continuidad y Plan de Recuperación de Desastres	21
9.1. Continuidad Operativa del PREP.	24
9.1.1. CATD para contingencias.....	25
9.1.2. Continuidad en el Consejo General del ITE.	25



Glosario

AEC.- Acta de Escrutinio y Cómputo.

ATI.- Área Técnica de Informática.

CATD.- Centro de Acopio y Transmisión de Datos.

DOECyEC.- Dirección de Organización Electoral, Capacitación y Educación Cívica.

ITE.- Instituto Tlaxcalteca de Elecciones.

LGIPE.- Ley General de Instituciones y Procedimientos Electorales.

LIPEET.- Ley de Instituciones y Procedimientos Electorales para el Estado de Tlaxcala.

Paquete Electoral Municipal Local. - Caja de plástico que contiene las Actas de la Jornada, Escrutinio y Cómputo e Incidentes, así mismo debe contener las boletas electorales y los materiales utilizados durante el desarrollo de la Jornada Electoral.

PREP.- Programa de Resultados Electorales Preliminares

RE.- Reglamento de Elecciones

Sobre PREP.- Sobre integrado por fuera de la caja paquete electoral distrital local, contiene la segunda copia del AEC de cada elección.

1. Introducción

El 28 de noviembre de 2021 se celebrarán elecciones extraordinarias en el estado de Tlaxcala; para renovar los cargos Presidencias de Comunidad a través de voto constitucional.

Ante éste panorama el Instituto Tlaxcalteca de Elecciones, organismo público encargado de la organización de los procesos electorales en la entidad; debe desarrollar e implementar aquellos mecanismos que considere necesarios para dar certeza y legalidad a la recopilación y publicación de los resultados electorales preliminares; apegando en todo momento a los principios, criterios y lineamientos establecidos por el Instituto Nacional Electoral así como al Acuerdo de Colaboración celebrado entre el Instituto Tlaxcalteca de Elecciones y el Instituto Nacional Electoral para el desarrollo de las actividades del Programa de Resultados Electorales Preliminares.

Derivado de lo anterior, el propósito del Programa de Resultados Electorales Preliminares es, que a partir de la captura y el procesamiento de la información contenida en cada una de las Actas de Escrutinio y Cómputo (AEC) mediante la herramienta informática diseñada para esta etapa del proceso electoral local; se pueda generar la información estadística que en conjunto con los datos capturados de los resultados electorales le sean presentados a la ciudadanía como parte del seguimiento al desarrollo de la Jornada Electoral.

2. Objetivos

2.1. Objetivo General

Establecer una estrategia para salvaguardar la integridad, disponibilidad y confidencialidad de la Información del PREP; identificando los riesgos de seguridad de la información en las diferentes etapas del Programa; a nivel de procedimientos, tecnología, recursos humanos y seguridad física, para así establecer los controles de seguridad apropiados que permitan mitigar el riesgo o reducirlo a un nivel tal que garantice la confiabilidad y continuidad de los sistemas y servicios informáticos.

Aunado a ello, definir y garantizar la seguridad, transparencia y confiabilidad de las actividades que se realizarán como parte de los procesos que lo integran; garantizando la operatividad y continuidad del PREP, reduciendo los riesgos que se pudieran presentar, asegurando la continuidad del Programa a través de mecanismos alternativos.

2.2. Objetivos Particulares

- Elaborar las directrices de seguridad de la información para el PREP, las cuales fungirán como soporte al presente Plan de Seguridad y deberán ser acatadas por todos los servidores públicos o entes externos al OPL que interactúen de manera directa o indirecta con el Programa.
- Aplicar una Metodología de Administración de Riesgos para llevar a cabo el análisis de riesgos permitiendo identificar las vulnerabilidades de seguridad que enfrenta el PREP y se pueda llevar a cabo el tratamiento adecuado de los mismos.

- A partir del análisis de riesgos, identificar e implementar los controles de seguridad en los distintos procesos de operación del PREP, así como en la infraestructura tecnológica, de tal forma que se pueda mitigar el riesgo.
- Fortalecer la infraestructura tecnológica a través de la generación de guías de configuración técnica estándar (baseline), orientadas a los sistemas operativos y dispositivos de comunicación.
- Implantar soluciones de seguridad perimetral tales como firewall, IDS/IPS y/o WAF con la finalidad de controlar y vigilar el tráfico de la red de datos que soporta al PREP.
- Definir el esquema de control de acceso hacia los diferentes sistemas del PREP, incluyendo CATD e infraestructura para difusión y publicación de resultados.
- Establecer un plan de concientización para capacitar y transmitir el sentido de seguridad de la información a todo el personal del PREP.
- Definir la estrategia a seguir referente al monitoreo y respuesta a incidentes, creando los procedimientos y/o estándares de seguridad necesarios para dicho fin.
- Establecer un Plan de Continuidad que permita minimizar el impacto a la operación, así como los planes de recuperación de pérdida de activos de información (que pudieran ser el resultado de desastres naturales, accidentes, fallas de equipos y/o acciones deliberadas).
- Elaborar el soporte documental y los registros necesarios que permitan establecer las condiciones favorables a cualquier entidad interesada en evaluar y auditar las medidas de seguridad implantadas o implementadas, como parte del presente Plan de Seguridad.

3. Alcance.

El alcance del plan de seguridad y continuidad se circunscribe al sistema informático desarrollado por el Instituto Tlaxcalteca de Elecciones, específicamente para el Proceso Electoral Local Extraordinario 2021, así como sus componentes físicos o modelos tecnológicos alojados en servidores nube; así como a los recursos materiales y humanos contemplados en el CATD a ubicar en las oficinas centrales del ITE, donde operará la base central de las operaciones y el CATD previsto para contingencias.

4. Marco Normativo

El artículo 41 base V apartado C, numeral 8 establece que los organismos públicos locales, tienen como función, entre otras los resultados preliminares de las elecciones. Asimismo, el artículo 95 de la Constitución Política del Estado Libre y Soberano de Tlaxcala, faculta al Instituto Tlaxcalteca de Elecciones, como organismo autónomo a preparar y desarrollar los comicios electorales en la Entidad.

El artículo 51 fracción X de la LIPEET, establece como atribución del ITE implementar y operar el PREP, de conformidad con las reglas, lineamientos y criterios que al efecto emita el INE; de acuerdo con lo establecido en el artículo 235 del mismo ordenamiento establece que el Instituto podrá efectuar el acopio y la difusión de

los resultados electorales preliminares de la Jornada Electoral, al término de ésta. La difusión de estos resultados siempre se efectuará haciendo saber al público que sólo tienen carácter de preliminares.

