

ANÁLISIS DE RIESGOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN, PLAN DE SEGURIDAD Y PLAN DE CONTINUIDAD

ÍNDICE

ANÁLISIS DE RIESGOS EN MATERIA D SEGURIDAD DE LA INFORMACIÓN.....	3
Introducción.....	3
Antecedentes	4
Objetivo.....	5
Factores de Riesgo.....	6
Activos Críticos.....	8
Áreas de Amenaza.....	18
Identificación de Riesgos.....	22
Estrategia de Gestión de Riesgos.....	31
PLAN DE SEGURIDAD.....	39
Introducción.....	39
Objetivos	40
Bases de la seguridad informática.....	41
PLAN DE CONTINUIDAD	49
Introducción	49
Objetivos	49
Metodología	49
Bases de la seguridad informática.....	41

ANÁLISIS DE RIESGOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Introducción:

Hoy en día los sistemas de información son el alma de organizaciones, empresas y entidades, el grado de responsabilidad reposa en los sistemas, datos e información encaminados al logro de los objetivos internos, estos se pueden mejorar y mantener teniendo una adecuada sistematización y documentación.

El tratamiento de la información abarca aspectos que van desde el manejo de documentos en medio físico como el proceso de almacenaje y recuperación conocido también como proceso de gestión documental, hasta los sistemas de información que tenga la organización o sistemas externos a los que esté obligada a reportar información, pasando por aspectos tan importantes como la forma de almacenamiento de los datos digitales, modelos de respaldo de información y planes de contingencia o de continuidad del negocio, si existen, claro está, incluyendo además los sistemas físicos de protección y accesibilidad a sitios o áreas restringidas.

Es por esto que los activos de información han pasado a formar parte de la actividad cotidiana de organizaciones e individuos; los equipos de cómputo almacenan información, la procesan y la transmiten a través de redes y canales de comunicación, abriendo nuevas posibilidades y facilidades a los usuarios, pero se deben considerar nuevos paradigmas en estos modelos tecnológicos y tener muy claro que no existen sistemas cien por ciento seguros, porque el costo de la seguridad total es muy alto (aunque en la realidad no es alcanzable idealmente), y las organizaciones no están preparadas para hacer este tipo de inversión.

Derivado de lo anterior, a continuación, se describe el análisis realizado de acuerdo a la metodología descrita en las normas ISO 27001 Sistemas de Gestión de Seguridad de la Información y la ISO 27005 Gestión de los Riesgos Relativos a la Seguridad de Información.

Antecedentes

En el Anexo 13 del Reglamento de Elecciones, en su Título II de la Implementación, Capítulo IV de las Consideraciones de Seguridad Operativa, en su Numeral 12 establece:

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. **Áreas de Amenaza:** identificar y describir cuál es la situación o condición – técnica, legal, económica, política, social, etc.- que pueda afectar los procedimientos del PREP;
 - IV. **Identificación de riesgos:** deberá describirse claramente cuáles son los impactos que se pueden tener en el caso que una amenaza se materialice durante los procedimientos del PREP;
 - V. **Estrategia de gestión de riesgos:** se deberá definir y documentar la respuesta respecto de cada uno de los riesgos identificados, es decir, definir si los riesgos serán aceptados, mitigados, transferidos o eliminados, y
 - VI. **Plan de seguridad:** se deberá elaborar un plan de seguridad basado en los resultados de la estrategia de gestión de riesgos, que permita llevar a cabo la implementación de controles en los distintos procedimientos de operación del PREP, así como en la infraestructura tecnológica.
13. Se deberá implementar un **plan de continuidad** para 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.

El plan deberá ser comunicado al personal involucrado en su ejecución y formar parte de los ejercicios y simulacros.

Objetivo

La finalidad del presente análisis es identificar los activos a proteger o evaluar, inherentes al Programa de Resultados Electorales Preliminares (PREP) que se ha de implementar para el Instituto Estatal Electoral de Baja California Sur, durante la Jornada Electoral a verificarse el próximo Domingo 1 de Julio del 2018, durante la cual se habrán de renovar los cargos de Diputados y Ayuntamientos de la entidad.

La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis, con criterios de riesgo establecidos en este documento.

Los resultados obtenidos de este análisis, van a permitir el desarrollo de un Plan de Seguridad orientado a prevenir la ocurrencia de los riesgos identificados mediante medidas específicas, esto involucra identificar el conjunto de opciones que existen para tratar los riesgos y evaluarlas.

Consecuencia de este documento, 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.

El plan deberá ser comunicado al personal involucrado en su ejecución y formar parte de los ejercicios y simulacros.

Para la realización del análisis de riesgos, se requiere evaluar los siguientes elementos:

I. Factores de Riesgo

Los criterios que se deberán tomar en cuenta para la valoración de los posibles riesgos van de la mano con el nivel de impacto que éstos pudieran tener en el desarrollo y funcionamiento del PREP en caso de ocurrir. Dependiendo de su intensidad se valorará el grado de magnitud en el daño potencial que represente para el PREP y estos factores se clasifican de la siguiente forma:

Matriz de Riesgos

Matriz de calificación, evaluación y respuesta a los riesgos

PROBABILIDAD	ALTA	Zona de Riesgo Moderado	Zona de Riesgo Importante	Zona de Riesgo Inaceptable
	MEDIA	Zona de Riesgo Tolerable	Zona de Riesgo Moderado	Zona de Riesgo Importante
	BAJA	Zona de Riesgo Aceptable	Zona de Riesgo Tolerable	Zona de Riesgo Moderado
		BAJO	MEDIO	ALTO
		IMPACTO		

- A. Riesgo Bajo:** Los elementos a los que afecte no detendrán el funcionamiento del PREP, mas 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 mismo, representar el entorpecimiento del desarrollo de otras actividades lo cual en cadena representaría un Riesgo Medio o 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 presente 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.

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 del mismo, se tipificarán de acuerdo a su naturaleza y se detallará en qué áreas de amenaza se localizan para su focalización y continuo monitoreo.

Clasificaciones y definiciones de la de los Activos por Áreas de Localización

Recursos Humanos	Equipamiento	Telecomunicaciones
Centros de Acopio y Transmisión de Datos (CATD)	Centros de Acopio y Transmisión de Datos (CATD)	Centros de Acopio y Transmisión de Datos (CATD)
Centro de Captura y Verificación (CCV)	Centro de Captura y Verificación (CCV)	Centro de Captura y Verificación (CCV)
Nube de Internet	Nube de Internet	Nube de Internet

Acorde a lo anterior, se determinaron tres tipos de activos críticos:

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

Las Áreas en que se localizarán los Activos Críticos son:

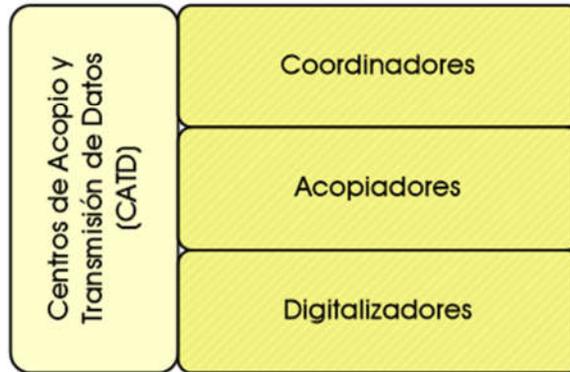
- a) Centros de Acopio y Transmisión de Datos (CATD)**
- b) Centro de Captura y Verificación (CCV)**
- c) Nube de Internet**

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

- A. Recursos Humanos:** Se detalla al personal que ha de participar en los CATD, el CCV y la nube de Internet:

a) Centros de Acopio y Transmisión de Datos

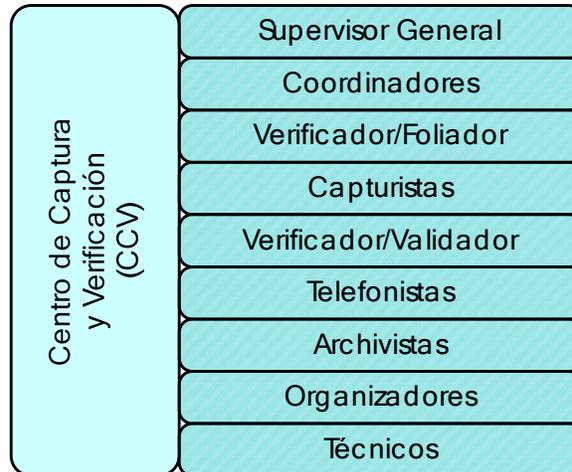
Recursos Humanos por Área de Localización



1. **Coordinadores:** Estarán a cargo de la operación del CATD, incluyendo Instalación, Adecuación, Personal, Materiales y elaboración de informes. Es el enlace entre el CATD y el CCV, toma decisiones en su ámbito de operación.
2. **Acopiadores:** Recibirán los sobres con las Actas PREP, verificará su contenido y datos de identificación, detectará inconsistencias, registra en su Bitácora para Acopio de Actas PREP la fecha y hora de recepción de las Actas PREP y las entregará a los Digitalizadores.
3. **Digitalizadores:** Digitalizarán las actas verificando su correcta legibilidad, en caso necesario repetirá el procedimiento asegurando la calidad de la imagen generada.

b) Centro de Captura y Verificación

Recursos Humanos por Área de Localización



1. **Supervisor General:** Estará a cargo de la operación del personal y equipos, supervisará la capacitación, estará a cargo de los CATD y el CCV.
2. **Coordinadores:** Coordinarán al personal a su cargo por áreas, dará seguimiento al funcionamiento del equipamiento y elaborará informes.
3. **Verificador/Foliador:** Verificarán la correcta identificación de las imágenes de las actas, revisará inconsistencias.
4. **Capturistas:** Revisarán los votos obtenidos para los partidos o candidatos y los captará en el sistema.
5. **Verificador/Validador:** Verificarán la información capturada de las imágenes de las actas, corregirá y procesará inconsistencias.
6. **Telefonistas:** Realizarán el pase de lista de los CATD, darán las instrucciones de arranque, verificarán el avance de sus CATD y canalizará llamadas a los técnicos y al Supervisor General.
7. **Archivistas:** Estarán a cargo de los expedientes del personal y el soporte documental generado en los ejercicios.
8. **Organizadores:** Recibirán y generarán toda la información requerida en el PREP, elaborarán la Memoria del PREP.

9. **Técnicos:** Realizarán la instalación de los CATD y CCV, darán soporte al funcionamiento de la totalidad del Equipamiento.

c) **Nube de Internet**

Recursos Humanos por Área de Localización



1. **Técnicos:** El personal técnico estará a cargo de monitorear permanentemente las telecomunicaciones y los enlaces a la nube de Internet, asegurando la operación continua del servicio.
- B. **Equipamiento:** Aquí detallaremos el equipamiento que ha de emplearse en los CATD, el CCV y la nube de Internet:

a) **Centros de Acopio y Transmisión de Datos**

Equipamiento por Área de Localización

Centro de Acopio y Transmisión de Datos (CATD)	Módem ADSL
	Cable Módem
	Módem Banda Ancha Móvil
	Teléfono
	Computadora
	Scanner
	Webcam
	Ups
	Regulador
	Planta de Energía

1. **Módem ADSL:** La red estatal estará compuesta por enlaces ADSL para la conexión con la red de Internet y la conexión se realizará mediante módems provistos con esta tecnología.

2. **Cable Módem:** En caso de no existir facilidades de enlaces ADSL y exista la conexión a Internet con la compañía de Cable Local se usará este servicio.
3. **Módem Banda Ancha Móvil:** Como medio contingente en todas las localidades donde se cuente con cobertura Celular, se emplearán Módems de Banda Ancha Móvil para la transmisión de la información.
4. **Teléfono:** Se instalarán aparatos telefónicos en cada uno de los CATD para entablar comunicación diaria permanente con el CCV. En los CATD donde no pueda proveer el servicio de telefonía fija, se empleará telefonía celular.
5. **Computadora:** Para operar el equipo de digitalización y transmitir las imágenes digitalizadas se emplearán equipos de cómputo en cada uno de los CATD.
6. **Scanner:** La digitalización de las imágenes de las actas de escrutinio y cómputo se realizará mediante Scanner o Multifuncionales que permitan preparar la información para digitalizarla y transmitirlas al CCV.
7. **Webcam:** Cada uno de los CATD estará permanentemente monitoreado con cámaras Web para vigilar el funcionamiento de los mismos.
8. **Ups:** En caso de interrupciones cortas en la energía eléctrica se asegurará el funcionamiento del equipo de cómputo y telecomunicaciones, para lo cual se deberá instalar un Ups en cada CATD.
9. **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.
10. **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.

b) Centro de Captura y Verificación

Equipamiento por Área de Localización

Centro de Captura y Verificación (CCV)	Módem ADSL
	Cable Módem
	Teléfonos
	Switches
	Computadoras
	Video Cámaras
	Csñones de Proyección
	Ups
	Reguladores
	Plantas de Energía

- Módems ADSL:** Para el enlace principal de salida a la nube de Internet se contratará un servicio con las características necesarias para prever la demanda de información requerida por el CCV, esto se podrá hacer vía un Enlace ADSL de alta velocidad, siempre y cuando haya facilidades para la contratación del servicio.
- Cable Módem:** Como enlace redundante a la nube de Internet se podrá emplear un enlace a Internet con la compañía de Cable Local, siempre y cuando existan facilidades en sitio.
- Teléfonos:** Se instalarán aparatos telefónicos en el CCV para entablar una comunicación diaria permanente con los CATD localizados en todo el estado.
- 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.
- Computadoras:** 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.
- Video Cámaras:** Se instalará un sistema de video vigilancia que permita mantener la vigilancia permanente de todas las áreas que componen el CCV, tanto en interiores como en exteriores, almacenando la evidencia en una unidad DVR para su consulta y custodia.

8. **Cañones de Proyección:** Se montarán cañones 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.
9. **Ups:** Como primera medida contingente de fallo de energía, se instalarán fuentes de poder ininterrumpida (UPS) a los cuales se conectarán todos los equipos de telecomunicaciones de la red y el equipo de cómputo, asegurando su funcionamiento en caso de falla en el suministro de energía por parte de CFE.
10. **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.
11. **Plantas de Energía:** Se deberá contar con plantas de energía auxiliar como segunda medida emergente para usarse en casos de fallo de la energía principal proveniente de la CFE.

c) **Nube de Internet**

Equipamiento por Área de Localización



1. **Servidores:** Es importante que los servidores empleados para este proyecto sean monitoreados permanentemente para asegurar el funcionamiento del PREP, lo que se realizará a través de las herramientas propietarias del proveedor del servicio. Cabe mencionar que los servidores empleados son arrendados en los servicios de Amazon y Rackspace, lo que implica contar con el respaldo de la infraestructura y seguridad ya existente en estas compañías líderes de mercado.

- C. Telecomunicaciones:** Para la construcción de la red estatal del PREP se deberá realizar con las siguientes características:

a) Centros de Acopio y Transmisión de Datos

Equipamiento por Área de Localización

Centro de Acopio y Transmisión de Datos (CATD)	Línea Telefónica
	Enlace ADSL
	Enlace Vía Cable
	Enlace Banda Ancha Móvil

- Línea Telefónica:** Se contratarán líneas telefónicas para cada uno de los CATD donde se cuente con facilidades, los sitios donde no sea posible se instalará telefonía Celular, el principal medio de comunicación entre los CATD y el CCV será la vía telefónica.
- Enlace ADSL:** En todos los municipios donde se cuente con facilidades técnicas, se contratarán servicios de Internet ADSL como medio primario de transmisión de la información.
- Enlace Vía Cable:** Donde no se hallen 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 fija igualmente se contratará con la Compañía de Cable Local.
- Banda Ancha Móvil:** Como medio de respaldo en caso de contingencia en todas las localidades se verificará la disponibilidad de red para Banda Ancha Móvil para en caso de requerirse usarla como medio de transmisión de información emergente.

b) Centro de Captura y Verificación

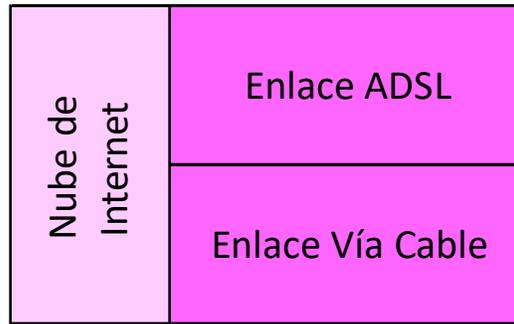
Telecomunicaciones por Área de Localización

Centro de Captura y Verificación (CCV)	Líneas Telefónicas
	Enlace ADSL
	Enlace Vía Cable

1. **Líneas Telefónicas:** Se contratarán líneas telefónicas suficientes para establecer comunicación diaria con cada entre el CCV y los CATD en razón de un máximo de 5 CATD's por cada línea, teniendo 4 servicios disponibles.
2. **Enlace ADSL:** Se podrá contar con conexión a Internet mediante Enlaces ADSL de alta velocidad, los cuales proveerán el medio de transmisión requerido para los volúmenes de transmisión de información necesarios para el CCV, siempre y cuando haya facilidades para la contratación del servicio.
3. **Enlace Vía Cable:** Se instalará el servicio de Internet con la Compañía de Cable Local como medio de conexión redundante a la nube de Internet, siempre y cuando existan facilidades del servicio.

c) Nube de Internet

Telecomunicaciones por Área de Localización

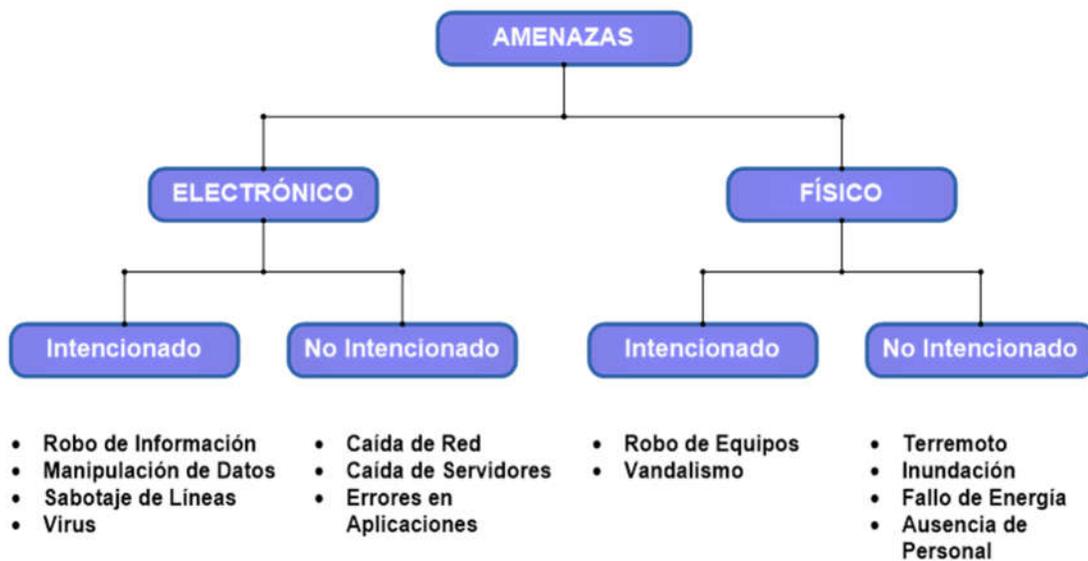


1. **Enlace ADSL:** Se podrá contar con conexión a Internet mediante Enlaces ADSL de alta velocidad, los cuales proveerán el medio de transmisión requerido para los volúmenes de transmisión de información necesarios para el CCV, siempre y cuando haya facilidades para la contratación del servicio.
2. **Enlace Vía Cable:** Se instalará el servicio de Internet con la Compañía de Cable Local como medio de conexión redundante a la nube de Internet, siempre y cuando existan facilidades del servicio.

