PLAN DE SEGURIDAD Y CONTINUIDAD 2021

Programa de Resultados Preliminares del estado de Tabasco

Proceso Electoral Local Ordinario 2020-2021

Unidad de Tecnologías de la Información y Comunicación

Versión 4.0 3 de marzo de 2021
Revisado por COTAPREPET

3-04-2021

Contenido

Contenido *2*
Introducción *4*
Objetivos *5*
Directrices de seguridad de la información *6*
Normatividad y medidas de seguridad 6
Análisis de riesgos en materia de seguridad de la información *8*
Proceso de análisis de riesgos (metodología) 8
Activos Críticos 9
Identificación de amenazas 10
Análisis de riesgos de seguridad 10
Implementación del plan de tratamiento de riesgos *10*
Análisis de riesgos sobre PREPET Casilla 12
Control de acceso *13*
Plan de Concientización *13*
Monitoreo y respuesta a incidentes de seguridad *14*
Lineamientos para la seguridad 15
Lineamientos de seguridad para el PREP Casilla 17
Listas de verificación 17
Seguridad Perimetral 17
Plan de Continuidad y plan de recuperación de desastres *18*
Análisis de riesgos para la continuidad 18
Lineamientos para la continuidad 19
Procedimientos previos 19
Acopio 20
Digitalización y Captura 20
Verificación 23

Lineamientos de continuidad para el PREP Casilla **24**
Plan de comunicación **25**
Matriz de escalamiento **25**
Simulacro de failover **26**
Auditoría externa en materia de seguridad de la información ***26***
Glosario ***27***
Referencias ***28***

Introducción

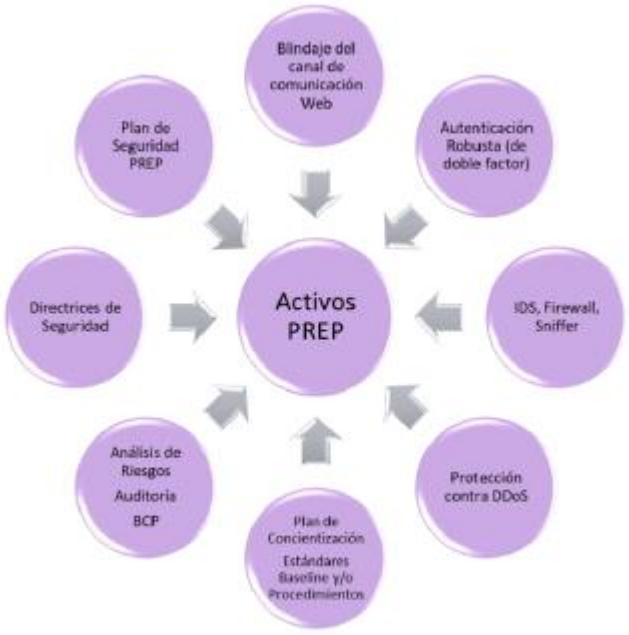
El presente **Plan de seguridad y continuidad** se establece con fundamento en el Articulo 348, numeral 1 del Reglamento de Elecciones del Instituto Nacional Electoral (INE) y los numerales 12 y 13 del Anexo 13 del mismo ordenamiento, con la finalidad de implementar las medidas de seguridad necesarias para la protección, procesamiento y publicación de datos, imágenes y bases de datos del Programa de Resultados Electorales Preliminares del Estado de Tabasco (PREPET).

De la misma forma determina las acciones que garantizan la ejecución de los procedimientos de acopio, digitalización, captura, verificación y publicación, en caso de que se suscite una situación adversa o de contingencia, de acuerdo al PTO, involucrando a través de la comunicación y socialización al personal que participe en su desarrollo a través de los ejercicios y simulacros.

Para este fin, se revisan los activos críticos, procedimientos, sistema informático, personal e instalaciones, para confrontar distintos escenarios técnicos y sociales que pudieran afectar el desarrollo continuo del sistema informático del PREPET, con la finalidad de que el modelo PTO que se empleará para la realización del PREPET, no se vea afectado en su ejecución, ni detenga el procesamiento continuo de la información de las actas que vayan siendo procesadas para su publicación.

Posterior a esto se desarrolla un análisis de riesgos en materia de seguridad aplicable a los distintos procedimientos del PREPET, donde se identifican los escenarios y las situaciones que se clasifican por su nivel de severidad, para determinar las acciones que hay que realizar para remediar las fallas que puedan presentarse.

Figura 1. Aspectos relacionados con los activos PREP



Objetivos

Objetivo General

Establecer la base de operación que permita la ejecución del PTO con seguridad y de manera tal que cada etapa se ejecute de forma continua y secuencial.

Objetivos específicos

1. Establecer los aspectos críticos de seguridad para la operación del PREPET. Su alcance se limita a los posibles riesgos, prioritariamente de alto impacto o probabilidad, de algún riesgo relativo a las etapas del PTO.

2. Contar con procedimientos previamente definidos que permitan la continua operación de los procesos del PTO ante alguna contingencia prevista tomando en cuenta la posibilidad de que ocurra.
3. Contar con la previsión de detectar riesgos relacionados con la operación de PREPET Casilla.

Alcance

El alcance de los presentes Planes de seguridad y Plan de continuidad aplican para todo el sistema informático, proceso técnico operativo, recursos humanos y procedimientos que se realicen con la finalidad de ejecutar el PREPET durante los simulacros y la Jornada Electoral.

Por lo anterior deberá socializarse y tomar en cuenta dentro de las actividades de capacitación para poderse aplicar desde el día 16 de mayo y hasta el día 7 de junio.