Asimismo, el artículo 237 de la LIPEET refiere que toda la documentación relativa al Programa de Resultados Preliminares Electorales deberá contener mención expresa del mismo.

Con fundamento en los numerales 1 y 2 del artículo 338 del RE, en el que establece que los OPL en el ámbito de sus atribuciones legales, son responsables directos de coordinar la implementación y operación del PREP cuando se trate de elecciones que por disposición legal o por mandato de autoridad, corresponda al OPL llevar a cabo, lo cual para la elección concurrente es titularidades de Presidencias de Comunidad.

5. Directrices de Seguridad de la información para el PREP

La finalidad de estas directrices es proporcionar los lineamientos, políticas y responsabilidades para la necesaria seguridad de la información para el sistema informático del PREP.

Así como proteger los activos de información del Instituto Tlaxcalteca de Elecciones, los recursos y soluciones tecnológicas para el procesamiento y publicación del Programa de Resultados Electorales Preliminares, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurando la implementación de las medidas de seguridad comprendidas en esta directriz, identificando los recursos, alcances y requerimientos mínimos necesarios para un correcto funcionamiento del aplicativo.

A. Organización interna

I. Asignación de responsabilidades y roles para la seguridad de la información

- i. La institución identificará, definirá y asignará todas las responsabilidades y roles de seguridad de la información necesarias para el correcto cumplimiento de esta directriz, tal como se muestra en la siguiente tabla

RESPONSABILIDADES Y ROLES PARA LA SEGURIDAD DE LA INFORMACIÓN	
ROL	RESPONSABILIDAD
SYSADMN	Encargado de realizar las configuraciones basadas en las buenas prácticas, y soporte de 3er nivel a la infraestructura instalada en la nube, durante la jornada electoral
DBA	Encargado de realizar la configuración del manejador de base de datos en la modalidad de alta disponibilidad y soporte de 3er nivel al servidor instalado en la nube, durante la jornada electoral.

COMISION DE SEGUIMIENTO DE SISTEMAS INFORMATICOS	Comisión encargada de supervisar la operación del PREP, correspondiente al sistema informático utilizado durante la jornada electoral.
INSTANCIA INTERNA	La dirección de organización, capacitación y educación cívica y la unidad técnica de informática, responsable de la operación del PREP.
SUPERVISOR	Encargado de reportar cualquier incidencia de cualquier índole (operativa o informática) en el CATD a la instancia interna responsable de la operación (enlace) y funcionamiento del PREP del Instituto Tlaxcalteca de Elecciones.
ENLACE	Encarga de monitorear el funcionamiento del PREP en los CATD, y el enlace de comunicación entre los supervisores y la instancia interna responsable de la operación y funcionamiento del PREP.
MONITOR	Responsable del monitoreo del desempeño y el estatus de la infraestructura instalada en la nube, para la operación del PREP durante la jornada electoral.
OPERADOR	Personal responsable de operar el sistema informático del PREP (Capturista, Verificador y Digitalizador)

II. Coordinación con Supervisor en CATD

- i. La unidad técnica de Informática del Instituto Tlaxcalteca de Elecciones designará a un enlace el cual tendrá la comunicación directa con el supervisor del CATD. La comunicación será a través de las siguientes vías:
 - a) Comunicación Telefónica al CATD
 - b) Comunicación móvil con supervisor o supervisora del CATD
 - c) Grupo de comunicación entre supervisor o supervisora del CATD y el enlace
 - d) Extensión en la unidad técnica de informática dedicada para el reporte de incidencias en el CATD.

III. Coordinación con Proveedor de infraestructura del PREP en la nube

- i. La unidad técnica de informática del Instituto Tlaxcalteca de Elecciones mantendrá contacto con el proveedor por medio de vía telefónica o correo electrónico con el personal designado, en caso de tener algún incidente en la infraestructura o para tratar cualquier tema relacionado con la seguridad de la información. El cual se contará con profesionistas y expertos en la materia.

B. Términos y definiciones

- I. La unidad técnica de informática a efectos de la presente metodología se entiende por:

- i. **Amenaza.** Es una situación o acontecimiento que pueda causar daño a los bienes informáticos; puede ser una persona, un programa malicioso o un suceso natural o de otra índole y representan los posibles atacantes o factores que inciden negativamente sobre el sistema
- ii. **Análisis de riesgo.** El proceso dirigido a determinar la probabilidad que las amenazas se materialicen sobre los bienes informáticos e implica la identificación de los bienes a proteger, las amenazas que actúan sobre ella, su probabilidad de ocurrencia y el impacto que puede causar
- iii. **Bienes Informáticos o Activos.** Los elementos componentes del sistema informático que deben ser protegidos en evitación de que como resultado de la materialización de una amenaza sufran algún tipo de daño
- iv. **Impacto.** Es el daño producido por la materialización de una amenaza
- v. **Riesgo.** Es la probabilidad que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto negativo en la operación
- vi. **Vulnerabilidad.** En un sistema informático es un punto o aspecto susceptible de ser atacado o de dañar su seguridad; representan las debilidades o aspectos falibles o atacables en el sistema informático y califican el nivel de riesgo del mismo.

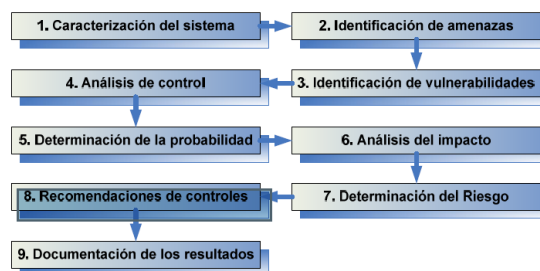
C. Criterios para evaluación de riesgos

- I. A continuación, se menciona de manera detallada la metodología a utilizar para la administración de riesgo y el cálculo del mismo.