III. Áreas de Amenaza

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

Áreas de Amenaza de Riesgos



Las Áreas en que se localizarán las Amenazas son:

A. Centros de Acopio y Transmisión de Datos

En cada uno de los Consejos Electorales Distritales definidos por el Instituto Estatal Electoral de Baja California Sur, se instalará un CATD, el cual Acopiará y Digitalizará las Actas de Escrutinio y Cómputo para las elecciones de Diputados y Ayuntamientos, 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 de los CATD, capturar la información contenida en las mismas y publicar el resultado en la nube de 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 los 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 los CATD al CCV, como de la publicación de los datos procesados desde el CCV 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 penetración de intrusos en la red local y la red estatal del PREP.

Para simplificar el desglose de estas Áreas de Amenaza, en cada una de las Áreas en que se localizarán, las referiremos como:

1. **Amenazas Electrónicas Intencionadas (AEI).**
2. **Amenazas Electrónicas No Intencionadas (AEN).**
3. **Amenazas Físicas Intencionadas (AFI).**
4. **Amenazas Físicas No Intencionadas (AFN).**

Es importante destacar que en todos los ámbitos del software que se empleará y que ha sido desarrollado por la empresa, será obligatorio el uso de las Contraseñas para el acceso a los diversos módulos (Digitalización, Foliación, Captura y Verificación), contarán con las características necesarias para ser robustas en su construcción, cada usuario sólo podrá tener acceso a las opciones del Sistema que sólo sean intrínsecas a su rol, así como su localización, evitando con ello el mal uso, tanto de sus cuentas como de sus funciones.

En cuanto a las actualizaciones de los servidores, estas estarán sincronizadas y monitoreadas permanentemente tanto en los servidores del Data Center Primario como del Data Center Redundante, de tal manera que la información contenida en ambos siempre será consistente.

De igual forma la totalidad del equipamiento que será utilizado para operación del PREP, utilizará un Sistema Operativo Linux, con distribución propia, la cual no permitirá que ninguno de los usuarios de la Red del PREP tenga acceso a ninguna opción aplicación no residente en los mismos (navegadores, correo electrónico, etc.), en igual forma se inhabilitarán el uso de dispositivos externos que se puedan conectar a dichos equipos por ninguna vía, evitando con ello la intromisión de código malicioso en el Sistema (como virus o malware). Asimismo, al no existir ningún software para la transmisión de correos electrónicos se descarta completamente la posibilidad de que se presenten ataques de suplantación de identidad que pudiesen derivar en la obtención no autorizada de contraseñas o información de los sistemas y aplicativos del PREP.

En el mismo sentido, la totalidad de la Red del PREP se encontrará cerrada y aislada de tal forma que ningún equipo ajeno a la red pueda hacer uso de la misma, tanto

en los CATD como en el CCV, no podrán ser conectados ningún tipo de dispositivos ajenos a la propia red. La totalidad de la Red del PREP será alámbrica y no existirá ningún punto de acceso inalámbrico en la misma. Siendo el personal de soporte técnico el responsable del equipamiento del PREP, siendo el único con acceso a la configuración de los mismos, y dado que la totalidad de la red se encuentra aislada y monitoreada permanentemente, cualquier intrusión a la misma sería detectada de inmediato.

En lo concerniente a la posibilidad de la incidencia de algún fallo en el equipo de cómputo que compone la infraestructura tecnológica, cabe mencionar que se cuentan con sistemas de Monitoreo permanente los cuales, en caso de detectar fallas en cualquiera de los componentes del PREP, envían señales de alarma para su atención inmediata. Adicionalmente tanto en el Plan de Seguridad como en el Plan de Continuidad, se hace mención de que se contará con personal Técnico de Soporte permanente, para que en caso de detectarse algún fallo en cualquiera de los componentes del equipamiento del PREP, se atienda de forma expedita. Una vez instalada la red del PREP, la totalidad del equipo permanece encendido de manera permanente hasta el Cierre del PREP, de tal manera que pueda ser Monitoreado en cuanto a su comportamiento.

Igualmente es importante destacar que la Red del PREP, está basada en una VPN de acceso exclusivo para el PREP, la cual cuenta con mecanismos de Firewall que evitarán la intromisión de entes ajenos a la misma, esto en virtud de que la información de punto a punto viaja encriptada mediante llaves que sólo el emisor y el receptor conocen, por lo que no existe ser posibilidad de que un supuesto atacante intercepte la comunicación entre los distintos módulos del sistema consiguiendo incluso su alteración. Cabe mencionar que, aunado a los mecanismos de seguridad mencionados, también existe una política de monitoreo permanente a la red interna del PREP para evitar accesos no autorizados en el momento en que éstos pudieran intentar la penetración.

En este respecto, es importante detallar que existen 2 protocolos de monitoreo del equipamiento, divididos en el monitoreo local y central. El monitoreo local comprende la designación de un técnico en turno de acuerdo al rol determinado por el Jefe de Técnicos, que está al pendiente de diversos parámetros de los equipos de los CATD como son el estado de la red y su enlace redundante, la temperatura de los equipos y la webcam. En lo referente al monitoreo central, se refiere al personal especializado designado por las oficinas centrales de PoderNet para la guardia de la Red Privada Virtual, así como los servicios de almacenamiento contratados que suponen riesgos de mayor complejidad e impacto en el servicio.

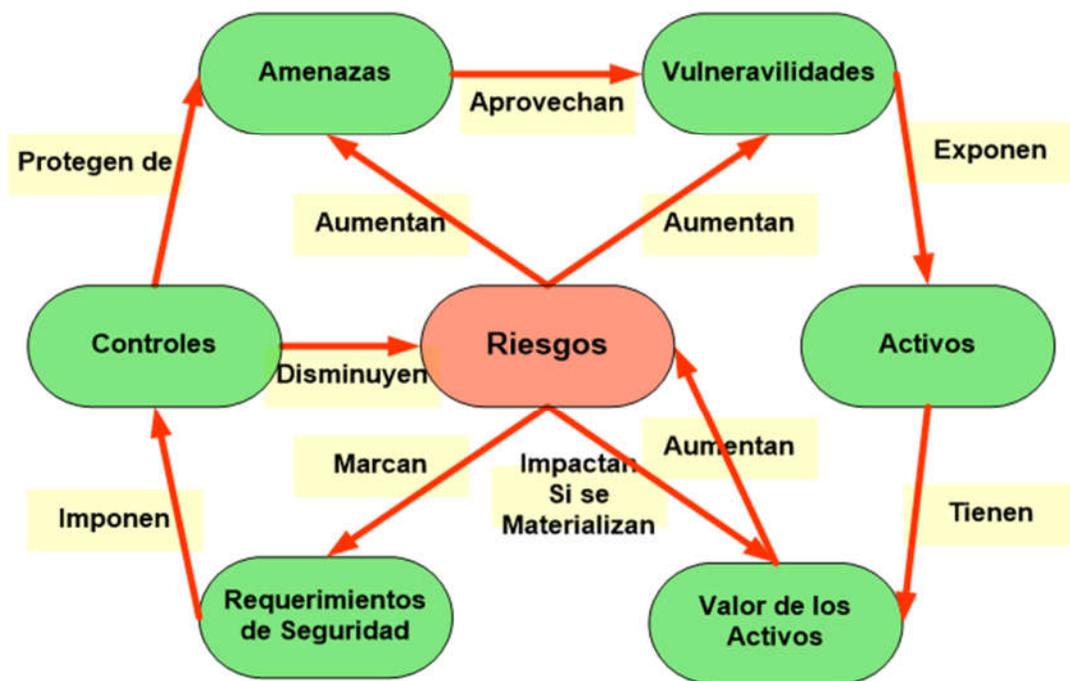
En relación al riesgo de que exista un ataque de denegación de servicio lanzado por un atacante que pretenda hacer que el sitio de publicación del PREP sea inaccesible para su navegación, es importante destacar que los Servidores del PREP, como se ha mencionado previamente, se hallan en Data Centers separados y redundantes, los cuales cuentan con mecanismos de configuración y protección contra este tipo de ataques. En este sentido, es importante mencionar que se tienen prevista la realización de pruebas de denegación de servicio al sitio de publicación del PREP, está prevista tal cual lo marca el documento "**Requisitos mínimos para la elaboración del anexo técnico para la contratación de servicios de auditoría al sistema informático y a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares**".

En cuanto a los riesgos de una intrusión a la aplicación PREP Casilla, se han tomado diversas medidas para el reforzamiento de la seguridad en este rubro, tal como el caso de la validación de la autorización que exista de la terminal móvil para conectarse al servicio, mediante la implementación de una lista blanca referente al IMEI, así como el mecanismo de validación de las credenciales de usuario asignadas a cada CAE sólo podrán ser usadas en un equipo a la vez.

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.

Identificación de Riesgos



Matriz de Identificación de Riesgos

Activo Crítico	Área de Localización	Área de Amenaza	Afectación
Recursos Humanos	CATD	AB	Aplica
		AEN	No Aplica
		AFI	Aplica
		AFN	Aplica
	CCV	AB	Aplica
		AEN	No Aplica
		AFI	Aplica
		AFN	Aplica
	Nube de Internet	AB	Aplica
		AEN	No Aplica
		AFI	No Aplica
		AFN	No Aplica
Equipamiento	CATD	AB	Aplica
		AEN	Aplica
		AFI	Aplica
		AFN	Aplica
	CCV	AB	Aplica
		AEN	Aplica
		AFI	Aplica
		AFN	Aplica
	Nube de Internet	AB	Aplica
		AEN	Aplica
		AFI	No Aplica
		AFN	Aplica
Telecomunicaciones	CATD	AB	Aplica
		AEN	Aplica
		AFI	Aplica
		AFN	Aplica
	CCV	AB	Aplica
		AEN	Aplica
		AFI	Aplica
		AFN	Aplica
	Nube de Internet	AB	Aplica
		AEN	Aplica
		AFI	Aplica
		AFN	Aplica

- A. **Recursos Humanos:** Aquí detallaremos al personal que ha de participar en los CATD, el CCV y en la Nube de Internet:

Elementos de Riesgo

Activo Crítico	Área de Localización	Área de Amenaza	Afectación	Elementos	Nivel de Riesgo
Recursos Humanos	CATD	AE	Aplica	1. Coordinadores	Bajo
		AEN	No Aplica	2. Acopiadores	Bajo
		AFI	Aplica	3. Digitalizadores	Bajo
		AFN	Aplica	3. Digitalizadores	Bajo
	CCV	AE	Aplica	1. Supervisor General	Alto
			Aplica	2. Coordinadores	Medio
			Aplica	3. Verificador/Foliador	Medio
		AEN	No Aplica	4. Capturistas	Bajo
			No Aplica	5. Verificador/Validador	Medio
			Aplica	6. Telefonistas	Bajo
			Aplica	7. Archivistas	Bajo
	AFI	Aplica	8. Organizadores	Bajo	
		Aplica	9. Técnicos	Medio	
Nube de Internet	AE	Aplica	1. Técnicos	Alto	
		No Aplica			
		No Aplica			
		No Aplica			

a) Centros de Acopio y Transmisión de Datos

- Coordinadores:** Representan un nivel Bajo de Riesgo dado que en su ausencia el Acopiador podrán suplir sus funciones.
- Acopiadores:** Se tipificó un Riesgo de nivel Bajo puesto que, en caso de ausentarse, sus funciones podrán ser realizadas por su compañero el Digitalizador o el Coordinador.
- Digitalizadores:** En caso de que no se presentara, la ausencia del Digitalizador representa un nivel de Riesgo Bajo, ya que sus funciones podrán ser realizadas por su compañero el Acopiador o el Coordinador.

b) Centro de Captura y Verificación

1. **Supervisor General:** Este puesto conlleva un nivel de Riesgo Alto, ya que esta persona tiene a su cargo el funcionamiento del CCV.
2. **Coordinadores:** Se deberán contar con un grupo de Coordinadores 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.
3. **Verificador/Foliador:** Ya que esta función en primera instancia es quien recibe e identifica las actas su nivel de riesgo es Medio.
4. **Capturistas:** La confiabilidad de la información depende del personal de Captura, de ahí que el nivel de Riesgo para los mismos es Bajo y deberán implementarse mecanismos para asegurar el buen proceso de la información alimentada por ellos.
5. **Verificador/Validador:** Este es el filtro final antes de la publicación de la información, por lo que su nivel de riesgo es Medio.
6. **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.
7. **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.
8. **Organizadores:** Dadas sus funciones netamente administrativas la falta de alguno no tendría repercusiones serias en el proyecto, por ello su nivel de Riesgo es Bajo.
9. **Técnicos:** Para el caso de los Técnicos el nivel de Riesgo se tipificó como Medio, ya que en caso de ausencia o mal desempeño de los mismos serían suplidos por un compañero de reserva.

c) Nube de Internet

1. **Técnicos:** Este personal, dada su función será Crítico para el desarrollo del proyecto y por ende el nivel de Riesgo que representa es Alto.

- B. Equipamiento:** Aquí detallaremos los niveles de Riesgo para el equipamiento que ha de emplearse en los CATD, el CCV y en la nube de Internet:

Elementos de Riesgo					
Activo Crítico	Área de Localización	Área de Amenaza	Afectación	Elementos	Nivel de Riesgo
Equipamiento	CATD	AEI	Aplica	1. Módem ADSL	Medio
			Aplica	2. Cable Módem	Medio
		AEN	Aplica	3. Módem Banda Ancha Móvil	Medio
			Aplica	4. Teléfonos	Bajo
		AFI	Aplica	5. Computadoras	Alto
			Aplica	6. Scanner	Alto
			Aplica	7. Webcam	Bajo
			Aplica	8. Ups	Bajo
		AFN	Aplica	9. Regulador	Bajo
			Aplica	10. Planta de energía	Alto
	CCV	AEI	Aplica	1. Módem ADSL	Medio
			Aplica	2. Cable Módem	Medio
		AEN	Aplica	3. Teléfonos	Bajo
			Aplica	4. Switches	Bajo
		AFI	Aplica	5. Computadoras	Bajo
			Aplica	6. Video camaras	Bajo
		AFN	Aplica	7. Cañones de Proyección	Bajo
			Aplica	8. Ups	Bajo
		AFN	Aplica	9. Regulador	Bajo
			Aplica	10. Plantas de Energía	Alto
Nube de Internet	AFI	Aplica	1. Servidores	Alto	
		Aplica			
		No aplica			
		Aplica			

a) Centros de Acopio y Transmisión de Datos

- Módems ADSL:** En aquellos Consejos donde la conexión a la red de Internet sea mediante Telmex, el módem ADSL será el medio primario de envío de información, de ahí que su función es de Riesgo Medio.
- Cable Módem:** Donde no se cuente 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 Riesgo Medio.
- Módems Banda Ancha Móvil:** Al ser un medio secundario y redundante su nivel de Riesgo es Medio en cuanto al desempeño de la Red.
- Teléfonos:** Ya que existe cobertura de telefonía Celular en todas las cabeceras municipales el nivel de Riesgo se tipifica en Bajo.

5. **Computadora:** 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 de cómputo en cada CATD y se justifica como de Alto Riesgo.
6. **Scanner:** Conjuntamente al equipo de cómputo, el Scanner representa un elemento crucial en la digitalización de la información, por ello su riesgo es Alto.
7. **Webcam:** El monitoreo por cámara en cada municipio es requerido más no indispensable de ahí que su nivel de riesgo es Bajo.
8. **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 plante de energía auxiliar, por ello su nivel de Riesgo es Bajo.
9. **Regulador:** La buena alimentación de Voltaje eléctrico es indispensable para el funcionamiento de los CATD y los reguladores representan un activo crítico con Bajo Riesgo puesto que se deberán tener suficientes de respaldo.
10. **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.

b) Centro de Captura y Verificación

1. **Módem ADSL:** La primera opción de enlace será mediante el uso de diversos enlaces ADSL de alta velocidad, por ello su nivel de Riesgo es Medio, siempre y cuando existan facilidades de servicio.
2. **Cable Módem:** El Módem para Internet por Cable es el equipo para establecer el enlace secundario redundante a la red de Internet y por ello su nivel de Riesgo es Medio, siempre y cuando existan facilidades de servicio.
3. **Teléfonos:** Ya que existe cobertura de telefonía Celular en todas las cabeceras municipales el nivel de Riesgo se tipifica en Bajo.
4. **Switches:** Se requieren diversos tipos de Switches para conformar la Red Local, y se podrán sustituir por equipo de soporte, por ello su prioridad de Riesgo es Bajo.
5. **Computadoras:** 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.

6. **Video Cámaras:** Las cámaras de video representan un nivel de Riesgo Bajo ya que no son indispensables para funcionamiento continuo del PREP.
7. **Cañones de Proyección:** El uso de los cañones para la exhibición interna de los resultados es de Riesgo Bajo, ya que la misma información estará visible en cualquier equipo conectado a Internet.
8. **UPS:** El uso de las fuentes de poder ininterrumpido no es vital para evitar cortes de alimentación en el voltaje, ya que se contará con plante de energía auxiliar, por ello su nivel de Riesgo es Bajo.
9. **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.
10. **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.
11. **Aire Acondicionado:** Se cuenta con una capacidad de refrigeración de 9.5 toneladas instaladas en el Centro de Captura y Verificación derivado del volumen de personal que estará laborando en las instalaciones para mantener los equipos en una temperatura de trabajo adecuada, evitando el sobrecalentamiento y consecuente baja de rendimiento o fallos de dicho equipo.

c) Nube de Internet

1. **Servidores:** Todos los servidores empleados para el proceso son intrínsecamente indispensables para el funcionamiento del PREP por eso su nivel de Riesgo es Alto.

