

ANÁLISIS DE RIESGOS Y PLANES DE SEGURIDAD, CONTINUIDAD DE LA OPERACIÓN Y DE SIMULACROS DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES, PARA LAS ELECCIONES EXTRAORDINARIAS 2022 EN EL ESTADO DE OAXACA

PRESENTACIÓN.

El presente documento integra el análisis realizado para identificar los activos a proteger o evaluar, inherentes al Programa de Resultados Electorales Preliminares (PREP) que ha de implementar el Instituto Estatal Electoral y de Participación Ciudadana de Oaxaca (IEEPCO), durante las Elecciones Extraordinarias a verificarse el próximo domingo 27 de marzo del 2022, durante la cual habrán de elegirse dos concejalías en igual número de municipios en el Estado de Oaxaca.

Derivado de lo anterior, se presenta la evaluación de riesgos, lo que ha involucrado comparar el nivel de riesgo detectado con criterios establecidos en este documento.

Los resultados obtenidos, hacen posible el desarrollo de un Plan de Seguridad orientado a prevenir la ocurrencia de los riesgos identificados, a través de medidas específicas que involucran, identificar el conjunto de opciones que existen para tratar los riesgos y evaluarlas, así como preparar y ejecutar un plan de contingencia para su tratamiento.

Como consecuencia última, se ha generado un Plan de Continuidad encaminado a determinar las acciones que garanticen la ejecución de los procedimientos de acopio, digitalización, captura, verificación y publicación, en caso de que se suscite una situación adversa o de contingencia.

CONTENIDO.

I. FACTORES DE RIESGO²

II. ACTIVOS CRÍTICOS²

III. ÁREAS DE AMENAZA⁵

IV. IDENTIFICACIÓN DE RIESGOS⁶

V. ESTRATEGIA DE GESTIÓN DE RIESGOS.⁹

VII. PLAN DE SEGURIDAD¹²

VII. PLAN DE CONTINUIDAD Y CONTINGENCIAS¹⁵

VIII. PLAN DE EJERCICIOS Y SIMULACROS²¹

I. FACTORES DE RIESGO

Los criterios que se deberán tomar en cuenta para la valoración de los riesgos van de la mano con el impacto que el riesgo en su ocurrencia tiene en el desarrollo y funcionamiento del PREP. En su intensidad estará el grado de magnitud en el daño potencial que represente para el PREP y estos factores los valoraremos en:

- A. Riesgo Bajo.** - Los elementos a los que afecte no detendrán el funcionamiento del PREP, sin embargo, entorpecerán el desarrollo del mismo. Es importante al momento de determinar un Riesgo Bajo, el daño que en su ocurrencia repetitiva pueda, por sí misma, representar un entorpecimiento del desarrollo de otras actividades lo cual en cadena representaría un Riesgo Alto.
- B. Riesgo Medio.** - Cuando el nivel de afectación puede ser mediado con la utilización de una medida emergente sin afectar el desarrollo del PREP, será considerado que el elemento presenta un nivel de riesgo medio. Para los elementos definidos en este nivel será necesario que se instrumente paralelamente la medida contingente para su atención.
- C. Riesgo Alto.** - Los elementos que afecte este nivel de riesgo podrán poner en peligro la continuidad del PREP y deberán tener la mayor prioridad en su inmediata atención. A estos elementos se les deberá poner atención permanente e implementar un plan de contingencia para solventar los daños generados por el mismo.

La forma en como han de medirse estos factores de riesgo dependerá directamente de las consecuencias de los mismos y de que en su ocurrencia afecten a otros elementos codependientes.

Para la determinación del nivel de riesgo, se deberá tomar en cuenta el tiempo que pudiese detener -en su eventual aparición-, el funcionamiento del proyecto. En igual manera se medirán los tiempos para solventar la situación una vez presentada, incluyendo los recursos requeridos para su atención, ya sean humanos, financieros o materiales.

II. ACTIVOS CRÍTICOS

Los activos críticos del PREP son los elementos clave para el funcionamiento de este, se tipificarán de acuerdo a su naturaleza y se detallará en qué áreas de amenaza se localizan para su focalización y continuo monitoreo. Se determinaron tres tipos de activos críticos:

- A) Recursos Humanos**
- B) Equipamiento**
- C) Telecomunicaciones**

Cada uno de estos activos críticos se describen en detalle a continuación:

ACTIVOS CRÍTICOS			
EN EL ÁREA DE	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
CENTRO DE ACOPIO Y TRANSMISIÓN DE DATOS (CATD)	<p>Personas Acopiadoras: Recibirán los sobres con las Actas, verificará su contenido, detectará incidencias y entregará las actas a las personas Digitalizadoras y generarán la bitácora.</p> <p>Personas Digitalizadoras:</p>	<p>Módems ADSL: La red estará compuesta por enlaces ADSL proveídos por Telmex para la conexión con la red de Internet y la conexión se realizará mediante módems provistos por la misma.</p> <p>Cable Módems: En caso de no</p>	<p>Línea Telefónica: Se contratarán líneas telefónicas para el CATD si Telmex cuenta con facilidades, si no es posible se instalará telefonía Celular. El principal medio de comunicación con los CATD será la vía telefónica.</p>

ACTIVOS CRÍTICOS

EN EL ÁREA DE	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
	<p>Digitalizarán las actas verificando su correcta legibilidad. Esta digitalización puede realizarse desde la casilla con la aplicación móvil o desde el CATD con la misma aplicación.</p>	<p>existir facilidades de Telmex y exista la conexión a Internet con la compañía de Cable Local se usará este servicio.</p> <p>Módems 3G: Como medio contingente en todas las localidades donde se cuente con cobertura Celular, se empleará el Módem 3G de estos equipos para la transmisión de la información.</p> <p>Teléfonos: Se instalarán aparatos telefónicos en cada uno de los CATD para entablar comunicación diaria permanente con el CCV. En los CATD donde Telmex no pueda proveer el servicio se empleará telefonía Celular.</p> <p>Teléfonos Celulares: Para realizar la digitalización y transmitir las imágenes digitalizadas se emplearán equipos celulares en cada uno de los CATD y desde las casillas con el apoyo de los CAEs.</p> <p>Scanner: La digitalización de las imágenes de las actas de escrutinio y cómputo se realizará mediante la aplicación web móvil que permitan preparar la información para digitalizarla y transmitirlos al CCV.</p> <p>Regulador: La corriente eléctrica deberá estar regulada para proteger el equipo de cómputo y telecomunicaciones, para lo cual se deberá instalar un regulador de voltaje en cada CATD.</p> <p>Planta de Energía: En prevención de fallos en el suministro de la energía eléctrica provista por CFE, en cada uno de los CATD se deberá instalar una Planta de Energía Portátil.</p>	<p>Conexión ADSL: Si en el Consejo Distrital Telmex cuenta con facilidades técnicas, se contratará el servicio de Internet ADSL como medio primario de transmisión de la información.</p> <p>Conexión vía Cable: Si no se encuentran facilidades de conexión vía ADSL se buscará la contratación de Internet con la Compañía de Cable Local y en caso de no contar con telefonía de Telmex igualmente se contratará con la Compañía de Cable Local.</p> <p>Conexión 3G: Como medio de respaldo en caso de contingencia en la localidad se verificará la disponibilidad de red 3G para en caso de requerirse usarla como medio de transmisión de información emergente.</p>
<p align="center">CENTRO DE CAPTURA Y VERIFICACIÓN (CCV)</p>	<p>La o el Supervisor General: Estará a cargo de la operación del personal y equipos, supervisará la capacitación y estará a cargo del CCV.</p> <p>Personas Coordinadoras: Coordinarán al personal a su cargo, darán seguimiento a la instalación del equipamiento y elaborarán informes.</p> <p>Persona Verificadora / Cotejadora: Verificarán la correcta identificación de las imágenes de las actas y</p>	<p>NTU (Network Termination Unit): Para el enlace principal de salida a la nube de Internet se cuenta con un servicio de banda ancha con las características necesarias para prever la demanda de información requerida por el CCV, esto se hace vía un enlace dedicado de alta velocidad.</p> <p>Módem ADSL: Se contratarán servicios de internet con Telmex con el mayor ancho de banda disponible para ser usados</p>	<p>Líneas Telefónicas: Se cuenta con líneas telefónicas suficientes para establecer comunicación diaria con el CATD.</p> <p>Internet Dedicado: Se cuenta con un enlace dedicado de Internet de Alta Velocidad (Clear Channel) el cual provee el suficiente ancho de banda para abastecer los requerimientos del CCV.</p> <p>Conexión ADSL: Se cuenta con conexiones adicionales a</p>