La Guía para la administración de riesgos para las tecnologías de sistemas de información consta de nueve pasos:

- a) Caracterización del sistema
- b) Identificación de amenazas
- c) Identificación de vulnerabilidades
- d) Análisis de Control
- e) Determinación de la probidad
- f) Análisis del impacto
- g) Determinación del riesgo
- h) Recomendación de controles
- i) Documentación de los resultados

Esquematizados en la siguiente figura:



Para determinar la probabilidad de una vulnerabilidad se debe tomar en cuenta:

- a) La motivación de la fuente de la amenaza y su capacidad
- b) La naturaleza de la vulnerabilidad

c) La existencia y efectividad de los controles existentes
Esta probabilidad se expresa como alta, media o baja según la siguiente tabla:

NIVELES DE PROBABILIDAD DE AMENAZAS	
NIVEL DE PROBABILIDAD	DEFINICIÓN
ALTA	La fuente de amenaza es altamente motivada y suficientemente capaz, los controles para prevenir la vulnerabilidad son inefectivos
MEDIA	La fuente de amenaza es motivada y capaz, pero los controles pueden impedir la explotación de la vulnerabilidad
BAJA	Existe poca motivación o capacidad de la fuente de amenaza, o los controles existentes impiden significativamente que la vulnerabilidad se pueda explotar

Para analizar el impacto, se determina basado al impacto resultante de que pueda explotar una vulnerabilidad. Este impacto se describe en términos de pérdida o degradación de la integridad, disponibilidad o confidencialidad de los sistemas. Este impacto se cuantifica según la siguiente tabla:

NIVELES DE IMPACTO	
NIVEL DE IMPACTO	DEFINICIÓN
ALTO	La materialización de la amenaza produce una costosa pérdida de los activos más sensibles. Puede significar la violación, daño o impedimento de la misión, reputación o interés de la organización.
MEDIO	La materialización de la amenaza puede causar una costosa pérdida de los activos, causando la degradación del servicio o suspensión temporal de la misión.
BAJO	La materialización de la amenaza puede causar algún daño a los activos. Puede afectar la misión, reputación o interés de la organización

El riesgo se determinará en función de:

- La probabilidad de que una fuente de amenaza intente explotar una vulnerabilidad
- La magnitud del impacto si la fuente de amenaza explota la vulnerabilidad

- c) La adecuación de controles existentes o planeados para reducir o eliminar el riesgo.

El riesgo se calcula tal como se muestra en la siguiente tabla.

PROBABILIDAD DE AMENAZA	IMPACTO		
	BAJO(10)	MEDIO(50)	ALTO(100)
ALTO (1.0)	Bajo($10 \times 1.0 = 10$)	Medio($50 \times 1.0 = 50$)	Alto($100 \times 1.0 = 100$)
MEDIO (0.5)	Bajo($10 \times 0.5 = 5$)	Medio($50 \times 0.5 = 25$)	Medio($100 \times 0.5 = 50$)
BAJO (0.1)	Bajo($10 \times 0.1 = 1$)	Bajo($50 \times 0.1 = 5$)	Bajo($100 \times 0.1 = 10$)

El riesgo se interpreta según la siguiente tabla

NIVELES DE RIESGO	
NIVEL DE RIESGO	RESPONSABILIDAD
ALTO	Existe una fuerte necesidad para implementar controles correctivos. El sistema puede seguir operando, pero una acción correctiva debe ponerse en práctica cuanto antes.
MEDIO	Las acciones correctivas son necesarias y se debe desarrollar un plan para incorporar estas acciones en un tiempo razonable.
BAJO	Es necesario determinar si realmente se requieren acciones correctivas o decidir aceptar el riesgo.

5.1. Análisis de riesgos en materia de seguridad de la información

El OPL aplicará una Metodología de Administración de Riesgos para el análisis y evaluación de riesgos en materia de seguridad de la información para así detectar brechas de seguridad y poder aplicar controles con la finalidad de reducir los riesgos encontrados. En la siguiente imagen se presenta un flujo general del análisis de riesgos.

Núm.	Escenario	Factor de Riesgo	Control
1	La falta de controles de acceso al centro de datos utilizado para el PREP, podría terminar en robo de activos o en el sabotaje de los activos (servidores, bases de datos, dispositivos de comunicación durante el PREP)	Alto	El acceso solo se podrá realizar desde la Unidad Técnica de Informática a través de un VPN site to site. Se contará con contraseñas fuertes a los servidores, así mismo se contará con ESET Authentication Security que nos darán un token de seguridad para ingresar al servidor adicional a las credenciales. Se llevará una bitácora de ingreso a cada servidor.
2	El uso de contraseña débiles y la falta de actualizaciones en los servidores Web de publicación de resultados PREP podrían ocasionar que un atacante publicara algo ajeno al PREP (defacement) en el sitio Web del PREP impactando en la credibilidad de la elección	Alto	En frente de los servidores de publicación del PREP, contara con un firewall para que regulara el tráfico, los servidores de publicación contara con una contraseña robusta para su ingreso, así como el token de acceso. El servidor contara con las últimas actualizaciones de seguridad y de SO Se cuenta con un método de seguridad para el consumo de servicios web, el cual se debe de registrar la IP o DNS autorizado para el consumo del mismo.
3	La inexistencia de un programa para detectar código malicioso (antivirus) en los dispositivos tecnológicos (PC, laptops, servidores, dispositivos móviles, etc.) podría provocar alteración en el funcionamiento normal en el dispositivo.	Alto	Se instalará en cada dispositivo un antivirus actualizado
4	Debido a la falta de redundancia de energía eléctrica en la infraestructura tecnológica (dispositivos de red, servidores, pc, laptop entre otras), en caso de una interrupción en el suministro de energía podría afectar la continuidad de la operación del PREP	Alto	El data center de la nube, contara con esta redundancia de energía eléctrica. Con respecto al CATD en caso de que exista una interrupción de energía eléctrica mayor a 2 horas, se dotara de una planta eléctrica para el suministro de energía.

			En el CATD de contingencia se contará con una planta de luz asignada por cualquier corte de energía eléctrica
5	Debido a la falta de redundancia en los dispositivos críticos del PREP, tales como dispositivos de comunicación, servidores y base de datos, en caso de falla de alguno de estos el PREP, podría dejar de operar		El data center donde se encontrarán los servidores contará con redundancia.
6	La falta de mantenimiento preventivo a la infraestructura tecnológica (dispositivos de red, servidores, pc, laptop, etc.), podría provocar fallas en el funcionamiento normal de los equipos durante el PREP.	Alto	La infraestructura se realizará únicamente para la operación del PREP, y esta será virtual a través de VPS.
7	Por falta de una guía de configuración de seguridad para dispositivos de comunicación (firewall, routers, switches, balanceadores), servidores y bases de datos, un atacante podría aprovechar las vulnerabilidades de dichos dispositivos para comprometerlos y usarlos durante el PREP para su beneficio personal.	Medio	La configuración de cada uno de los componentes de la infraestructura será configurada por el proveedor encargado de proveer el servicio. Adicional a esto se contará con soporte durante la jornada electoral
8	Debido a la falta de segregación o Separación de la red del PREP, usuarios de forma consiente o inocente podrían sabotear la infraestructura que soporta el PREP.	Medio	Los servidores de base de datos y API se encontrarán en una red privada y la red del CATD contará con un firewall para el control de tráfico de la red. El acceso a la infraestructura solo se podrá ingresar desde la red
9	Debido a falta de un mecanismo seguro por el que viaje la información entre los MCAD/TCA y los servidores del aplicativo, un atacante podría interceptar la comunicación no cifrada y podría alterarla.	Medio	Se contará con certificados SSL, para que la información viaje encriptada y se utilizara el protocolo https
10	Debido a la ausencia de un mecanismo de protección contra ataques de denegación de servicio, un atacante podría lanzar una gran cantidad de tráfico al sitio de publicación de resultados del PREP para hacer que dicho sitio no se encuentre disponible durante el PREP.	Medio	Implementar una solución de mitigación para ataques de denegación de servicio a través de un firewall.
11	Debido a la falta de un control acceso lógico perimetral a la red interna de los OPL, un atacante podría ingresar hasta los servidores y/o bases de datos modificando la información del PREP y comprometiendo las elecciones.	Medio	Los servidores no se encontrarán físicamente en nuestras instalaciones si no en la nube, el ingreso a estos será a través de un VPN y adicional a esto. Para el ingreso a los servidores además de las credenciales correspondientes, deberá de ingresarse el token de seguridad.
12	Debido a la falta de un sistema de detección y prevención de intrusos, podrían presentarse dentro de la red del PREP accesos no autorizados.	Bajo	Se contarán con un monitoreo en tiempo real del tráfico de la red