- B. **Telecomunicaciones:** En cuanto a las telecomunicaciones se identificaron los siguientes elementos:

Elementos de Riesgo					
Activo Crítico	Areas de Localización	Area de Amenaza	Afectación	Elementos	Nivel de Riesgo
Telecomunicaciones	CATD	AEI	Aplica	1.- Línea Telefónica	Medio
		AEN	Aplica	2.-Enlace ADSL	Medio
		AFI	Aplica	3.-Enlace Vía Cable	Medio
		AFN	Aplica	4.-Enlace Banda Ancha Móvil	Bajo
	CCV	AEI	Aplica	1.-Línea Telefónica	Medio
		AEN	Aplica	2.-Enlace ADSL	Alto
		AFI	Aplica	3.-Enlace Vía Cable	Medio
		AFN	Aplica	1.-Enlace Dedicado	Alto
	Nube de Internet	AEI	Aplica	2.-Enlace vía Cable	Medio
		AEN	Aplica		
		AFI	Aplica		
		AFN	Aplica		

a) **Centros de Acopio y Transmisión de Datos**

- Línea Telefónica:** Las líneas telefónicas serán los principales medios de que se emplearán para establecer la comunicación entre los CATD con el CCV, más aún en los sitios donde se emplearán enlaces 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.
- Enlace ADSL:** Donde existan 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.
- Enlace Vía Cable:** Si algún municipio 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.
- Enlace Banda Ancha Móvil:** En todos los municipios donde se tenga 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.

b) Centro de Captura y Verificación

1. **Línea Telefónica:** Desde el CCV se llevará el monitoreo de todos los Centros de Acopio y Transmisión de Datos, esto realizará tanto por vía telefónica como por un sistema dedicado de monitoreo, es por ello que las líneas telefónicas son vitales para este propósito siendo de Medio Riesgo su disponibilidad.
2. **Enlace ADSL:** La conexión principal con la Nube de Internet será primariamente Enlace 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.
3. **Enlace vía Cable:** El enlace redundante secundario para la transmisión y recepción de información será mediante un enlace vía la Compañía de Cable Local, el cual deberá funcionar permanentemente desde su instalación hasta el día posterior a la Jornada Electoral, su prioridad de riesgo es Medio.

c) Nube de Internet

1. **Enlace ADSL:** La conexión principal con la Nube de Internet será primariamente Enlace 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, siempre y cuando existan facilidades de servicio.
2. **Enlace Vía Cable:** El enlace redundante secundario para la transmisión y recepción de información será mediante un enlace vía la Compañía de Cable Local, el cual deberá funcionar permanentemente desde su instalación hasta el día posterior a la Jornada Electoral, su prioridad de riesgo es Medio. Nota se evaluará cuál de los dos medios proporciona el mejor servicio para seleccionar cual será el principal y cuál será el redundante, ya sea ADSL o Cable, siempre y cuando existan facilidades de servicio.

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.

Estrategia de Gestión de Riesgos



De acuerdo con la Identificación de Riesgos, seleccionaremos la estrategia para afrontar cada uno de ellos:

- A. **Recursos Humanos:** Aquí detallaremos al personal que ha de participar en los CATD, el CCV y en la nube de Internet:

Estrategia de Gestión de Riesgos

Activo Crítico	Área de Localización	Área de Amenaza	Afectación	Elementos	Nivel de Riesgo	Estrategia
Recursos Humanos	CATD	AE	Aplica	1 Coordinadores	Bajo	Mitigar
		AEN	No Aplica	2 Acopiadores	Bajo	Mitigar
		AFI	Aplica	3 Digitalizadores	Bajo	Mitigar
		AFN	Aplica			
	CCV	AE	Aplica	1 Supervisor General	Alto	Mitigar
				2 Coordinadores	Medio	Mitigar
			No Aplica	3 Verificador/Foliador	Medio	Mitigar
		AEN	No Aplica	4 Capturistas	Bajo	Mitigar
				5 Verificador/Validador	Medio	Mitigar
			Aplica	6 Telefonistas	Bajo	Mitigar
				7 Archivistas	Bajo	Mitigar
	AFN	Aplica	8 Organizadores	Bajo	Mitigar	
	Nube de Internet	AFN	No Aplica	9 Técnicos	Medio	Mitigar
Alto					Mitigar	
Alto					Mitigar	
Alto					Mitigar	

a) Centros de Acopio y Transmisión de Datos

- Coordinadores:** La contingencia es mitigable ya que, en caso de no presentarse, el Acopiador o el Digitalizador podrá suplir su ausencia.
- Acopiadores:** De no presentarse durante la Jornada, el Digitalizador o el Coordinador podrá mitigar su ausencia asumiendo sus responsabilidades.
- Digitalizadores:** En caso de que no se presentara, se podrá mitigar su ausencia, ya que sus funciones podrán ser realizadas por su compañero el Acopiador o el Coordinador.

b) Centro de Captura y Verificación

- Supervisor General:** Para poder mitigar su ausencia, se deberá prever dicha contingencia con la capacitación de los Coordinadores para asumir sus funciones.

2. **Coordinadores:** Se deberán contar con suficientes Coordinadores para que la ausencia de uno pueda ser mitigada con la ayuda de un similar.
3. **Verificador/Foliador:** Se mitigará la ausencia de alguno capacitando adecuadamente a Capturistas en esta función.
4. **Capturistas:** Previendo la contingencia de ausencia de Capturistas se deberá contar con personal adicional al requerido que mitigará como comodines a los Verificadores y Capturistas.
5. **Verificador/Validador:** Se mitigará la ausencia de alguno capacitando adecuadamente a Capturistas en esta función.
6. **Telefonistas:** En caso de ocurrir la inasistencia de alguna, se mitigará con el auxilio de su Coordinador.
7. **Archivistas:** En caso de no contar con algún archivista, dicha inasistencia podrá ser mitigable con la asistencia de los Organizadores.
8. **Organizadores:** Si no se contara con alguno de los Organizadores, se mitigará su falta con el auxilio de una Archivista.
9. **Técnicos:** Dado lo crítico de sus funciones, 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.

c) Nube de Internet

1. **Técnicos:** Previendo la ausencia de alguno de estos técnicos, se mitigará con la presencia de técnicos de reserva, contando con el nivel de experiencia requerido.

- B. **Equipamiento:** Aquí detallaremos los niveles de Riesgo para el equipamiento que ha de emplearse en los CATD, el CCV y en la nube de Internet:

Estrategia de Gestión de Riesgo						
Activo Crítico	Areas de Localización	Area de Amenaza	Afectación	Elementos	Nivel de Riesgo	Estrategía
Equipamiento	CATD	AEI	Aplica	1.Módem ADSL	Medio	Mitigar
			Aplica	2.Cable Módem	Medio	Transferir
		AEN	Aplica	3.Módem Banda Ancha Móvil	Medio	Mitigar
			Aplica	4.Teléfonos	Bajo	Mitigar
		AFI	Aplica	5.Computadoras	Alto	Mitigar
			Aplica	6.Scanner	Alto	Mitigar
		AFN	Aplica	7.Webcam	Bajo	Mitigar
			Aplica	8.Ups	Bajo	Mitigar
			Aplica	9.Regulador	Bajo	Mitigar
			Aplica	10.Planta de energía	Alto	Mitigar
	CCV	AEI	Aplica	1.Módem ADSL	Medio	Mitigar
			Aplica	2.Cable Módem	Medio	Transferir
		AEN	Aplica	3.Teléfonos	Bajo	Mitigar
			Aplica	4.Switches	Bajo	Mitigar
		AFI	Aplica	5.Computadoras	Bajo	Mitigar
			Aplica	6.Video camaras	Bajo	Mitigar
		AFN	Aplica	7.Cañones de Proyección	Bajo	Mitigar
			Aplica	8.Ups	Bajo	Mitigar
			Aplica	9.Regulador	Bajo	Mitigar
			Aplica	10.Plantas de Energía	Alto	Mitigar
Nube de Internet	AEI	Aplica	1.Servidores	Alto	Transferir	
	AEN	Aplica				
	AFI	No aplica				
	AFN	Aplica				

a) **Centros de Acopio y Transmisión de Datos**

- Módems ADSL:** Previendo la falla en alguno de estos equipos, se mitigará la posible falla de alguno solicitando con anticipación equipos de respaldo para ser sustituidos de forma inmediata.
- Cable Módem:** Previendo la falla en alguno de estos equipos, se transferirá al proveedor la posible falla de alguno, solicitando su reposición inmediata, contando con equipo suficiente de respaldo para esta contingencia y mitigarlo de forma inmediata.
- Módem Banda Ancha Móvil:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.

4. **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.
5. **Computadoras:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
6. **Scanner:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
7. **Webcam:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
8. **Ups:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
9. **Regulador:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
10. **Planta de Energía:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.

b) Centro de Captura y Verificación

1. **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 y mitigarlo de forma inmediata.
2. **Cable Módem:** Previendo la falla en alguno de estos equipos, se transferirá al proveedor la posible falla de alguno, solicitando su reposición inmediata, contando con equipo suficiente de respaldo para esta contingencia y mitigarlo de forma inmediata.
3. **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.

4. **Switches:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
5. **Computadoras:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
6. **Video Cámaras:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
7. **Cañones de Proyección:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
8. **Ups:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
9. **Reguladores:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
10. **Plantas de Energía:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.

c) Nube de Internet

1. **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 redundantes para esta contingencia.

C. **Telecomunicaciones:** En cuanto a las telecomunicaciones se identificaron los siguientes elementos:

Estrategia de Gestión de Riesgos						
Activo Crítico	Areas de Localización	Area de Amenaza	Afectación	Elementos	Nivel de Riesgo	Estrategía
Telecomunicaciones	CATD	AEI	Aplica	1.Línea Telefónica	Medio	Transferir
		AEN	Aplica	2.Enlace ADSL	Medio	Transferir
		AFI	Aplica	3.Enlace vía cable	Medio	Transferir
		AFN	Aplica	4.Enlace Banda Ancha Móvil	Bajo	Mitigar
	CCV	AEI	Aplica	1.Línea Telefónica	Medio	Transferir
		AEN	Aplica	2.Enlace ADSL	Alto	Transferir
		AFI	Aplica	3.Enlace vía cable	Medio	Transferir
		AFN				
	Nube de Internet	AEI	Aplica	1.Enlace Dedicado	Alto	Transferir
		AEN	Aplica			
		AFI	Aplica	2.Enlace Vía Cable	Medio	Transferir
		AFN	Aplica			

a) **Centros de Acopio y Transmisión de Datos**

- Línea Telefónica:** De presentarse fallas en las líneas se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usarán líneas celulares.
- Enlace ADSL:** De presentarse fallas en los servicios se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usarán conexiones de Banda Ancha Móvil.
- Enlace Vía Cable:** De presentarse fallas en los servicios se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usarán conexiones Banda Ancha Móvil.
- Conexión Banda Ancha Móvil:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia, siendo los comandos técnicos quienes tendrán un equipo de banda ancha móvil a su disposición para proveerlo en caso de ser necesario.

b) **Centro de Captura y Verificación**

- Línea Telefónica:** De presentarse fallas en las líneas se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usarán líneas celulares.

2. **Enlace ADSL:** De presentarse fallas en el servicio se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se emplearán otro enlace redundante o el enlace Vía Cable.
3. **Enlace Vía Cable:** De presentarse fallas en el servicio se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usará el Enlace ADSL.

c) Nube de Internet

1. **Enlace ADSL:** De presentarse fallas en el servicio se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se emplearán El enlace Vía Cable.
2. **Enlace Vía Cable:** De presentarse fallas en el servicio se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usará la el Enlace ADSL.

Plan de Seguridad.

Introducción

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

$$\text{riesgo} = (\text{amenaza} * \text{vulnerabilidad}) / \text{contramedida}$$

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.

Objetivos

El desarrollo del presente plan de seguridad tiene como objetivo la identificación de los recursos críticos para la operación del PREP, así como la estimación del impacto e identificación de las consecuencias de la materialización de las amenazas aquí descritas.

Asimismo, se deberán identificar los controles que actualmente se tienen implementados y que serán los que coadyuven en la mitigación de los riesgos.

En esta virtud se deberá dar a conocer el contenido de este documento a la totalidad del personal técnico operativo que conforma el proyecto de acuerdo a lo descrito en el **Anexo I** denominado "*Plan de Concientización*"

Bases de la seguridad informática

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

- I. **Confidencialidad.** - La confidencialidad consiste en hacer que la información sea ininteligible para aquellos individuos que no estén involucrados en la operación.
- II. **Integridad.** - La verificación de la integridad de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente).
- III. **Disponibilidad.** - El objetivo de la disponibilidad es garantizar el acceso a un servicio o a los recursos.
- IV. **Evitar el rechazo.** - Evitar el repudio de información constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada.
- V. **Autenticación.** - La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite (por ejemplo, gracias a una contraseña codificada) garantizar el acceso a recursos únicamente a las personas autorizadas.

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**
- D. **Aplicativo PREP Casilla**

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

A. 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 deberá contar con vehículo y chofer, y en el vehículo deberá cargar 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 contará 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 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.

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

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.

a) Recursos Humanos

Una de las medidas de seguridad requeridas por el PREP es que, a partir del funcionamiento 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 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.

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 a cualquier CATD.

Durante la Jornada Electoral se le requerirá 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 negará el acceso a cualquier persona que se presente al CATD.

1. **Coordinadores:** Se preverá que, en caso de falla en su asistencia, el Acopiador o el Digitalizador, por lo que deberán dominar las actividades del mismo para suplir su inasistencia.
2. **Acopiadores:** Igualmente se deberá contar con un plan emergente para que, en caso de no asistir esta persona, su compañero el Digitalizador o el Coordinador pueda suplir la ausencia del mismo.
3. **Digitalizadores:** En caso de no asistir deberán contar con una persona que pueda suplir sus funciones pudiendo ser un Acopiador o el Coordinador.

b) Equipamiento

Como parte de la seguridad requerida, cada CATD deberá contar con una cámara de web. Dicha cámara deberá grabar 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 podrán ser observadas en tiempo real mediante un Sistema de Monitoreo que se instalará en el CCV, en el cual podrá observarse la actividad en todos y cada uno de los CATD.

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.

Como medida de seguridad a los CATD, se deberá enviar 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 en caso de falla de energía eléctrica, provista por la Comisión Federal de Electricidad.

c) Telecomunicaciones

En igual forma como medida de protección para el equipamiento electrónico y de Telecomunicaciones que se usará en los CATD, se les deberá instalar un Regulador de Voltaje que protegerá al equipo del PREP contra posibles variaciones de voltaje.

Las telecomunicaciones deberán contemplar 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 deberá ser reportada de inmediato al CCV del PREP para que se implementen las medidas emergentes necesarias.

Igualmente se deberá implementar una Bitácora que dé 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.

B. Centro de Captura y Verificación

Al igual que los CATD, en el CCV se deberán contemplar 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 del CCV, se cuente con personal de Seguridad proporcionado por el Instituto Estatal Electoral de Baja California Sur, que no sólo vigile el área del interior del PREP, sino que hagan vigilancia perimetral.

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 se realizará el enrolamiento de su huella digital en el sistema checador ubicado a la entrada del inmueble, por lo que en caso de no contar con identificación o de que su huella no se encuentre registrada, el elemento de seguridad encargado del control de acceso le negará la entrada.

De igual manera, durante la jornada electoral se solicitará el apoyo de las corporaciones de seguridad pertinentes para contar con personal adicional que proporcione una mayor seguridad al equipamiento y recursos humanos contando con capacidad suficiente para contener manifestaciones o aglutinamientos públicos que pudieran suponer un riesgo físico intencional que pretenda impedir los trabajos, manteniendo siempre como prioridad la integridad física del personal que laborará en el PREP, así como el personal encargado de la seguridad misma, quien contará con el equipamiento y la cadena de mando pertinente que será la encargada de tomar la decisión, de acuerdo a sus capacidades, de la cantidad de gente que pudiera ser contenida, así como el nivel de agresividad con la que pudieses lidiar, por lo que en el caso de que los elementos de la fuerza pública fuesen superados se ordenaría al personal de PoderNet detener la operación y retirarse de manera ordenada de acuerdo al "Plan de Emergencias y Evacuación" previamente mencionado, realizando la migración del CCV a una sede alterna que sería habilitada en otro CCV que esté siendo operado por la empresa, conservando el avance de captura que se tenía hasta el momento de la interrupción.

En caso de existir riesgo de impacto de algún fenómeno meteorológico será la entidad de Protección Civil responsable en la entidad quien indique si se podrán realizar las labores concernientes al total de la elección o si debieran ser pospuestas en su totalidad, como lo sería el caso de un huracán o tormenta tropical. Si el fenómeno en cuestión no puede ser previsto se deberá hacer una valoración de los activos y ante algún indicio de riesgo se decidirá sobre la factibilidad de migrar el equipo a una sede alterna que sería facilitada por el OPLE y en caso de no ser posible se decidirá sobre la migración de las labores a un CCV alterno que se encuentre en operación por parte de la empresa.

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

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

a) Recursos Humanos

- 1. Supervisor General:** Instrumentará un “*Plan de Emergencias y Evacuación*” (**Anexo II**) y realizará simulacros, verificará que la señalética se encuentre debidamente localizada, incluyendo extintores, salidas de emergencia, etc. Verificará con los responsables de seguridad del inmueble que sólo personal autorizado tenga acceso al mismo, nombrará 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.
- 2. Coordinadores:** Serán capacitados en el control del personal a su cargo y por ello serán los encargados de implementar los planes de evacuación y emergencia que se instrumenten para el 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. Capturistas:** Para poder llevar un control efectivo de la información que alimentan los capturistas al sistema, se asignarán claves personales de acceso a cada 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.

5. **Verificador/Validador:** Como última medida de revisión de la captura se contará con Validadores que revisarán todas las actas que se detecten con inconsistencias para que con la autorización de su Coordinador sean procesadas y subidas a Internet.
6. **Telefonistas:** Tendrán a la mano los teléfonos de emergencia para contingencias, para en caso de cualquier eventualidad, puedan 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 de Baja California Sur
 - ✓ CATD's
7. **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.
8. **Organizadores:** Los organizadores serán los 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.
9. **Técnicos:** 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 atenderlas de inmediato.

Su función adicional de los Técnicos, 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.

b) Equipamiento

Como parte de la seguridad requerida, el CCV deberá contar con cámaras de vigilancia. Dichas cámaras deberán grabar la actividad registrada en las áreas del CCV para que en caso de que se presente alguna anomalía, ésta quede registrada en video.

