HIDALGO
IEE
INSTITUTO ESTATAL ELECTORAL

PODERNET
El Poder de Internet

Plan de Seguridad para el Programa de Resultados Electorales Preliminares

Proceso Electoral Local 2023-2024

Contenido

Glosario

ADSL	Acrónimo en inglés de Asymmetric Digital Subscriber Line, es un tipo de tecnología de línea telefónica para transmitir Voz y Datos.
Algoritmos de Criptografía	Los algoritmos de criptografía, es un algoritmo que modifica los datos de un documento con el objetivo de alcanzar algunas características de seguridad como autenticación, integridad y confidencialidad.
ARE	Área de Responsabilidad Electoral asignada a un CAEL o SEL.
CAEL	Capacitador Asistente Electoral Local, es en primera instancia el encargado de la implementación del Mecanismos para la Digitalización de las Actas PREP desde las Casillas.
CATD	Centros de Acopio y Transmisión de datos, son los centros oficiales para el acopio de las Bolsas-PREP y unidades básicas en las cuales se pueden realizar actividades de acopio, digitalización y transmisión de las imágenes de las Actas de Escrutinio y Cómputo del PREP.
CCV	Centros de Captura y Verificación, en estos se llevan a cabo las actividades de Captura, Verificación y Publicación de los resultados provenientes de las Actas de Escrutinio y Cómputo del PREP.
HTTPS	Hyper Text Transfer Protocol Secure (Protocolo seguro de transferencia de hipertexto) es un protocolo que permite establecer una conexión segura entre el servidor y el cliente, que no puede ser interceptada por personas no autorizadas.
IEEH	Instituto Estatal Electoral de Hidalgo.
Logs de Acceso	Son bitácoras que se almacenan en un Sistema, las cuales permiten registrar los intentos de acceso, ya sea permitidos o no, al mismo.
OPL	Organismo Público Local, Cada estado cuenta con un Instituto Electoral Local quienes se encargan de la organización de las elecciones para designación de: Gobernador, Diputados Locales, Integrantes de Ayuntamientos, entre otros.

PREP	Programa de Resultados Electorales Preliminares, es un sistema que provee los resultados preliminares de las elecciones, a través de la captura y publicación de los datos plasmados por los funcionarios de casilla en las actas de escrutinio y cómputo.
SEL	Supervisor Electoral Local, es la persona encargada de la Supervisión del Personal CAEL.
UPS	Uninterruptable Power Supply, Sistema de Alimentación Ininterrumpida, es un dispositivo permite tener flujo de energía eléctrica mediante baterías, cuando el suministro eléctrico falla.
Cámara Web	Es un dispositivo para trasmitir video a través de una red (web), ya sea de manera local o a través de internet.

Introducción

Los riesgos, en términos de seguridad, se caracterizan por lo general mediante la siguiente ecuación:

riesgo = (amenaza * vulnerabilidad) / contramedida

La amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad (conocida a veces como falencias (flaws) o brechas (breaches)) representa el grado de exposición a las amenazas en un contexto particular. Finalmente, la contramedida representa todas las acciones que se implementan para prevenir la amenaza.

Las contramedidas que deben implementarse no solo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas.

Para que un sistema sea seguro, deben identificarse las posibles amenazas y, por lo tanto, conocer y prever el curso de acción del enemigo. Por tanto, el objetivo de este informe es brindar una perspectiva general de las posibles motivaciones de los hackers, categorizarlas, y dar una idea de cómo funcionan para conocer la mejor forma de reducir el riesgo de intrusiones.

Una vez analizados los posibles factores de riesgo que podrían interferir en el funcionamiento del PREP, se determinan a continuación las medidas de seguridad que habrán de implementarse para aceptar, mitigar, transferir o eliminar cada uno de los riesgos identificados que pudiesen entorpecer el funcionamiento del PREP, permitiendo con ello mediante un plan de continuidad el funcionamiento continuo del Programa de Resultados Electorales Preliminares.

Normatividad Aplicable

Reglamento de Elecciones

- De conformidad con el artículo 347, el numeral 1 y 2, del Reglamento de Elecciones, para la auditoría de verificación y análisis en sistema informático para los distintos procedimientos del PREP, se considerarán como mínimo los siguientes puntos, que a la letra dicen:

  1. El Instituto y los OPL deberán someter su sistema informático a una auditoría técnica para lo cual se deberá designar un ente auditor. El alcance de la auditoría deberá cubrir, como mínimo, los puntos siguientes:

  (a) Pruebas funcionales de caja negra al sistema informático para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares.
  (b) Análisis de vulnerabilidades, considerando al menos pruebas de penetración y revisión de configuraciones a la infraestructura tecnológica del PREP.

  2. Para la designación del ente auditor se dará preferencia a instituciones académicas o de investigación y deberá efectuarse a más tardar, cuatro meses antes del día de la jornada electoral. El ente auditor deberá contar con experiencia en la aplicación de auditorías con los alcances establecidos en el numeral anterior"

- De conformidad con el artículo 348, el numeral 1 del Reglamento de Elecciones, para implementación de controles de seguridad operativa del PREP con base a los análisis de riesgos, que a la letra dice:

  1. El Instituto y los OPL deberán implementar las medidas de seguridad necesarias para la protección, procesamiento y publicación de datos, imágenes y bases de datos. Asimismo, deberán desarrollar en sus respectivos ámbitos de competencia, un análisis de riesgos en materia de seguridad de la información, que permita identificarlos y priorizarlos, así como implementar los controles de seguridad aplicables en los distintos procedimientos del PREP, conforme a las consideraciones mínimas descritas en el Anexo 13."