5.2. Implementación de Plan de Tratamiento de Riesgos

La implementación del Plan de Tratamiento de riesgos será trabajado por la instancia interna en desarrollo y operación del PREP, bajo el siguiente tratamiento. Tal como se muestra en la siguiente tabla.

OPCIONES DE TRATAMIENTO DE RIESGO	
EVITAR EL RIESGO	Se han tomado las medidas y las herramientas tecnológicas necesarias para mitigar los riesgos analizados anteriormente
REDUCIR EL RIESGO	Se han tomado las medidas necesarias encaminadas a disminuir la probabilidad, como el impacto, a través de la optimización de los procedimientos y la implementación de controles eficientes, eficaces y efectivos
COMPARTIR O TRANSFERIR EL RIESGO	Se ha transferido el riesgo al proveedor que nos proveerá la infraestructura de la nube
ASUMIR EL RIESGO	Es necesario determinar si realmente se requieren acciones correctivas o decidir aceptar el riesgo.

5.3. Fortalecimiento de las Actividades Operativas

Los controles operativos identificados a partir del análisis de riesgos, estarán consolidados básicamente en los siguientes documentos:

- Lista de verificación (Cheklist), antes de operar el PREP
- Manuales de operación
- Manual para reporta contingencia
- Escalamiento de atención de contingencias
- Directorio de números de emergencia

Estos documentos serán emitidos al coordinador del CATD, los cuales serán una base y guía para que puedan contar con las mejores prácticas de seguridad alineadas a los objetivos del PREP

5.4. Fortalecimiento de las Infraestructura Tecnológica

Con base en el análisis de riesgos, serán consolidados los controles de seguridad para los distintos dispositivos de la infraestructura tecnológica. Las actividades generales para el desarrollo, implementación, pruebas y verificación de los controles tecnológicos se enlistan a continuación:

- a) Generación de listas de verificación de seguridad de los componentes tecnológicos como son:
 - Sistemas operativos
 - Software de gestión de base de datos
 - Balanceadores de Carga
 - Certificados SSL
 - Servidores de procesamiento
 - Firewall
 - ESET authentication security
 - Servidores Web
 - Servidor Linux (PREP Casilla)
- b) Implementación de seguridad en CATD y perimetral
 - Implementar Firewall perimetral en el CATD, para limitar el acceso a la red del PREP del OPL
- c) Pruebas de negación de servicio
 - Ejecutar pruebas de denegación de servicio a los sitios del PREP para comprobar que la mitigación y los controles de seguridad funcionen adecuadamente.

5.5. Control de Acceso

Para robustecer el proceso de autenticación de los sistemas del PREP se debe controlar el acceso a los activos importantes de información, esto a través de tecnología conforme a las necesidades del PREP y con base en los resultados del análisis de riesgos, por lo que se tomaran las siguientes medidas de seguridad al control de acceso.

- Los servidores de procesamiento y de base de datos se encontrarán en la nube y en una red privada y separada al del Instituto Tlaxcalteca de Elecciones.
- El ingreso a los servidores será solo desde el Instituto Tlaxcalteca de Elecciones y a través de una VPN (site to site)
- Cada uno de los servidores contarán con contraseñas diferentes
- Adicional a las credenciales de acceso a los servidores, se contará con un token de ingreso. El cual este es generado en tiempo real y autorizado por un servidor, para validar si el token ingresado es autorizado y valido para poder ingresar a los servidores.
- Se contará con una bitácora de ingreso a los servidores de base de datos, en donde se llevará el record de la persona que ingresó, justificación, hora de entrada y salida.
- Solo podrá haber un solo usuario concurrente en los servidores

5.6. Monitoreo y Respuesta a Incidentes de Seguridad

Durante la operación del PREP, la unidad técnica de informática designará a un recurso del área para el monitoreo de los siguientes rubros como mínimo:

- a) Trafico de RED
- b) Control de la bitácora de entrada a los servidores

- c) Control del Token de seguridad
- d) Monitoreo de usuario(s) conectados a la VPN
- e) Usuario conectado en los servidores

6. Directrices de Seguridad Operativa del PREP

Los espacios destinados a la ubicación del CATD como el área de operación central, instalados en el Instituto Tlaxcalteca de Elecciones debe garantizar la seguridad de la información. Por lo que se prevén las siguientes acciones:

- Proporcionar al personal operativo la identificación necesaria para su acceso a las instalaciones del CATD, y
- El personal habilitado contará con identificaciones en el sistema, que podrán ser habilitados y deshabilitados desde el área de operación central del PREP.

6.1. Factores de Riesgo.

Los factores operativos de riesgo recaen en la seguridad de la sede del CATD, que implica un análisis respecto a la ubicación del mismo. En tal sentido derivado de la aprobación del Acuerdo ITE-CG 278/2021 de fecha tres de octubre de dos mil veintiuno, el Consejo General del Instituto Tlaxcalteca de Elecciones asume las atribuciones y funciones de los Consejos Municipales. En este sentido, es oportuna la modificación en el número de Centros de Acopio y Transmisión de Datos a instalar, reduciéndolo a uno e instalándolo en la sede de este Instituto. Por lo que a continuación se establece el análisis de riesgos basados en el Proceso Electoral Local inmediato anterior:

NIVEL DE RIESGO	TOTAL	SEDE MUNICIPAL	COMUNIDADES
Mínimo	1	Instituto Tlaxcalteca de Elecciones	Colonia Agrícola San Luis, Santa Cruz Guadalupe, La Candelaria Teotlalpan, Guadalupe Victoria y Tepunte

En tal sentido, el plan de continuidad establecerá el CATD para contingencias, en caso de que se presentare algún escenario que ponga en riesgo la captura y publicación de datos en el CATD instalado en el ITE.