Dichas cámaras serán observadas mediante un Sistema de Monitoreo al que tendrá acceso el Supervisor General del PREP, en el cual podrá observarse la actividad en todas y cada uno de las áreas del CCV en tiempo real, dejando evidencia almacenada en un DVR para su posterior consulta en caso necesario.

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.

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.

c) Telecomunicaciones

De la totalidad de los servicios instalados como:

1. **Líneas Telefónicas**
2. **Enlace ADSL**
3. **Enlace Vía Cable**

Se deberán contemplar las siguientes medidas de seguridad:

1. **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.
2. **Enlace ADSL.** Se podrá contratar un segundo Enlace ADSL por diferentes vías, para que en caso de fallo en uno se utilice otro. Como medida adicional de redundancia se contratará por lo menos un Enlace Vía Cable.
3. **Enlace Vía Cable.** Se deberá contar 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, siempre y cuando existan facilidades en el sitio.

C. Nube de Internet

a) Recursos Humanos

1. **Técnicos:** 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, los técnicos en conjunto la resuelvan de inmediato, por ende, deberán contar con personal de respaldo.

b) Equipamiento

1. **Servidores:** Para proteger el funcionamiento continuo del Programa de Resultados Electorales Preliminares en su conjunto, se deberán contar 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 podrán contratar dos Enlace ADSL de alta velocidad por diferentes vías, para que en caso de fallo en uno se utilice otro. Como medida adicional de redundancia se contratará por lo menos un Enlace Vía Cable.
2. **Enlace Vía Cable.** Se podrá contar 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, siempre y cuando existan facilidades en el sitio.

D. Aplicativo PREP Casilla

a) Telecomunicaciones

1. **Enlace 3G/4G.** Se contratará un plan de datos que permita la conectividad a Internet de la red celular, en caso de que no exista un enlace disponible se almacene la imagen capturada en el equipo hasta que se establezca una conexión que permita hacer el envío de forma automática.

Plan de Continuidad

Introducción

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.

Objetivos

Como parte de los trabajos orientados Asegurar la continuidad de la operación del Programa de Resultados Electorales Preliminares en caso de que se presente una contingencia que pudiese poner en riesgo cualquiera de los activos críticos del PREP.

De igual manera, el presente documento se hará del conocimiento de la totalidad del personal mediante los procedimientos establecidos en el **Anexo I** denominado "*Plan de Concientización*", permitiendo de esta forma contar con personal capacitado para reaccionar con serenidad y prontitud ante una eventualidad.

Asimismo, se tiene contemplado realizar un simulacro de *failover* durante el Tercer Simulacro del PRERP, de acuerdo a lo descrito en el mismo, adjunto al presente identificado como **Anexo III** – "*Plan de Simulacros*", mediante la recreación de una falla en el suministro de la energía eléctrica en el CCV y los CATD's que cuenten con un comando técnico de cabecera.

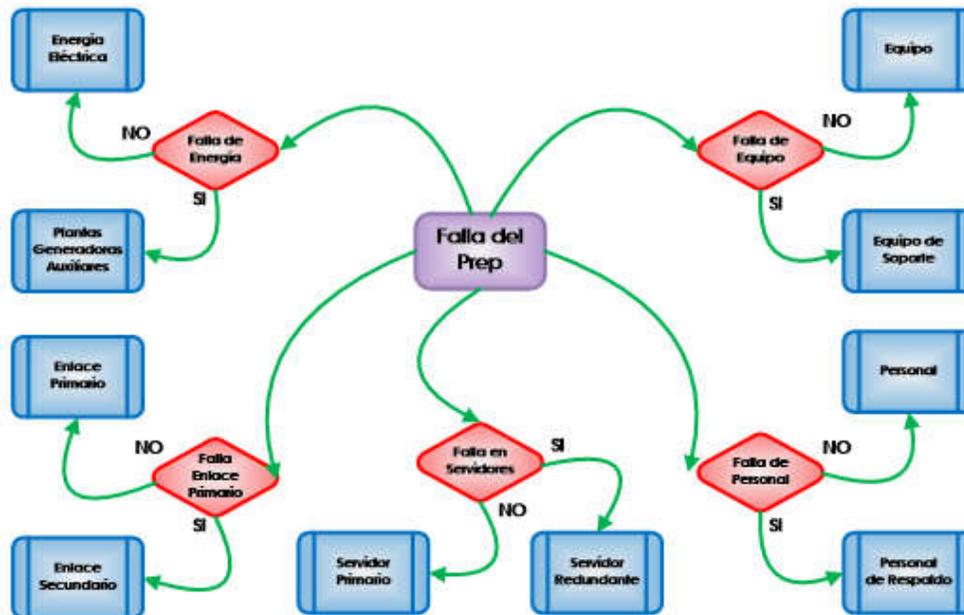
Metodología

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. Aplicativo PREP Casilla**

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

Esquema de Contingencia en Caso de Fallas del PREP



A. Centros de Acopio y Transmisión de Datos

Las medidas a implementarse en este plan se avocan en los siguientes Activos Críticos:

- a) **Recursos Humanos**
- b) **Equipamiento**
- c) **Telecomunicaciones**

En los CATD se llevarán a cabo los procesos de Acopio, Digitalización y Transmisión de las imágenes digitalizadas de las Actas de Escrutinio y Cómputo para cada una de la elección de Diputados Locales y Ayuntamientos a llevarse a cabo en el presente Proceso Electoral Local Ordinario 2017-2018 por el Instituto Estatal Electoral de Baja California Sur.

a) **Recursos Humanos**

En caso de fallas en los Recursos Humanos, Equipamiento o Telecomunicaciones, se hará el reporte inmediato del mismo al CCV del PREP para que se ejecuten las siguientes medidas:

A partir de las 17:00 horas del día de la Jornada Electoral, todo el personal del PREP a nivel estatal se presentará a cumplir sus funciones.

Las telefonistas que operan en el Centro de Llamadas del CCV, harán el pase de lista a los CATD, si se detectan faltantes de personal, se realizarán las siguientes medidas:

1. **Acopiador:** En caso de Inasistencia del Acopiador, se le instruirá al Digitalizador para que realice ambas funciones.
2. **Digitalizador:** En caso de Inasistencia del Digitalizador, se le instruirá al Acopiador para que realice ambas funciones.
3. **Coordinador:** En caso de Inasistencia del Coordinador, se le instruirá al Acopiador ó al Digitalizador para que realice ambas funciones.

En caso de Inasistencia de dos o más personas, se le instruirá al Personal de Soporte Técnico que cubra esa zona, para que del CATD más cercano, traslade a un Acopiador o Digitalizador hasta el CATD en cuestión y con ello se corrija la contingencia.

b) Equipamiento

En el momento que se reciba reporte o se detecte malfuncionamiento del equipamiento, o de algún elemento del equipamiento o por la recepción de un reporte de fallas desde algún CATD, en primera instancia el Centro de Llamadas transferirá la llamada un técnico de guardia en el CCV quien remotamente tratará de darle solución a la falla.

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.

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.

En casos de falla de energía eléctrica, se le instruirá al personal del CATD para que manualmente ponga en funcionamiento la planta de energía portátil que les fue instalada, misma que deberá contar con gasolina previamente cargada en su tanque y que deberá encenderse según los procedimientos explicados durante la capacitación y que estarán disponibles mediante ayuda visual colocada en el embalaje de las mismas para previamente proceder a la conexión de una extensión de corriente previamente proporcionada, a la cuál deberán ser conectados los reguladores que se encuentren en el equipamiento del CATD en cuestión, por ser estos los concentradores de las conexiones de los UPS que a su vez concentran la totalidad de los equipos electrónicos que conforman la estación de trabajo.

c) Telecomunicaciones

En caso de fallas en las telecomunicaciones en el medio de transmisión primario, el sistema se switcheará al medio de transmisión redundante de manera automática estando ya conectado el dispositivo en el equipo de digitalización, el cual consistirá de un enlace de banda ancha, mismo que deberá haber sido previamente configurado y probado para continuar transmitiendo. Se levantará un reporte con el proveedor del servicio para que sea atendido a la brevedad posible y se le dará seguimiento a su pronta solución.

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.

B. Centro de Captura y Verificación

Para el CCV se implementarán medidas de continuidad en los siguientes activos:

a) Recursos Humanos

b) Equipamiento

c) Telecomunicaciones

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:

Recursos Humanos

- 1. Supervisor General:** 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 los Coordinadores del área en cuestión, realizará los ajustes al personal requeridos. En caso de que se deba ausentar de sus funciones el Supervisor General, los Coordinadores previamente capacitados para ello suplirán las mismas.
- 2. Coordinadores:** En caso de detectar cualquier problema de salud en el personal, lo llevará al área de servicios médicos 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. En caso de que requiera ausentarse de sus funciones, el

Supervisor General requerirá a otro Coordinador disponible que supla esta eventualidad.

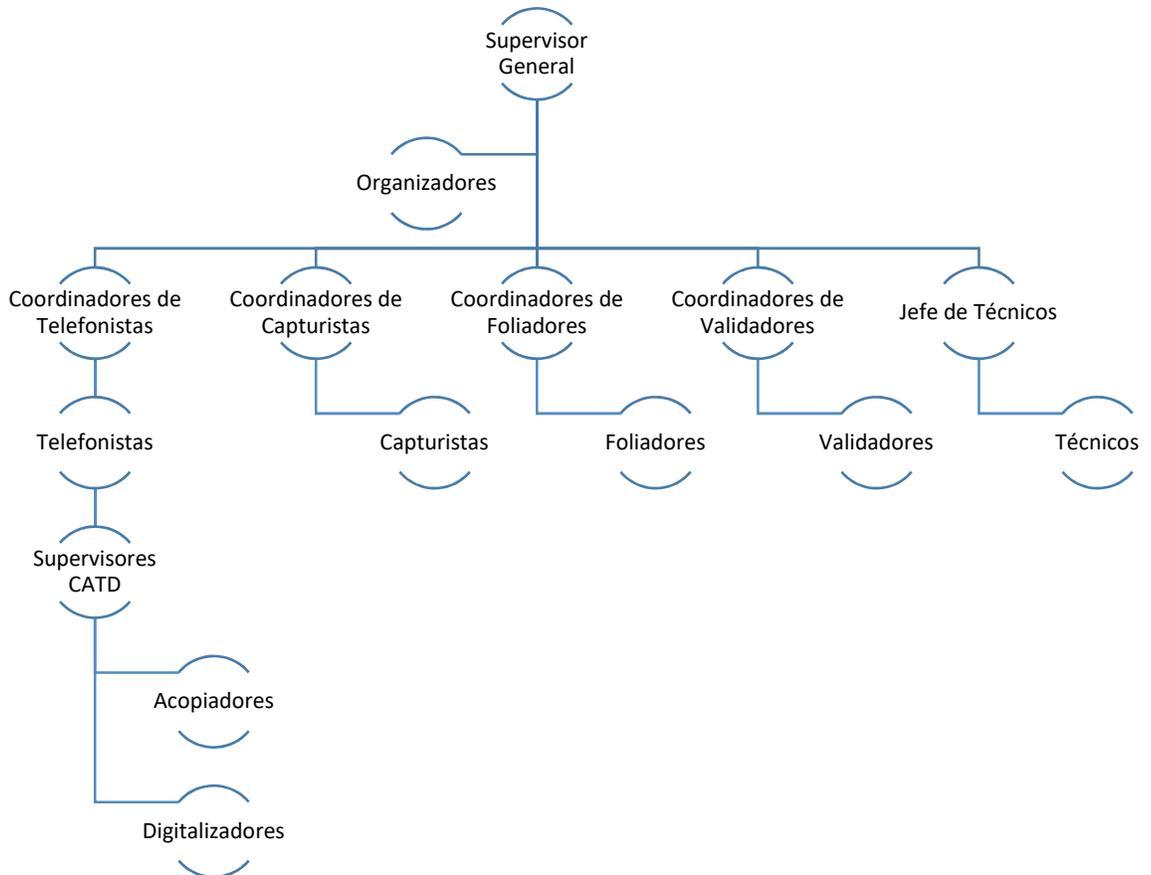
3. **Verificador/Foliador:** Cuando falte algún miembro de esta área, se tomará un Capturista de reserva para que supla sus funciones; igualmente se realizará este procedimiento en caso de presentarse problemas de salud en uno de estos elementos.
4. **Capturistas:** En caso de detectar inasistencia en un Capturista se 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 Coordinador para que este le canalice y se le brinde la atención requerida.
5. **Verificador/Validador:** Si no se presenta alguna persona de esta área, se tomará a un 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.
6. **Telefonistas:** En caso de cualquier emergencia, de acuerdo a las instrucciones de su Coordinador, 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 Coordinador para que este le canalice y se le brinde la atención requerida. En caso de inasistencia el Coordinador balanceará las cargas de trabajo entre las demás telefonistas.
7. **Archivistas:** Ayudarán a los Coordinadores 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 un Organizador.
8. **Organizadores:** Se deberán preparar simulacros de evacuación para en caso de una contingencia mayor, evacuar al personal. Se coordinarán con los Coordinadores de personal y los servicios médicos para tener a la mano el botiquín de emergencias. Si se presenta inasistencia de alguno o tienen problemas médicos, serán ayudados por los Archivistas.
9. **Técnicos:** Se contará con técnicos 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 cualquiera de sus CATD asignados y ejecuten el plan correspondiente, de acuerdo a la siguiente distribución de los comandos por ciudad:
 - Guerrero Negro: 1
 - Santa Rosalía: 1
 - Loreto: 1
 - Ciudad Constitución: 1
 - La Paz: 1

- Cabo San Lucas: 1
- San José del Cabo: 1

En caso de una contingencia mayor como sismo o incendio, se deberá ejecutar el “Plan de Emergencias y Evacuación”, adjunto al presente documento e identificado como **Anexo II** que previamente se habrá implementado y ejercitado, con el propósito de salvaguardar la integridad del personal en primera instancia.

Dentro de 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.

En este respecto se definirán los canales de comunicación para el personal de acuerdo al siguiente diagrama:



b) Equipamiento

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:

- ✓ **Computadoras**
- ✓ **Teléfonos**
- ✓ **Cámaras**
- ✓ **Switches**
- ✓ **Cableado**
- ✓ **Ups y Reguladores**
- ✓ **Cañones**
- ✓ **Plantas de Energía**

Se deberán reemplazar de inmediato por un equipo del mismo tipo previamente probado y configurado para las funciones que se requieran.

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. Cabe mencionar que el generador que se utilizará para el CCV será arrancado de manera manual cuando se requiera mediante el sistema de llave con que cuenta, para posteriormente conectarla al circuito eléctrico mediante el cable disponible para este propósito, el cuál estará conectado al interruptor de doble tiro que se utilizará como último paso del proceso de activación para seleccionar el suministro eléctrico.

c) Telecomunicaciones

De la totalidad de los servicios instalados como:

1. **Líneas Telefónicas**
2. **Enlace ADSL**
3. **Enlace Vía Cable**

Se deberán contemplar las siguientes medidas de contingencia:

1. **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 en caso de emergencia puedan establecer comunicación.

En caso de fallas en las líneas telefónicas del CCV se deberá recurrir a líneas de teléfono celulares como plan emergente.

2. Enlace ADSL

El Enlace primario de recepción y transmisión de la información será la conexión a Internet por Enlace ADSL, más si esta igualmente fallara, se deberán contar con por lo menos otro Enlace ADSL alternativo que servirá para enlazarse como medio de contingencia. En caso de falla total de estos servicios se switcheará al Enlace Vía Cable en caso de existir facilidades para su contratación.

3. Enlace Vía Cable

Si fallase el enlace primario de comunicación que es el Enlace ADSL de Alta velocidad, se switcheará al Enlace Vía Cable mientras se resuelve la falla del Enlace ADSL. Se contará por lo menos con dos Enlaces Vía Cable, en caso de existir facilidades como redundancia, para que en caso de que fallara el primer Enlace Vía Cable, se switcheará al servicio del siguiente Enlace Vía Cable.

C. Nube de Internet

a) Recursos Humanos

1. **Técnicos:** Se deberá contar con Personal de Soporte Técnico especializado para el monitoreo de la publicación de la información en la Nube de Internet.

Se deberá contar con Personal Técnico tanto por parte de la empresa responsable del PREP, como preferentemente de la empresa que provee la señal de Internet en sitio.

b) Equipamiento

1. **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 redundante de respaldo el cual en caso de falla en cualquier servidor primario, el redundante se activará para evitar interrupciones en flujo de la información.

c) Telecomunicaciones

Para asegurar el poder contar con señal permanente de Internet, se contará con:

1. Enlace ADSL

El Enlace primario de recepción y transmisión de la información será la conexión a Internet por Enlaces ADSL de alta velocidad, más si esta igualmente fallara, se deberán contar con por lo menos otro Enlace ADSL alternativo que servirá para enlazarse como medio de contingencia. En caso de falla total de estos servicios se switcheará al Enlace Vía Cable en caso de existir facilidades para su contratación.

2. Enlace Vía Cable

Si fallase el enlace primario de comunicación que es el Enlace ADSL, se switcheará al Enlace Vía Cable mientras se resuelve la falla del Enlace ADSL. Se contará por lo menos con dos Enlaces Vía Cable, en caso de existir facilidades como redundancia, para que en caso de que fallara el primer Enlace Vía Cable, se switcheará al servicio del siguiente Enlace Vía Cable.

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.

D. Aplicativo PREP Casilla

a) Telecomunicaciones

1. **Enlace 3G/4G.** En caso de que existiera una falla en el enlace a Internet de la red celular, ya sea por falta de cobertura u otra razón, el o las actas digitalizadas se almacenarán en el dispositivo hasta que el mismo disponga de un enlace activo que permita el envío automático. De igual forma, aunque no exista una conexión a Internet activa, el aplicativo permitirá realizar nuevas digitalizaciones, siempre y cuando el usuario haya iniciado su sesión con anterioridad en el sistema.

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

Comandos Técnicos

Habrán Comandos Técnicos localizados estratégicamente en el Estado, los cuales llevarán vehículo, 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. Cada comando cuenta adicionalmente con todas las herramientas necesarias para su labor, incluyendo botiquines, teléfonos celulares, cables, mapas, hojas de instrucciones, manuales, etc. Dichos comandos se desplegarán de acuerdo a la siguiente distribución geográfica:

- Guerrero Negro: 1
- Santa Rosalía: 1

- Loreto: 1
- Ciudad Constitución: 1
- La Paz: 1
- Cabo San Lucas: 1
- San José del Cabo: 1

Coordinación con la Gerencia de Desastres Telmex

Dada la importancia de la Red y la relación de PoderNet con Telmex, se podrá contar con el apoyo del Área de Desastres para coordinar medidas adicionales de Seguridad en la Red de Datos, entre las que se cuentan:

Los apoyos proporcionados por parte del Área de Desastres de Telmex son los siguientes:

- Personal de Soporte en Sitio para resolución de fallas, tanto en las Centrales de Telmex en el interior del Estado como en el CCV del PREP.
- Vehículos y personal con equipamiento y herramientas para atención inmediata de fallas.
- Número directo para reporte de fallas de los servicios en el CAS.
- Sellado de Distritos en su infraestructura para evitar sabotajes.
- Personal Directivo de Telmex tanto en el CCV como en la Sala de Consejo del OPL.