- De conformidad con el artículo 348 del Reglamento de Elecciones, con respecto a la Seguridad Operativa, que a la letra dice:

  1. El Instituto y los OPL deberán implementar las medidas de seguridad necesarias para la protección, procesamiento y publicación de datos,

imágenes y bases de datos. Asimismo, deberán desarrollar en sus respectivos ámbitos de competencia, un análisis de riesgos en materia de seguridad de la información, que permita identificarlos y priorizarlos, así como implementar los controles de seguridad aplicables en los distintos procedimientos del PREP, conforme a las consideraciones mínimas descritas en el Anexo 13.

Anexo 13 "Lineamientos del Programa de resultados Electorales preliminares (PREP)" del Reglamento de Elecciones

- De conformidad con el numeral 4, del Anexo 13 del Reglamento de Elecciones para la implementación de la seguridad y la continuidad en los distintos procedimientos del PREP, se considerarán como mínimo los siguientes puntos, que a la letra dicen:

  4. El Instituto y los OPL tienen la facultad y responsabilidad de implementar y operar el sistema informático del PREP. Para el desarrollo del sistema informático se deberán cumplir las siguientes etapas mínimas y contar con evidencia documental de las mismas:

  I. Análisis: en esta etapa se deben llevar a cabo la investigación y revisión de todos los aspectos (técnicos y legales) relacionados con la implementación y operación de los procesos y del sistema informático que conformarán el PREP;
  II. Diseño: esta etapa consiste en utilizar la información recolectada en la etapa de análisis con el propósito de desarrollar un modelo con las correspondientes especificaciones de cada uno de los componentes del sistema informático (hardware, software), así como de los procesos; tomando en cuenta aspectos de funcionalidad, capacidad, continuidad y seguridad;
  III. Construcción: en esta etapa se utiliza el modelo o los modelos establecidos en la etapa de diseño con el objetivo de llevar a cabo las adquisiciones de bienes, la contratación de servicios, así como la instalación y configuración de hardware y software, y el desarrollo de las aplicaciones; y,
  IV. Pruebas: esta etapa consiste en verificar y asegurar que todos los componentes que integran el sistema informático operan conforme a los requerimientos establecidos en la etapa de análisis, cumplen con el modelo determinado en la etapa de diseño y aseguran la integridad en el procesamiento de la información. Las pruebas deben realizarse tanto de forma unitaria como de manera integral, cubriendo los aspectos de funcionalidad, capacidad, continuidad y seguridad."

- De conformidad con el numeral 9 del Anexo 13 del Reglamento de Elecciones, para la ejecución de la Auditoría, se considerará como mínimo el siguiente punto, que a la letra dice:

9. La auditoría deberá ejecutarse sobre todos los módulos del sistema informático previo al inicio de los simulacros. Si de las pruebas y simulacros resultara necesario realizar ajustes al sistema, esto deberá hacerse del conocimiento del ente auditor para contar con un margen de tiempo que permita aplicar las medidas que resulten necesarias y se garantice que el sistema auditado sea el que opere para el PREP."

- De conformidad con el numeral 12, del Anexo 13 del Reglamento de Elecciones, para la implementación de los controles de seguridad aplicables en los distintos procedimientos del PREP, se considerarán como mínimo los siguientes puntos, que a la letra dicen:

12. Para la implementación de los controles de seguridad aplicables en los distintos procedimientos del PREP, se considerarán como mínimo los siguientes puntos:

I. Factores de riesgo: establecer e identificar el conjunto de medidas específicas para evaluar los riesgos con base en su impacto y la probabilidad de ocurrencia;
II. Activos críticos: identificar cuáles son los recursos humanos y materiales, servicios e información (en sus diferentes formatos) de valor para los procedimientos del PREP;
III. Identificación, evaluación y gestión de riesgos: deberá identificarse y describirse la situación o condición –técnica, legal, económica, política, social, entre otros – que pueda afectar los procedimientos del PREP; posteriormente, deberá describirse claramente cuáles son los impactos que se pueden tener en el caso que una amenaza se materialice; finalmente, se deberá definir y documentar la respuesta respecto de cada uno de los riesgos identificados, precisando si los riesgos serán aceptados, mitigados, transferidos o eliminados; y;
IV. Plan de seguridad: se deberá elaborar un plan de seguridad basado en los resultados de un análisis de riesgos, que permita llevar a cabo la implementación de controles en los distintos procedimientos de operación del PREP, así como en la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP. Dicho plan deberá ser elaborado por la instancia interna y, en su caso, en coordinación con el tercero que auxilie en la implementación y operación del PREP."

- De conformidad con el numeral 13, del Anexo 13 del Reglamento de Elecciones, para la implementación de los controles de seguridad aplicables en los distintos procedimientos del PREP, se considerarán como mínimo los siguientes puntos, que a la letra establecen:

13. Se deberá implementar un plan de continuidad para determinar las acciones que garanticen la ejecución de los procedimientos relativos a las fases establecidas en el proceso técnico operativo del Instituto o de los OPL, en caso de que se suscite una situación adversa o de contingencia, el cual deberá incluir a los responsables y los medios de contacto para llevar a cabo la resolución de contingencias.