6.2. Activos críticos.

Los recursos esenciales para la implementación del PREP el día de la jornada electoral, se han establecido en el Proceso Técnico Operativo del PREP, aprobado mediante Acuerdo ITE-CG 05/2021, que prevé tanto recursos materiales como humanos para su adecuado desarrollo, por lo que, en parámetros mínimos, se define el personal como los insumos establecidos y que son parte esencial para el desarrollo y operatividad.

6.3. Áreas de amenaza.

Los procedimientos del PREP pueden verse afectados por los siguientes factores:

- a) **Técnica.** La incorrecta operación en cada uno de los roles del personal, desde el acopio hasta la publicación de datos, sea por error humano o por la incorrecta utilización del Sistema o de la digitalización en casilla, lo que acarrearía la falta y/o duplicación de la información.
- b) **Sociales.** La sede del Consejo General del ITE puede verse afectada por movimientos político-sociales que no permitan el adecuado funcionamiento del CATD.

6.4. Identificación de riesgos.

Los riesgos que se han descrito en los apartados anteriores se resumen en los siguientes escenarios:

A. Fallas en equipos de cómputo. En el supuesto de que el funcionamiento de algún equipo de cómputo presente alguna falla, se deberá proceder de la siguiente forma:

- a. El operador deberá informarlo al Coordinador para que sea atendida.
- b. En caso de que la falla persista se deberá informar al Área Técnica de Informática para que tome las medidas necesarias para la solución del problema.
- c. En la sede del Consejo General del ITE deberán existir equipos de cómputo adicionales para la prevención de alguna falla irreparable del o los equipos de cómputo.

B. Fallas eléctricas. En el supuesto de falla eléctrica en el CATD, durante un tiempo mayor a 30 minutos, previo y durante el inicio de operaciones:

- a. El Coordinador deberá comunicarse a la Comisión Federal de Electricidad explicando la urgencia de restaurar el servicio.
- b. En caso de no tener respuesta pronta se deberá informar al instituto para apoyar a la solución y en caso de restablecimiento del servicio menor a 2 horas, se proporcionará por parte del ITE una planta de energía eléctrica.
- c. El acopiador se quedará en el CATD para continuar recibiendo las actas faltantes y se adoptará un mecanismo de recolección para continuar con la captura y publicación en el CATD para contingencias.

C. Inestabilidad en la sede del ITE. En el supuesto de que las instalaciones del CATD sean invadidas de forma tal que se vea comprometida la seguridad del equipo y personal del CATD:

- a. El Coordinador deberá avisar de inmediato al Consejo General del ITE y deberá ponerse en contacto con las fuerzas policiales asignadas a la sede del ITE.

- b. Si no es posible retirarse del CATD, y las condiciones permiten el desarrollo del proceso operativo del PREP; se ejecutará dicho proceso.
- c. En caso de que las condiciones no permitan ejecutar el proceso operativo del PREP el personal deberá trasladarse junto con las actas recibidas hasta ese momento, al CATD para contingencias ubicado en las instalaciones del instituto.
- d. El acopiador se quedará en el CATD para continuar recibiendo las actas faltantes; si las condiciones lo permitieran.
- e. En caso de que las condiciones no permitan continuar con la recepción de los sobres PREP, el acopiador deberá trasladarse en conjunto con el resto del equipo operativo del PREP al CATD de contingencia.

C. Falla en el servicio de internet. En el supuesto de falla del servicio de internet (durante un tiempo mayor a 30 minutos)

- a. El supervisor deberá comunicarse con el ATI quien a su vez el personal designado se pondrá en contacto con el proveedor de internet, explicando la urgencia del servicio.
- b. En caso de no tener respuesta en menos de 2 horas se informará al Instituto para la evaluación de la contingencia.
- c. Si la falla no podrá ser reestablecida en menos de 8 horas se trasladará el supervisor junto con las actas recibidas (hasta ese momento) al CATD de contingencias. El acopiador se quedará en el CATD para continuar recibiendo las actas faltantes, y se adoptará un mecanismo de recolección de las AEC.
- d. En el supuesto de suficiencia presupuestal, adquirirse bams de prepago para continuar con el servicio.

D. Personal del CATD. Cuando por causas de fuerza mayor algún integrante del equipo operativo del CATD no pueda realizar o continuar con sus actividades:

- a. Dichas actividades serán asumidas por personal disponible dentro del CATD.
- b. En el supuesto de que las actividades no puedan ser cubiertas en su totalidad por el personal ubicado en el CATD se informará al Coordinador para solicitar apoyo al Instituto.
- c. El Coordinador deberá informar a las instancias internas del Instituto encargadas del Desarrollo e implementación del PREP para que se pueda disponer del personal necesario para el funcionamiento del CATD.

Dado que el equipo correspondiente al servidor del sistema informático a utilizar como parte del Programa de Resultados Preliminares Electorales estará concentrado en el Instituto Tlaxcalteca de Elecciones; se prevén los siguientes escenarios de riesgo:

A. Fallas eléctricas. En el supuesto de falla eléctrica en las instalaciones eléctricas:

- a. Deberá entrar en operación las plantas eléctricas, que para el día de la jornada electoral hayan sido contratadas.
- b. La duración de la falla deberá ser reportada a la CFE para su atención y solución.

B. Inestabilidad en la Sede del Consejo General. En el supuesto de intentos de bloqueo de accesos o invasión de las instalaciones:

- a. Se prevé un convenio de apoyo con las fuerzas de Seguridad Pública del Estado, mediante el cual deberá considerarse la asignación de elementos y unidades dispuestos para contener cualquier tipo de intento de invasión u obstrucción a las instalaciones del Instituto.

7. Seguridad y riesgos del Sistema Informático PREP

Dado que la infraestructura que soportará el sistema informático para el desarrollo del PREP, estará ubicado en la nube se prevén los siguientes escenarios de riesgo:

A. En el supuesto que algún servidor de presentación del portal de publicación sufra algún desperfecto o caída de servicio.

- a. El personal encargado del monitoreo de los servidores, para la operación del PREP, deberá reportárselo al Titular del Área Técnica de Informática y a la Comisión de Seguimiento de Sistemas Informáticos.
- b. Éste realizará el análisis de la incidencia y reportará este en menos de 20 minutos.
- c. En caso de que la recuperación del servicio sea mayor 1 hora, se agregará al balanceador de carga el servidor designado para contingencias.