ANEXO I

Plan de Concientización

Derivado del análisis de riesgos a la seguridad de los activos que componen la totalidad de la operación del PREP se ha generado un Plan de Seguridad y de Continuidad en los que se contemplan los distintos escenarios de fallos que pudieran suscitarse durante el día de la jornada electoral, así como las acciones que se deberán llevar a cabo para mitigar, transferir, aceptar o eliminar los riesgos, así como los mecanismos que permitirán mantener la operación de dicho programa, garantizando la su completa ejecución.

En esta virtud, será de máxima importancia realizar diversas acciones tendientes a concientizar y sensibilizar al personal que forma parte del presente proyecto, entre las cuales se tienen los siguientes

Objetivos:

1. Dar a conocer al personal los riesgos existentes que pudiesen poner en peligro la operación del PREP, así como las medidas de seguridad que ha considerado la empresa para el tratamiento de los mismos y las acciones que se deberán llevar a cabo en caso de que se presente alguna de estas situaciones.
2. Poner en práctica los planes simulando contingencias previo a la fecha de la jornada electoral para lograr una mayor asimilación de los procedimientos establecidos.
3. Realizar ensayos del plan de evacuación incorporados durante el periodo de capacitación diaria.

Acorde a los objetivos planteados se determinó incluir una presentación del análisis de riesgos y los planes de Seguridad, Continuidad y Evacuación durante el curso de inducción a la totalidad del personal de nuevo ingreso, misma que será reforzada durante los días subsecuentes

mediante la simulación de la aparición de diversos riesgos, así como la inclusión de éstos en el Plan de Simulacros oficial, que se pondrá en marcha los tres domingos previos a la jornada de acuerdo a los lineamientos del Instituto Nacional Electoral.

Con estas acciones se espera conseguir una correcta asimilación de los procesos descritos en los multicitados documentos con lo que se espera que, en caso de existir alguna situación extraordinaria que ponga en riesgo el Programa de Resultados Electorales Preliminares, se obtenga una respuesta inmediata, profesional y ordenada por parte del personal, logrando así mitigar en tiempo y forma las amenazas presentadas, salvaguardando a la vez la seguridad del personal y la integridad de la información que será procesada por la empresa.



ANEXO II

PLAN DE EMERGENCIAS Y EVACUACIÓN

CONTENIDO

1. POLÍTICA
2. ALCANCE
3. MARCO DE REFERENCIA
4. OBJETIVOS
5. IDENTIFICACIÓN DE LA EMPRESA
6. ESTRUCTURA ORGANIZACIONAL PARA LA PREVENCIÓN Y ATENCIÓN DE EMERGENCIAS
 - 6.1 Organización para el manejo de emergencias
 - 6.2 Administración del plan de emergencia
 - 6.3 Comité de Emergencia
 - 6.4 Responsabilidades del comité de emergencias
 - 6.5 Brigada de emergencia
 - 6.6 Coordinadores de evacuación
7. ACTUALIZACIÓN DEL PLAN DE EMERGENCIAS
8. PLAN DE EVACUACIÓN
 - 8.1 Rutas de Evacuación
 - 8.2 Avisos de Emergencia y orden de Evacuación
 - 8.3 Sitios de conteo o reunión final (Punto de Encuentro)
 - 8.4 Proceso de evacuación
 - 8.5 Zonas de Evacuación
 - 8.6 Normas de Evacuación para visitantes y personal ajeno a la institución
 - 8.7 Alarma de evacuación
 - 8.8 Comportamiento en el punto de reunión final
 - 8.9 Procedimiento para retornar a los sitios de trabajo
9. PROTOCOLO GENERAL DE EMERGENCIAS
10. INVESTIGACIÓN, EVALUACIÓN DE LA EMERGENCIA Y AUTOEVALUACIÓN DEL PLAN DE EMERGENCIA
11. COMUNICACIONES Y FUNCIONES
12. ACCIONES A REALIZAR
 - 12.1 Plan de actividades formativas

1. POLÍTICA

Establecer planes de prevención, rutas de evacuación y preparación para emergencias que tengan en cuenta las necesidades laborales y superen las exigencias legales. Para generar un verdadero desarrollo a las organizaciones, propendiendo de la calidad y seguridad de PODERNET, sede en La Paz Baja California Sur.

2. ALCANCE

El Plan de Emergencia ha sido diseñado para dar respuesta inicial a sucesos repentinos no deseados, cubre todas las áreas, actividades productivas, personal propio y visitantes, éste contempla la asistencia de organismos de socorro o de apoyo externo como Bomberos, Cruz Roja, Entidades Prestadoras de Servicios de Salud y otras relacionadas con la atención de emergencias para el control total de los sucesos ocurridos.

3. MARCO DE REFERENCIA

3.1 MARCO CONCEPTUAL

Activos Críticos: Son los elementos claves para el funcionamiento del PREP, se tipificarán de acuerdo a su naturaleza, en tres áreas:

- a) **Recursos Humanos**
- b) **Equipamiento**
- c) **Telecomunicaciones**

Alarma: Aviso o señal que se da para que se sigan instrucciones específicas, debido a la presencia real o inminente de un evento adverso.

Alerta: Señal o aviso que advierte la existencia de un peligro.

Amenaza: Peligro latente asociado con un fenómeno físico de origen natural, de origen tecnológico o provocado por el hombre que puede manifestarse en un sitio específico y en un tiempo determinado, produciendo efectos adversos en las personas, los bienes, servicios y el medio ambiente. Técnicamente se refiere a la probabilidad de ocurrencia de un evento con una cierta intensidad, en un sitio específico y en un periodo de tiempo determinado.

APH: Atención Pre-Hospitalaria.

Consecuencias: Alteración del estado de salud de las personas y los daños materiales que resultan de la exposición al factor de riesgo.

Control: Acción de eliminar o limitar el desarrollo de un siniestro, para evitar o minimizar sus consecuencias.

Desastre: Alteraciones intensas en las personas, los bienes, los servicios y el medio ambiente, causadas por un suceso natural o generado por la actividad humana, que exceden la capacidad de respuesta de la comunidad afectada.

Emergencia: Toda situación generada por la ocurrencia real o inminente de un evento adverso, que requiere de una movilización de recursos sin exceder la capacidad de respuesta.

Escenario: Descripción de un futuro posible y de la trayectoria asociada a él.

Evacuación: Es el conjunto integral de acciones tendientes a desplazar personas de una zona de mayor amenaza a otra de menor peligro.

Impacto: Acción directa de una amenaza o riesgo en un grupo de personas.

Mitigación: Acción desarrollada durante o después de un siniestro, tendiente a contrarrestar sus efectos críticos y asegurar la supervivencia del sistema, hasta tanto efectúe su recuperación.

Nivel estratégico: Estamento de una estructura del plan de emergencia responsable de coordinar las diferentes funciones de emergencia. Su papel consiste en definir QUE HACER, debe ser desempeñado por una sola persona cada vez, correspondiendo al cargo de "Coordinador de Emergencia".

Nivel de Tarea: Estamento de una estructura del Plan de Emergencia responsable de ejecutar las diferentes acciones de emergencia. Su papel consiste en HACER mediante el uso de recursos de emergencias, debe ser desempeñado por tantas personas como sean necesarias.

Nivel Táctico: Estamento de una estructura del Plan de Emergencia responsable de Coordinar los diferentes recursos de emergencia. Su papel consiste en definir COMO HACERLO puede ser desempeñado por varias personas simultáneamente (una por función) tal como jefe de brigada, jefe de atención médica, coordinador general de evacuación, etc.

Plan de Emergencias: Definición de políticas, organizaciones y métodos, que indican la manera de enfrentar una situación de emergencia o desastre, en lo general y en lo particular, en sus distintas fases.

Preparación: Tiempo transcurrido desde que se comunica la decisión de evacuar, hasta que empieza a salir la primera persona.

Prevención: Conjunto de acciones cuyo objeto es impedir o evitar que sucesos naturales, tecnológicos o generados por la actividad humana, causen desastres.

Recuperación: Actividad final en el proceso de respuesta a una emergencia. Consiste en restablecer la operatividad de un sistema interferido.

Respuesta: Acciones llevadas a cabo ante un evento adverso y que tienen por objeto salvar vidas, reducir el sufrimiento humano y disminuir pérdidas.

Riesgo: Es definido como la probabilidad de ocurrencia de un evento con consecuencias, económicas, sociales o ambientales en un sitio particular y durante un tiempo de exposición determinado. Se obtiene de relacionar la amenaza con la vulnerabilidad de los elementos expuestos.

Simulacro: Ejercicio de juego de roles que se lleva a cabo en un escenario real o construido en la mejor forma posible para asemejarlo.

Siniestro: Es un evento no deseado, no esperado, que puede producir consecuencias negativas en las personas y en los bienes materiales. El siniestro genera la emergencia, si la capacidad de respuesta de la empresa es insuficiente para controlarlo.

Seguridad: Nivel "aceptable" de riesgo. Riesgo que ha sido controlado adecuadamente.

Triaje: Clasificación de heridos según el tipo de lesión, en un evento de emergencia.

Vulnerabilidad: Condiciones en las que se encuentran las personas y los bienes expuestos ante una amenaza. Se relaciona con la incapacidad de una comunidad para afrontar y controlar con sus propios recursos una situación de emergencia.

3.2 MARCO LEGAL

Este programa se fundamenta en las normas nacionales e internacionales planteadas para el control de una emergencia.

- ∞ Declaración Universal de Derechos Humanos (ONU diciembre 10 de 1948.): Artículo 3., "Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona".

- ∞ Resolución 442 -.169 de las Naciones Unidas: "Por la cual se designa el período de 1990 – 2000 como el decenio internacional para la reducción de los desastres naturales".

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Establecer y generar destrezas, condiciones y procedimientos que les permita a los ocupantes y usuarios de las instalaciones del Centro de Captura y Verificación del PREP, con sede en La Paz, Baja California Sur, prevenir y protegerse en caso de desastres o amenazas colectivas que puedan poner en peligro su integridad.

4.2 OBJETIVOS ESPECÍFICOS

- ∞ Identificar y aplicar un proceso de planeación en prevención, previsión, mitigación, preparación, atención y recuperación en caso de desastres.
- ∞ Contar con adecuada estructura organizativa en casos de emergencia.
- ∞ Estructurar un proceso normalizado de evacuación.
- ∞ Generar destrezas para que el personal pueda ponerse a salvo en caso de emergencias.

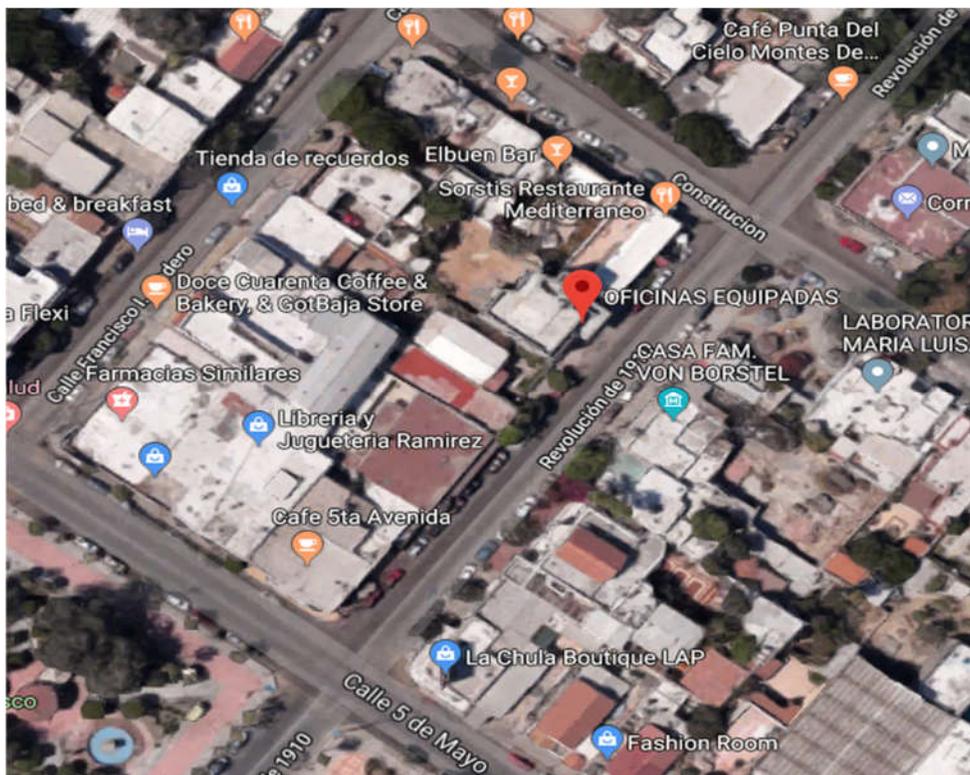
5. IDENTIFICACIÓN GENERAL DE LA INSTITUCIÓN

RAZÓN SOCIAL	PODERNET, S.A. DE C.V.
DIRECCIÓN	Gobernador Ignacio Esteva No. 57 Col. San Miguel Chapultepec Del. Miguel Hidalgo C.P.11850 México D.F.
TELÉFONO	01 55 5257-0730

5.1 LOCALIZACIÓN

Las instalaciones del Centro de Captura y Verificación del PREP, para el Proceso Electoral Local Ordinario 2018, tienen como sede La Paz, Baja California Sur, se encuentran ubicadas en Av. Revolución de 1910, N. 365 tercer piso, entre 5 de mayo y Constitución, zona centro.

Ubicación geográfica general



PoderNet, S.A. de C.V. • www.podernet.com.mx
Gobernador Ignacio Esteva No. 57 Col. San Miguel Chapultepec Del. Miguel Hidalgo C.P.11850 México D.F.
122-5372 y 01 55 5257-0730 correo electrónico: cesar.jimenez@podernet.com.mx

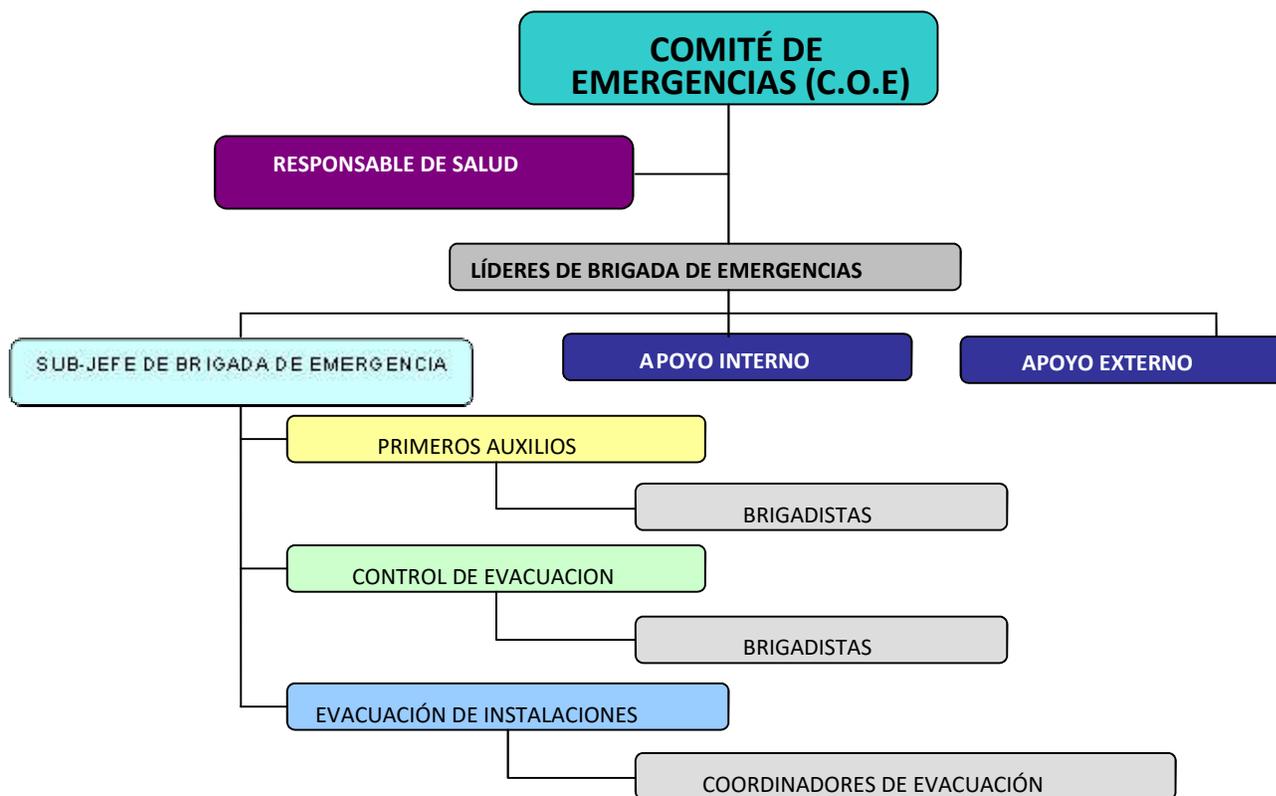
5.2 ELEMENTOS ESTRUCTURALES

Las instalaciones del Centro de Captura y Verificación, están constituidas en su mayoría con estructura de concreto con divisiones internas elaboradas con tablaroca y estructura metálica cubierta con yeso y pintura, loza en concreto e impermeabilizado.

5.3 INSTALACIONES ESPECIALES

INSTALACIÓN	S/N	FUENTE
AGUA	S	Red Urbana (SAPA), Cisterna de 10,000 Litros y 5 tinacos de 1100 litros
ELECTRICIDAD	S	Red Urbana (CFE)
PLANTA ELÉCTRICA	S	Propia
AIRE ACONDICIONADO	S	Mini Split, 9.5 toneladas (5 equipos)
ESTACIONAMIENTO	S	Parte trasera del Edificio

6. ESTRUCTURA ORGANIZACIONAL PARA LA PREVENCIÓN Y ATENCIÓN DE EMERGENCIAS



Las entidades que conforman la organización para emergencias tienen las siguientes responsabilidades, definidas así:

6.1 ORGANIZACIÓN DE PODERNET EN MANEJO DE EMERGENCIAS

Parte del interés de PoderNet en implementar acciones enfocadas a la prevención y atención de posibles emergencias, para esto se cuenta con el plan de emergencia, el cual se constituye en la columna vertebral para afrontar situaciones adversas, éste debe ser lo más práctico posible y de fácil entendimiento para quienes lo consulten.