Dicho plan deberá ser elaborado por la instancia interna y, en su caso, en coordinación con el tercero que auxilie en la implementación y operación del PREP.

El plan de seguridad y plan de continuidad deberá ser comunicado al personal involucrado en su ejecución en función de las actividades a desempeñar por cada rol operativo, con la suficiente antelación para formar parte de los ejercicios y simulacros.”.

- De conformidad con el numeral 16, del Anexo 13 del Reglamento de Elecciones para la implementación de la seguridad y la continuidad en los distintos procedimientos del PREP, se considera como mínimo el siguiente punto, que a la letra dice:

16. Los OPL deberán ejecutar, al menos, una prueba que tendrá como objetivo verificar el correcto funcionamiento del sistema informático del PREP en la que se contemplen, como mínimo, las fases de digitalización, captura, verificación y publicación de los datos asentados en los formatos aprobados del AEC.

El sistema informático que sea sometido a la o las pruebas, deberá integrar todos los componentes que permitan verificar la totalidad de las funcionalidades necesarias para ejecutar íntegramente el proceso técnico operativo aprobado.

Para la ejecución de la o las pruebas, los OPL deberán considerar, por lo menos, los siguientes aspectos:

I. Deberá ejecutarse, a más tardar, mes y medio antes del día de la jornada electoral, en el día establecido por cada OPL.
II. Deberá contar con la participación presencial de las y los integrantes de la Comisión que dé seguimiento a la implementación y operación del PREP, del COTAPREP y del ente auditor, de acuerdo con sus atribuciones y funciones.
III. Se procesará la cantidad de actas que permita verificar los distintos flujos del funcionamiento integral del sistema informático del PREP, considerando para ello los criterios mínimos que establezca el Instituto.
IV. La instancia interna deberá elaborar un informe de evaluación, de acuerdo con el formato establecido por el Instituto; dicho informe

deberá hacerse del conocimiento de las y los integrantes de la Comisión que dé seguimiento a la implementación y operación del PREP y del COTAPREP, a efecto de que se tomen las determinaciones necesarias con base en los resultados obtenidos. Dicho informe deberá ser remitido al Instituto dentro de los cinco días posteriores a la ejecución de la prueba.

Si como resultado de la prueba no ha sido posible verificar el correcto funcionamiento del sistema informático, se deberán ejecutar las pruebas necesarias hasta cumplir con el objetivo de la misma.

La fecha, hora y lugar en la que se ejecutará la o las pruebas deberá hacerse del conocimiento de las y los integrantes de la Comisión, del COTAPREP, del ente auditor y del Instituto al menos 5 días previos a su ejecución, asimismo, se deberán brindar las facilidades necesarias para el seguimiento presencial.

En la realización de los simulacros se deberá cubrir lo siguiente:

I. Ejecución de todos los procesos y procedimientos operativos relacionados con la digitalización, captura, verificación y publicación de las Actas PREP.
II. Aplicación total o parcial del plan de continuidad, y.
III. Procesamiento de, al menos, la cantidad total estimada de Actas PREP que se prevén acopiar, el día de la Jornada Electoral, empleando los formatos de AEC aprobados por el Instituto. En caso de que durante los simulacros no pueda procesarse el cien por ciento de las Actas esperadas, se deberá dejar constancia de tal circunstancia en el informe correspondiente y la instancia interna responsable de coordinar el PREP determinará la necesidad de ejecutar un simulacro adicional.
IV. En todos los simulacros deberán procesarse Actas PREP que contemplen todos los supuestos de inconsistencia: excede lista nominal, algún campo ilegible, algún campo sin dato, todos los campos ilegibles, todos los campos sin dato, así como, los supuestos de Sin Acta y fuera de catálogo. Se procurará la distribución de las inconsistencias y supuestos antes señalados de manera igualitaria en todos los centros en los que se realice la captura de datos.”

Objetivo General

El objetivo principal del presente Plan de Seguridad, es establecer las normas y procedimientos que minimicen los riesgos en los Recursos Humanos, el Equipamiento y las Telecomunicaciones que son parte de la columna vertebral del PREP. Estos procedimientos describen los mecanismos de seguridad aplicables para la prevención de los riesgos que pudiese presentarse durante la Jornada Electoral.

Así mismo, contempla restricciones a ciertos lugares, autorizaciones, perfiles de los usuarios, protocolos y todo lo necesario que permita del desarrollo del PREP, minimizando la probabilidad de posibles contingencias.

Objetivos Específicos

El Plan de Seguridad está concebido para proteger los activos críticos del PREP, para lo cual se deben considerar:

- **Los Recursos Humanos**: Son las y los usuarios que utilizan la infraestructura tecnológica, las telecomunicaciones y que gestionan la información del PREP. El sistema debe protegerse en general para que el uso por parte de los usuarios no pueda poner en peligro la seguridad de la información del PREP y tampoco que la información que procesan sea vulnerable.