B. En el supuesto que algún servidor de presentación del API sufra algún desperfecto o caída de servicio.

- a. El personal encargado del monitoreo de los servidores, para la operación del PREP, deberá reportárselo al Titular del Área Técnica de Informática y a la Comisión de Seguimiento de Sistemas Informáticos.
- b. Éste realizará el análisis de la incidencia y reportará este en menos de 20 minutos.
- c. En caso de que la recuperación del servicio sea mayor 1 hora, se agregará al balanceador de carga el servidor designado para contingencias.

C. En el supuesto que el servidor de Base de Datos sufra algún desperfecto o caída de servicio.

- a. El personal encargado del monitoreo de los servidores, para la operación del PREP, deberá reportárselo al Titular del Área Técnica de Informática y a la Comisión de Seguimiento de Sistemas Informáticos.
- b. Éste realizará el análisis de la incidencia y reportará este en menos de 15 minutos.
- c. En caso de que la recuperación del servicio sea mayor veinte minutos, entrará el servidor de base de datos de espejo como principal, en lo que se recupera al servidor de base de datos principal

D. En el supuesto que la infraestructura instalada para la operación del Programa de Resultados Electorales Preliminares sufra un incidente de desastre en el datacenter de la región.

- a. El personal encargado del monitoreo de los servidores, para la operación del PREP, deberá reportárselo al Titular del Área Técnica de Informática y a la Comisión de Seguimiento de Sistemas Informáticos.
- b. Éste realizará el análisis de la incidencia y reportará este en menos de 15 minutos.

8. Implementación del Plan de Tratamiento de Riesgos.

8.1. Fortalecimiento de las actividades operativas del PREP

De la información concentrada en el presente documento, así como en el Proceso Técnico Operativo aprobado por el Consejo General del ITE, y del Capítulo VII del Anexo 13 del Reglamento de Elecciones, la Dirección de Organización Electoral, Capacitación y Educación Cívica elaborará un manual para la capacitación del personal asignado para la ejecución de los procedimientos del PREP.

Asimismo, el Área Técnica de Informática elaborará un Manual del Usuario del Sistema Informático del PREP, que contendrá la operación del sistema en cada uno de los roles.

En dichos manuales se generarán los apartados de **seguridad de la información, seguridad del sistema y seguridad en la operación del PREP**.

Aunado a ello se prevé listas de verificación de insumos en el CATD, a verificar por el Coordinador, para contemplar los requerimientos tecnológicos y materiales necesarios para la operación del PREP. Asimismo, lista de verificación requisitada por el Coordinador, respecto a la entrega recepción del AEC, la captura, verificación, digitalización, publicación y resguardo de las mismas. Por último, se contempla una lista de reporte de incidentes para generar el seguimiento y ruta de atención de las mismas.

8.2. Fortalecimiento de la Infraestructura Tecnológica

Para la consolidación de los controles tecnológicos se hará uso de los documentos y recomendaciones emitidas por organismos internacionales especializados en la materia, tales como:

ISO: Organización Internacional para la Estandarización que se encarga de agrupar diferentes organizaciones nacionales para crear estándares internacionales en materia de calidad, medio ambiente, seguridad de la información y demás temas de la industria y mercado internacional.

NIST: El Instituto Nacional de Estándares y Tecnologías es una agencia del Departamento de Comercio de los Estados Unidos, cuya misión es promover la innovación y competitividad industrial.

CSD: División de Seguridad en Cómputo, la cual es parte del NIST, desarrolla y publica estándares que apoyan en el establecimiento de requisitos mínimos de seguridad para diversos sistemas.

CIS: El Centro para la Seguridad del Internet es un organismo sin fines de lucro que emite recomendaciones en materia de seguridad en Internet a entidades públicas y privadas de Norte América.

SANS: El Instituto SANS es uno de los principales centros de certificación y entrenamiento para profesionales de Seguridad de la Información a nivel mundial. Como parte de sus tareas desarrolla, mantiene y pone a disposición de la comunidad de Internet documentos que cubren varios aspectos de seguridad de la información.

Con base en el análisis de riesgos y tomando en cuenta las recomendaciones de los organismos internacionales que se consideren pertinentes, serán consolidados los controles de seguridad para los distintos dispositivos de la infraestructura tecnológica. Las actividades generales para el desarrollo, implementación, pruebas y verificación de los controles tecnológicos se enlistan a continuación:

A. Generación de las listas de verificación de seguridad de los componentes tecnológicos como son:

- Sistemas operativos.
- Consolas de monitoreo de infraestructura.
- Servidores de capa de aplicativo central, capa de base de datos, capa de extracción/publicación y arreglo de servidores para difusión de actas.
- Software de gestión de bases de datos (captura y actas digitalizadas).
- Servidores web.
- Dispositivos de comunicaciones.
- Aplicativo central.
- Infraestructura en la nube.

B. Implementación de los baselines de seguridad

Con base en las mejores prácticas de seguridad de la información por organismos internacionales como el CIS, SANS y NIST y con base en las necesidades del PREP, generar los baselines de seguridad.

- Coordinar la implementación de los baselines de seguridad con las diferentes áreas responsables.
- Ejecutar el robustecimiento a los diferentes sistemas operativos usados como MCAD, TCA y consolas de monitoreo.

C. Implementación de seguridad perimetral

Implementar Firewall perimetral para limitar el acceso a la red del PREP del OPL, así como tráfico de salida de los usados del PREP.

Implementar un Sistema de Detección de Intrusos (IDS) para verificar el tráfico de la red interna del PREP en busca de patrones anormales en dicha red.

8.3. Control de Acceso

Para robustecer el proceso de autenticación de los sistemas del PREP se debe controlar el acceso a los activos importantes de información, esto a través de tecnología conforme a las necesidades del PREP y con base en los resultados del análisis de riesgos. Para ello se deberá revisar información y tecnología disponible, tal como software de doble factor de autenticación, directorio activo o DAP, token en software y/o hardware para enrolamiento y demás soluciones disponibles con el fin de poder definir el esquema a implantar para el control de acceso lógico a los activos del PREP. Dentro del alcance de esta actividad, se llevará a cabo:

Definición de esquema de trabajo a seguir para el control de acceso al aplicativo central, a la aplicación móvil, a la base de datos, servidores y demás infraestructura que da soporte al PREP.

Arquitectura para la autenticación desde los dispositivos móviles y desde los MCAD y TCA.

En su caso, desarrollo de investigación de mercado para la adquisición de soluciones de autenticación.

Implementación de los controles necesarios para fortalecer el acceso de los usuarios al aplicativo central y a la aplicación móvil.

Implementación de los controles necesarios para fortalecer el acceso de los usuarios a bases de datos, servidores, equipos de comunicaciones y equipos de cómputo personal.

Emisión de lineamientos para control de acceso lógico.