6.2 ADMINISTRACIÓN DEL PLAN DE EMERGENCIA

Esta fase corresponde al Comité de Emergencia e implica el diseño, aprobación, implementación, divulgación, actualización y auditoría del plan de emergencia, la administración del plan inicia desde la institucionalización en todos los niveles desde el interior de la institución, hasta el nivel local; así mismo aprobará los

alcances, contenido y presupuesto del cual se gestionarán los recursos necesarios para tal fin.

NIVEL OPERACIONAL

Esta fase ejecuta y hace operables los procedimientos ya establecidos en el plan de emergencia, la respuesta dada en las etapas incipientes por parte del mismo personal de la institución marca la diferencia entre la pérdida total o parcial de personas, procesos o bienes.

La actuación se desarrolla en tres niveles definidos así:

Nivel Estratégico: Con un ámbito de acción "global total" asumiendo la máxima responsabilidad y autoridad. Este nivel corresponde al Comité de emergencia, Coordinador De La Emergencia y a su grupo de apoyo (áreas de soporte). Su papel básico es tomar decisiones y coordinar funciones. Su acción se centra en definir QUE HACER.

Nivel Táctico: De ámbito "parcial" y en quien recae la responsabilidad operativa del manejo de la emergencia. El nivel corresponde a los Líderes de brigada su papel básico es definir acciones según el curso de actuación determinado por el nivel estratégico y coordinar recursos para su implementación. Su acción se centra en definir COMO HACER.

Nivel de Tarea: De acción "Puntual y restringida" y en quién recae la responsabilidad por las actividades específicas. Este nivel corresponde al Grupo de brigada para quienes su función es definir y supervisar procedimientos, asignar y utilizar recursos. Su acción se centra en definir DONDE HACERLO y además en HACERLO.

6.3 COMITÉ DE EMERGENCIA

De carácter administrativo, lo conforman las personas responsables en toma de decisiones, con poder de decisión en cabeza directa del Representante Legal o quién cumpla esta función, le siguen directores de procesos o según el organigrama de la institución, lo jefes de cada área, sección, recursos humanos, Área de Soporte Técnico, quienes se constituyen en asesores (grupo de apoyo) que plantearán las consecuencias positivas o negativas de cada circunstancia. Es la estructura responsable de coordinar la ejecución de las operaciones antes, durante y después de la emergencia.

6.3 RESPONSABILIDADES DEL COMITÉ DE EMERGENCIA

ANTES	DURANTE	DESPUÉS
<ul style="list-style-type: none"> ☞ Establecer la política para la prevención y respuesta a emergencias. ☞ Presidir reuniones periódicas orientadas a divulgar y/o actualizar el Plan de Emergencias. ☞ Liderar la elaboración y documentación del plan de emergencias. 	<ul style="list-style-type: none"> ☞ Coordinar administrativamente la emergencia. ☞ Asegurarse en donde se coordina inicialmente la emergencia y su desarrollo inicial. ☞ Autorizar la inversión de recursos físicos, financieros, técnicos y humanos para la atención eficaz de la emergencia manteniendo la continuidad del negocio. ☞ Establecer los contactos con los grupos externos de socorro (Policía, Bomberos, Cruz Roja, Comités Locales de Emergencia, Grupos de Socorro, Administración del edificio, etc.). ☞ Priorizar las necesidades de recursos y garantizar que sean atendidas en este orden. ☞ Decidir si existe la necesidad de evacuación total o parcial de los sitios de trabajo y el momento de continuar con el proceso después de revisar la normalidad de los hechos y las instalaciones. ☞ Preparar los comunicados oficiales 	<ul style="list-style-type: none"> ☞ Determinar por orden directa de los organismos de socorro o brigada de emergencia, si la emergencia ha sido controlada para realizar su posterior evaluación. ☞ Finalizar la emergencia si esta ha sido controlada y es seguro reiniciar las labores sin poner en riesgo la integridad de los ocupantes y los bienes materiales. ☞ Presidir y orientar reuniones para evaluar la eficacia del Plan de Emergencias / Simulacros. ☞ Determinar el método de recuperación / adecuación de equipos y áreas deterioradas. ☞ Determinar las acciones correctivas a implementar para evitar que las deficiencias observadas durante la atención de la emergencia se repitan.



PODERNET

El Poder de Internet

2018
22 años
Sirviendo a la Democracia

RESPONSABILIDADES DEL COORDINADOR DE EMERGENCIA:

ANTES	DURANTE	DESPUÉS
<ul style="list-style-type: none"> ✓ Liderar la elaboración y documentación específica del plan de emergencias de su sede. ✓ Seguir la política de salud para la prevención y respuesta a emergencias. ✓ Garantizar la implementación del plan de emergencias. ✓ Mantener conformada, capacitada y entrenada la brigada de emergencias. ✓ Actualizar el plan de emergencias de acuerdo a las disposiciones de salud y normatividad legal aplicable. 	<ul style="list-style-type: none"> ✓ Ubicar un lugar fijo para realizar la coordinación de la emergencia. ✓ Mantenerse comunicado con el comité de emergencias e informar cómo transcurre el evento. ✓ Asegurarse de proteger la integridad física de todos los ocupantes de las instalaciones. ✓ Establecer el enlace con los organismos de socorro. ✓ Asignar un coordinador en el sitio específico de la emergencia y mantenerlo informado de las necesidades y desarrollo del evento. ✓ Priorizar las necesidades de recursos y garantizar que sean atendidas en este orden. ✓ Decidir si existe la necesidad de evacuación total o parcial de los sitios de trabajo y el momento de continuar con el proceso después de revisar la normalidad de los hechos y las instalaciones. ✓ Llevar una lista de ocupantes evacuados en donde discrimina funcionarios y visitantes. ✓ Identificar el número de brigadistas y las áreas en donde intervienen. 	<ul style="list-style-type: none"> ✓ Determinar por orden directa de los organismos de socorro o brigada de emergencia, si la emergencia ha sido controlada para realizar su posterior evaluación. ✓ Finalizar la emergencia si esta ha sido controlada y es seguro reiniciar las labores sin poner en riesgo la integridad de los ocupantes y los bienes materiales. ✓ Dirigir y orientar reuniones para evaluar la eficacia del Plan de Emergencias / Simulacros. ✓ Determinar el método de recuperación / adecuación de equipos y áreas deterioradas ✓ Determina las acciones correctivas a implementar para evitar que las deficiencias observadas durante la atención de la emergencia se repitan.

6.5 BRIGADA DE EMERGENCIA

Lo constituye el personal que voluntariamente o por condición de la institución se prepara y entrena en aspectos de prevención y atención de emergencias. La brigada es el primer grupo que de manera incipiente contrarresta la emergencia, actuando de acuerdo a los procedimientos establecidos en el plan de emergencia y con los recursos destinados para tal fin.



PODERNET

El Poder de Internet

2018
22 años
Sirviendo a la Democracia

RESPONSABILIDADES DE LA BRIGADA DE EMERGENCIAS:

ANTES	DURANTE	DESPUÉS
<ul style="list-style-type: none"> ☞ Asistir y participar activamente en las capacitaciones, prácticas y entrenamientos que se programen. ☞ Asegurar que todos los equipos y elementos de emergencia que puedan ser requeridos en caso de una emergencia estén en buen estado y listos para ser utilizados en cualquier momento. ☞ Aprender a reconocer las instrucciones referentes al llamado de emergencia de la brigada. ☞ Establecer un lugar previo a donde debe acudir en caso de ser llamados. ☞ Mantener una permanente integración con los demás integrantes de la brigada estimulando el espíritu de trabajo en equipo y vocación voluntaria en su actividad de brigadista. ☞ Informar de cualquier violación de seguridad. ☞ Conocer el plan de emergencias y darlo a conocer a todos los funcionarios de la sede. ☞ Colaborar con el diseño e implementación de Procedimientos Operativos Normalizados frente a los principales riesgos detectados en la sede. ☞ Asegurar que se cumplan a cabalidad con los programas de mantenimiento, capacitación y dotación de la brigada de emergencia. 	<ul style="list-style-type: none"> ☞ Atender en primera instancia la emergencia e informar al coordinador de emergencias el tipo y las acciones que se están tomando para lograr su control. ☞ Establecer un sistema de comunicación confiable con el coordinador de emergencias. ☞ En caso de peligro inminente o duda sobre el control de la situación, apoyarse con los coordinadores de evacuación que haya. ☞ Una vez que el coordinador de emergencias se haga presente en el sitio, seguir sus instrucciones y no obstaculizar su acción. ☞ Realizar acciones de búsqueda y rescate según sea el caso, siempre en compañía de otro brigadista e informándole al coordinador de emergencias. ☞ Mantener el contacto permanente con los demás brigadistas, coordinadores de evacuación, organismos externos de socorro. ☞ Al remitir lesionados, asegurarse que la institución a la cual desea ser remitido sea informada para que se prepare a recibirlos y atenderlos, apóyense para esto con gestión humana. ☞ Una vez que se hagan presentes la Policía, Bomberos, las autoridades, hacer la entrega formal de la 	<ul style="list-style-type: none"> ☞ Trabajar en coordinación con el coordinador de emergencias en actividades de consolidación del control, verificación de daños, informes a las directivas, a compañías aseguradoras, etc. ☞ Realizar las acciones de reacondicionamiento de las instalaciones. ☞ Establecer las necesidades primarias de equipos de emergencia que se necesitan para poder reiniciar las labores con seguridad. ☞ Reunir a la brigada para evaluar la actuación en la emergencia y levantar un acta de las conclusiones y recomendaciones. ☞ Participar en las actividades de evaluación y consolidación del control de la emergencia, revisión de instalaciones, ventilación de áreas, clausura de ventanas, áreas con peligro potencial y recuperación de equipos de emergencia. ☞ Asegurarse que todos los elementos y equipos a su cargo utilizados durante la emergencia queden en óptimas condiciones para ser utilizados en cualquier momento.



PODERNET

El Poder de Internet

2018
22 años
Sirviendo a la Democracia

<ul style="list-style-type: none">☞ Ayuda a mantener actualizados y disponibles los planos de las instalaciones, incluyendo ubicación de extintores, señales, botiquines, controles eléctricos.☞ Ayudar a mantener un alto grado de motivación e integración entre todos los miembros de la brigada.☞ Capacitarse y entrenarse conjuntamente con los organismos de emergencia y los recursos existentes en la sede.	<p>emergencia a los responsables de estos grupos, sin embargo, estar alerta en todo momento para dar apoyo e información ya que de esto depende que se tomen decisiones acertadas.</p> <ul style="list-style-type: none">☞ Notificar al coordinador de emergencias cualquier situación anormal observada.☞ Abstenerse de dar declaraciones no autorizadas.	
---	---	--



PODERNET

El Poder de Internet

2018
22 años
Sirviendo a la Democracia

PRIMEROS AUXILIOS	EVACUACIÓN Y BÚSQUEDA
<ul style="list-style-type: none"> ☞ Atender a quién lo requiera y realizar estabilización. ☞ Determinar quién necesita ayuda para ser transportado por el método más conveniente. ☞ Colaborar con los organismos de socorro cuando ellos lo soliciten. ☞ Acompañar a los lesionados en su desplazamiento hacia los centros asistenciales. ☞ Cuando la emergencia sea de tal naturaleza que haya personas atrapadas o gran cantidad de lesionados, participar en la activación y funcionamiento del "TRIAGE", con la siguiente clasificación. <p>Lesiones leves</p> <ul style="list-style-type: none"> ☞ Suministrar apoyo emocional y suministrar primeros auxilios a magulladuras o heridas superficiales, accesos de ansiedad sin mayor daño físico. <p>Lesiones moderadas</p> <ul style="list-style-type: none"> ☞ Estabilizar y transportar de manera adecuada a la víctima para la realización de procedimientos, como vendajes, curaciones, pero que en general no tenga indicios de daños mayores. <p>Lesiones severas</p> <ul style="list-style-type: none"> ☞ Remitirlos a un centro asistencial directamente en una ambulancia, como trauma de abdomen con 	<ul style="list-style-type: none"> ☞ Instalar un centro de coordinación y designar un líder de equipo. ☞ En todo momento solicitar ayuda a los organismos de socorro. ☞ Revisar el estado de salud de los brigadistas y la dotación a ser utilizada. ☞ Obtener una copia de los planos de las instalaciones. ☞ Diseñar la ruta de entrada para iniciar la búsqueda y determinar el tiempo en que se demorará haciendo el recorrido. ☞ Buscar siempre en pareja y mantener contacto con el Coordinador de Emergencias. ☞ Nunca cambiar su ruta de búsqueda. ☞ Llevar siempre consigo linternas tipo frontal para mantener libre las manos. ☞ En lo posible acompañar y guiar a los grupos de socorro. ☞ Si se encuentra con una persona tratando de evacuar ayudarla a evacuar y acompañarla hasta el punto de encuentro. ☞ Si la persona se encuentra atrapada y no presenta lesiones arrastrarla o cargara hasta el punto de encuentro. ☞ Si se asume lesión traumática evacuar en camilla rígida. ☞ Una vez revisado el recinto, dejar una señal indicando que ya busco en ese lugar, voltear una silla, marcar con



PODERNET

El Poder de Internet

2018
22 años
Sirviendo a la Democracia

<p>signos de lesión visceral, herida profunda en tórax, hemorragias abundantes, trauma de cráneo, víctimas inconscientes con signos vitales alterados.</p> <p>En caso de necesitarse otros vehículos por exceso de víctimas a remitir, buscar de preferencia vehículos amplios y que dispongan de sirena y comunicación por radio.</p> <p>Inmediatamente pasada la situación de emergencia, iniciar el aviso a los familiares de los lesionados con el apoyo de gestión humana.</p>	<p>un marcador o una tiza o hacer una equis con cinta.</p> <p>En caso que los rescatadores pierdan la comunicación con el líder, enviar inmediatamente un grupo para realizar la búsqueda de estos.</p>
---	---

6.6 RESPONSABILIDADES DE LOS COORDINADORES DE EVACUACIÓN

ANTES	DURANTE	DESPUÉS
<ul style="list-style-type: none"> ☞ Asegurarse de conocer las rutas de salida y la ubicación de los diversos recursos disponibles en su área en caso de emergencia, brigadistas, extintores, botiquines y teléfonos. ☞ Verificar las condiciones de las vías de evacuación y riesgo de su área trabajo de acuerdo con la periodicidad establecida o inmediatamente si considera que el riesgo es alto. ☞ Participar activamente en las prácticas y simulacros, aprender a reconocer la alarma con su tono de alerta. ☞ Orientar a las personas nuevas de su área sobre el plan de evacuación, enterarse de impedimentos físicos para asignarles un acompañante. ☞ Asegurarse de portar en todo momento su identificación personal. 	<p><u>Si es en su área</u></p> <ul style="list-style-type: none"> ☞ Iniciar la respuesta liderada por usted, asegurarse de informar a los brigadistas para activar el plan de evacuación. ☞ En caso de peligro inminente o duda sobre el control de la situación, dar la orden de salir a los ocupantes de su área. <p><u>Si es en otra área</u></p> <ul style="list-style-type: none"> ☞ Al ser notificado por cualquier medio, suspender actividades para dirigirse al punto de encuentro asignado. <p><u>En la preparación para salir</u></p> <ul style="list-style-type: none"> ☞ Repasar rápidamente la información sobre los ocupantes de su área. ☞ Recordarles por donde es la salida y el punto de reunión final y No intentar regresar. <p><u>En la salida</u></p> <ul style="list-style-type: none"> ☞ Verificar que todos salgan, inspeccionar rápidamente baños, cuartos aislados, etc. salir y cerrar la puerta sin seguro detrás de usted. ☞ En todo caso si alguien se niega a salir, no se quede, salga con el grupo. ☞ Evitar que se regresen. ☞ Repetir frases como: no corran, conserven la calma, por la derecha, en fila, no se detenga. ☞ Asegurarse que se ayude a quienes lo necesiten. 	<ul style="list-style-type: none"> ☞ Dirigirse con el grupo al punto de encuentro previsto por la brigada. ☞ Verificar la salida de sus compañeros y demás ocupantes. ☞ Si alguien no pudo salir, asegurarse que se notifique a la brigada, indicando de quien se trata y el posible sitio donde se puede encontrar la persona, no tratar de iniciar el rescate. ☞ Asegurarse de que se atienda a las personas de su grupo lesionadas o afectadas por la emergencia en el puesto de primeros auxilios. ☞ Notificar situaciones anormales observadas, pero absténgase de dar declaraciones no autorizadas a los medios de comunicación y de difundir rumores. ☞ Mantener unido a su grupo para evitar la infiltración de personas ajenas a la sede. ☞ Cuando la brigada de la orden de regresar comunicarlo a su grupo. ☞ Al regresar colaborar en la inspección e informe sobre las anomalías encontradas. ☞ Elaborar el reporte, inclusive en simulacros. ☞ Asistir y participar en la reunión de evaluación, comentar con sus



PODERNET

El Poder de Internet

2018
22 años
Sirviendo a la Democracia

	<ul style="list-style-type: none">☞ Estar atento a instrucciones como puede ser la modificación en la ruta de salida.☞ Si no puede salir, por obstrucción o riesgo inminente, buscar quedarse en un sitio con características refugio según el tipo de emergencia.	<p>compañeros los resultados obtenidos.</p> <ul style="list-style-type: none">☞ Verificar el restablecimiento de los sistemas de protección de su área.
--	---	---



PODERNET

El Poder de Internet

2018
22 años
Sirviendo a la Democracia

6.7 RESPONSABILIDADES EMPLEADOS EN GENERAL

ANTES	DURANTE	DESPUÉS
<ul style="list-style-type: none"> ☞ Conocer las instalaciones físicas de la empresa. ☞ Identificar la ruta de evacuación. ☞ Reconocer la ubicación de los extintores y demás equipos que puedan ser usados en emergencias. ☞ Mantener consigo la siguiente documentación mientras permanece en las instalaciones de la empresa: <ul style="list-style-type: none"> • Documento de identidad • Carnet de Identificación 	<ul style="list-style-type: none"> ☞ Si se entera de una situación de riesgo, informar de inmediato a algún brigadista o al vigilante. ☞ Si escucha la orden de evacuación, suspender completamente sus actividades. ☞ Dirigirse por la ruta de evacuación establecida. ☞ Si tiene algún visitante, llevarlo con usted hasta el punto de encuentro. ☞ Evitar difundir rumores y ayudar a mantener la calma. ☞ Ayudar a personas que lo necesitan, como mujeres en estado de embarazo, enfermo, lesionado y/o con discapacidad. ☞ Si hubo alguna persona que no pudo evacuar, informar a los brigadistas, vigilantes u organismos de socorro. ☞ Cumplir con las instrucciones que reciba del coordinador de emergencias o la brigada. ☞ Si ha evacuado mencionar su nombre y lugar de procedencia a los brigadistas. 	<ul style="list-style-type: none"> ☞ Informar sus acciones, beneficios y fallas durante la evacuación. ☞ Reanudar sus actividades tan pronto reciba la orden para ello. ☞ Abstenerse de dar información no autorizada a medios de comunicación u otras personas.