- **El Equipamiento**: Es un elemento fundamental para la captura, proceso y transmisión de la información del PREP, así como para el asegurar el publicar la información de manera oportuna. La función del plan de seguridad es asegurar por que los equipos funcionen correctamente y anticiparse en caso de fallos, robos, incendios, sabotajes, desastres naturales, fallos en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura tecnológica del PREP.

- **Las Telecomunicaciones**: En los proyectos de misión crítica, como lo es el PREP, las telecomunicaciones desempeñan un papel elemental, ya que el no poder acceder o transmitir la información, detiene el flujo de datos referentes a los resultados obtenidos de las Actas PREP que se requieren publicar

Baseline

La seguridad informática se resume, por lo general, en cinco objetivos principales:

I. **Confidencialidad**, que asegura que solo las y los individuos autorizados tengan acceso a los recursos que se intercambian;

II. **Integridad**, que garantiza que los datos sean los que se supone que son;

III. **Disponibilidad**, que garantiza el correcto funcionamiento de los sistemas de información;

IV. **Evitar el rechazo**, que garantiza de que no pueda negar una operación realizada;

V. **Autenticación**, que asegura que solo las y los individuos autorizados tengan acceso a los recursos.

Alcance

Este documento está dirigido a todo el personal vinculado con las Tecnologías de la Información del PREP, ya sea por la responsabilidad que tienen asignada con relación a los bienes informáticos o por los beneficios que de ellos obtienen.

Los primeros destinatarios de esta metodología son el personal que participará en el PREP, que responden por el buen funcionamiento de las tecnologías y la información que en ellos se procesa.

El alcance expresa el radio de acción que abarca el Plan de Seguridad, de acuerdo al Sistema Informático del PREP, para el cual fueron determinados los riesgos y diseñado el Plan de Seguridad. La importancia de dejar definido claramente el alcance del Plan (y de ahí su inclusión al comienzo del mismo) consiste en permitir tener a priori una idea precisa de la extensión y los límites en el que el mismo tiene vigencia.

Una vez definido el alcance del Plan de Seguridad, y realizada una detallada descripción del sistema informático, corresponde finalizar esta primera parte con la formulación de las conclusiones obtenidas durante la determinación de las necesidades de protección, mediante la evaluación sistemática de los riesgos.

Directrices de Seguridad informática

Tanto el Plan de Seguridad como el Plan de Continuidad están basados en los resultados de la estrategia de Gestión de Riesgos, derivada del Análisis de Riesgos, que permite llevar a cabo la implementación de controles en los distintos procedimientos de operación del PREP, así como en la infraestructura tecnológica.

El PREP requiere un alto nivel de seguridad en el manejo de la información, por lo que es necesario implementar medidas que permitan fortalecer la seguridad y disminuir el riesgo, por lo que será de observancia general el cumplimiento mínimo de los siguientes puntos:

1. Debe considerarse la protección de la información en el flujo de datos tanto dentro de los CCV como en los CATD, empleando canales de comunicación seguros y protocolos cifrados. Los medios de transmisión serán seguros. El objetivo es que se impida la alteración de la información electoral en tránsito, a través de la red de comunicaciones, así como el acceso de manera no autorizada a los equipos de cómputo que intervienen en el proceso.

2. Se contempla el uso de algoritmos de criptografía con reconocida robustez en la industria y una buena administración de claves, que aseguren la adecuada protección de la confidencialidad de los datos. Entre ellos, canales seguros mediante protocolo HTTPS y utilizar métodos de verificación de integridad de la información enviada y recibida.

3. Se considera para la operación del Sistema del PREP, el uso de funciones restringidas de acuerdo al rol de los usuarios y así limitar la exposición del servicio ante incidentes.

4. Se incluye la implementación de Logs de acceso, los cuales permiten la trazabilidad de las transacciones realizadas por cada uno de los usuarios.

5. Se implementan controles de Monitoreo que permitan conocer el estado tanto del equipamiento instalado, como de las telecomunicaciones en cada uno de los CATD.

6. La totalidad de los equipos de cómputo empleados serán validados, además de los mecanismos de cifrado, mediante las MAC Address provenientes *de los mismos, así como las IP's asignadas a cada uno.*

7. Cada computadora tendrá instalado el software requerido para el Sistema del PREP, con el Sistema Operativo cerrado, de tal forma que no permita la instalación de ningún otro tipo de Software al requerido para el PREP.

8. La red del equipamiento del PREP es de uso exclusivo, por lo que ningún otro equipo ajeno a la misma podrá hacer uso de la conexión a internet instalado para el PREP, tanto en los CATD como en los CCV.

9. El equipamiento de Cómputo del PREP está restringido para que no se pueda conectar al mismo, ningún otro componente de Hardware, por lo que estará prohibido a las y los usuarios el hacerlo.

10. La totalidad del equipamiento del PREP debe contar con monitoreo vía video, para verificar el acceso a cada una de las áreas del PREP, tanto en los CATD como en los CCV.

11. El acceso a las áreas del PREP en los CATD, está restringido y se incorporan bitácoras de registro en cada uno de ellos. Para el caso de los CCV, se cuenta con acceso vía bitácoras de registro en cada uno de ellos para poder ingresar a los mismos.