Adicionalmente al robustecimiento del control de acceso a los sistemas del PREP, se debe tomar en cuenta el control de acceso físico, en particular al Centro de datos que se utilice para el PREP, mediante lineamientos para control de acceso físico.

8.2. Plan de Concientización

Para el ITE, es muy importante que tanto el personal operativo del PREP, como los demás actores involucrados, (Consejeros del ITE, Representantes de Partido Político acreditados para el acompañamiento en los DAT, entre otros) conozcan los posibles escenarios de riesgo que pudieran afectar la correcta implementación del Programa, tanto de manera operativa como de seguridad del sistema y de la información que se contemplan en el presente documento, por lo que se elaborará un Plan de concientización, dirigido al personal y demás involucrados en la operación y supervisión del PREP, el cual se regirá bajo el siguiente índice analítico:

- **Presentación del Plan.** Explicación breve y amigable del contenido del Plan buscando destacar la importancia y necesidad del mismo.
- **Objetivos:** Uno general que se basa en la generación de conocimiento de los posibles riesgos en la operación del PREP, así como específicos que determinarán en base al conocimiento previo, las rutas para mitigar o reducir los efectos de los diferentes escenarios en caso de que se presenten.

- **Análisis de Información.** Se basará en una evaluación diagnóstica al personal operativo del PREP previo a las capacitaciones a realizar en el mes de noviembre; para conocer si tienen experiencia previa y de manera general si conocen los riesgos que se podrían presentar en el ejercicio de sus funciones, así como en su caso la posible solución del mismo.
- **Diseño y contenido de formatos y materiales de capacitación.** El diseño de los materiales de capacitación se realizará de manera conjunta por la Dirección de Organización Electoral, Capacitación y Educación Cívica del ITE, con el contenido que provea el Proceso Técnico Operativo apropiado para el presente proceso electoral y de este Plan, y de conformidad con lo que se establece en el apartado 8.1.
- **Plan de Trabajo.** Para la implementación del plan de seguridad y continuidad se presente el siguiente cronograma de actividades.
- **Reporte de situación final.** Una vez realizado, presentado y capacitado al personal involucrado en la operación del PREP y previo a la ejecución de sus funciones el día de la jornada electoral, se les realizará una evaluación final que tendrá por objetivo entre otros el determinar la apropiación de los escenarios de riesgo y las acciones de continuidad que en su caso deberán realizar.

Monitoreo y respuesta a incidentes de Seguridad

La operación de un sistema eficiente de monitoreo de la infraestructura del PREP permitirá detectar y en su caso contener oportunamente ataques por medio de procedimientos de respuesta a incidentes de seguridad. Para tal monitoreo se recomienda considerar los siguientes aspectos como mínimo:

- Monitoreo y análisis del tráfico de red
- Análisis de los logs de la infraestructura del PREP.
- Así mismo las etapas de implementación del sistema de monitoreo recomendadas se enlistan a continuación:
- Requerimientos y planeación del proyecto de monitoreo
- Diseño y arquitectura
- Instalación y configuración de equipos de monitoreo
- Pruebas de funcionalidad
- Monitoreo y generación de reportes

9. Plan de Continuidad y Plan de Recuperación de Desastres

El plan de seguridad se determina con base en los factores establecidos en los apartados anteriores y se resume en la seguridad del desarrollo y operación del PREP el día de la jornada electoral, y en la seguridad del Sistema Informático a operar, así como de la información generada y almacenada en el propio Sistema.

El plan de continuidad busca establecer rutas críticas para que el PREP siga operando en caso de una interrupción sea operativa o de sistema, minimizando los impactos que se pudieran generar y previniendo un paro total del programa.

De los antecedentes descritos y documentados, el plan de seguridad establece los siguientes supuestos:

- a) **Continuidad de los procedimientos del CATD.** La captura, verificación, digitalización y publicación de los resultados del PREP, estarán a cargo del personal designado, por lo que el Área Técnica de Informática establecerá un mecanismo de autenticación para el acceso al sistema, y cada rol tendrá solo acceso a su función específica; en caso de que el personal no continúe con las actividades por cualquier causa, se podrá eliminar o modificar la autenticación de manera inmediata para dar acceso a quien se haga cargo de las funciones que correspondían al personal que no las realice o abandone. Asimismo, en caso de paro parcial o total de actividades del CATD, se podrán reasignar los roles respectivos al CATD para contingencias.

El Coordinador del CATD, llevará una lista de cotejo, que asegurará la operatividad del CATD desde el acopio hasta la publicación y resguardo del AEC. Asimismo, llevará un control de reporte de incidentes, para generar la ruta de atención y solución, que además servirá de insumo para generar un reporte final de la ejecución del PREP.

La capacitación, simulacros y materiales de apoyo que el personal involucrado de manera directa o indirecta que ofrezca información de los escenarios, factores y activos de riesgo, así como las alternativas para su mitigación o reducción de efectos perniciosos.

- b) **El plan de continuidad del negocio:** De los escenarios de riesgos, es importante establecer la ruta para salvaguardar la información y continuidad de las operaciones del PREP, el plan de continuidad de negocio es un procedimiento. El estándar internacional para la continuidad del negocio, ISO 22301, la define como la “capacidad (de una organización) de continuar la prestación de productos o servicios en los niveles predefinidos aceptables tras incidentes de interrupción de la actividad”; de manera genérica se desarrolla en los siguientes puntos que se adecuan al presente:

1. **Análisis del riesgo.** El Coordinador determina el tipo y nivel de riesgo al que se enfrenta en el CATD:
 - Tipo: De Información, de Sistema, Operativo.
 - Nivel: Alto-Medio-Bajo.
2. **Manejo de crisis.** El coordinador del CATD determina si el riesgo es manejable por el personal operativo a su cargo, por algún actor involucrado o requiere de auxilio. Informa a la base central de operaciones del PREP y genera el reporte en la lista de incidentes.

Para determinar el manejo, dependerá de los factores de tiempo, recursos y nivel de riesgo:

- Recursos para atender el nivel de riesgos suficientes/insuficientes.
 - Temporalidad: menor a 30 minutos / mayor a 30 minutos.
 - Nivel: Alto-Medio-Bajo.
3. **Respuesta de emergencia.** En caso de que el personal del CATD cuente con los recursos suficientes o se pueda dar respuesta inmediata al conflicto por parte de la base central de operaciones del PREP, se informará y/o solicitará a través de los canales de comunicación

disponibles (Telefonía, internet). Los escenarios descritos en los apartados 5 y 6 del presente, proveen de las alternativas generales de solución a los escenarios de riesgo más comunes.