Directrices de seguridad de la información

Normatividad y medidas de seguridad

Reglamento de Elecciones, emitido en el ACUERDO INE/CG661/2016, Aprobado en Sesión Extraordinaria del Consejo General, celebrada el 07 de septiembre de 2016.

Conforme a lo establecido en el Artículo 348 numeral1, del Reglamento de Elecciones, los Organismos Públicos Locales deberán implementar las medidas de seguridad necesarias para la protección, procesamiento y publicación de datos, imágenes y bases de datos. Asimismo, deberán desarrollar en sus respectivos ámbitos de competencia, un análisis de riesgos en materia de seguridad de la información, que permita identificarlos y priorizarlos, así como implementar los controles de seguridad aplicables en los distintos procedimientos del PREP, conforme a las consideraciones mínimas descritas en el Anexo 13.

Implementación de controles de seguridad. Conforme a lo establecido los puntos 12 y 13 del Anexo 13, 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 de 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.

VI. Plan de seguridad: se deberá elaborar un plan de seguridad basado en los resultados de un análisis de riesgos, que permita llevar a cabo la implementación de controles en los distintos procedimientos de operación del PREP, así como en la infraestructura tecnológica. Dicho plan deberá ser elaborado por la instancia interna y, en su caso, en coordinación con el tercero que auxilie en la implementación y operación del PREP

Implementación del plan de continuidad. 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.

Con base en lo anterior, se elaborará el análisis de riesgos que servirá de base para delimitar los alcances del Plan de seguridad y continuidad.

Análisis de riesgos en materia de seguridad de la información

Proceso de análisis de riesgos (metodología)

Se define el término riesgo como un incidente o situación, que ocurre en un lugar, proceso o equipo, en un intervalo de tiempo determinado, con consecuencias negativas que pueden afectar el cumplimiento de los objetivos. El proceso de análisis de riesgo genera habitualmente una matriz de riesgo, en la cual se muestran los elementos identificados, la manera en que se relacionan, sus probabilidades y las posibles soluciones.

El análisis de riesgo es indispensable para lograr una correcta administración del riesgo. La administración del riesgo hace referencia a la gestión de los recursos de la organización. Existen diferentes tipos de riesgos como el riesgo residual y riesgo total, así como también el tratamiento del riesgo, evaluación del riesgo y gestión del riesgo entre otras.

Para el presente plan, la UNITIC y el COTAPREPET proponen una lista inicial de riesgos, la cual es consensuada previo al desarrollo de los temas de seguridad y continuidad. Lo anterior en base a las experiencias en desarrollos previos de PREPET. Mediante reuniones de trabajo con el COTAPREPET se propuso inicialmente dos planes, los cuales después de una evaluación, se llegó a la conclusión de incluirlos en un solo documento. Para su valoración final se desarrolló una lluvia de ideas que forman parte del presente documento, el cual recaba los comentarios y sugerencias individuales de todos los miembros del COTAPREPET.

La metodología finalmente consistirá en la emisión de puntos que se deberán cumplir por todos los actores que intervengan en el desarrollo y operación del PREPET en cada una de las etapas del PTO, con la finalidad de contar con estrategias para el manejo de solamente aquellos riesgos relacionados con el PREPET y que puedan afectarlo para el proceso actual.

Activos Críticos

Existen diversos tipos de activos, incluyendo:

a) Activos de información: bases de datos y archivos de datos, hojas electrónicas con datos, documentación del sistema, información de investigaciones, material de capacitación, procedimientos operacionales o de soporte, planes de seguridad, planes de continuidad, acuerdos para contingencias, rastros de auditoría e información archivada.
b) Activos de software: software de aplicación, software del sistema, herramientas de desarrollo.
c) Activos físicos: equipo de cómputo, equipo de comunicación, medios removibles y otros equipos.
d) Servicios: servicios de computación y comunicación, servicios generales.
e) Personas: competencias, habilidades, experiencia y sus roles que desempeñan.

Se identifican los siguientes activos críticos:

1. Personal de coordinación. Coordinadores del PREPET que se requiere estén presentes durante su operación.
2. Personal operativo. El establecido para la ejecución de cada una de las etapas del PTO.
3. Servidores. Los equipos de cómputo que almacenan y procesan la información.
4. Enlaces de red. Servicios de redes y telecomunicaciones necesarios para la interconexión de sistemas informáticos y para la conexión hacia la red de Internet.
5. Bases de datos. La información electoral de base tal como lista de casillas, listado nominal por casillas, información de las candidaturas, logotipos de partidos, candidaturas comunes, coaliciones y candidatos independientes.
6. Equipo de cómputo y de digitalización. Computadoras laptop y escáneres que operarán para la ejecución del PREPET.
7. Actas PREPET de prueba. Se requieren de aproximadamente 6000 actas para los simulacros.

Identificación de amenazas

Las amenazas no identificadas y tratadas pueden conllevar a que un evento o ataque que logre realizar algún fraude o tener como consecuencia la pérdida o robo de información. Esto puede presentarse debido a sucesos físicos como puede ser un incendio o una inundación. Otro factor que puede permitir la afectación de la información puede ser debido a negligencia y decisiones institucionales que permitan el mal manejo de contraseñas o debido también a no usar cifrado. Desde el punto de vista de una organización pueden ser tanto internas como externas.