12. Se implementa un Plan de Concientización, mismo que se realiza durante la capacitación del Personal del PREP.

13. Se contempla la implementación de una Auditoría Externa, por parte del Ente Auditor que para ello determine el IEEH.

Desarrollo

Tanto el **Plan de Seguridad** como el **Plan de Continuidad**, contemplan cuatro Áreas de Amenaza identificadas en el análisis de Riesgos:

A. Utilización del Aplicativo para la Digitalización de las Actas PREP desde las Casillas.

B. Centros de Acopio y Transmisión de Datos (CATD)

C. Centros de Captura y Verificación (CCV)

D. Nube de Internet

Se describen medidas específicas para cada una de estas tres áreas, mismas que se describen a continuación:

A. Utilización del Aplicativo para la Digitalización de las Actas PREP desde las Casillas

Conforme a la metodología para su implementación, se contemplan los siguientes Activos Críticos:

a) Recursos Humanos

b) Equipamiento

c) Telecomunicaciones

A continuación, describimos cada uno de ellos:

a) Recursos Humanos

En la operación de mecanismos para la Digitalización de las Actas PREP desde las casillas, participarán:

1. Capacitadores Asistentes Electorales Locales (CAEL)

2. Supervisores Electorales Locales (SEL)

En primera instancia, los o los Capacitadores Asistentes Electorales Locales serán las personas encargadas de realizar el procedimiento de Digitalización y Transmisión de las Actas PREP desde las Casillas.

En caso de que durante la implementación del Mecanismo para la Digitalización de las Actas PREP desde las Casillas, al o el CAEL no pueda realizar su función, al o el SEL podrá realizar las funciones del CAEL.

b) Equipamiento

Con respecto a la utilización del Aplicativo para la Digitalización de las Actas PREP desde las Casillas, se contempla que el Dispositivo que será utilizado para este procedimiento, será proporcionado por el IEEH.

La instalación del Aplicativo para la Digitalización de las Actas PREP desde las Casillas, estará a cargo del propio IEEH, y la Aplicación PREP Casilla será proporcionada por PoderNet.

Como parte de los mecanismos de seguridad, la totalidad de los dispositivos que se empleen para la Digitalización de las Actas PREP desde las casillas, serán administrados mediante un Knox, el cual permite cerrar los dispositivos a efectos de que no se pueda manipular su contenido, ni instalar cualquier aplicación que no sean las administradas y distribuidas por el Knox.

Mediante el Knox, se podrá controlar los dispositivos y la instalación remota de las actualizaciones del Aplicativo PREP Casilla, dando un seguimiento puntual sobre el control de las versiones que se instalen.

Adicionalmente, se tendrán un control de acceso a la Aplicación PREP Casilla, validando los usuarios mediante una clave de usuario y una contraseña que van ligadas a la o el CAEL o la o el SEL asignados al número telefónico del Dispositivo Móvil.

En igual forma, mediante el catálogo de Usuarios CAEL o SEL se podrá verificar que sólo puedan digitalizar las imágenes de las casillas asignadas a su Distrito y ARE.

c) Telecomunicaciones

El Aplicativo PREP Casilla, permitirá la digitalización de las imágenes de las Actas PREP, con o sin señal de Internet en los Dispositivos.

Cada vez que se digitalice la Imagen de un Acta PREP, el Aplicativo PREP Casilla verificará la disponibilidad de la señal de Internet en el Dispositivo Móvil, en caso de contar con señal de Internet, la

imagen Digitalizada de las Actas PREP, se transmitirá de manera inmediata a los Servidores de Internet, los cuales la enviarán para su proceso a los CCV.

En caso de que no se cuente con señal de Internet en la ubicación del Dispositivo Móvil, la o el CAEL o la o el SEL, podrán continuar digitalizando las imágenes de las Actas PREP y cuando el dispositivo detecte señal de Internet, serán transmitidas las imágenes de las Actas PREP pendientes de enviar a los Servidores de Internet.

B. Centros de Acopio y Transmisión de Datos

Primeramente, para resolver cualquier tipo de contingencia que pudiese presentarse en el interior del estado, es indispensable se cuente con un equipo de Personal de Soporte Técnico Especializado denominado Comando Técnico, el cual durante la Jornada Electoral estará situado en zonas de cobertura, en las cuales dichos Técnicos puedan presentarse en Sitio en un tiempo máximo de una hora para solventar cualquier tipo de contingencia que se presentare en los siguientes Activos Críticos:

a) Recursos Humanos

b) Equipamiento

c) Telecomunicaciones

Este personal cuenta con vehículo y chofer, y en el vehículo carga equipo y material de soporte igual a los empleados en cada uno de los CATD, para que en caso de que sea necesario, puedan reemplazar cualquier equipo que pudiera fallar durante el desarrollo de la Jornada Electoral en su zona de cobertura.

Dicho personal cuenta con teléfono celular, mapas de localización de cada uno de sus CATD, relación de personal con nombres, domicilios y teléfonos de los mismos y equipamiento de soporte igual al instalado en cada uno, relación de los domicilios y números de teléfono de los CATD del PREP, así como de los teléfonos de los Consejos Electorales, Presidentes y Secretarios de los mismos. En igual forma contará botiquín de primero auxilios y con los teléfonos de emergencia de los CCV.

En todo momento el Personal de Soporte Técnico mantiene comunicación continua con los CCV y está listo para que en cualquier momento que se le requiera, pueda trasladarse al sitio que le sea designado desde los CCV.