4. **Comunicación de crisis.** De manera invariable el Coordinador deberá informar el tipo de crisis que se presente en el CATD a la base central de operaciones del PREP, sea o no susceptible de resolución en el mismo; para que en un primer momento se conozca el escenario y posteriormente se dé la mejor solución de mitigación y en su caso, se prevea el auxilio necesario.
5. **Análisis de impacto al negocio.** En su caso determinar la pérdida generada, sea por tiempo o por información, los alcances de la misma y el nivel de afectación al PREP, para la toma de decisiones alternativas que prevengan su reincidencia, mismo que la base central de operaciones del PREP generará. Este paso auxiliará para la evaluación y en su caso readecuación de la respuesta.

Para la Continuidad del Negocio, existen responsables que realizan diversos roles que permiten definir funciones en cada una de las etapas y que se describen a continuación

- c) **Continuidad de los procedimientos del Sistema Informático.** El plan de recuperación de desastres además de lo establecido en el apartado anterior deberá generar una respuesta eficaz a la interrupción del PREP, por escenarios de riesgo que afecten directamente la continuidad del sistema o de la información:

1. Recuperación de desastres. En caso de que la crisis sea en el sistema o la información alojada, la base central de operaciones del PREP determinará y operará la recuperación inmediata, previendo los intervalos de publicación y actualización de resultados.

- d) **Procedimientos de continuidad operativos en el CATD.** Como se ha establecido en párrafos anteriores, se prevé la firma de un convenio con la Secretaría de Seguridad Pública Estatal para contemplar la custodia del ITE y por ende, la operatividad y funcionamiento correcto del CATD.

Asimismo, en caso de alguna contingencia que impida el funcionamiento del CATD, se tiene previsto un mecanismo de traslado de actas al CATD para contingencias. Este mecanismo será operado por le DOECyEC y se tiene previsto al menos los siguientes requerimientos.

El procedimiento será el siguiente:

1. El Coordinador notifica el motivo de la suspensión de actividades del CATD, trasladándose al CATD designado para contingencias con las AEC que se tengan.
2. Las AEC serán entregadas en el CATD para contingencias y el personal del CATD en dicho escenario, realizará las actividades respectivas.
3. El ATI, realizará las gestiones técnicas necesarias a efecto de que el CATD para contingencias pueda ser operado por el personal del CATD, brindará las facilidades para que la captura, verificación, digitalización y publicación de resultados se realicen de manera más ágil.

9.1. Continuidad Operativa del PREP.

Si bien es cierto, la seguridad del PREP, recae precisamente en la continuidad de su implementación el día de la jornada electoral, y que de conformidad con los escenarios previstos en el presente documento los riesgos impactan directamente en el desarrollo adecuado de éste; las previsiones de continuidad que se establecen a continuación garantizan que en su caso, la suspensión de actividades de los CATD sean mínimas y se contemplen los mecanismos de control que garanticen los procedimientos de acopio, captura, verificación, digitalización y publicación de los resultados electorales preliminares. Por lo que a continuación se especifican dichos mecanismos:

- a) **Materiales y servicios del CATD.** De los escenarios previstos, en caso de falla de equipos de cómputo parcial o total se prevé asignar a personal del ITE para atender las incidencias, así como tener equipos de cómputo para contingencias.

EQUIPOS DE CÓMPUTO PARA CONTINGENCIAS	TOTAL	PERSONAL DE LA ATI
Computadora	5	1
No break	5	1
Scanner	1	1

Relativo a los servicios de energía eléctrica e internet, se prevé la adquisición/renta de plantas de energía eléctrica y en su caso, adquisición de bams de prepago, cuando éstos no sean reinstalados dentro de los tiempos establecidos en el apartado respectivo.

MATERIALES PARA CONTINGENCIAS			
PLANTAS DE ENERGÍA ELÉCTRICA PARA CONTINGENCIA	2	BAMS DE PREPAGO	1

- b) **Personal del CATD.** En este supuesto es necesario establecer que las actividades encomendadas al personal por rol en el CATD derivarán de la asignación de autenticaciones, por lo que el ITE, prevé capacitar al personal del ATI y personal auxiliar del ITE para que en su caso auxilien en las labores que el personal designado al CATD, pudiera dejar o no realizar.

Por tanto, las capacitaciones previstas en el Proceso Técnico Operativo del PREP, estarán dirigidas también al personal con que cuente el ATI, en su caso las y los integrantes del Consejo General, y

demás personal que se faculte para dicha actividad; contemplando dos personas en función de auxilio, asignando una por CATD.

9.1.1. CATD para contingencias.

De conformidad con el Proceso Técnico Operativo del PREP, aprobado para el Proceso Electoral Local Ordinario 2020-2021, se prevé instalar un CATD para contingencias en las instalaciones del Área Técnica de Informática; mismo que deberá estar habilitado para ocuparse en caso de que las actividades del CATD instalado en el ITE sean suspendidas y no se pueda continuar con las mismas en dichas instalaciones.

Para el buen funcionamiento del CATD para contingencias, se requiere de la infraestructura necesaria misma que se establece a continuación:

- a) Instalaciones: Área Técnica de Informática.


RECURSOS MATERIALES	
MATERIAL	TOTAL
Computadoras	5
Scanner	1
No break	5
Mesas de Trabajo	2
Sillas	5

Con este material se pretende habilitar en su caso, un punto de captura, verificación, digitalización y publicación de resultados, contemplando que el personal del CATD con el escenario de riesgo se traslade a la sede del CATD para contingencias y pueda realizar sus funciones en él; en su caso con el personal auxiliar que se haya capacitado al efecto.

9.1.2. Continuidad en el Consejo General del ITE.

Además de las previsiones que aplican para el CATD, reviste mayor importancia la continuidad de la implementación del PREP en la sede del Consejo General del ITE, en primer término, porque en sus instalaciones, se encontrará el Área Técnico-Operativa Central del mismo y derivado de ello, su buen funcionamiento impactará en el correcto desarrollo e implementación del PREP en el CATD. Por lo que se describen de manera específica los mecanismos de continuidad para la sede del Consejo General del ITE:

- a) Respecto a fallas eléctricas, se contratará una planta de luz de la Comisión Federal de Electricidad, para proveer de la energía eléctrica, en caso de contingencia. Dicha planta estará conectada con por lo menos 3 días de anticipación para realizar simulacros y determinar el tiempo de restablecimiento de energía eléctrica.

- 
- b) Respecto a fallas en el internet, se contratará un servicio adicional que se encontrará habilitado para que en caso de falla del servicio base, se pueda realizar la conexión de manera inmediata al servicio adicional
 - c) En caso de intento de bloqueo o invasión de las instalaciones del ITE, se prevé la habilitación y ubicación de todos los accesos del mismo, la custodia del Instituto con las fuerzas de policía estatal y municipal.
-
- 