Análisis de riesgos de seguridad

Este análisis tiene como finalidad establecer las bases y procedimientos para proteger la información durante la ejecución del PREPET. Analizando en principio tenemos que un firewall puede limitar los vectores de ataque, pero, si no se protege el Sistema Operativo y la aplicación o los servicios que se publican, éste pudiera permitir explotar las vulnerabilidades de los servicios publicados. En los componentes desplegados dentro del espacio en Internet se implementan las herramientas de seguridad y alta disponibilidad del prestador del servicio, pero además se imponen controles adicionales, por ejemplo, configuración de aplicaciones y buenas prácticas, según se requiera, para asegurar la salvaguarda de la información.

Implementación del plan de tratamiento de riesgos

Es importante definir el alcance de la seguridad informática, ya que hay que especificar los riesgos y las probabilidades de incidencia, ya identificadas se informa a las áreas de competencia para que realicen las configuraciones necesarias para subsanar las eventualidades consideradas, como se establece en la tabla 1:

Tabla 1. Análisis de los factores de riesgo priorizados

Escenario de riesgo	Nivel de riesgo	Detección	Controles de seguridad	Nivel de probabilidad
DDoS. Ataques de Denegación de servicio, sobrecarga de los servicios de red y bajo esta condición servicios como los de página web no pueden operar	Alto	Auditoría informática	Empleo de Nube, FW, configuración de DNS y Switches	Bajo
Ataques internos y externos. Hackeo de una página o servicios de red para obtener control. Control de acceso lógico perimetral	Medio	Auditoría informática	Firewall	Medio
Bugs de código, SQL Injection, entre otros	Bajo	Auditoría informática	Revisión de código y aplicación de parches	Bajo
Virus	Medio	reporte de usuarios	Instalación y reportes de antivirus	Medio
Configuraciones erróneas en los servidores	Bajo	reporte de usuarios	Checklist de configuración	Medio
Configuraciones erróneas en los equipos de comunicaciones	Bajo	reporte de usuarios	Checklist de configuración	Medio
Problemas con la autenticación de usuarios y manejo de contraseñas	Bajo	reporte de usuarios	Empleo de mejores prácticas	Bajo
Fallo de monitoreo. Pérdida de información sobre el estado de los servicios y equipos activos	Bajo	reporte de usuarios	Sistema de monitoreo alterno	Bajo
Falta de segregación o separación de la red	Medio	Auditoría informática	Red INTERNET en enlaces principales y VPN en enlaces redundantes	Bajo
Falta de filtrado de contenido para los servicios de correo electrónico	Bajo	Auditoría informática	Módulos antiphising del Firewall perimetral	Bajo
Uso de contraseñas débiles y la falta de actualizaciones en los servidores web del sitio de publicación de resultados lectorales preliminares, lo que podría ocasionar que un atacante publique información ajena al PREP (defacement).	Bajo	Auditoría informática	Checklist	Bajo
La falta de un control de acceso lógico perimetral a la red interna que podría provocar que un atacante	Medio	Auditoría informática	Firewall	Medio

ingrese a los servidores y bases de datos				
Falta de controles de acceso físico a los CATD y CCV	Bajo	Reporte de usuarios	Empleo de identificaciones visibles y registro de personal en bitácora para acceder a las áreas PREPET	Bajo
Fallas en el funcionamiento normal de los equipos por falta de mantenimiento	Bajo	Reporte de mantenimiento	Calendario de programación de mantenimientos por tipo de equipamiento	Bajo

Análisis de riesgos sobre PREPET Casilla

Los dispositivos que tendrán la aplicación del PREP Casilla serán asignados a los CAE Local para cada una de las rutas previstas, se entregarán con el 100% de batería para así evitar que, al momento de estar operando, el equipo se quede sin batería. Los riesgos analizados para el PREP Casilla se consideran en la tabla 2.

Tabla 2. Análisis de riesgos del PREPET Casilla

Contingencia	Nivel de riesgo	Etapas PTO	Acciones remediales	Nivel de probabilidad
Robo o extravío del dispositivo móvil	Bajo	Digitalización desde la casilla	Las actas se digitalizarán desde el CATD al que deban enviarse, de acuerdo al PTO	Bajo
Problemas con la autenticación de usuarios y manejo de contraseñas	Bajo	Digitalización desde la casilla	Empleo de mejores prácticas	Bajo
Fallo en la cobertura de red 3G o 4G	Medio	Digitalización desde la casilla	El CAE Local se desplazará al siguiente casilla o zona	Medio

			donde tenga cobertura 3G, para lograr la trasmisión	
Ausencia del CAE Local	Bajo	Digitalización desde la casilla	Las actas se digitalizarán desde el CATD al que deban enviarse, de acuerdo al PTO	Bajo
Pérdida de cuentas	bajo	Digitalización desde la casilla	El CAE Local deberá solicitar apoyo al coordinador del PREPET mediante llamada telefónica	bajo

Control de acceso

Los mecanismos de control de acceso están definidos por los privilegios y roles de usuarios definidos en los sistemas informáticos: los del PREPET y los de PREP Casilla.

Plan de Concientización

El objetivo de este plan será establecer acciones para que los usuarios que intervengan en el PREPET puedan conocer los riesgos y amenazas que puedan presentarse, así como saber la forma en que se puedan minimizar dichos riesgos o prevenir algún incidente de seguridad.

El alcance del Plan de Concientización cubrirá a todos los operadores y coordinadores del PREPET, así también aquellos que en su ámbito les corresponda la supervisión, como son en el caso de los CATD, los vocales ejecutivos. Para este fin se emplearán materiales didácticos en formato electrónico los cuales permitan su fácil distribución y reúso.