Para los casos específicos, de los CATD cuya localización quedase lejana a cualquier base de Comando Técnico se contempla un comando fijo, el cual durante la Jornada Electoral está permanentemente en Sitio para resolver cualquier tipo de contingencia que se pudiese presentar. Igualmente, en dichos CATD se envía equipo doble para solventar cualquier falla en equipamiento.

Durante los ejercicios y simulacros del PREP, el Personal de Soporte Técnico se encuentra residente en las instalaciones de los CCV a fin de atender los reportes de asistencia técnica que se presenten durante este periodo del PREP.

a) Recursos Humanos

Una de las medidas de seguridad requeridas por el PREP es que, a partir de la instalación del mismo, se cuente con personal de Seguridad proporcionado por el Consejo Electoral donde se instale cada CATD, que no sólo vigile el área del PREP, sino sean el encargado de vigilancia para todo el Consejo Electoral.

Como medida de seguridad adicional, en todos los Consejos Electorales se restringe el acceso al área destinada para el CATD, y sólo pueden tener acceso al equipo de digitalización y transmisión de información, personal acreditado del PREP. Esto es durante la capacitación todo el personal del PREP porta su credencial de identificación del PREP y en caso de no contar con ella se le niega el acceso. Todo el Personal de Soporte Técnico del PREP igualmente porta su credencial de identificación con la leyenda de Soporte Técnico, sin la cual se les niega acceso a cualquier CATD. Para el acceso del personal, se cuenta con una Bitácora de Asistencia, en la cual el personal del PREP registra su llegada y salida de manera diaria.

En caso de presentarse cualquier persona que solicite acceso al CATD, el Coordinador del CATD solicita autorización al CCV primario, en caso de autorizarse su acceso, dicha persona se registra su acceso en la Bitácora de Visitantes, así como los motivos de su visita, las actividades que realice, así como hora de llegada y salida.

Durante la Jornada Electoral se le requiere adicionalmente al personal del PREP que porten una camiseta distintiva del PREP para que sólo ellos puedan estar en el área del CATD dentro del Consejo Electoral. Sin estas medidas de identificación se le niega el acceso a cualquier persona que se presente al CATD.

1. **Coordinadores**: Se prevé que, en caso de falla en su asistencia, la o el Acopiador o la o el Digitalizador suplirán su ausencia, por lo que deberán dominar las actividades del mismo para suplir su inasistencia.

2. **Acopiadores**: Igualmente se debe contar con un plan emergente para que, en caso de no asistir esta persona, su la o el Digitalizador o la o el Coordinador pueda suplir la ausencia del mismo.

3. **Digitalizadores**: En caso de no asistir cuenta con una persona que pueda suplir sus funciones pudiendo ser otra u otro Acopiador o la o el Coordinador.

Durante la Jornada Electoral, en caso de inasistencia o contingencia en dos o más de las personas que laboran en el mismo, se prevé el traslado del personal necesario de los CATD más cercanos, esto será realizado por el Comando Técnico.

En caso de que se detecte alguna situación de peligro o contingencia mayor, el Coordinador lo reporta de inmediato al CCV primario, para recibir instrucciones sobre el procedimiento a seguir.

b) Equipamiento

Como parte de la seguridad requerida, cada CATD cuenta con una cámara de web. Dicha cámara graba la actividad registrada en el área del CATD, para que en caso de que se presente alguna anomalía, ésta quede registrada en video. Dichas cámaras pueden ser observadas mediante un Sistema de Monitoreo que se instala en el CCV primario, en el cual puede observarse y registrarse la actividad en todos y cada uno de los CATD.

El Programa de Resultados Electorales Preliminares, cuenta en todo momento, dentro de sus instalaciones de los CCV, con equipamiento de respaldo y soporte para que, en caso de fallas del equipamiento en cualquier CATD ya sea durante los Ejercicios o Simulacros, se pueda enviar Personal de Soporte Técnico que reemplaza preferentemente durante el mismo día del reporte o a más tardar a las 9:00 horas del día siguiente, cualquier equipo que fallase durante los ejercicios, simulacros y durante la Jornada Electoral.

Como medida de seguridad en los CATD, se envía una Planta de Energía Portátil de capacidad suficiente para soportar el funcionamiento de la totalidad del equipo a instalarse en el CATD, una linterna portátil, más un foco que prevé de iluminación al CATD en caso de falla de energía eléctrica, provista por la Comisión Federal de Electricidad.

La totalidad del equipamiento de los CATD, está conectado a un UPS, así como a un regulador de voltaje, para que de esta manera se proteja el equipo contra variaciones de voltaje, y se asegure su funcionamiento continuo en caso fallas en el suministro de energía por parte de la CFE.

Durante la Jornada Electoral, se tiene un equipo de Comandos Técnicos, los cuales cuentan con equipamiento de soporte, igual al instalado en los CATD, para que, en caso de presentarse fallas de equipamiento en cualquiera de los CATD, sea reemplazado a la brevedad.

c) Telecomunicaciones

En igual forma como medida de protección para el equipamiento electrónico y de Telecomunicaciones que se usará en los CATD, se les instala un Regulador de Voltaje que protege al equipo del PREP contra posibles variaciones de voltaje. Igualmente contará con UPS.