7.- PLAN DE EVALUACIÓN Y ACTUALIZACIÓN DEL PLAN DE EMERGENCIA

El presente plan de emergencias deberá ser actualizado cada año de manera periódica normal, pero en el evento en que se tengan modificaciones importantes en las características de la empresa, de los procesos, en el personal involucrado en el plan, en los mecanismos de administración del riesgo, entre otros, se deberán hacer los ajustes respectivos de forma inmediata. La complementación y modificación de contenidos del plan se realizarán en el momento que se considere conveniente por el Comité de Emergencia o la brigada de emergencias y cuando se realicen recomendaciones específicas tras la realización de simulacros.

8.- PLAN DE EVACUACION

8.1 RUTAS DE EVACUACIÓN:

Salidas Normales: Son aquellas por donde entra y sale usualmente el personal.

Salidas de Emergencia: Son aquellas debidamente señalizadas y usadas sólo para salir en casos de una emergencia.

8.2 AVISOS DE EMERGENCIA

En caso de accidentes que requieran atención médica de urgencia, (**VER ANEXO: INFORMACIÓN TELEFÓNICA PARA EMERGENCIAS**)

8.3 SITIOS DE CONTEO O REUNIÓN FINAL

Son aquellos lugares previamente seleccionados, hacia donde toda persona que evacúe, debe dirigirse para presentarse a su líder de Evacuación de área.

AREA	PUNTO DE ENCUENTRO	SALIDAS DE EMERGENCIA	PROCEDIMIENTO DE EVACUACIÓN
SEDE LA PAZ, B.C.S.	<p>PRINCIPAL Frente del edificio planta baja.</p> <p>ALTERNO: parte trasera del edificio planta baja.</p>	<p>En la sede hay 3 salidas</p> <ul style="list-style-type: none"> ☞ Salida tercer nivel. ☞ Salida hacia estacionamiento. ☞ Salida hacia el frente del edificio. 	<p>Los empleados, y visitantes, al escuchar la alarma saldrán de su puesto de trabajo y se ubicarán en el punto de encuentro principal.</p> <p>Si se requiere evacuar hasta el punto de encuentro alterno, el coordinador de evacuación determinará la salida de emergencia a utilizar dependiendo de la ubicación de la emergencia.</p>

Nota:

- ∞ El Coordinador de emergencia con ayuda de los Coordinadores de evacuación de cada área, determinarán el punto de encuentro más seguro dependiendo de la ubicación y magnitud de la emergencia.

CAMBIO SITIO DE CONTEO O REUNIÓN: Esta determinación corresponde al Coordinador de emergencia o por el funcionario de más alto cargo presente (solo en caso de no encontrarse disponible el coordinador de emergencia)

8.4 PROCESO DE EVACUACIÓN

Declarada la emergencia y activada la alarma de evacuación, todo el personal de la Institución incluidos los visitantes, salen de sus puestos de trabajo y se ubican en el punto de encuentro (principal o alterno) que indique el Coordinador de emergencia dependiendo de la ubicación y magnitud del evento.

Los Coordinadores de evacuación verificarán a través de listado e información de control de acceso a los estudiantes que todo el personal se encuentra a salvo a través del censo o conteo de evacuados. Los Coordinadores de evacuación informarán al coordinador de emergencia el número total de evacuados y en qué condiciones se encuentran (si hay lesionados o falta alguien).

Este procedimiento se realizará cada vez que se active la alarma de evacuación.

El Coordinador de emergencia, una vez ha recibido la notificación del control de la misma, informará a los trabajadores, estudiantes y visitantes lo sucedido y dará la orden de retorno a las áreas de trabajo, que se hará de manera organizada (de la misma forma en que evacuaron)

8.5 ZONAS DE EVACUACIÓN Y GRUPOS DIRECTIVOS DE EVACUACIÓN

Son aquellas áreas en las cuales se ha dividido las instalaciones para asignar Coordinadores de Evacuación.

Se encargarán de dirigir la evacuación y ayudar a las personas que no pueden o tienen dificultad para evacuar, según lo estipulado en el plan.

En cada zona, se tienen personas que han sido designadas con anterioridad para coordinar la evacuación, contará con un auxiliar que lo reemplaza en caso necesario.

Para poder lograr una buena actuación todos los integrantes del grupo de emergencia deben tener a su disposición el distintivo (camiseta) que los identifica y estar dotados con los elementos que requieren para llevar a cabo sus funciones y responsabilidades en la prevención y atención de emergencias dentro de PODERNET, sede en La Paz, B. C.S.

Las siguientes son algunas recomendaciones para los Coordinadores de evacuación:

- ∞ Conocer el plan de emergencia.
- ∞ Conocer las rutas de salida de emergencia, inspeccionar periódicamente dichas rutas.
- ∞ Desarrollar rutas de evacuación alternas y la factibilidad de refugios temporales seguros, en caso que sean necesarios, dar a conocer estas alternativas al coordinador de emergencia.
- ∞ Mantener un listado actualizado del personal a su cargo
- ∞ Estar pendientes de las variaciones que se presentan en su área
- ∞ Efectuar inspecciones de seguridad e informar anomalías periódicamente
- ∞ Colaborar con el plan de evacuación y en el programa de señalización de rutas de evacuación
- ∞ Programar charlas y conferencias dirigidas al personal a su cargo para que conozcan el plan y se familiaricen con el método general de evacuación
- ∞ Dirigir el proceso de evacuación de acuerdo con lo planeado y una vez recibida la orden para hacerlo; supervisar que se ejecuten las acciones de evacuación preestablecidas
- ∞ Elaborar un informe de la actuación antes de pasados tres días del hecho.

Algunas normas que deben tener en cuenta los trabajadores en el momento de evacuar, son:

- ∞ Desconectar equipos eléctricos, apagar luces, cerrar grifos.
- ∞ No olvidar la orientación, observación y retentiva de salidas, escaleras, sitios de ubicación, etc.

- ∞ No se debe correr
- ∞ En caso de humo, desplazarse a nivel del piso gateando, cubriéndose nariz y boca con textil húmedo
- ∞ Dar prioridad a las personas con mayor exposición al riesgo
- ∞ Las mujeres se deben quitar los zapatos de tacón alto para bajar las escaleras (únicamente si en el piso no hay elementos cortantes que generen riesgo de heridas cortantes)
- ∞ No devolverse por ningún motivo
- ∞ Antes de salir verificar el estado de las vías de evacuación.
- ∞ Si tiene que refugiarse deje una señal

8.6 NORMAS DE EVACUACIÓN PARA VISITANTES Y PERSONAL AJENO A PODERNET, S. A. de C. V., SEDE EN LA PAZ, BAJA CALIFORNIA SUR

En caso de una emergencia, el trabajador que los esté atendiendo, deberá guiarlos hacia la salida de emergencia más cercana, evacuar junto a ellos y trasladarse hasta el punto de reunión, para ello se les indicará al inicio del evento al que asistan, ya sea un simulacro oficial o la jornada electoral, quién será el personal oficial de PoderNet que se hará cargo de ellos, quienes portarán camisas de color blanco con el logo de la empresa a efecto de distinguirlos del resto del personal que contará con playeras blancas.

8.7 SISTEMA DE ALARMA PARA EVACUACIÓN

La alarma de evacuación es la señal que permite dar a conocer a todo el personal, en forma simultánea, la necesidad de evacuar un lugar ante una amenaza determinada; por esta razón, es de suma importancia que sea dada en el menor tiempo posible después que se ha detectado la presencia del peligro. La alarma de evacuación será activada por el Coordinador de Emergencia.

¿Cuándo se debe activar la alarma? Se debe dar la alarma en las siguientes situaciones:

- ∞ Cuando detecte un incendio en el lugar donde se encuentre, y este fuego no pueda ser controlado de manera inmediata.
- ∞ Cuando observe la presencia de humo en grandes proporciones dentro de la institución.
- ∞ Cuando se presenten daños graves en la estructura de la empresa, que pongan en peligro a sus ocupantes en forma inmediata.
- ∞ Cuando se descubra o sospeche la presencia de artefactos explosivos en cualquier área.
- ∞ Cuando sospeche de un riesgo colectivo sistemático (que afecte de manera progresiva a varias personas).
- ∞ Cuando se sepa de un riesgo en los alrededores a la empresa y que pueda afectarla.

Procedimiento para notificación de alerta y alarma:

Alerta: Es el aviso de que una situación crítica se está presentando. Debe servir para activar el Plan y prepararse para una posible emergencia.

SITUACIÓN	NOTIFICACIÓN DE ALERTA
Una vez se haya comprobado la existencia de la emergencia, y mientras se da la orden de evacuación, se dará inicio al proceso de alerta	Aviso de manera telefónica o personal

Alarma: Indica lo inminente de un riesgo y que se considera más seguro abandonar las instalaciones, activando el plan de evacuación

SITUACIÓN	NOTIFICACIÓN DE ALARMA
Según las indicaciones de los Coordinadores de Evacuación de cada área, se inicia la evacuación total de la institución hasta el punto de encuentro previamente establecido.	Sede Cuenta con alarma sonora ubicada en el área de entrada.

8.8 COMPORTAMIENTO EN EL PUNTO DE REUNIÓN O CONTEO

- ∞ Las filas de evacuados que lleguen al sitio mencionado permanecerán unidas, junto a sus Coordinadores de evacuación por grupos, e iniciarán el conteo o revisión para detectar quién/es falta/n.
- ∞ Los Coordinadores de evacuación informarán al Coordinador de emergencia sobre el personal faltante para buscar ayuda.
- ∞ NO abandonar el Sitio de Reunión o Conteo sin autorización del Coordinador de evacuación del área al que pertenece.

8.9 PROCEDIMIENTO PARA RETORNAR A LOS SITIOS DE TRABAJO

- ∞ Una vez han evacuado todos los ocupantes y se ha dado la información de control de la emergencia, el Coordinador de emergencia enviará a un grupo de brigadistas para que realice barrido de las áreas con el fin de descartar nuevos peligros o rescatar lesionados que aún se encuentren en el área.



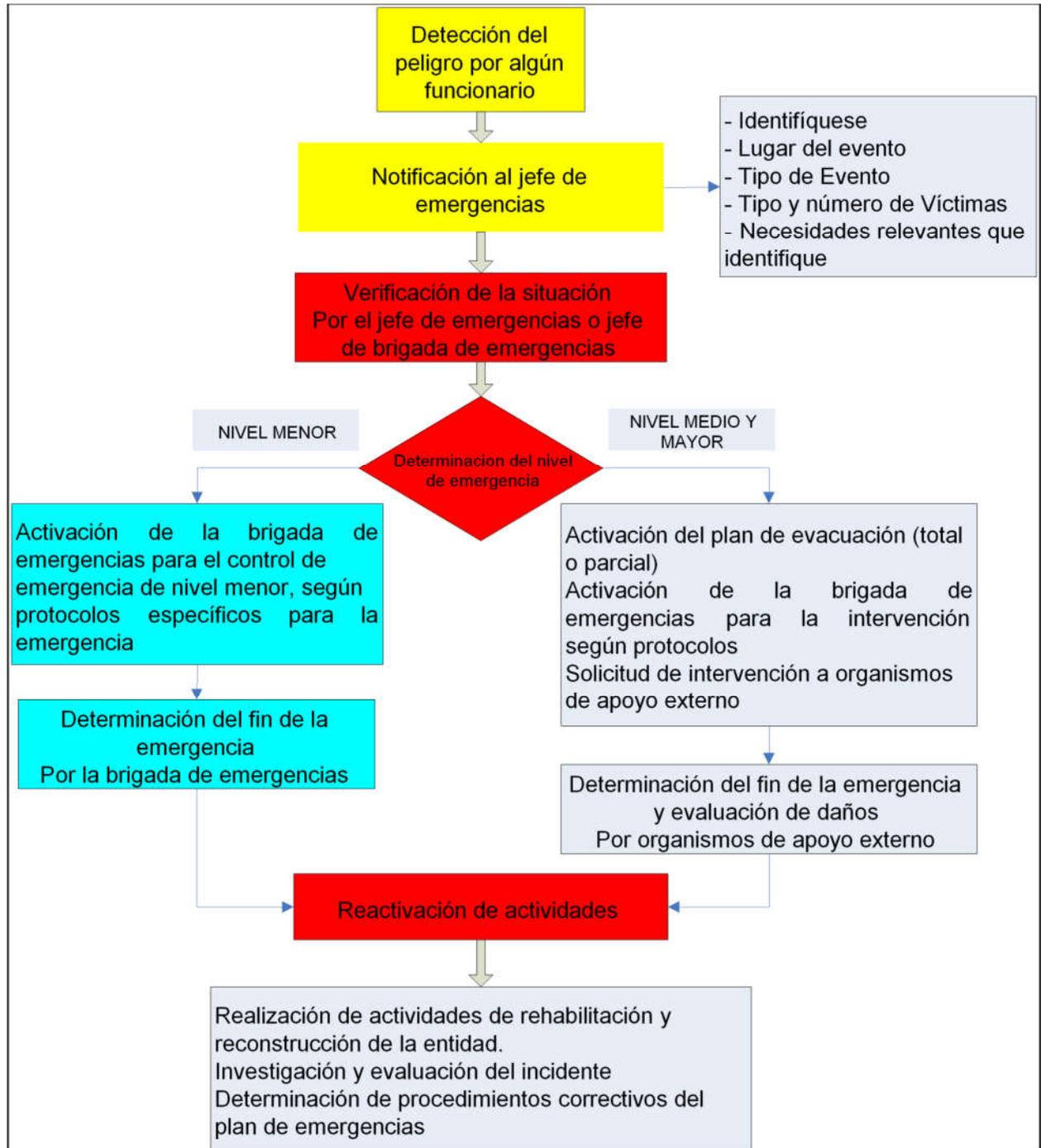
PODERNET

El Poder de Internet

2018
22 años
Sirviendo a la Democracia

- ∞ Una vez realizado el barrido y dado la información de control total de la emergencia, el Coordinador de la emergencia, avisará en el Sitio de Reunión, para que los Coordinadores de Evacuación organicen el retorno de los evacuados.

PROTOCOLO GENERAL DE EMERGENCIAS



10.- INVESTIGACIÓN, EVALUACIÓN DE LA EMERGENCIA Y AUTOEVALUACIÓN DEL PLAN DE EMERGENCIA

ASPECTOS BÁSICOS.

La investigación de los eventos adversos deberá considerar, como mínimo, los siguientes aspectos:

¿Qué sucedió?: Este factor está orientado a determinar los hechos sucedidos, incluyendo:

- ∞ Tipo de emergencia
- ∞ Tamaño o magnitud del evento
- ∞ Desarrollo de la emergencia
- ∞ Efectos de la emergencia

¿Cuándo sucedió?: Este factor está orientado a establecer las condiciones de tiempo de la emergencia, incluyendo:

- ∞ Fecha de ocurrencia
- ∞ Día de la semana de la presentación del hecho
- ∞ Hora probable de su presentación
- ∞ Hora estimada de su detección
- ∞ Fecha y hora de su terminación
- ∞ Si el día era laborable o no
- ∞ Condiciones climáticas reinantes en el sitio.

¿Dónde sucedió?: Este factor está orientado a establecer las condiciones de lugar asociadas al hecho, incluyendo:

- ∞ Área de servicios
- ∞ Piso
- ∞ Equipo de origen del siniestro
- ∞ Parte del equipo
- ∞ Personal presente en el lugar
- ∞ Protecciones existentes en el lugar

¿Cómo sucedió?: Este factor está orientado a establecer la forma como la emergencia se inició y desarrolló, incluyendo:

- ∞ Descripción del proceso de ocurrencia
- ∞ Área afectada
- ∞ Personas afectadas
- ∞ Información y/o valores afectados



PODERNET

El Poder de Internet

2018
22 años
Sirviendo a la Democracia

- ∞ Equipos afectados
- ∞ Materiales afectados
- ∞ Procesos afectados
- ∞ Descripción de las circunstancias asociadas
- ∞ Descripción de los antecedentes de la emergencia
- ∞ Factores que facilitaron su propagación o desarrollo
- ∞ Factores que dificultaron su propagación o desarrollo
- ∞ Actuación de las personas presentes
- ∞ Forma como fue controlado
- ∞ Organismos que participaron
- ∞ Funcionarios que fueron notificados.

¿Por qué sucedió?: Este factor está orientado a determinar las causas de la emergencia, incluyendo:

- ∞ Origen accidental o intencional
- ∞ Factores que facilitaron su ocurrencia

Factores Complementarios: Este factor está orientado a determinar aquella información que facilitará la investigación y entendimiento de la emergencia, incluyendo.

- ∞ Testigos presenciales
- ∞ Hechos similares presentados anteriormente
- ∞ Últimas inspecciones efectuadas al lugar
- ∞ Últimas verificaciones o pruebas a los equipos
- ∞ Opiniones o comentarios
- ∞ Conclusiones preliminares

12.- ACTIVIDADES DURANTE LA EMERGENCIA

Se inicia con el evento adverso (incendio, explosión, movimiento sísmico, etc.) seguido de la fase de emergencia propiamente dicha, lo cual genera:

- ∞ Evacuación total o parcial
- ∞ Despliegue de la cadena de socorro

IDENTIFICACIÓN	RESPONSABILIDADES / FUNCIONES
<p align="center">COORDINADORES DE EVACUACIÓN</p>	<ul style="list-style-type: none"> ∞ Coordinan el proceso de evacuación en cada una de sus áreas por las respectivas vías de evacuación más seguras. ∞ Realizan el conteo del personal de su área. ∞ Revisan que no quede ninguna persona dentro de la empresa luego de dada la orden de evacuación. ∞ En caso de quedar personal en las instalaciones informar al coordinador de emergencia, quien y por qué no evacua. ∞ En caso de encontrarse personal herido informar a la brigada de primeros auxilios y rescate para trasladarlo hasta un punto seguro para ser atendido.
<p align="center">BRIGADA DE EMERGENCIA</p>	<ul style="list-style-type: none"> ∞ En caso de incendio la brigada de control de incendios, procederá en forma técnica y ordenada a realizar la extinción del fuego o conato de incendio mientras llegan los Bomberos. ∞ Ayudan en el salvamento de bienes y equipos. ∞ Después de la emergencia la brigada colaborará en la investigación de las causas de incendios o conatos de incendios.
<p align="center">BRIGADA DE EMERGENCIA GRUPO DE PRIMEROS AUXILIOS</p>	<ul style="list-style-type: none"> ∞ Prestarán los primeros auxilios al personal que sufre alguna lesión o trauma hasta el momento en que se hagan presentes las unidades de socorro y/o paramédicos. ∞ De acuerdo al plan de acción definido para enfrentar la emergencia, el grupo de primeros auxilios deben llevar consigo los elementos que necesitan para cumplir con sus funciones (botiquín de primeros auxilios) y trasladarlos hasta el punto de atención.
<p align="center">GRUPO DE SEGURIDAD – (VIGILANTES)</p>	<p>Proveer vigilancia a las áreas que indique el coordinador de emergencias, teniendo en cuenta:</p> <ul style="list-style-type: none"> ∞ No permitir la movilización ni salida de equipos o elementos. ∞ Retener todo elemento que trate de ser sacado de las áreas. ∞ A menos que se cuente con autorización del coordinador de emergencias, no permitir remover escombros ni tomar fotografías. ∞ Restringir la entrada de personal, con excepción de integrantes de los cuerpos de socorro.