ACTIVOS CRÍTICOS

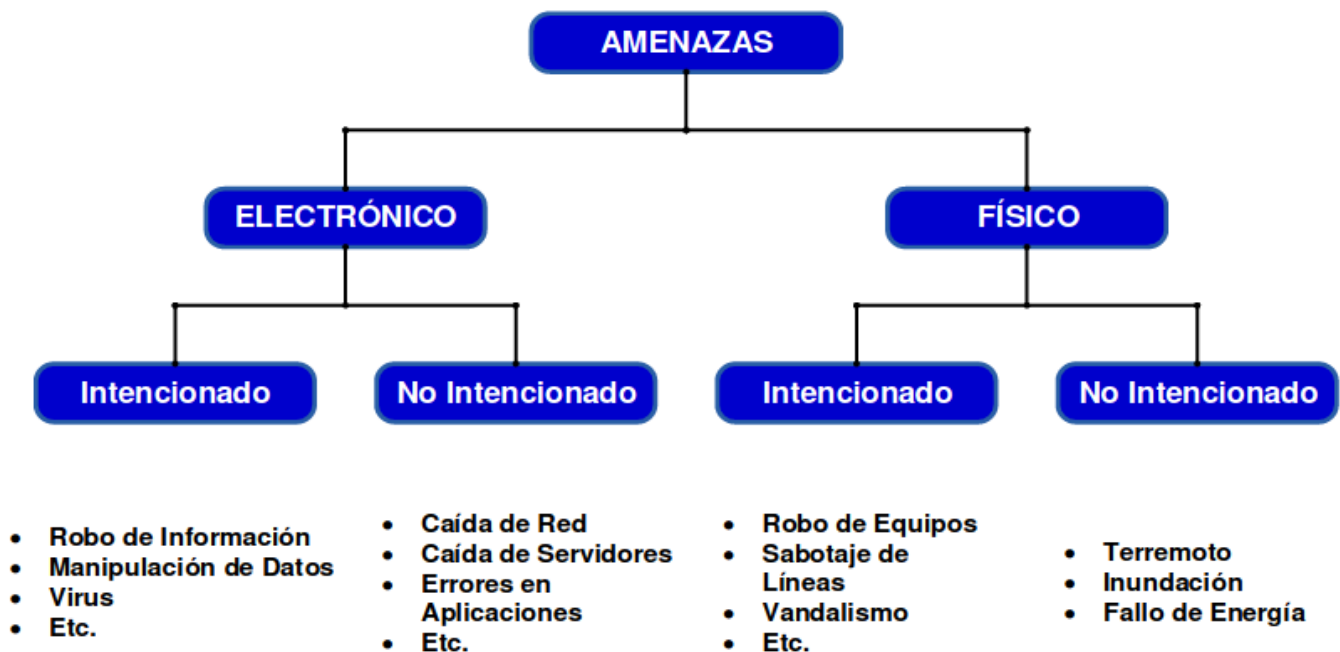
EN EL ÁREA DE	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
	<p>revisará inconsistencias.</p> <p>Personas Capturistas: Revisarán los votos obtenidos para los partidos y candidatos y los capturará en el sistema.</p> <p>Persona Verificadora / Validadora: Verificarán la información capturada de las imágenes de las actas, corregirá y procesará inconsistencias.</p> <p>Personas Telefonistas: Harán el pase de lista de los responsables del PREP en el CATD, darán las instrucciones de arranque, verificarán el avance de sus CATD y canalizará llamadas a las o los técnicos y a la o al Supervisor General.</p> <p>Personas Archivistas: Estarán a cargo de los expedientes del personal y el soporte documental generado en los ejercicios.</p> <p>Personas Organizadoras: Recibirán y generarán toda la información requerida en el PREP, elaborarán la Memoria del PREP.</p> <p>Personal Técnico: Realizarán la instalación de los CATD y CCV, darán soporte al funcionamiento de la totalidad del Equipamiento.</p>	<p>como segundo enlace emergente para lo cual se emplearán los módems apropiados.</p> <p>Ruteadores: En caso de requerirse se emplearán para controlar el tráfico de la conexión con la nube de internet podrá hacerse uso de Ruteadores adecuados al tipo de conexión usada para este propósito.</p> <p>Switches: Para establecer la red local de datos, esta será controlada mediante los switches requeridos para enlazar todos los equipos por áreas a la red local.</p> <p>Equipos de Cómputo: Se instalarán computadoras para todas las áreas del CCV tanto para la captura de las actas de escrutinio y cómputo, como para el monitoreo de los sistemas.</p> <p>Ups (Uninterruptible power supply): Como primera medida contingente de fallo de energía, se instalarán fuentes de poder ininterrumpida a los cuales se conectarán todos los equipos de cómputo y telecomunicaciones de la red, asegurando su funcionamiento en caso de falla en el suministro de energía por parte de CFE.</p> <p>Reguladores: Con el propósito de proporcionar un suministro de voltaje estable al equipamiento de cómputo y telecomunicaciones se instalarán reguladores de voltaje a la totalidad de estos equipos.</p> <p>Cañones o Pantallas de Proyección: Se montarán cañones o pantallas de Proyección en el CCV para monitorear el avance del proceso electoral y como medio de transparencia para los representantes de los partidos políticos acreditados ante el PREP.</p> <p>Plantas de Energía: Se contará con plantas de energía auxiliar como segunda medida emergente para usarse en casos de fallo de la energía principal proveniente de la CFE.</p>	<p>Internet mediante servicios ADSL los cuales proveen el medio de respaldo requerido para los volúmenes de transmisión de información necesarios para el CATD, estos serán el segundo medio de contingencia redundante para envío de información.</p>

ACTIVOS CRÍTICOS			
EN EL ÁREA DE	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
NUBE DE INTERNET	<p>Personal Técnico: Deberá contarse con personal técnico especializado en telecomunicaciones quienes estarán a cargo de monitorear permanentemente las telecomunicaciones y los enlaces a la nube de Internet, asegurando la operación continua del servicio.</p>	<p>Servidores: Es importante que los servidores empleados para este proyecto cuenten con la capacidad requerida de acuerdo con el servicio que prestarán.</p> <p>Firewalls: La implementación de Firewalls será de importancia crítica para el aseguramiento de la red, evitando la intrusión de agentes externos a la red local y a la red estatal.</p>	<p>Clear Channel: La única forma de asegurar el ancho de banda requerido para la Recepción / transmisión de información es mediante el uso de enlaces Clear Channel, estos enlaces son conexiones directas al Back Bone de Internet, sin compartir el canal con otros usuarios, asegurando con ello la continuidad del servicio y al ser simétricos no hay detrimento en los anchos de banda puesto que brindan un ancho de banda asegurado.</p>

III. ÁREAS DE AMENAZA

De acuerdo con el análisis del PREP, se detectaron tres áreas de amenaza que deberán ser consideradas durante todo el presente análisis:

Identificación de Riesgos



A. Centros de Acopio y Transmisión de Datos

En cada uno de los Consejos Distritales Electorales definidos por el Instituto Estatal Electoral y de Participación Ciudadana de Oaxaca, se instalará un CATD, el cual se Acopiarán, y Digitalizarán las Actas de Escrutinio y Cómputo de la elección, estos a su vez transmitirán la información de manera electrónica al CCV del PREP para su proceso y publicación en la nube de Internet.

B. Centro de Captura y Verificación

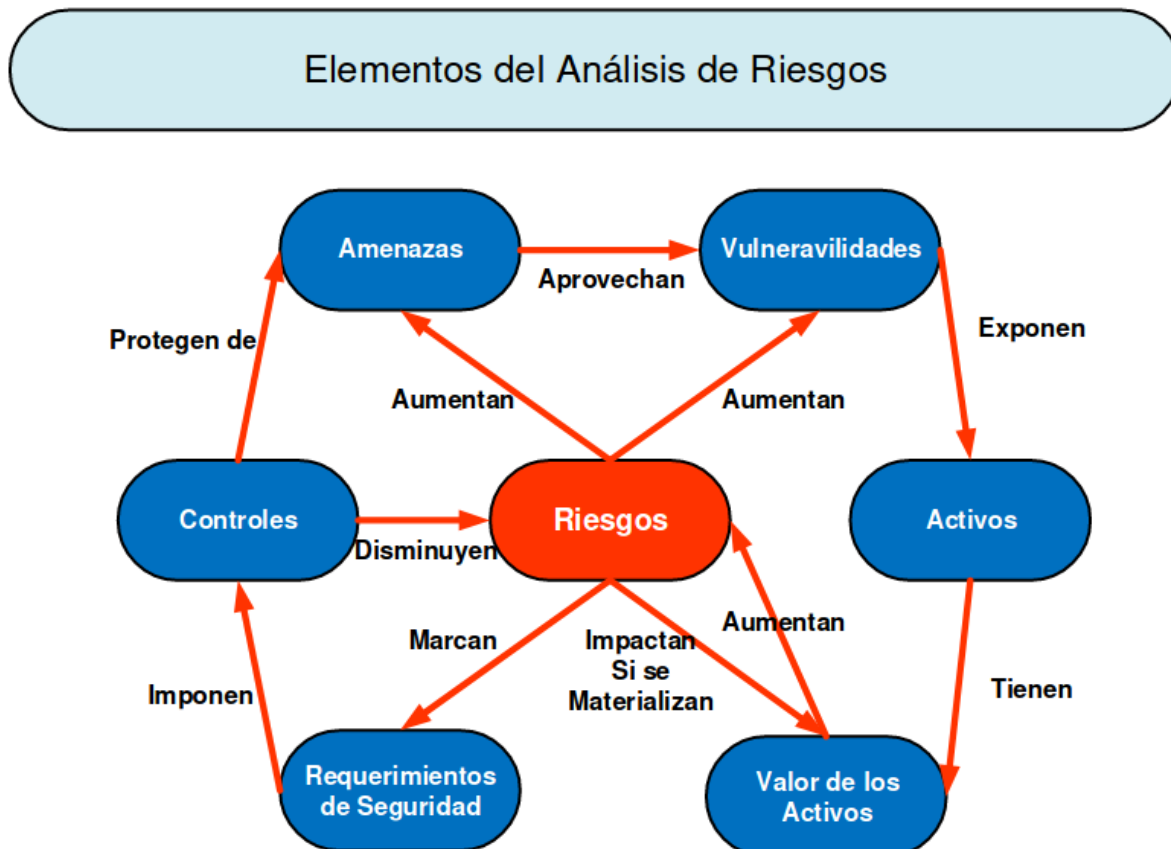
En la Capital del Estado se instalará un CCV el cual será el ente neural del PREP y sus funciones serán las de recibir las imágenes de las actas procedentes del CATD, capturar la información contenida en las mismas, procesar y publicar el resultado en Internet, incluyendo tanto las imágenes de las actas de escrutinio y cómputo como los datos capturados de estas.