Se deberá impartir un curso relacionado con los temas de seguridad de impacto al PREPET a todo el personal antes mencionado cubriendo los aspectos de seguridad para cada etapa del PTO. Previo a la impartición del curso de seguridad se deberá realizar una evaluación diagnostica sobre el manejo de estos temas. Posterior al curso se deberá realizar un examen final el cual deberá tener una ponderación mínima a cubrir, de forma tal que se tenga registro de que el personal que operará el PREPET tenga los conocimientos mínimos sobre aspectos de seguridad requeridos para el cumplimiento del Plan de seguridad y continuidad.

Las actividades para la concientización deberán estar incluidas en los calendarios de actividades de capacitación, del PREPET y de los simulacros.

Tabla 3 Actividades de concientización dentro de la capacitación PREPET

Actividad	Personal	Fecha o periodo
Plática de concientización sobre seguridad informática	Todos los tipos	Abril 2021
Capacitación de seguridad PTO y en general	Programadores, área de sistemas, área de infraestructura y área de redes	Abril 2021
Capacitación sobre seguridad de las etapas del PTO	Personal de Coordinación, Vocales ejecutivos de CATD y personal de la Dirección Ejecutiva de Organización y Educación Cívica, entre otras	Abril 2021
Capacitación sobre seguridad de las etapas del PTO	Personal de Operativo	Abril 2021

Monitoreo y respuesta a incidentes de seguridad

Para constatar la operación eficiente de la infraestructura y del sistema PREPET se establecerá el monitoreo de lo siguiente:

1. Tráfico de red por enlace o segmento de red. Esto se realizará mediante las gráficas de paquetes de entrada y salida generadas con apoyo del protocolo de SNMP y de la herramienta CACTI.

2. Tráfico de red por enlace o segmento de red para la RED INTERNET. Esto se realizará mediante las gráficas de paquetes de entrada y salida generadas del proveedor de servicios colocadas en su Centro de Operaciones (NOC).
3. Verificación de estatus de servidores y activos críticos. Los equipos como servidores, routers, switches y equipo de cómputo que son indispensables para la operación del sistema PREPET se agregarán a un grupo de monitoreo gráfico y envío de alertas, esto mediante la aplicación NAGIOS, la cual hace uso de protocolos SNMP e ICMP para tal fin.
4. Los reportes de ambos sistemas serán publicados en páginas web con contraseñas solamente disponibles para el personal autorizado.
5. Monitoreo del personal de operación.
6. Las acciones para el monitoreo del desempeño de las actividades y funciones del personal de operación.
7. Monitoreo por video del personal PREPET en las juntas.
8. Reportes de actas procesadas por operador.
9. Uso de las cámaras web de los equipos laptop para el monitoreo del personal

Lineamientos para la seguridad

El Plan de seguridad y Continuidad se desarrolla tomando como base los riesgos que en las experiencias previas del IEPCT se puedan presentar, así como también en una revisión de posibles riesgos en el manejo y estrategias de gestión de riesgos resultados de otros escenarios. El PREPET requiere un alto nivel de seguridad en el manejo de la información, por lo que es necesario implementar las presentes medidas que permitan fortalecer la seguridad y disminuir el riesgo, por lo que se establece la necesidad de observancia y cumplimiento mínimo de los siguientes puntos:

1.- Deberá considerarse la protección de la información en el flujo de datos tanto dentro del CCV como fuera de él, y hacia los CATD, empleando canales de comunicación seguros y protocolos cifrados. Los medios de transmisión serán seguros. El objetivo es que se impida la alteración de la información electoral en tránsito, a través de la red de comunicaciones, así como el acceso de manera no autorizada a los equipos de cómputo que intervienen en el proceso.
2.- Se considerará el uso de algoritmos de criptografía con reconocida robustez en la industria y una buena administración de claves, que aseguren la adecuada protección de la confidencialidad de los datos. Entre ellos, canales seguros mediante protocolo HTTPS (usando TLS) y utilizar métodos de verificación de integridad de la información enviada y recibida como, por ejemplo, utilizar HMAC.

3.-. Se debe considerar el empleo de las técnicas de programación segura acorde al lenguaje de programación utilizado.
4.- Se debe considerar para el diseño del sistema el Principio del Menor Privilegio y así limitar la exposición del servicio ante incidentes.
5.- Todo acceso administrativo a servidores o dispositivos de red en los cuales esté disponible se deberá realizar a través del protocolo SSH, solo se encuentran activos los servicios necesarios para apoyar la operatividad. La autenticación de usuarios administrativos es personalizada y centralizada.
6.- Los eventos deberán ser registrado por SYSLOG o sistemas de bitácoras e inspeccionados por los operadores de monitoreo.
7.- Se deberá realizar un fortalecimiento de servidores y terminales que incluya:

a. Remover y restringir en la medida de lo posible aquellos servicios que históricamente son considerados inseguros tales como *telnet, traceroute, FTP, TFTP, etc*.
b. Deshabilitar y remover todos los puertos de escucha de red no requeridos por los servicios utilizados en la plataforma electoral
c. Deshabilitar y remover los servicios y aplicaciones locales innecesarios
d. Mantener el sistema operativo actualizado con los últimos parches de seguridad
e. Utilizar políticas de contraseñas robustas
f. Usar cuentas de usuarios individuales para los accesos interactivos
g. Cifrar datos sensibles en almacenamiento y en tráfico
h. Usar verificador de integridad de archivos
i. Mantener la hora y la fecha sincronizada
j. Realizar periódicamente verificación de vulnerabilidad