Las telecomunicaciones contemplan preferentemente, por lo menos un medio de redundancia, para que en caso de contingencia de fallo en el medio de transmisión primario entre en funcionamiento el medio redundante, asegurando con ello la transmisión continua de la información. En caso de cualquier contingencia que se presente en los CATD, ésta debe ser reportada de inmediato al CCV primario del PREP para que se implementen las medidas emergentes necesarias.

Igualmente se implementa una Bitácora que da seguimiento a todos los reportes de fallas en los Recursos Humanos, Equipamiento y las Telecomunicaciones con el propósito de dar un seguimiento a las mismas y poder implementar medidas de contingencia para la prevención de los mismos.

De la totalidad de los servicios instalados como:

1. **Líneas Telefónicas**

2. **Enlace ADSL**

3. **Enlace Satelital**

4. **Enlace Banda Ancha Móvil**

Se contemplan las siguientes medidas de seguridad:

1. **Líneas Telefónicas.** Se contempla una línea telefónica en cada CATD, en caso de presentarse fallas en el funcionamiento de la misma, se mantiene comunicación con los CCV mediante telefonía celular.

2. **Enlace ADSL.** Se cuenta con un Enlace ADSL, para la conectividad con Internet. Como medida adicional de redundancia se contratará con un enlace mediante Banda Ancha Móvil.

3. **Enlace Satelital.** Si en algún Consejo Distrital no existe ningún tipo de servicio local de Internet, se emplea señal de

Internet Vía Satelital. Como medida adicional de redundancia se contratará con un enlace mediante Banda Ancha Móvil.

4. **Enlace Banda Ancha Móvil**: Se tiene una conexión vía Banda Ancha Móvil como medio alternativo redundante para transmisión de información a la Nube de Internet.

C. Centros de Captura y Verificación

Al igual que los CATD, en los CCV se contemplan medidas de seguridad en los siguientes Activos Críticos:

a) Recursos Humanos

b) Equipamiento

c) Telecomunicaciones

Una de las medidas de seguridad requeridas por el PREP, es que, a partir de la instalación de los CCV, se cuente con personal de Seguridad proporcionado por **PoderNet**, que no sólo vigile el área del interior del PREP, sino que hagan vigilancia perimetral.

Como medida de seguridad, en los CCV se restringe el acceso a cualquier persona ajena al PREP, sólo pueden ingresar al mismo personal acreditado del PREP. Esto es durante la capacitación a todo el personal del PREP se le proporciona credencial de identificación del PREP y en caso de no contar con ella se le niega el acceso. Se cuenta con un registro de acceso del personal mediante huella digital, el cual indicará si el personal que se presenta está autorizado para ingresar a los CCV.

En caso de presentarse cualquier persona que solicite acceso a los CCV, el Supervisor General o Supervisor Técnico son los únicos quienes pueden autorizarlo, en caso de autorizarse su acceso, dicha persona debe registrar su acceso en la Bitácora de Visitantes, así como los motivos de su visita, las actividades que realice, así como hora de llegada y salida.

Durante la Jornada Electoral se le requiere adicionalmente al personal del PREP que porten una camiseta distintiva del PREP para que sólo ellos puedan estar en los CCV del PREP.

Para solventar cualquier tipo de contingencia que pudiese presentarse en los CCV será necesario implementar las siguientes medidas de seguridad:

a) Recursos Humanos

1. **Supervisor General:** Instrumenta un plan de evacuación y realiza simulacros, verifica que la señalética se encuentre debidamente localizada, incluyendo extintores, salidas de emergencia, etc. Verifica con los responsables de seguridad del inmueble que sólo personal autorizado tenga acceso al mismo, nombra un técnico responsable del monitoreo de las cámaras de video vigilancia locales y remotas. Asegura que durante la Jornada Electoral se cuente con personal de Servicios Médicos al igual que botiquines de Emergencia. Durante los ejercicios y simulacros verificará la ejecución del Plan de Continuidad.

2. **Coordinadores:** Son capacitados en el control del personal a su cargo y por ello son los encargados de implementar los planes de evacuación y emergencia que se instrumenten para los CCV.

3. **Verificador/Foliador:** Ejecutará sus funciones de acuerdo a su manual de procedimientos, teniendo sumo cuidado en la identificación de las Actas de Escrutinio y Cómputo que identifique en su pantalla y en caso de dudas las consultará de inmediato con su Coordinador para que éste determine el proceso que se le dará a la misma.

4. **Capturista/Verificador:** Para poder llevar un control efectivo de la información que alimentan los Capturistas/Verificadores al sistema, se asignan claves personales de acceso a cada capturista, de tal forma que se puede consultar en cualquier momento quien ha capturado cada una de las actas. Como medida de seguridad se realiza una doble captura por cada documento por cualquier otra persona de tal forma que el sistema pueda validar que las dos capturas coinciden antes de subir la información a la Internet. Se cuenta con personal adicional al requerido para que en caso de inasistencia de algún capturista no afecte al proceso de la información.

5. **Verificador/Validador:** Como última medida de revisión de la captura se cuenta con Validadores que revisan todas las actas que se detecten con inconsistencias para que con la autorización de su Coordinador sean procesadas y subidas a Internet.