C. Nube de Internet

Tanto la transmisión de los resultados desde el CATD al CCV, como la publicación de los resultados del PREP será a través del uso de Servidores en la Nube de Internet. Es por ello que los mecanismos de transmisión desde el CATD al CCV, como de la publicación del proceso de los datos desde el CATD en la Nube de Internet, deberá incluir mecanismos de encriptación de la información de alta seguridad, los cuales garantizarán la confiabilidad de los datos recibidos y transmitidos de un punto a otro. Así mismo se contarán con mecanismos de Firewall internos que garanticen la no intromisión de intrusos en la red local y la red del PREP.

IV. IDENTIFICACIÓN DE RIESGOS

Para la identificación de los riesgos potenciales del proyecto, tomaremos en cuenta los activos críticos previamente identificados de acuerdo a su área de amenaza y los elementos que le componen. Así mismo detallaremos su nivel de riesgo en cuanto al grado de afectación en el desarrollo del PREP.



RIESGOS			
EN LAS ÁREAS DE	HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
CENTRO DE ACOPIO Y TRANSMISIÓN DE DATOS (CATD)	<p>Personas Acopiadoras: Se tipificó un Riesgo de nivel Bajo puesto que, en caso de ausentarse, sus funciones podrán ser realizadas por la persona Digitalizadora.</p> <p>Personas Digitalizadoras: En caso de que no se presentara, la ausencia de la o el Digitalizador representa un nivel de Riesgo Bajo, ya que sus funciones podrán ser realizadas por la persona Acopiadora.</p>	<p>Módems ADSL: Si en el Consejo la conexión a la red de Internet es mediante Telmex, el módem ADSL será el medio primario de envío de información, de ahí que su función es de Medio Riesgo.</p> <p>Cable Módem: Si no se cuenta con servicio ADSL para conexión a Internet, en caso de existir este servicio, será el medio primario de envío de información por lo que su función es de Medio Riesgo.</p> <p>Módems 3G: Al ser un medio secundario y redundante su nivel de Riesgo es Medio en cuanto al desempeño de la Red.</p> <p>Teléfonos: Ya que existe cobertura de telefonía Celular en todas las cabeceras distritales el nivel de Riesgo se tipifica en Bajo.</p> <p>Teléfonos Celulares: La transmisión de la información digitalizada del contenido de las actas de escrutinio y cómputo a la nube de Internet estará controlada por un equipo celular en el CATD y se justifica como de Alto Riesgo.</p> <p>Scanner: Conjuntamente al equipo celular, el Scanner representa un elemento crucial en la digitalización de la información, por ello su riesgo es Alto.</p> <p>Regulador: La buena alimentación de Voltaje eléctrico es indispensable para el funcionamiento del CATD y los reguladores representan un activo crítico con Bajo Riesgo puesto que se deberán tener suficientes de respaldo.</p> <p>Planta de Energía: Dada la frecuencia de recortes en el suministro de energía en el interior del estado, las plantas de energía tienen una prioridad de Alto Riesgo.</p>	<p>Línea Telefónica: Las líneas telefónicas serán los principales medios de que se emplearán para establecer la comunicación entre el CATD y el CCV, más aún si en el sitio se empleara enlace ADSL, el buen funcionamiento de la línea es crítico para portar esta señal ADSL, es por ello que el nivel de Riesgo para las mismas es Medio.</p> <p>Conexión ADSL: Si existen facilidades de Telmex, el principal medio de transmisión de información será la señal ADSL, de ahí que se dará prioridad al buen funcionamiento de la misma elevando con ello el Riesgo a Medio, salvo de no existir cobertura 3G se pudiera considerar Alto.</p> <p>Conexión vía Cable: Si algún distrito no cuenta con infraestructura de Telmex se buscará la disponibilidad de señal de Internet Vía la Compañía de Cable Local como medio primario de transmisión de información siendo un nivel de Riesgo Medio.</p> <p>Conexión 3G: Si en el distrito se tiene cobertura celular se tendrá una conexión vía Banda Ancha Móvil como medio alternativo redundante para transmisión de información más al ser redundante no resulta crítico y su nivel de Riesgo será Bajo.</p>

RIESGOS			
EN LAS ÁREAS DE	HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
CENTRO DE CAPTURA Y VERIFICACIÓN (CCV)	<p>Persona Supervisora General: Este puesto conlleva un nivel de Riesgo Alto, ya que esta persona tiene a su cargo el funcionamiento del Centro de Captura y Verificación.</p> <p>Personas Coordinadoras: Se deberá contar con una persona Coordinadora para cada 8 a 12 personas por área de trabajo, dada su función de Coordinación y la toma de decisiones que se le encomendarán el nivel de Riesgo se tomará como Medio.</p> <p>Persona Verificadora / Cotejadora: Ya que esta función en primera instancia es quien recibe e identifica las actas su nivel de riesgo es Medio.</p> <p>Personas Capturistas: La confiabilidad de la información depende del personal de Captura, de ahí que el nivel de Riesgo para los mismos es Bajo y se implementará un mecanismo para asegurar el buen proceso de la información alimentada por ellos.</p> <p>Persona Verificadora / Validadora: Este es el filtro final antes de la publicación de la información, por lo que su nivel de riesgo es Medio.</p> <p>Personas Telefonistas: Puesto que la función informativa que desempeñan no es en ninguna situación crítica para el proyecto, se les da un nivel de Riesgo Bajo.</p> <p>Personas Archivistas: La actividad administrativa que desarrollan los Archivistas, es de bajo impacto en el desempeño que requiere el proyecto, por ello su nivel de Riesgo es Bajo.</p> <p>Personas Organizadoras: Dadas sus funciones netamente administrativas la falta de alguno no tendría repercusiones serias en el proyecto, por ello su nivel de Riesgo es Bajo.</p> <p>Personal Técnico: Para el caso de las o los Técnicos el nivel de Riesgo se tipificó</p>	<p>NTU: El principal equipo de comunicación para establecer el enlace de alta velocidad son los NTU, su prioridad de Riesgo es Alto.</p> <p>Módem ADSL: La segunda opción de enlace será mediante el uso de diversos enlaces ADSL por ello su nivel de Riesgo es Medio.</p> <p>Ruteadores: Para poder controlar el tráfico de la red es crítico el uso de ruteadores y por ello su nivel de Riesgo es Alto.</p> <p>Switches: Se requieren diversos tipos de Switches para conformar la red Local, por ello su prioridad de Riesgo es Bajo.</p> <p>Equipos de Cómputo: Los equipos de Cómputo son el medio principal de Alimentación de información al sistema y su Riesgo es Bajo dado que habrá suficientes equipos de respaldo.</p> <p>Up's: El uso de las fuentes de poder ininterrumpido no es vital para evitar cortes de alimentación en el voltaje, ya que se contará con plantas de energía auxiliar, por ello su nivel de Riesgo es Bajo.</p> <p>Reguladores: Al igual que los Up's los reguladores son de nivel de Riesgo Bajo para el buen funcionamiento de la red eléctrica, ya que deberá haber suficiente equipo de respaldo.</p> <p>Cañones de Proyección o Pantallas: El uso de los cañones o pantallas para la exhibición interna de los resultados es de Riesgo Bajo, ya que la misma información estará visible en cualquier equipo conectado a Internet.</p> <p>Plantas de Energía: Es de suma importancia asegurar el suministro continuo de la energía eléctrica de ahí que las Plantas de Energía son de nivel Alto de Riesgo.</p>	<p>Línea Telefónica: Desde el CCV se llevará el monitoreo del Centros de Acopio y Transmisión de Datos, esto realizará por vía telefónica, es por ello por lo que las líneas telefónicas son vitales para este propósito siendo de Medio Riesgo su disponibilidad.</p> <p>Internet Dedicado: La vía primaria de transmisión y recepción de información será mediante un enlace dedicado de Internet de Alta Velocidad, el cual deberá funcionar permanentemente desde su instalación hasta el día posterior a la Jornada Electoral, su prioridad de riesgo es Alto.</p> <p>Conexión ADSL: Como un tercer medio redundante se contratarán enlaces ADSL para en caso fortuito de fallo en el enlace primario y fallo en el enlace secundario se active la transmisión y recepción de información mediante ADSL, los cuales deberán funcionar permanentemente desde su instalación hasta el día posterior a la Jornada Electoral, su prioridad de riesgo es por lo mismo Alto.</p>

RIESGOS			
EN LAS ÁREAS DE	HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
	como Medio, ya que en caso de ausencia o mal desempeño de estos serían suplidos por alguna persona de reserva.		
NUBE DE INTERNET	Personal Técnico: Este personal, dada su función será Crítico para el desarrollo del proyecto y por ende el nivel de Riesgo que representa es Alto.	Servidores: Todos los servidores empleados para el proceso son intrínsecamente indispensables para el funcionamiento del PREP por eso su nivel de Riesgo es Alto. Firewalls: La seguridad de la red estará administrada primariamente a partir de los Firewalls que se implementen en la misma, de ahí que el nivel de Riesgo en la implementación de los Firewalls es Alto.	Enlace Dedicado de Internet: La conexión principal con la Nube de Internet será primariamente con un Enlace Dedicado de Internet, el cual deberá ser permanentemente monitoreado por personal técnico especializado y su prioridad de riesgo es Alto.