PERSONAL DE LA EMPRESA	<ul style="list-style-type: none"> ∞ Acatar las instrucciones del Grupo de emergencia (Comité, coordinadores de evacuación y Brigadistas) ∞ Realizar la evacuación hasta el punto de encuentro de forma rápida, sin correr. ∞ Evitar aglomeraciones en las puertas
-------------------------------	---

12.1 - PLAN DE ACTIVIDADES FORMATIVAS

Para el diseño e implementación del Plan de Emergencias se programarán actividades de formación y refuerzo en temas de prevención y atención de emergencias para la Brigada de Emergencia, el Comité de Emergencias, coordinadores de Evacuación y los Trabajadores en General:

CAPACITACIÓN BÁSICA POR GRUPOS

Se relaciona los temas y grupos a quienes se debe dirigir las formaciones y entrenamientos que permitan el dinamismo y continuidad del plan de emergencias.

PERSONAL GENERAL DE LA EMPRESA

- ∞ Socialización plan de emergencia
- ∞ Plan de evacuación (Rutas, Salidas de emergencias y Punto de Encuentro)
- ∞ Procedimientos y reconocimiento del sistema de alerta y alarma
- ∞ Relación de Brigadistas y Coordinadores de Evacuación.
- ∞ Procedimientos para actuar en emergencias

COMITÉ DE EMERGENCIA

- ∞ Funciones y responsabilidades
- ∞ Administración de la emergencia
- ∞ Plan de evacuación (Rutas, Salidas de emergencias y Punto de Encuentro)
- ∞ Procedimientos y reconocimiento del sistema de alerta y alarma
- ∞ Relación de integrantes de Brigada y Coordinadores de Evacuación.
- ∞ Procedimientos para actuar en emergencias
- ∞ Simulacros y simulaciones de emergencia.

COORDINADORES DE EVACUACIÓN

- ∞ Socialización plan de emergencia
- ∞ Funciones y responsabilidades
- ∞ Plan de evacuación (Rutas, Salidas de emergencias y Punto de Encuentro)
- ∞ Procedimientos y reconocimiento del sistema de alerta y alarma
- ∞ Relación de integrantes de Brigada y Comité de emergencia.
- ∞ Procedimientos para actuar en emergencias
- ∞ Fases y procedimiento de evacuación
- ∞ Simulacros y simulaciones de emergencia.

BRIGADA DE EMERGENCIA

- ∞ Socialización plan de emergencia
- ∞ Plan de evacuación (Rutas, Salidas de emergencias y Punto de Encuentro)
- ∞ Procedimientos y reconocimiento del sistema de alerta y alarma
- ∞ Relación de Integrantes del Comité de Emergencia y Coordinadores de Evacuación.
- ∞ Procedimientos para actuar en emergencias
- ∞ Funciones y responsabilidades como brigadistas
- ∞ Seguridad en operaciones de emergencia
- ∞ Simulacros de atención de víctimas y evacuación.

PRIMEROS AUXILIOS

- ∞ Signos vitales
- ∞ Valoración de lesionados
- ∞ Heridas de tejido blando
- ∞ Lesiones
- ∞ Alteraciones de la conciencia
- ∞ Cuerpos extraños
- ∞ Obstrucción de la vía aérea
- ∞ Soporte Vital
- ∞ Transporte de lesionados

ANEXO

TELÉFONOS DE EMERGENCIA EN BCS

LA PAZ BCS

Cruz Roja Mexicana
1221111/1221101

Tránsito Municipal
1220477

Heroico Cuerpo de Bomberos
Comandancia 1654343
Caseta 1220054
Sub Estación Los Olivos 1226807

Policía Ministerial del Estado
1257541 Dto.117

Policía Federal
1146597, 1146605

Policía Estatal
1750400

Protección Civil Municipal
1213634 / 1213214

Protección Civil Estatal
1229008

MUNICIPIO LOS CABOS

Policía Ministerial
6241725356

Cruz Roja Mexicana
6241433300

Protección Civil Municipal
6241435123 / 6241439120

Heroico Cuerpo de Bomberos
6241433577

Tránsito Municipal
6241435766

SAN JOSÉ DEL CABO

Dirección De Seguridad Pública
6241457450 / 6241420361

Tránsito Municipal
6241467600 Conmutador 6241422835

Policía Ministerial del Estado
6241424104

Cruz Roja Mexicana
6241420316

Protección Civil Municipal
6241423748 / 1420067

Policía Federal
6241461240 Y 41

Heroico Cuerpo de Bomberos
6241422466

COMONDÚ

Cruz Roja Mexicana
6131321111

Heroico Cuerpo de Bomberos
6131320955

Policía Ministerial del Estado
6131320899

Tránsito Municipal
6131326883

Policía Federal
6131323836

Protección Civil Municipal
Director Francisco Mosqueda
6131002423
Subdirector Juan Manuel Mata Carrillo
6131093124

LORETO

Cruz Roja Mexicana
6131351111

Heroico Cuerpo de Bomberos
6131351566

Policía Ministerial del Estado
6131352309

Tránsito Municipal
6131350035

Policía Federal
6131330794
Dir. Oficial Luis Carlos Garza Oviedo
6621910814

Capitanía De Puerto
6131350465

MULEGÉ

Cruz Roja Mexicana
6151063013 / 6151530110

Heroico Cuerpo de Bomberos
6151530297

Delegación Municipal
Tránsito Municipal 6151530056



PODERNET

El Poder de Internet

Guerrero Negro Policía Federal
6151570848

Protección Civil Municipal
6151598969

Policía Ministerial del Estado
6151530804

2018
22 años
Sirviendo a la Democracia



ANEXO III

Plan de Simulacros

Acorde a lo estipulado en el Reglamento de Elecciones emitido por el INE, en su Sección Sexta, de los Ejercicios y Simulacros, Artículo 349, se establece:

1. *El Instituto y los OPL, conforme a sus respectivas competencias, deberán realizar ejercicios y simulacros obligatorios para verificar que cada una de las fases de la operación del PREP funcione adecuadamente, y prever riesgos o contingencias posibles durante el desarrollo de las mismas.*
2. *Los ejercicios tendrán como objetivo que el personal o los prestadores de servicios del PREP lleve a cabo la repetición de las actividades necesarias para la operación del programa, a fin de adiestrarse en su ejecución.*
3. *El objeto de los simulacros es replicar, en su totalidad, la operación del PREP, desarrollando cada una de las fases del proceso técnico operativo en el orden establecido. Se deberán realizar como mínimo, tres simulacros durante los tres domingos previos al de la jornada electoral.*

En igual forma en el Anexo 13, del mismo Reglamento de Elecciones, en su Capítulo VI de los Ejercicios y Simulacros, Numeral 16, determina:

16. *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 PREP, 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.*

Al término de los simulacros, se deberá realizar una evaluación a efecto de tomar las medidas preventivas y correctivas que correspondan. Asimismo, la instancia interna responsable de coordinar el PREP, deberá realizar un informe general del desarrollo de los simulacros.

17. *A los simulacros podrán acudir como observadores los miembros del Consejo General o del Órgano de Dirección Superior que corresponda, o sus representantes.*

Atendiendo a lo anteriormente descrito a continuación, presentamos el presente Plan de Simulacros:

PLAN DE SIMULACROS

Acorde a lo establecido en los Planes de Seguridad y Continuidad, el Programa de Resultados Electorales Preliminares amalgama de manera global los siguientes recursos:

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

Los tres comparten el mismo nivel de importancia para el funcionamiento del PREP, de ahí que deberemos medir el desempeño individual y grupal de los mismos.

Para ello una vez instalado el Equipamiento y establecidas las Telecomunicaciones, se capacitará a los Recursos Humanos que operarán el PREP.

Dicha capacitación será Teórico – Práctica. Se le proporcionará al personal que labore en el PREP, un manual en línea donde se describirán sus respectivas funciones en base al rol que desempeñará.

La única forma de evaluar estos recursos, es mediante su puesta en funcionamiento conjunta y esto se llevará a cabo en base a simulacros diarios.

Por ello en el Cronograma General de Actividades del PREP se describe que, a partir de concluida la capacitación de todo el personal, se iniciarán de forma periódica los Ejercicios Diarios del PREP. Se realizarán ejercicios diarios parciales y totales sobre el funcionamiento del PREP, todos los días ininterrumpidamente, aumentando cada vez el grado de complejidad en las mismas hasta llegar a un nivel óptimo de desempeño.

Estas pruebas iniciarán posterior a la capacitación y concluirán el 29 de Junio. Esto es dos días antes de la Jornada Electoral del 1 Julio, ya que el día previo a la Jornada se descansa a todo el personal de Acopio, Digitalización y Captura de datos para que no lleguen presionados y cansados a la Jornada Electoral.

Para efectos de evaluación se tienen previstos tres Simulacros Generales del PREP, mismos que están descritos en el Cronograma General de Actividades del PREP.

Se efectuará un Primer Simulacro General de funcionamiento del PREP en el Centro de Captura y Verificación del PREP y los Centro de Acopio y Transmisión de Datos evaluando el desempeño de las comunicaciones, el equipamiento y el personal. Este simulacro será sólo para propósitos de evaluación y participarán en él Personal del PREP y los miembros del Comité Técnico Asesor del PREP. Acorde por lo establecido por el INE, se llevará a cabo el Domingo 10 de Junio.

El Segundo Simulacro General del PREP se llevará a cabo con todos los CATD y el CCV simulando fallas en sus elementos y evaluando su desempeño. Es recomendable que en éste participen el personal del PREP, los miembros del Comité Técnico Asesor del PREP y miembros del Consejo General del OPL. Acorde por lo establecido por el INE, se llevará a cabo el Domingo 17 de Junio.

Se realizará el Tercero y último Simulacro General del PREP, al cual se recomienda participen la totalidad del Personal del PREP, los miembros del Comité Técnico Asesor del PREP, los miembros del Ente Auditor del PREP, los miembros del Consejo General del OPL, los representantes acreditados de los Partidos Políticos y Candidatos Independientes, así como los medios de Prensa. Acorde por lo establecido por el INE, se llevará a cabo el Domingo 24 de Junio.

Para llevar cabo estos Simulacros Generales del PREP el procedimiento será el siguiente:

PRIMER SIMULACRO GENERAL DEL PREP

El Primer Simulacro General de funcionamiento del PREP, será el Domingo 10 de Junio del 2018, en el Centro de Captura y Verificación y los Centros de Acopio y Transmisión de Datos, el primero instalado en la capital del Estado, a cargo del Supervisor General del PREP, en tanto que los CATD están instalados en los inmuebles de los Consejos Electorales.

Al citado simulacro, deberán asistir la totalidad del personal del PREP y los integrantes del Comité Técnico Asesor del PREP.

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 del PREP como en cada uno de los CATD instalados en todo el Estado.
2. A las 9:15 horas, dará inicio al pase de lista en todo el Estado, 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.
3. A las 10:00 horas se les solicitará a los integrantes del Comité Técnico Asesor del PREP, que determinen una leyenda que se escribirá sobre la primera acta de escrutinio y cómputo de la elección de Diputados de los CATD que se instalarán, para que se den instrucciones a dichos CATD, de anotarlas debajo de la sección de los datos de identificación en las Actas, se les pedirá que sean Acopiadas y Digitalizadas en los mismos, para su transmisión y proceso al CCV.
4. A la misma hora, se ordenará a los Coordinadores del CCV que indiquen a su personal que accedan al sistema y esperen el arribo de la información.
5. Una vez Capturadas dichas actas, se mostrarán en pantalla para que todos los asistentes observen y tengan certeza del funcionamiento del sistema.
6. A las 10:30 horas, se le darán instrucciones a la totalidad de los CATD para que simulen la Inconsistencia de Paquete No Entregado en la última casilla descrita en su bitácora para la elección de Diputados y la Digitalicen.
7. A las 11:00 horas, se darán instrucciones a todos los CATD, para que inicien el procedimiento de Acopio/Digitalización total en cada uno de ellos.
8. Conforme los CATD terminen su procedimiento de Acopio/Digitalización de información, tendrán que informar al CCV del PREP y esperarán instrucciones.
9. 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 del CCV.
10. Se emitirá un informe al Comité Técnico Asesor para el Programa de Resultados Electorales Preliminares sobre las cifras obtenidas en el Simulacro General del PREP y éste deberá informar al Presidente y Consejeros Electorales el mismo día del simulacro.

SEGUNDO SIMULACRO GENERAL DEL PREP

El Segundo Simulacro general de funcionamiento del PREP, será el Domingo 17 de Junio del 2018, en el Centro de Captura y Verificación y los Centros de Acopio y Transmisión de Datos, el primero instalado en la capital del Estado, a cargo del Supervisor General del PREP, en tanto que los CATD están instalados en los inmuebles de los Comités Electorales.

Al citado simulacro, deberán asistir la totalidad del personal del PREP, los integrantes del Comité Técnico Asesor del PREP, el Ente Auditor del PREP y los integrantes del Consejo General del OPL.

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 del PREP como en cada uno de los CATD instalados en todo el Estado.
2. A las 9:15 horas, dará inicio al pase de lista en todo el Estado, 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 Inconsistencias que han de simular durante el ejercicio.
3. A las 10:00 horas se les solicitará a los integrantes del Consejo General del OPL, que determinen una leyenda que se escribirá sobre la última acta de escrutinio y cómputo de la elección de Diputados de los CATD que se instalarán, para que se den instrucciones a dichos CATD, de anotarlas debajo la sección de los votos en las Actas, se les pedirá que sean Acopiadas y Digitalizadas en los mismos, para su transmisión y proceso al CCV.
4. A la misma hora, se ordenará a los Coordinadores del CCV que indiquen a su personal que accedan al sistema y esperen el arribo de la información.
5. Una vez Capturadas dichas actas, se mostrarán en pantalla para que todos los asistentes observen y tengan certeza del funcionamiento del sistema.
6. A las 10:30 horas, se les darán instrucciones a la totalidad de los CATD para que simulen la Inconsistencia de Casilla No Instalada en la primera casilla descrita en su bitácora para la elección de Diputados y la Digitalicen.
7. A las 11:00 horas, se darán instrucciones a todos los CATD, para que inicien el procedimiento de Acopio/Digitalización total en cada uno de ellos.
8. A las 12:00 horas, se realizará el simulacro de falla de energía en los CATD donde se encuentren los Comandos técnicos de cabecera para verificar el funcionamiento de los mismos en esta eventualidad.
9. A las 13:00 horas se pondrá en marcha el simulacro de terremoto y se desarrollará el Plan de Emergencias y Evacuación en el CCV.
10. Conforme los CATD terminen su procedimiento de Acopio/Digitalización de información, tendrán que informar al CCV del PREP y esperarán instrucciones.

11. 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 del CCV.

12. Se emitirá un informe al Comité Técnico Asesor para el Programa de Resultados Electorales Preliminares sobre las cifras obtenidas en el Simulacro General del PREP y éste deberá informar al Presidente y Consejeros Electorales el mismo día del simulacro.

TERCER SIMULACRO GENERAL DEL PREP

El Tercer Simulacro General de funcionamiento del PREP, será el Domingo 24 de Junio del 2018, en el Centro de Captura y Verificación y los Centros de Acopio y Transmisión de Datos, el primero instalado en la capital del Estado, a cargo del Supervisor General del PREP, en tanto que los CATD están instalados en los inmuebles de los Comités Electorales.

Al citado simulacro, deberán asistir la totalidad del personal del PREP, los integrantes del Comité Técnico Asesor del PREP, los integrantes del Ente Auditor, los integrantes del Consejo General del OPL, los Representantes acreditados de los Partidos Políticos y Candidatos Independientes, así como 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 instalados en todo el Estado.
2. Se darán instrucciones a los comandos técnicos del PREP para que se localicen en sus Cabeceras de Comando para atención de fallas simuladas. Dichos comandos estarán listos en los sitios predeterminados a las 9:00 horas.
3. A las 9:15 horas, dará inicio al pase de lista en todo el Estado, 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 10:00 horas se les solicitará a los integrantes del Consejo General del OPL, que determinen una leyenda que se escribirá sobre la primera acta de escrutinio y cómputo de la elección de Diputados de los CATD que se instalarán, para que se den instrucciones a dichos CATD, de anotarlas sobre la sección de los votos en las Actas, se les pedirá que sean Acopiadas y Digitalizadas en los mismos, para su transmisión y proceso al CCV.
5. A la misma hora, se ordenará a los Coordinadores del CCV que indiquen a su personal que accedan al sistema y esperen el arribo de la información.
6. Una vez Capturadas dichas actas, se mostrarán en pantalla para que todos los asistentes observen y tengan certeza del funcionamiento del sistema.
7. A las 10:30 horas, se les darán instrucciones a la totalidad de los CATD para que simulen la incidencia de Paquete Entregado Sin Sobre en la última casilla descrita en su bitácora para la elección de Diputados.
8. A las 11:00 horas, se darán instrucciones a todos los CATD, para que inicien el procedimiento de Acopio/Digitalización total en cada uno de ellos.
9. A las 12:00 horas, se realizará el simulacro de falla de energía en los CATD donde se encuentren los Comandos técnicos de cabecera para verificar el funcionamiento de los mismos en esta eventualidad.

10. A las 12:30 horas, se simulará la pérdida de señal en los CATD donde se encuentren Comandos Técnicos de cabecera 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 del PREP 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 del CCV.
13. Se emitirá un informe al Comité Técnico Asesor para el Programa de Resultados Electorales Preliminares sobre las cifras obtenidas en el Simulacro General del PREP y éste deberá informar al Presidente y Consejeros Electorales el mismo día del simulacro.