6. **Telefonistas:** Tienen a la mano los teléfonos de emergencia para reporte de contingencias, para en caso de cualquier eventualidad, pueden solicitar la ayuda de cualquiera de los servicios de emergencia:

   - ✓ Comisión Federal de Electricidad
   - ✓ Bomberos y Protección Civil
   - ✓ Cruz Roja
   - ✓ Telmex
   - ✓ Policía
   - ✓ Personal del PREP
   - ✓ Personal de Soporte Técnico del PREP
   - ✓ Instituto Estatal Electoral Hidalgo
   - ✓ CATD's

7. **Archivistas:** Tienen a la mano la información de todo el personal que labora en el PREP, nombres, domicilios y teléfonos para usarse de ser necesarios en cualquier contingencia.

8. **Organizadores:** Son los encargados de colocar la señalética de todas las áreas del PREP, tanto de servicios como las rutas de evacuación y salidas de Emergencia. En igual forma tienen a la mano botiquines de emergencia para cualquier eventualidad en el personal. En caso de evacuación ayudan a su coordinación.

9. **Técnicos:** Es de suma importancia el Personal de Soporte Técnico, el cual solventa todo tipo de contingencias que se presenten en los CCV para atenderlas de inmediato.

   Su función adicional de los Técnicos, es la de permanecer durante los ejercicios, simulacros y durante la Jornada Electoral, en el área de Telefonía para que, en caso de recibir un reporte de contingencia técnica de los CATD, éste reporte sea atendido de forma inmediata vía telefónica. En caso de ser necesario, se coordinarán con los Comandos Técnicos para la atención de contingencias.

b) Equipamiento

Como parte de la seguridad requerida, los CCV cuentan con cámaras de vigilancia. Dichas cámaras graban la actividad registrada en las áreas de los CCV y el perímetro del inmueble, para que en caso de que se presente alguna anomalía, ésta quede registrada en video.

Dichas cámaras son observadas mediante un Sistema de Monitoreo al que tiene acceso el Técnico encargado y el Supervisor General del PREP, en el cual puede observarse la actividad en todas y cada uno de las áreas de los CCV en tiempo real.

El Programa de Resultados Electorales Preliminares, cuenta en todo momento en sus instalaciones de los CCV con equipamiento de respaldo y soporte para que en caso de fallas del equipamiento éste pueda ser reemplazado a la brevedad durante los ejercicios y simulacros del PREP.

Como medida de seguridad también en los CCV se cuenta con Plantas de Energía de capacidad suficiente para soportar el funcionamiento de la totalidad del equipo en caso de falla de la energía eléctrica provista por la Comisión Federal de Electricidad. La totalidad del equipamiento contará con reguladores de voltaje y UPS.

c) Telecomunicaciones

De la totalidad de los servicios instalados como:

1. **Líneas Telefónicas**

2. **Enlace ADSL**

3. **Enlace Vía Cable**

Se contemplan las siguientes medidas de seguridad:

1. **Líneas Telefónicas.** Se contemplan líneas telefónicas suficientes para que puedan soportar el tráfico de llamadas desde los CATD, contando con un promedio de 5 CATD por cada línea telefónica, en igual forma como medida emergente se tienen pares de telefonía de soporte que pueden usarse en caso de fallar alguno y como medida extra se tienen disponibles líneas de teléfonos celulares. Adicionalmente en caso de fallas en las líneas telefónicas se puede mantener la comunicación con los CATD mediante telefonía celular.

2. **Enlace ADSL.** Se cuenta con un Enlace ADSL de alta velocidad, para la conectividad con Internet. Como medida adicional de redundancia se cuenta por lo menos un Enlace Vía Cable.

3. **Enlace Vía Cable.** Se cuenta con una Conexión a Internet con la Compañía de Cable Local como medida emergente para que, en caso de falla en el Enlace ADSL, se supla con la Conexión Vía Cable.

D. Nube de Internet

a) Recursos Humanos

1. **Técnicos**: Se cuenta con personal de Soporte Técnico para el control de la publicación en la Nube de Internet, para en caso de detectar cualquier contingencia, los técnicos en conjunto la resuelvan de inmediato, por ende, cuentan con personal de respaldo.

b) Equipamiento

1. **Servidores:** Para proteger el funcionamiento continuo del Programa de Resultados Electorales Preliminares en su conjunto, se cuentan con Servidores Redundantes en sus distintas modalidades asegurando que, en caso de falla de alguno, el redundante entre en funcionamiento.

c) Telecomunicaciones

1. **Enlace ADSL.** Se cuenta con un Enlace ADSL de alta velocidad, para la conectividad con Internet. Como medida adicional de redundancia se contrata por lo menos un Enlace Vía Cable.

2. **Enlace Vía Cable.** Se cuenta con una Conexión a Internet con la Compañía de Cable Local como medida emergente para que, en caso de falla en el Enlace ADSL, se supla con la Conexión vía Cable.

Niveles de Impacto

Una vez identificado el riesgo y el procedimiento específico a utilizar, es importante conocer los tiempos promedios de respuesta una vez que se ha notificado la contingencia.

Dicha información se muestra en la tabla siguiente de acuerdo con el nivel e impacto del evento:

Nivel de Impacto	Centros de Acopio y Transmisión de Datos	Centros de Captura y Verificación	Servidores en la Nube de Internet
Alto	1 hora	30 minutos	1 hora
Medio	2 horas	1 hora	2 horas
Bajo	4 horas	4 horas	4 horas