V. ESTRATEGIA DE GESTIÓN DE RIESGOS.

Con el propósito de dictar medidas tendientes a la Gestión de los Niveles de Riesgos identificados, se elaborará tanto un Plan de Seguridad tendiente a la prevención de los mismos, como un Plan de Continuidad que será implementado en caso de ocurrir cualquier contingencia.



GESTIÓN DE RIESGOS			
EN EL ÁREA DE	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
CENTRO DE ACOPIO Y TRANSMISIÓN DE DATOS	<p>Personas Acopiadoras: De no presentarse durante la Jornada, la persona Digitalizadora podrá mitigar su ausencia asumiendo sus responsabilidades.</p> <p>Personas Digitalizadoras: En caso de que no se presentara, se podrá mitigar su ausencia, ya que sus funciones podrán ser realizadas por la persona Acopiadora.</p>	<p>Módems ADSL: Previendo la falla en alguno de estos equipos, se transferirá al proveedor la posible falla de alguno, solicitando con anticipación equipos de respaldo.</p> <p>Cable Módem: Previendo la falla en alguno de estos equipos, se transferirá al proveedor la posible falla de alguno, solicitando su reposición inmediata.</p> <p>Módems 3G: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.</p> <p>Teléfonos: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia. Adicionalmente se contará con equipos celulares de respaldo.</p> <p>Teléfonos Celulares: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.</p> <p>Regulador: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.</p> <p>Planta de Energía: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.</p>	<p>Línea Telefónica: De presentarse fallas en las líneas se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usarán líneas celulares.</p> <p>Conexión ADSL: De presentarse fallas en los servicios, se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usarán conexiones 3G.</p> <p>Conexión vía Cable: De presentarse fallas en los servicios se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usarán conexiones 3G.</p> <p>Conexión 3G: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.</p>
CENTRO DE CAPTURA Y VERIFICACIÓN (CCV)	<p>La o el Supervisor General: Para poder mitigar su ausencia, se deberá prever dicha contingencia con la capacitación de las personas Coordinadoras para asumir sus funciones.</p> <p>Personas Coordinadoras: Se deberán contar con suficientes personas Coordinadoras para que la ausencia de uno pueda ser mitigada con la ayuda de un similar.</p> <p>Persona Verificadora / Cotejadora: Se mitigará la ausencia de alguno capacitando adecuadamente a personas Capturistas en esta función.</p> <p>Personas Capturistas: Previendo la contingencia de ausencia de personas Capturistas se deberá contar con personal</p>	<p>NTU: De presentarse fallas en este equipamiento se transferirá al proveedor el reporte para su sustitución inmediata.</p> <p>Cable Módem: Previendo la falla en alguno de estos equipos, se transferirá al proveedor la posible falla de alguno, solicitando su reposición inmediata.</p> <p>Módem ADSL: Previendo la falla en alguno de estos equipos, se transferirá al proveedor la posible falla de alguno, solicitando con anticipación equipos de respaldo.</p> <p>Ruteadores: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.</p> <p>Switches: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.</p> <p>Equipos de Cómputo: En caso de falla en alguno de estos equipos, se mitigará</p>	<p>Línea Telefónica: De presentarse fallas en las líneas se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usarán líneas celulares.</p> <p>Internet Dedicado: De presentarse fallas en el servicio se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usará la Conexión vía Cable o la Conexión ADSL.</p> <p>Conexión ADSL: De presentarse fallas en el servicio se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se emplearán más de un servicio de este tipo.</p>

GESTIÓN DE RIESGOS

EN EL ÁREA DE	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
	<p>adicional al requerido que mitigará como comodines a las personas Verificadoras y Capturistas.</p> <p>Persona Verificadora / Validadora: Se mitigará la ausencia de alguno capacitando adecuadamente a personas Capturistas en esta función.</p> <p>Personas Telefonistas: En caso de ocurrir la inasistencia de alguna, se mitigará con el auxilio de la persona Coordinadora.</p> <p>Personas Archivistas: En caso de no contar con alguna o algún archivista, dicha inasistencia podrá ser mitigable con la asistencia de las o los Organizadores.</p> <p>Personas Organizadoras: Si no se contara con alguna de las personas Organizadoras, se mitigará su falta con el auxilio de una persona Archivista.</p> <p>Personal Técnico: Dado lo crítico de sus funciones, las o los técnicos serán todos capacitados en las mismas funciones para que cualquiera de ellos pueda realizar la funciones de los demás mitigando esta posible contingencia de ausencia en alguno.</p>	<p>contando con equipo suficiente de respaldo para esta contingencia.</p> <p>Ups: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.</p> <p>Reguladores: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.</p> <p>Cañones de Proyección o Pantallas: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.</p> <p>Plantas de Energía: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.</p>	
NUBE DE INTERNET	<p>Personal Técnico: Previendo la ausencia de alguna de estas personas, se mitigará con la presencia de las o los técnicos de reserva, contando todos con el mismo nivel de experiencia requerido.</p>	<p>Servidores: Dado que los servidores se hallan en la nube de Internet se transferirá al proveedor la contingencia de falla en alguno, pero se contará adicionalmente con servidores espejo para esta contingencia.</p> <p>Firewalls: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.</p>	<p>Enlace Dedicado de Internet: De presentarse fallas en el servicio se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usará la Conexión vía Cable o la Conexión ADSL</p>

VII. PLAN DE SEGURIDAD

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.

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

- A. Centros de Acopio y Transmisión de Datos (CATD)
- B. Centro de Captura y Verificación (CCV)
- C. Nube de Internet

A continuación, se describen medidas específicas para cada una de estas tres áreas:

PLAN DE SEGURIDAD			
PARA EL ÁREA DEL	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
<p>CENTRO DE ACOPIO Y TRANSMISIÓN DE DATOS (CATD) Primeramente, para resolver cualquier tipo de contingencia que pudiese presentarse en los municipios con elección extraordinaria en el Estado de Oaxaca, es indispensable se cuente con un equipo de Personal de Soporte Técnico Especializado el cual durante la Jornada Electoral estará situado en las zonas de cobertura, en las cuales dichos Técnicos puedan presentarse en Sitio en un tiempo máximo de unos 30 minutos para solventar cualquier tipo de contingencia que se presente en los siguientes Activos Críticos:</p> <ul style="list-style-type: none"> a) Recursos Humanos b) Equipamiento c) Telecomunicaciones <p>Este personal deberá contar con vehículo y chofer, y en el vehículo deberá cargar equipo y material de soporte igual a los empleados en el CATD, para que en caso de que sea necesario, puedan reemplazar cualquier equipo que pudiera fallar durante el desarrollo de la Jornada Electoral en el CADT del distrito con atracción de la elección municipal, referido.</p> <p>Dicho personal contará con teléfono celular, mapa de localización del 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 la persona Responsable del PREP en el CATD, así como de los teléfonos de la o del Presidente y de la o el Secretario del mismo.</p>	<p>Una de las medidas de seguridad requeridas por el PREP es que, a partir del funcionamiento de este, se cuente con personal de Seguridad proporcionado por el Consejo Distrital Electoral que no sólo vigile el área del PREP, sino sean el encargado de la vigilancia en todo el Consejo Distrital Electoral.</p> <p>Como medida de seguridad, en el Consejo Distrital Electoral se deberá restringir el acceso al área destinada para el CATD, y sólo podrán estar cerca del equipo de digitalización y transmisión de información, personal acreditado del PREP. Esto es, durante la capacitación, todo el personal del PREP deberá portar su credencial de identificación del PREP y en caso de no contar con ella se le negará el acceso.</p> <p>Todo el Personal de Soporte Técnico del PREP igualmente deberá portar su credencial de identificación con la leyenda de Soporte Técnico, sin la cual se les negará acceso al CATD.</p> <p>Sin estas medidas de identificación se le negará el acceso a cualquier persona que se presente al CATD.</p> <p>Personas Acopiadoras: Igualmente se deberá contar con un plan emergente para que, en caso de no asistir esta persona, la persona Digitalizadora o la persona Coordinadora pueda suplir la ausencia del mismo.</p> <p>Personas Digitalizadoras: En caso de no asistir deberán contar con una persona que pueda suplir sus funciones pudiendo ser una persona Acopiadora o la persona Supervisora.</p>	<p>El Programa de Resultados Electorales Preliminares, deberá contar en todo momento en sus instalaciones del CCV con equipamiento de respaldo y soporte para que en caso de fallas del equipamiento en cualquier CATD se pueda enviar Personal de Soporte Técnico que reemplazará 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 y simulacros del PREP.</p> <p>Como medida de seguridad a los CATD, se enviará una Planta de Energía Portátil de capacidad suficiente para soportar el funcionamiento de la totalidad del equipo a instalarse en el CATD, más un foco que proveerá de iluminación al CATD Remoto en caso de falla de energía eléctrica, provista por la Comisión Federal de Electricidad.</p>	<p>En igual forma como medida de protección para el equipamiento electrónico y de Telecomunicaciones que se usará en el CATD, se les deberá instalar un Regulador de Voltaje que protegerá al equipo del PREP contra posibles variaciones de voltaje.</p> <p>Las telecomunicaciones deberán contemplar por lo menos un medio de redundancia, para que en caso de contingencia de fallo en el medio de transmisión primario entre en forma automática en funcionamiento el medio redundante, asegurando con ello la transmisión continua de la información.</p> <p>En caso de cualquier contingencia que se presente en los CATD, ésta deberá ser reportada de inmediato al CCV del PREP para que se implementen las medidas emergentes necesarias.</p> <p>Igualmente se deberá implementar una bitácora que dé seguimiento a todos los reportes de fallas tanto 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.</p>