8.- Se deberá realizar la **revisión** de las configuraciones físicas y lógicas de: firewalls, equipos de comunicaciones, servidores, servicios de red, bases de datos y de las terminales.
9.- Para confirmar que la información recibida proviene realmente de un CATD establecido, todas las terminales se validarán empleando mecanismos como la dirección MAC Address.
10.- Cada computadora tendrá instalado el software requerido para el sistema del PREPET, no se podrá instalar ningún otro software. Además, tendrá especificada una clave de acceso en el momento mismo de su encendido, posteriormente, para iniciar la digitalización de las AEC se necesita que cada operador registre su clave personal de acceso, evitando de esta forma que personal ajeno a esta actividad se involucre en ella. En caso de ausentarse el operador bloqueará el equipo de digitalización.
11.- Las comunicaciones al interior de los CATD y el CCV serán del tipo LAN de cobre o fibra óptica por lo menos de 100 Mbps redundantes, o enlaces privados Punto a Punto redundantes. La seguridad en estos enlaces deberá contar con una red VPN como mecanismo de comunicación en lo posible.

Lineamientos de seguridad para el PREP Casilla

1. Se tendrá el registro de usuarios y contraseñas en las bitácoras del sistema, aunado a métodos alternativos para la asignación de cuentas de usuario. Se deberá emplear una base de datos para listar los usuarios con su información y nivel de privilegios, preferentemente.
2. La comunicación con la API será por medio de HTTPS.
3. En caso de fallo de la aplicación PREP Casilla se podrá emplear la transmisión de imágenes mediante la aplicación “Dropbox”.

Listas de verificación

Se establecerán listas de verificación para la supervisión del estado de los equipos disponibles y configurados relacionados con la seguridad de la red, tales como ruteadores, cortafuegos, conmutadores y servidores. Otra lista de verificación deberá emplearse para cada uno de los CATD, en la que deberá corroborarse que están debidamente conectados y tomadas en consideración las principales recomendaciones de seguridad para la ejecución del PTO.

Seguridad Perimetral

Se contará con un equipo de cortafuegos o firewall como mecanismo principal para la seguridad perimetral. Este equipo aplicará las reglas de filtrado entre las redes internas del IEPCT y la red de Internet. Deberá aplicar reglas particulares para aplicar filtrado de protocolos que no se desea que pasen tráfico desde las redes internas hacia las externas y viceversa.

Plan de Continuidad y plan de recuperación de desastres

Análisis de riesgos para la continuidad

El presente proceso servirá para determinar acciones que garanticen las ejecuciones de los procesos de acopio, digitalización, captura, verificación, publicación, cotejo y empaquetado en los casos en que presente situaciones adversas o de contingencia para la restauración de la continuidad de la operación. Estas acciones aplicarán para todas las personas que participen en cada una de las fases del PREPET.

La tabla 4, especifica las probables contingencias que serán ejecutadas en las pruebas y los simulacros, lo anterior para dar una correcta solución y permitir la óptima operación del PREPET durante la jornada electoral.

Tabla 4. Análisis de riesgos acerca de posibles contingencias

Contingencia	Nivel de riesgo	Acciones	Probabilidad
Fallo de energía eléctrica CATD/CCV	Medio	Activar planta de energía de emergencia	Baja
Enlaces CATD -CCV	Bajo	Usar el enlace ADSL/VPN alterno, descarga fuera de línea a USB.	Baja
Enlaces Internet	Bajo	Usar el enlace de proveedor de servicios alterno	Baja
Equipo terminal de cómputo	Bajo	Emplear terminales de reemplazo	Baja
Periféricos	Bajo	Emplear terminales de reemplazo	Baja
Ausencia del personal de operación de CATD	Bajo	En primera instancia llamar al personal de reserva, luego operar mediante otro personal que esté capacitado para la función requerida y en último caso, se puede sustituir por un coordinador	Baja
Personal CCV Coordinación	Bajo	Si no llega un personal de operación se puede sustituir por un coordinador	Baja
Fallo de servidores	Bajo	Empleo de servidores de respaldo físicos y secundariamente de servidores colocados en la nube.	Baja
Cierre de acceso a los CATD y CCV debido a marchas,	Medio	Se podrán emplear sedes alternas para la operación, la lista se define en la tabla de sedes alternas	Medio

bloqueos, plantones, manifestaciones,			
Desastres naturales como sismos, inundaciones, incendios, entre otros	Bajo	Se deberán emplear sedes alternas y servicio de nube para los CATD y CCV que pudieran verse afectados por estos fenómenos	Bajo

Lineamientos para la continuidad

Se definen procesos ante contingencias, los cuales son necesarios para garantizar la continuidad de la operación durante del día de la jornada electoral ante cualquier eventualidad que pudiese presentarse, estos, están basados bajo los procedimientos de acopio, digitalización, captura, verificación y publicación, en caso de que se suscite una situación adversa o de contingencia.