PLAN DE SEGURIDAD

PARA EL ÁREA DEL	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
<p>En todo momento el Personal de Soporte Técnico mantendrá comunicación continua con el CCV y deberá estar listo para que en cualquier momento que se le requiera, pueda trasladarse al sitio que le sea designado desde el CCV.</p> <p>Durante los ejercicios y simulacros del PREP, el Personal de Soporte Técnico se encontrará residente en las instalaciones del CCV a fin de atender los reportes de asistencia técnica que se presenten durante este periodo del PREP.</p>			
<p>CENTRO DE CAPTURA Y VERIFICACIÓN (CCV) Al igual que el CATD, en el CCV se deberán contemplar medidas de seguridad en los siguientes Activos Críticos:</p> <ul style="list-style-type: none"> a) Recursos Humanos b) Equipamiento c) Telecomunicaciones <p>Una de las medidas de seguridad requeridas por el PREP, es que a partir de la instalación del CCV, se cuente con personal de Seguridad proporcionado por el Instituto Estatal Electoral y de Participación Ciudadana de Oaxaca, que no sólo vigile el área del interior del PREP, sino que hagan vigilancia perimetral. Además de que el CCV se ubica en la ciudad de Oaxaca y muy alejado del de los municipios de la elección, proporciona ventaja en la seguridad del CCV.</p> <p>Como medida de seguridad, en el CCV se deberá restringir el acceso a cualquier persona ajena al PREP, sólo podrán ingresar al mismo personal acreditado del PREP. Esto es, durante la capacitación a todo el personal del PREP se le proporcionará credencial de identificación del PREP y en caso de no contar con ella se le negará el acceso.</p> <p>Para solventar cualquier tipo de contingencia que pudiese presentarse en el CCV será necesario implementar las siguientes medidas de seguridad:</p>	<p>Persona Supervisora General: Instrumentará un plan de evacuación y realizará simulacros, verificará que la señalética se encuentre debidamente localizada, incluyendo extintores, salidas de emergencia, etc. Verificará con las personas responsables de seguridad del inmueble que sólo personal autorizado tenga acceso al mismo, nombrará una o un técnico responsable del monitoreo de las cámaras de video vigilancia locales y remotas. Asegurará 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.</p> <p>Personas Coordinadoras: Serán capacitadas en el control del personal a su cargo y por ello serán las personas encargadas de implementar los planes de evacuación y emergencia que se instrumenten para el CCV.</p> <p>Persona Verificadora: 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 la persona Coordinadora para que éste determine el proceso que se le dará a la misma.</p> <p>Personas Capturistas: Para poder llevar un control efectivo de la información que alimentan</p>	<p>Como parte de la seguridad requerida, el CCV deberá contar con cámaras de vigilancia. Dichas cámaras deberán grabar en tiempo real las 24 horas del día toda la actividad registrada en las áreas del CCV para que en caso de que se presente alguna anomalía, ésta quede registrada en video.</p> <p>Dichas cámaras serán observadas mediante un Sistema de Monitoreo al que tendrá acceso la persona Supervisora General del PREP, en el cual podrá observarse la actividad en todas y cada uno de las áreas del CATD Central en tiempo real.</p> <p>El Programa de Resultados Electorales Preliminares, deberá contar en todo momento en sus instalaciones del CCV con equipamiento de respaldo y soporte para que en caso de fallas del equipamiento éste pueda ser reemplazado de inmediato durante los ejercicios y simulacros del PREP.</p> <p>Como medida de seguridad también en el CCV se deberá contar con Plantas de Energía Portátil 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.</p>	<p>De la totalidad de los servicios instalados como:</p> <ol style="list-style-type: none"> 1. Líneas Telefónicas 2. Internet Dedicado 3. Conexión ADSL <p>Se deberán contemplar las siguientes medidas de seguridad:</p> <p>Líneas Telefónicas: Se deberán contemplar 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 deberán tener pares de soporte que puedan usarse en caso de fallar alguno y como medida extra se tendrán disponibles líneas de teléfonos celulares.</p> <p>Internet Dedicado: En caso de presentarse falla con el Internet Dedicado se deberá contar con servicio de Internet redundante al que se podrá switchear de forma automática para la recepción y transmisión de la información de forma continua e ininterrumpida.</p> <p>Conexión ADSL: Si llegasen a fallar el Internet Dedicado, el Internet vía Cable y en su última instancia el Internet ADSL se podrán contratar múltiples servicios ADSL por diferentes vías, para que en caso de fallo en uno se utilice otro.</p>

PLAN DE SEGURIDAD

PARA EL ÁREA DEL	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
	<p>las personas capturistas al sistema, se asignarán claves personales de acceso a cada persona capturista, de tal forma que se podrá consultar en cualquier momento quien ha capturado cada una de las actas. Como medida de seguridad se realizará 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 deberá contar con personal adicional al requerido para que en caso de inasistencia de algún capturista no afecte al proceso de la información.</p> <p>Persona Validadora: Como última medida de revisión de la captura se contará con personas Validadoras que revisarán todas las actas que se detecten con inconsistencias para que con la autorización de su persona Coordinadora sean procesadas y subidas a Internet.</p> <p>Personas Telefonistas: Tendrán a la mano los teléfonos de emergencia para contingencias:</p> <ul style="list-style-type: none"> • Comisión Federal de Electricidad • Bomberos y Protección Civil • Cruz Roja • Telmex • Policía • Personal del PREP • Personal de Soporte Técnico del PREP • Instituto Estatal Electoral y de Participación Ciudadana de Oaxaca • CATD's <p>Personas Archivistas: Tendrán a la mano la información de todo el personal que labore en el PREP, nombres, domicilios y teléfonos para usarse de ser necesarios en cualquier contingencia.</p> <p>Personas Organizadoras: Las personas organizadoras serán encargados de señalar todas las áreas del PREP, tanto de servicios como las rutas de evacuación y salidas de Emergencia. En igual forma tendrán a la mano botiquines de emergencia para cualquier eventualidad en el personal.</p> <p>Personal Técnico: Es de suma importancia contar con Personal de Soporte Técnico, el cual deberá solventar todo tipo de contingencias que se presenten en el CCV para</p>		

PLAN DE SEGURIDAD			
PARA EL ÁREA DEL	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
	atenderlas de inmediato. Su función adicional será la de permanecer durante los simulacros y ejercicios diarios 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.		
NUBE DE INTERNET	Personal Técnico: Se deberá contar con personal de Soporte Técnico para el control de la publicación en la Nube de Internet, para en caso de detectar cualquier contingencia, las o los técnicos en conjunto la resuelvan de inmediato, por ende, deberán contar con personal de respaldo,	Servidores: Para proteger el funcionamiento continuo del Programa de Resultados Electorales Preliminares en su conjunto, se deberán contar con Servidores Redundantes en todas sus modalidades asegurando que, en caso de falla de alguno, el redundante entre en funcionamiento de forma automática. Firewalls: Se deberán contar con Firewalls que permitan la no intromisión de información ajena a la propia red del PREP, dichos Firewalls habrán de implementarse tanto en los CATD como en el CCV.	Enlace Dedicado de Internet: La vía primaria de transmisión y recepción de información deberá ser mediante un Enlace Dedicado de Internet, pero como medidas de seguridad será imperante monitorear permanentemente el enlace por personal técnico especializado de la empresa proveedora del servicio, realizando pruebas continuas de esfuerzo y saturación para evaluar el desempeño del mismo. Independiente a el monitoreo permanente se deberán contemplar enlaces redundantes que puedan entrar en funcionamiento automático en caso de fallas en el enlace primario.

VII. PLAN DE CONTINUIDAD Y CONTINGENCIAS

El presente Plan de Continuidad, se ha desarrollado como consecuencia del Análisis de Riesgos, desarrollado para el Programa de Resultados Electorales Preliminares.

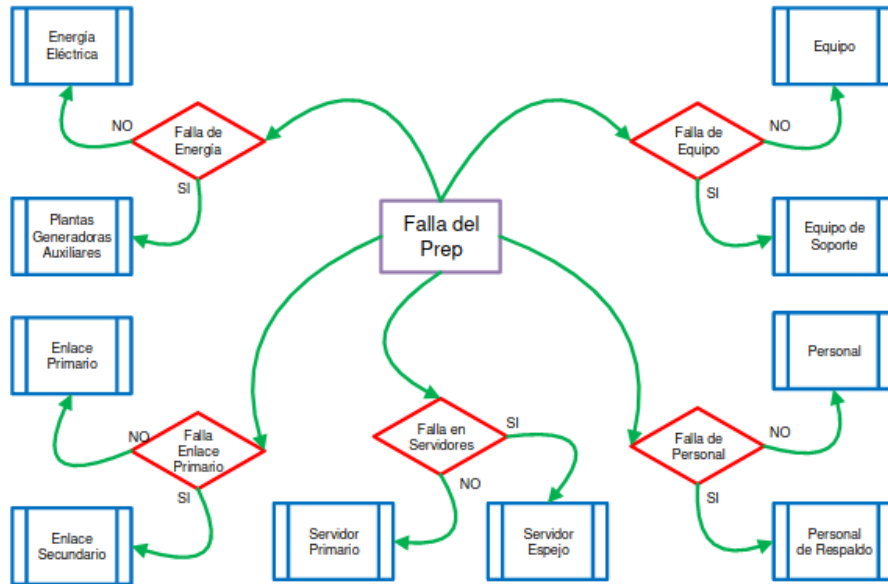
Una vez analizados los posibles factores de riesgo que podrían interferir en el funcionamiento del PREP, se determinaron las medidas de seguridad que habrán de implementarse para aceptar, mitigar, transferir o eliminar cada uno de los riesgos identificados que pudiesen entorpecer el funcionamiento del PREP; para ello se requiere la implementación de un Plan de Continuidad que definirá cuales son las acciones a implementar que garanticen la ejecución de los procesos de Acopio, Digitalización, Captura, Verificación y Publicación de los resultados del PREP, en caso de suscitarse alguna situación adversa o de contingencia, mismo que será parte de la capacitación al personal correspondiente en su implementación. Dicho plan deberá ser puesto en ejecución durante los ejercicios y simulacros.

Siguiendo la mecánica del Plan de Seguridad, dividiremos este Plan de Continuidad de acuerdo a las tres Áreas de Amenaza identificadas en el análisis de Riesgos:

- A. Centros de Acopio y Transmisión de Datos**
- B. Centro de Captura y Verificación**
- C. Nube de Internet**
- D. Técnicos de Informática**
- E. Coordinación con la Gerencia de Desastres Telmex**

A continuación, se describen las medidas específicas para cada una de estas tres áreas:

Esquema de Contingencia en Falla del Prep



PLAN DE CONTINUIDAD Y CONTINGENCIAS			
PARA LAS ÁREAS DEL	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
<p>CENTRO DE ACOPIO Y TRANSMISIÓN DE DATOS</p> <p>Las medidas a implementarse en este plan se avocan en los siguientes Activos Críticos:</p> <ul style="list-style-type: none"> a) Recursos Humanos b) Equipamiento c) Telecomunicaciones <p>En el CATD se llevarán a cabo los procesos de Acopio, Digitalización y Transmisión de las imágenes digitalizadas de las Actas de Escrutinio y Cómputo para la elección extraordinaria a llevarse a cabo en los municipios de San Santa Cruz Xoxocotlán y Pablo Villa de Mitla.</p>	<p>En caso de fallas en los Recursos Humanos, Equipamiento o Telecomunicaciones, se hará el reporte del mismo al CCV del PREP para que se ejecuten las siguientes medidas:</p> <p>A partir de las 17:00 horas del día de la Jornada Electoral, todo el personal del PREP de los municipios con elección extraordinaria se presentará a cumplir sus funciones en el CATD del Distrito correspondiente.</p> <p>Las personas telefonistas que operan en el CCV, harán el pase de lista a los CATD, si se detectan faltantes de personal, se realizarán las siguientes medidas:</p> <p>Persona Acopiadora: En caso de Inasistencia de la persona Acopiadora, se le instruirá a la persona Digitalizadora para que realice ambas funciones.</p> <p>Persona Digitalizadora: En caso de Inasistencia de la persona Digitalizadora, se le instruirá a la persona Acopiadora para que realice ambas funciones.</p> <p>En caso de Inasistencia de dos o más personas, se le instruirá al Personal de Soporte Técnico</p>	<p>En el momento que se reciba reporte o se detecte mal funcionamiento del equipamiento, de algún elemento del equipamiento o por la recepción de un reporte de fallas desde algún CATD, en primera instancia se atenderá la llamada por una o un técnico de guardia en el CCV quien remotamente tratará de darle solución a la falla.</p> <p>En caso de que la falla no pueda ser solucionada vía telefónica, se contactará al Personal de Soporte Técnico que corresponda a la Zona, y se le enterará de los pormenores del reporte, dándole instrucciones para que se traslade de inmediato al CATD reportado y atienda la contingencia.</p> <p>El Personal de Soporte Técnico reemplazará el equipo dañado por equipo previamente probado y lo instalará, realizando para ello pruebas de funcionamiento, asegurando que el equipo realizará la tarea asignada.</p> <p>En casos de falla de energía eléctrica se le instruirá al personal del CATD para que ponga en funcionamiento la planta de energía portátil que les fue instalada.</p>	<p>En caso de fallas en las telecomunicaciones en el medio de transmisión primario, el sistema se switcheará al medio de transmisión redundante para continuar transmitiendo. Se levantará de inmediato un reporte con el proveedor del servicio para que sea atendido a la brevedad posible y se le dará seguimiento a su pronta solución.</p> <p>En caso de fallas en ambos sistemas y el enlace primario ni el secundario se restablezcan, se le instruirá al Personal de Soporte Técnico adscrito a la zona para que se traslade al CATD en cuestión y respalde la información recabada en el mismo, para que desde el CATD más cercano se transmita dicha información al CCV del PREP.</p>

PLAN DE CONTINUIDAD Y CONTINGENCIAS			
PARA LAS ÁREAS DEL	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
	que cubra esa zona, para que del CATD más cercano, traslade a una persona Acopiadora o persona Digitalizadora hasta el CATD en cuestión y con ello se corrija la contingencia.		
<p>CENTRO DE CAPTURA Y VERIFICACIÓN</p> <p>Para solventar cualquier tipo de contingencia que pudiese presentarse en el CCV será necesario implementar las siguientes medidas de contingencia para garantizar la continuidad en su funcionamiento.</p>	<p>Persona Supervisora General: La o el Supervisor General mantendrá un monitoreo permanente tanto del CCV como de los CATD, para que en caso de presentarse alguna contingencia se instrumenten las medidas pertinentes para su atención inmediata. Si faltase alguna de las personas que laboran en los CATD realizará el plan descrito previamente. En caso de presentarse en el CCV, en conjunto con las personas Coordinadoras del área en cuestión, realizará los ajustes al personal requeridos.</p> <p>Personas Coordinadoras: En caso de detectar cualquier problema de salud en el personal, lo llevará a servicio médico que se destine para este propósito y la persona sea atendida de inmediato. Coordinarán horarios de descanso durante la Jornada Electoral para que el personal que muestre fatiga tenga intervalos de descanso. Igualmente asignarán al personal para tomar los alimentos en los intervalos de tiempo que les sean asignados.</p> <p>Persona Verificadora: Cuando falte algún miembro de esta área, se tomará una persona Capturista de reserva para que supla sus funciones; igualmente se realizará este procedimiento en caso de presentarse problemas de salud en uno de estos elementos.</p> <p>Personas Capturistas: En caso de detectar inasistencia en una persona Capturista se</p>	<p>De la totalidad del equipamiento instalado en el CCV, se deberá contar con equipo de soporte listo y preparado para en caso de fallas en el funcionamiento de:</p> <ul style="list-style-type: none"> • Ruteadores en caso de emplearse • Módems • Computadoras • Teléfonos • Cámaras • Switches • Cableado • Ups • Reguladores • Plantas de Energía <p>Se deberán reemplazar de inmediato por un equipo del mismo tipo previamente probado y configurado para las funciones que se requieran.</p> <p>En caso de falla total o parcial en el suministro de la energía eléctrica, deberán entrar en funcionamiento los Ups instalados para que no haya interrupciones en el flujo de la información, adicionalmente se deberá contar con plantas de energía que se pondrán en funcionamiento cuando el suministro por parte de la CFE falle. Se deberán probar durante los ejercicios y simulacros este tipo de fallas con la finalidad de verificar el buen funcionamiento de los Ups y las plantas de energía auxiliares.</p> <p>En caso de presentar contingencias en los equipos de captura, en cada sección se deberán instalar equipos extras que estarán permanentemente funcionando, para que, en caso de fallar alguno, se cambiará a la persona capturista asignado</p>	<p>De la totalidad de los servicios instalados como:</p> <ol style="list-style-type: none"> 1. Líneas Telefónicas 2. Internet Dedicado 3. Conexión Satelital 4. Conexión ADSL <p>Se deberán contemplar las siguientes medidas de contingencia:</p> <p>Líneas Telefónicas: A cada uno de los CATD se les asignará un número telefónico primario al cual deberán llamar para solicitar asistencia el cual usarán de manera regular, más en caso de que no le sea posible comunicarse con el mismo, se le deberá asignar un número secundario para que, en caso de emergencia puedan establecer comunicación.</p> <p>En caso de fallas en las líneas telefónicas del CATD se deberá recurrir a líneas de teléfono celulares como plan emergente.</p> <p>Internet Dedicado: El Internet dedicado estará monitoreado permanentemente y en caso de fallas en dicho servicio se deberá switchear al servicio de Internet Redundante, mientras se reportará de inmediato la falla con el personal técnico de soporte del proveedor para que la atiendan de inmediato, más el flujo de la información no se verá interrumpido.</p> <p>Conexión vía Cable: Si fallase el enlace primario de comunicación que es el Internet Dedicado, se switcheará al servicio de Internet vía Cable mientras se resuelve la falla del</p>