Procedimientos previos

1.- Se deberá definir el listado de los coordinadores, con la información del personal operativo y de la mesa de ayuda.
2.- A las 6:00 PM del 6 de junio de 2021 se iniciarán las actividades de diagnóstico en los CATD y en el CCV a fin de verificar el funcionamiento de los equipos e identificar posibles fallas que requieran reemplazo de los mismos.
3.- En caso de fallas en cualquiera de los CATD. Es importante acotar que las laptops contarán con una batería interna con capacidad de al menos hora y media de autonomía en caso de una falla eléctrica. Se dispondrá de cinco computadoras, cinco impresoras y cinco escáneres de reserva para todos los CATD, además de cinco computadoras y tres impresoras de reserva para el CCV.
4.- Para contar con restauración y recuperación, de la información contenida y generada por el sistema, durante la ejecución del PREPET, la información que se reciba en el CCV, será respaldada en servidores del CCV del IEPCT, en tiempo real, de forma tal que, si ocurriese una situación inmanejable en el CCV, los resultados serán recibidos y consolidados en el CCV del IEPCT. Los tiempos de recepción, procesamiento y envío de información a los sitios de difusión de resultados serán similares a los del funcionamiento del CCV. Esta información deberá estar disponible en el CCV colocada de modo visible en el área de servidores.
5.- En caso de ausentismo del personal operativo: Acopiadores, Digitalizadores, Capturistas y verificadores, se procederá a ejecutar el procedimiento del reemplazo de personal siguiente:

a. Se determina la ausencia, a través del chequeo telefónico de asistencia. Esto se logra cuando el supervisor del CATD, confirma la ausencia llamando ya sea el personal en cuestión, o bien a un operador en la misma ubicación
b. Si el supervisor confirma la ausencia, el coordinador de personal confirma al personal suplente, debidamente capacitado, para ir a la ubicación correspondiente, tomar el lugar y las responsabilidades del personal ausente
c. El sustituto reportará su asistencia al llegar a la ubicación respectiva
d. El sustituto quedará entonces a cargo de las operaciones en la ubicación asignada hasta el final del evento
e. Se establecerán los umbrales de tiempo necesarios que debe considerar el coordinador de personal para activar el proceso de reemplazo del personal

6.- Para la jornada electoral, en cada CATD contarán con una planta generadora de energía eléctrica que tendrá capacidad suficiente para abastecer el total de su demanda, incluyendo lámparas y equipamiento. El funcionamiento de la misma será probado antes de la jornada electoral; se simulará una interrupción de corriente eléctrica en algunos CATD durante el primer simulacro, así como las condiciones de previsión de planta eléctrica de respaldo en el CCV. En caso de detectar un riesgo potencial deberá corregirse y probarse durante en el mismo simulacro.
Las sedes de los CCV del IEPCT cuentan con una planta de energía de emergencia que entrará en funcionamiento en cinco minutos a partir de una falla de corriente eléctrica. Se deberá disponer de un sistema de energía ininterrumpida (UPS), con una autonomía suficiente para soportar a los equipos de red que conforman la solución del PREPET al menos hasta que entre la planta generadora de electricidad de emergencia. Las plantas generadoras de electricidad de emergencia deberán contar con suficiente combustible para poder mantener la continuidad del PREPET.

Acopio

1. Los problemas relacionados con la etapa de acopio deberán ser comunicados en primer nivel de atención al coordinador del PREPET.
2. El supervisor podrá coadyuvar a reasignar las funciones de los capturistas y digitalizadores disponibles, con la finalidad de atender la ausencia o problemática de operación de alguno de ellos.

Digitalización y Captura

1. Para la sustitución de equipos en la etapa de digitalización en caso de contingencia de deberá seguir el siguiente procedimiento:
a. El Digitalizador identifica la parte que necesita ser reemplazada

b. El Digitalizador llama al supervisor y solicita la autorización para la sustitución. Se requiere esta autorización para evitar los reemplazos no autorizados que terminan por agotar la contingencia sin la supervisión y conocimiento del personal técnico
c. El supervisor pide apoyo al coordinador de soporte y este autoriza la sustitución de los equipos y periféricos y determina de donde se trasladará el componente, dependiendo de la disponibilidad y proximidad del mismo en referencia al CATD
d. El Digitalizador recupera el componente de sustitución del CATD y lleva a cabo el procedimiento de sustitución.

2.- En caso de no poder llevar a cabo la transmisión de los datos de las imágenes desde algún CATD, bien sea por que el medio de transmisión no se encuentra disponible o por cualquier otra causa, el capturista o digitalizador podrá dar inicio al procedimiento de transmisión de contingencia.

a. Se emplearán los enlaces redundantes configurados previamente
b. Si se presentase daño en el enlace principal, entonces el dispositivo de la red cambiará automáticamente al enlace previsto como salvaguarda, de forma tal que la transmisión no sufra retraso importante en la práctica. Este hecho se inscribirá en la bitácora del CATD.

3.- En los casos de falla de los enlaces INTERNET que se empleen, deberán emplear redes privadas virtuales (VPN) sobre enlaces ADSL.
4. Los enlaces de telecomunicaciones serán probados en su funcionamiento a lo largo de las pruebas y simulacros, ya que los CATD contarán con sistemas de información automatizados que requieren estar enviando y recibiendo información, de manera similar a lo que se realizará el día de la jornada electoral.
5. Una vez instalados y configurados los enlaces, serán monitoreados por herramientas instaladas en el sistema operativo Linux. Si se detecta la caída de un enlace, estas herramientas notificarán al área correspondiente, quienes se podrán en contacto con el CATD o el CCV, para verificar y solucionar la posible falla, posterior a esto, confirmarán la continuidad de la operación.
6.- En los casos en que no se pueden capturar o verificar los datos de las actas digitalizadas por falla de equipos en el CCV se contará con lo siguiente:

a. Tres laptops de reemplazo en el CCV, se contará con equipos de remplazo tanto portátiles y escáneres ya conectados
b. Laptops de reemplazo para cuatro sectores que cubren los 22 CATD

7.- De no lograr la trasmisión de las actas digitalizadas. El digitalizador se comunica con el coordinador de soporte del CCV para verificar la configuración del equipo según el CATD que corresponda.
8. Si por alguna razón extraordinaria o un problema en alguna central telefónica (ISP), no se pudiera utilizar ninguno de los enlaces de telecomunicaciones con que cuente cada

CATD, se continuará con la digitalización de las AEC hasta su finalización. Cuando se concluya dicha actividad se trasladará una copia de los datos al punto señalado en la tabla 4, para continuar con el PTO.
9. La Unidad definirá las sedes alternas, desde donde enviarán sus imágenes en caso de contingencia. El procedimiento en casos de contingencia para la transmisión de datos desde otro CATD estará integrado por las siguientes actividades:

a. Obtener una copia en medio electrónico (disco compacto o USB)
b. Depositarlo en un sobre que será sellado y firmado por los integrantes del Consejo Distrital respectivo. La negativa a firmarlo por parte de alguno de ellos no impedirá el envío
c. Levantar un Acta Circunstanciada donde se dé cuenta de los hechos y de quiénes acompañan el traslado
d. Avisar al CCV que se inició el procedimiento extraordinario de envío
e. Llevar la información con una copia del Acta Circunstanciada a la sede establecida, en el traslado podrán participar los representantes que así lo deseen
f. En caso de que surja la necesidad de utilizar este procedimiento, deberán realizar el envío de información en dos ocasiones: una cuando hayan digitalizado el 50% de sus casillas y el otro al concluir con la digitalización de sus Actas PREP; en ambos casos levantará el acta circunstanciada y se formará una Comisión que realice el traslado.
g. En la sede alterna o destino, previa certificación y apertura por parte de al menos un consejero distrital y un representante de partido, se dará aviso al CCE, que ya se encuentren en la sede alterna o destino. Luego la información será incorporada a las terminales y posteriormente será transmitida al CCE. Se toman las sedes alternas en orden de prioridad como se establece en la tabla 5.

Tabla 5. Puntos alternos para la captura o trasmisión de datos

Punto	Sedes Alternas
CATD01	CATD15, CATD18
CATD02	CATD04, CATD03
CATD03	CATD02, CATD16
CATD04	CATD02, CATD03
CATD05	CATD10, CATD22, CCE
CATD06	CATD09, CATD12, CATD22, CCE
CATD07	CATD08, CATD09, CATD22, CCE
CATD08	CATD09, CATD12, CATD22, CCE
CATD09	CATD08, CATD12, CATD22, CCE
CATD10	CATD05, CATD12, CATD22, CCE
CATD11	CATD18, CATD22, CCE
CATD12	CATD06, CATD09, CATD22, CCE
CATD13	CATD20, CATD14, CCE
CATD14	CATD13, CATD20, CATD22, CCE
CATD15	CATD01, CCE
CATD16	CATD04, CCE
CATD17	CATD14, CATD19, CATD22, CCE
CATD18	CATD11, CATD22, CCE
CATD19	CATD12, CATD17, CATD22, CCE
CATD20	CATD13, CATD14, CCE
CATD21	CATD06, CATD08, CATD22, CCE
CCV	CATD22, CCE

10.- En caso de que falle el escáner o las terminales, la digitalización de las Actas PREPET se realizará en cuanto se cuente con la disponibilidad de los elementos necesarios enviando las imágenes en un lapso de tiempo menor a la duración del PREPET. Para ello podrán trasladarse las actas a las sedes ya establecidas en la tabla 5 para continuar con en esta actividad. Para los casos de los distritos cercanos al municipio de centro se contará con el apoyo y respaldo del CATD 22.

Verificación

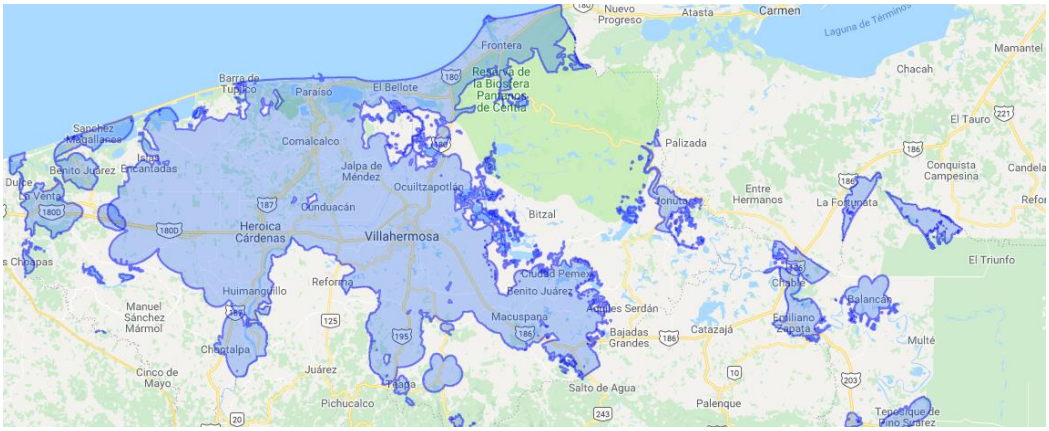
1. Los problemas relacionados con la verificación de actas serán atendidos en primer nivel de atención por los supervisores y coordinadores presentes en el CCV.

2. Se instalará el CCV del IEPCT como centro de captura y verificación, el cual, en caso de contingencia, deberá operar con una infraestructura de comunicaciones similar a la del CCV, así como equipo de cómputo con capacidades semejantes, dando prioridad a la captura y verificación de resultados.