**PLAN DE CONTINUIDAD Y
CONTINGENCIAS**

PARA LAS ÁREAS DEL	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
	<p>realizarán los ajustes necesarios en el personal de acuerdo a las cargas de trabajo que se tengan. Si presentara cualquier malestar físico o cansancio, lo reportará de inmediato a su persona Coordinadora para que este le canalice y se le brinde la atención requerida.</p> <p>Persona Verificadora / Validadora: Si no se presenta alguna persona de esta área, se tomará a una persona Capturista de reserva para que supla sus funciones, igualmente se realizará este procedimiento en caso de presentarse problemas de salud en uno de estos elementos.</p> <p>Personas Telefonistas: En caso de cualquier emergencia, de acuerdo a las instrucciones de su persona Coordinadora, solicitarán ayuda a los teléfonos de emergencia de acuerdo a la contingencia que se llegue a presentar. En caso de presentar cualquier malestar físico o cansancio, lo reportará de inmediato a su persona Coordinadora para que este le canalice y se le brinde la atención requerida. En caso de inasistencia la o el Coordinador balanceará las cargas de trabajo entre las demás personas telefonistas.</p> <p>Personas Archivistas: Ayudarán a las personas Coordinadoras de Personal con el control del personal en horarios de llegada, salida, alimentos, descanso, atención médica, etc. En caso de inasistencias o problemas de salud, sus funciones las podrá suplir una persona Organizadora.</p> <p>Personas Organizadoras: Se deberán preparar simulacros de evacuación para en caso de una contingencia mayor, evacuar al personal. Se coordinarán con las personas Coordinadoras de personal y los servicios médicos para tener la mano el botiquín de emergencias. Si se presenta inasistencia de alguno o tienen problemas médicos, serán ayudados por las personas Archivistas.</p> <p>Personal Técnico: Se contará con personal técnico permanentemente para cualquier contingencia que suceda en el CCV. Durante la Jornada Electoral se localizarán en sus zonas de cobertura para que en caso de suscitarse una contingencia se desplacen a</p>	<p>a dicho equipo, a otro que esté funcionando mientras se revisa y repara el que ha presentado la falla.</p>	<p>Internet dedicado. Más si fallara igualmente el Internet vía Cable, se switcheará al servicio de Internet por ADSL.</p> <p>Conexión ADSL: La última línea de respaldo de recepción y transmisión de la información será la conexión a Internet por ADSL, más si esta igualmente fallara, se deberán contar con por lo menos dos enlaces ADSL alternativos que servirán para enlazarse como medio de contingencia.</p>

PLAN DE CONTINUIDAD Y CONTINGENCIAS			
PARA LAS ÁREAS DEL	RECURSOS HUMANOS	EQUIPAMIENTO	TELECOMUNICACIONES
	<p>cualquiera de sus CATD asignados y ejecuten el plan correspondiente.</p> <p>En caso de una contingencia mayor como sismo o incendio, se deberá ejecutar el plan de evacuación que previamente se habrá implementado y ejercitado, con el propósito de salvaguardar la integridad del personal en primera instancia.</p> <p>Cercano a las instalaciones del CCV se deberá contar con personal médico calificado para que brinde ayuda a problemas de salud que se puedan presentar con el personal que labora en estas instalaciones. Este diagnosticará la gravedad del problema y en caso necesario solicitará el traslado de la persona a un hospital.</p>		
NUBE DE INTERNET	<p>Personal Técnico: Se deberá contar con Personal de Soporte Técnico especializado para el monitoreo de la publicación de la información en la Nube de Internet. Este personal estará disponible local y remotamente, para que desde diferentes puntos se pueda resolver cualquier tipo de contingencia que se presente durante la Jornada Electoral.</p> <p>Se deberá contar con Personal Técnico especializado tanto por parte del instituto responsable del PREP como de la empresa que provee la señal de Internet en sitio.</p>	<p>Servidores: Con respecto a los servidores que se emplearán en el PREP en sus diferentes etapas y servicios, cada uno de ellos deberá contar con por lo menos un servidor espejo de respaldo el cual en caso de falla en cualquier servidor primario, el espejo se activará de manera automática para evitar interrupciones en flujo de la información.</p> <p>Firewalls: La totalidad de los enlaces en cada punta deberán contar con un servicio de Firewall que impida el acceso de intrusos a la red. Estos Firewall deberán estar monitoreados permanentemente para reportar cualquier instrucción de inmediato y repelerla.</p>	<p>Enlace Dedicado de Internet: Se pondrá en funcionamiento un sistema de monitoreo que permanentemente esté verificando la integridad de la señal en los enlaces de Internet, dicho sistema deberá poder switchear de un servicio a otro sin menoscabo en la recepción y transmisión de la información.</p> <p>Es decir, si falla el enlace primario, se cambiará al secundario, si se restablece el primario se regresará al mismo. Si falla el servicio primario, se cambiará al redundante, si falla también el secundario se cambiará a un tercero y así sucesivamente.</p>

Adicionalmente como parte del Plan de Continuidad se preverán esquemas de contingencia en:

D. Personal Técnico de Informática

Habrá personal Técnico de Informática localizados cada Consejo Distrital, los cuales tendrán disponibles equipos de soporte (de cada tipo de equipo instalado), listos para resolver cualquier tipo de contingencia que se presente durante la Jornada Electoral, ya sea eventualidades en equipos o en personal, evitando con ello que no se tengan interrupciones en el acopio y digitalización de la información para el PREP.

E. Coordinación con la Gerencia de Desastres Telmex

Dada la importancia de la Red y la relación del Instituto con Telmex, se contará con el apoyo del Área de Desastres para coordinar medidas adicionales de Seguridad en la Red de Datos.

F. Contingencia por amenaza externa.

Una contingencia por amenaza externa, se presenta cuando se pone en peligro la

integridad de las personas involucradas en el proceso del PREP, algunos ejemplos de este tipo de contingencia son:

- Situaciones de alerta en las sedes de los CATD o el CCV, por desastres naturales, clima, incendio.
- Situaciones de alerta en las sedes de los CATD, debido a la toma de las instalaciones por manifestantes.

Para hacer frente a este tipo de contingencias en el CATD, se debe nombrar un responsable que asuma el liderazgo y coordine las acciones necesarias para enfrentar el incidente.

Procedimiento:

- Identificar la contingencia.
- Daño: Personas muertas, heridas o daños materiales en las sedes.
- Número de personas que se encuentran dentro de la sede afectada.

Esto con el objetivo de hacer una evaluación que permita, precisar información importante, a fin de determinar el tipo de ayuda que se requiere.

Avisar a cuerpos de emergencia:

Comunicar la situación de que se trate a las autoridades locales y, posteriormente, al CCV y a las autoridades del IEEPCO.

El reporte de ayuda deberá cubrir los siguientes puntos:

- Nombre que llama para realizar el reporte.
- Distrito electoral donde se ubica el CATD.
- Tipo de suceso ocurrido.
- Situación de la emergencia.

Ordenar la evacuación de acuerdo con la contingencia.

Debe tomarse como prioridad salvaguardar la vida e integridad de las personas, por ello las primeras acciones van encaminadas a eso; si la situación requiere efectuar la evacuación del CATD o en su caso el CCV, se deberá efectuar inmediatamente.

Dar aviso al Consejo General.

En caso de que la contingencia se presente en alguno de los CATD, después de avisar a las autoridades locales se deberá dar aviso al CCV, que a su vez comunicará el suceso a las autoridades del IEEPCO.

En caso de que la contingencia se suscite en el CCV, este deberá dar aviso, después de hacerlo a las autoridades locales, a las autoridades del IEEPCO.

Determinar fin de la contingencia.

Después de que las autoridades de seguridad, auxilio y rescate determinen el fin de la emergencia es necesario informar al CCV y a las autoridades del IEEPCO.

En su caso, organizar el reingreso a las instalaciones y vuelta a la normalidad de actividades.

Cuando la situación lo permita, la persona responsable podrá organizar el reingreso del personal a las instalaciones para retomar las actividades de operación del PREP.

En caso de que la contingencia continúe, por ejemplo, porque esta se dio por la toma de las instalaciones, y los manifestantes no se retiran de la sede del CATD, la persona responsable del CATD, deberá informar al respecto al CCV y a las autoridades del IEEPCO, a fin de determinar el traslado del personal y en su caso el material que haya sido resguardado al CATD más cercano y en su caso, continuar con las actividades desde la nueva sede.

Previsiones de seguridad en el CCV.

Para el caso del CCV que se instala en la ciudad de Oaxaca de Juárez, y debido a que la situación socio-política del Estado, siempre se considera un factor de posible riesgo, se toman las provisiones necesarias, lo cual incluye la instalación de vallas de seguridad alrededor de todo el edificio en donde se instala el CCV, el cual además es fuertemente custodiado por elementos de seguridad pública de la Policía Estatal, desde una noche antes y hasta el cierre del PREP.

VIII. PLAN DE EJERCICIOS Y SIMULACROS

Con la finalidad de evaluar el desempeño de los componentes del PREP, se ha creado el presente Plan de Ejercicios y Simulacros, el cual está encaminado a ordenar los procedimientos que habrán de realizarse de forma periódica y que permitirán valorar el correcto funcionamiento del PREP.

A partir de la instalación de la infraestructura del PREP, se procederá a ejecutar el Plan de Capacitación, el cual permitirá que el personal que labore en el PREP pueda dominar las áreas para las cuales ha sido contratado.

Terminada la fase de Capacitación, se iniciará el período de Ejercicios y Simulacros del PREP. Los Ejercicios del PREP nos brindarán una continua evaluación del funcionamiento de los siguientes elementos del PREP:

- a) **Procedimientos**
- b) **Recursos Humanos**
- c) **Equipamiento**
- d) **Telecomunicaciones**
- e) **Sistemas**
- f) **Energía**

La forma en que habrán de valorarse cada uno de ellos se detalla a continuación:

a) Procedimientos

Se verificará que los Procedimientos implementados funcionen acorde a lo esperado, midiendo la efectividad y eficiencia de los mismos. Se medirá el desarrollo de cada una de las actividades para valorar su implementación y en caso de ser necesario realizar adecuaciones que permitan lograr un mejor desempeño, mediante la aplicación de medidas orientadas a lograr de forma óptima los objetivos del PREP.

b) Recursos Humanos

En cuanto al personal, gracias a los ejercicios y simulacros programados, se podrá medir la efectividad de la capacitación impartida a en cada una de las actividades que deben realizar, revisando que sigan los procedimientos de acuerdo al orden establecido, midiendo los tiempos de ejecución en los mismos y asegurando el cabal cumplimiento de cada uno. En igual manera se disiparán dudas que pudieran tener en cuanto a la aplicación de sus actividades.

c) Equipamiento

Durante los ejercicios y simulacros, podrá medirse el desempeño del equipamiento instalado, verificando posibles fallas en su funcionamiento y en caso de detectarse problemas se reemplazarán para asegurar que la totalidad del equipamiento funcione adecuadamente y evitar que durante la Jornada Electoral pudiesen presentarse contingencias por desperfectos en su funcionamiento.

d) Telecomunicaciones

Gracias a la implementación de los ejercicios y simulacros se podrá medir el buen funcionamiento de las telecomunicaciones, pudiendo medir intermitencias, saturaciones en los anchos de banda y fallas en las mismas.

e) Sistemas

En el desarrollo de los ejercicios y simulacros, además de los procedimientos, equipamiento y telecomunicaciones, es posible en forma conjunta verificar el funcionamiento adecuado de los sistemas, revisando las tablas y gráficas generadas en el mismo, asegurando que cumpla con las especificaciones del diseño y permitiendo realizar las adecuaciones necesarias al mismo, acorde a los requerimientos presentados por el propio instituto.

f) Energía

Gracias a los ejercicios y simulacros, es posible realizar una capacitación exhaustiva al personal sobre la operación de las plantas de energía, esto mediante la simulación de cortes en el suministro de energía eléctrica de la CFE, verificando que las plantas de energía cumplan con la función para la cual se han suministrado tanto a los CATD como para el CCV, revisando que permita mantener la continua alimentación de la energía requerida para el equipamiento instalado.

También se contempla el inicio de la capacitación del personal, previo a la Jornada Electoral, dando por inicio los ejercicios reales dentro de la última semana previa a la Jornada Electoral, brindando con ello mayor certidumbre sobre el comportamiento de los procedimientos, recursos humanos, equipamiento, telecomunicaciones y energía para la operación del PREP. En igual forma se contemplará la ejecución de un simulacro del PREP, el cual tendrá lugar el 20 de marzo de 2022.

A continuación, se describe el programa para el desarrollo del Simulacro del PREP:

PROCEDIMIENTO TÉCNICO OPERATIVO PARA EL SIMULACRO DEL PREP

El Programa de Resultados Electorales Preliminares, combina de manera global los siguientes recursos:

- a) Procedimientos
- b) Recursos Humanos
- c) Equipamiento
- d) Telecomunicaciones
- e) Sistemas
- f) Energía

Estos recursos comparten el mismo nivel de importancia dentro de su funcionamiento para el PREP, de ahí que se debe medir y verificar el desempeño individual y grupal de los mismos.

Para ello, una vez instalado todo el equipo de cómputo que operará el PREP el día de la Jornada Electoral y establecidas las Telecomunicaciones que se utilizarán para el adecuado funcionamiento del programa, se capacitará a las personas que lo operarán.

Dicha capacitación será Teórico-Práctica para lo cual se le proporcionará al personal que labore en el PREP, la capacitación suficiente y necesaria en donde se describirán sus respectivas funciones con base en el puesto que desempeñará cada uno.

Para efectos de evaluación, se tiene previsto un simulacro del PREP, este se realizará el 20 de marzo de acuerdo a las determinaciones establecidas por el IEEPCO.

El Simulacro de funcionamiento del PREP, se realizará de manera conjunta en los Centros de Acopio y Transmisión de Datos (CATD) y el Centro de Captura y Verificación (CCV), el segundo instalado en la ciudad de Oaxaca, a cargo de la persona Supervisora General del PREP, en tanto que los CATD estarán instalados en los inmuebles de los Consejos Distritales Electorales designados por el IEEPCO en el Interior del Estado, conforme a las elecciones extraordinarias. El número de personas que operarán el PREP en estos centros, varía dependiendo del número de casillas que se recibirán en cada Consejo Distrital.

SIMULACRO DEL PREP

Al citado simulacro, deberán asistir la totalidad del personal de la UTSID del IEEPCO, el personal destinado para los Centros de Acopio y Transmisión de Datos (CATD) y el personal del Centro de Captura y Verificación (CCV), las personas integrantes del Consejo General del IEEPCO, las representaciones de los partidos políticos y los medios de comunicación.

El programa de actividades para este día será el siguiente:

1. La totalidad del personal se presentará a las 9:00 horas, tanto en el CCV como en cada uno de los CATD.
2. Se darán instrucciones al personal Técnico de Informática del PREP para que se localicen en

diferentes lugares de los Distritos para atención de fallas simuladas. Dicho personal técnico estará listo en los sitios predeterminados a las 9:00 horas.

3. A las 9:15 horas, dará inicio al pase de lista, verificando que la totalidad de las instalaciones estén abiertas y el personal se encuentre listo para laborar en el interior de las mismas. Así mismo, se darán instrucciones a todos los CATD sobre las eventualidades que han de simular durante el ejercicio.
4. A las 10:15 horas se les solicitará a las personas integrantes del Consejo General del IEEPCO, que determinen una leyenda que se escribirá sobre la primera acta de escrutinio y cómputo de la elección de Diputación Local o Ayuntamiento, para que se den instrucciones a dichos CATD, de anotarlas sobre la sección de los votos en las Actas, para que sean Acopiadas y Digitalizadas en los mismos, para su transmisión y proceso al CCV.
5. A la misma hora, se ordenará a las personas Coordinadoras del CCV que indiquen a su personal que accedan al sistema y esperen el arribo de la información.
6. Una vez Acopiadas, Digitalizadas, Transmitidas, Capturadas y Procesadas dichas actas, se mostrarán en pantalla para que todos los asistentes observen y tengan certeza del funcionamiento del sistema.
7. A las 11:00 horas, se le darán instrucciones a la totalidad de los CATD para que simulen la incidencia de Sobre Vacío en la última casilla descrita en su bitácora de la elección para la Diputación Local o de Ayuntamiento.
8. A las 11:30 horas, se darán instrucciones a todos los CATD, para que inicien el procedimiento de Acopio/Digitalización de sus demás Actas de Escrutinio y Cómputo en cada uno de ellos.
9. A las 12:00 horas, se realizará el simulacro de falla de energía en los CATD donde se encuentra el personal Técnico en Informática para verificar el funcionamiento de estos durante esta eventualidad.
10. A las 12:30 horas, se simulará la pérdida de señal de Internet en los CATD en donde se encuentra el personal Técnico de Informática para que realicen el procedimiento emergente de transmisión de información.
11. Conforme los CATD terminen su procedimiento de Acopio/Digitalización de información, tendrán que informar al CCV y esperarán instrucciones.
12. Una vez finalizada la captura y proceso de la información, se dará por terminado el Simulacro y se instruirá al personal para que se retiren de los CATD y posteriormente del CCV.
13. Se emitirá un informe a la UTSID sobre las cifras obtenidas en el Simulacro del PREPy esta deberá informar a la Presidencia del Consejo General del IEEPCO.