Lineamientos de continuidad para el PREP Casilla

1. En caso de robo o extravío del dispositivo móvil, el CAE Local debe trasladarse a las casillas asignadas para notificar el evento y se logre la continuidad de operación del PTO. Posteriormente el CAE Local se debe ubicar en el CATD más cercano e informar al vocal ejecutivo, con el objetivo de levantar el acta de circunstanciada de la eventualidad.
2. Al no presentarse el CAE Local en las casillas asignadas, la digitalización de las actas se realizará desde el CATD asignado de acuerdo al PTO.
3. Al no haber cobertura de red 3G o 4G, el CAE Local se desplazará a la siguiente casilla o zona donde tenga cobertura celular para lograr la trasmisión. Él área de cobertura estimada se obtuvo de la web de IFETEL, del mapa que comprende las zonas de cobertura dentro del Estado de Tabasco, ver figura 2.

Figura 2. Mapa de cobertura 3G en el estado de Tabasco



4. Dentro de la cobertura garantizada pueden presentarse condiciones que afecten el servicio, debido a las características técnicas y al estado de conservación del equipo móvil del usuario o a su uso en el interior de algunos edificios, sitios

subterráneos, elevadores, o en lugares que presenten una concentración inusual de usuarios.

Plan de comunicación

Los canales de comunicación para el PREPET serán principalmente mediante la información mediante llamadas telefónicas del conmutador interno del IEPCT. Secundariamente se podrán emplear el correo electrónico institucional.

Matriz de escalamiento

En caso de presentarse situaciones que afecten la continuidad de operación del PREPET, se establecen los responsables dependientes del primer, segundo y tercer nivel de notificación. A continuación, se enlistan por niveles y se incluye la información de contacto en caso de presentarse alguna contingencia. En caso de no resolverse se escalará al nivel superior, como se muestra en la tabla 6.

Tabla 6. Matriz de escalamiento

Primer nivel	Acopiador/ supervisor	Personal directamente presencial en cada CATD y CCV
		Se comunicará con ellos directamente para informales las situaciones que se presenten en los CATD.
		Deberán estar identificados mediante el gafete o uniforme distintivo.
Segundo Nivel	Coordinador	Personal de coordinación que supervisa cada una las cinco rutas de soporte y Coordinadores PREPET
		Se establece una coordinación por áreas de atención como son redes, infraestructura, programación, capacitación y seguridad
		Infraestructura extensión 1057 Redes extensión 1057 Sistemas extensión1056 Programación extensión 4104 Capacitación 2022 Seguridad 2022
Tercer nivel	Coordinador PREPET	Instancia responsable del PREPET Coordinación general del PREPET unitic@iepct.mx extensión 1055

Simulacro de failover

Debido a la importancia de considerar escenarios adversos, el IEPCT realizará durante el tercer simulacro programado para el día 30 de mayo, pruebas de "failover" principalmente en dos aspectos: pruebas de fallos de enlaces de internet y pruebas de fallos de interrupción de energía eléctrica.

Para las pruebas de fallos de conexión a Internet se prevé contar con un enlace redundante tipo satelital, el cual deberá entrar en operación de forma automática preferentemente. Se deberá medir el tiempo de recuperación del servicio de red.

En lo relativo a pruebas de fallos en el suministro eléctrico, la previsión será contar con plantas de energía eléctrica en cada CATD. Se deberá probar el acoplamiento de cada planta, así como medir el tiempo en el que estas entren en operación.

Otras pruebas podrán incluir la simulación de fallos de equipo de cómputo y de equipos de digitalización.

Auditoría externa en materia de seguridad de la información

Para la verificación de los aspectos señalados en el Anexo 13 del reglamento de elecciones se estable como parte del convenio de colaboración con la FES Acatlán de la UNAM el apoyo y seguimiento al presente Plan de seguridad y continuidad.

Glosario

Para los efectos del presente se entiende por:

Acta PREP	Copia del AEC destinada para el PREPET en su ausencia podrá tomarse cualquier otra copia de las AEC restantes
AEC	Acta de Escrutinio y Cómputo
CAE Local	Capacitador Asistente Electoral Local
CATD	Centro de Acopio y Transmisión de datos
CCV	Centro de Captura y Verificación de datos
CCE IEPCT	Centro de Computo Estatal del IEPCT ubicado en la calle Eusebio Castillo número 747, Puede cubrir las funciones de un CATD o CCV
COTAPREPET	Comité Técnico Asesor del PREPET
DDoS	Es un ataque de denegación de servicio, también llamado ataque DDoS (por sus siglas en inglés, *Distributed Denial of Service*), es un ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
Failover	Es el modo de funcionamiento de respaldo en el que las funciones principales de los dispositivos son preservadas por los componentes secundarios del dispositivo cuando sus componentes principales no están disponibles, ya sea, por una falla o inactividad de estas.
Firewall	Dispositivos de seguridad perimetral de la red que monitorea el tráfico de red - entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.
IDS	Sistema de Detección de Intrusos, por sus siglas en inglés "*Intrusion Detection System*".
IEPCT	Instituto Electoral y de Participación Ciudadana de Tabasco
IPS	Sistema de Prevención de Intrusos, por sus siglas en inglés "*Intrusion Prevention System*".
PREPET	Programa de Resultados Electorales Preliminares del Estado de Tabasco
PTO	Proceso Técnico Operativo
Sniffer	Es una aplicación especial para redes informáticas, que permite como tal capturar los paquetes que viajan por una red.
Sobre PREP	Sobre diseñado especialmente para cada proceso electoral en el que se guarda la copia del Acta PREP de la casilla la cual se coloca por fuera del paquete electoral
WAF	Firewall de Aplicaciones Web, por sus siglas en inglés "Web Application Firewall".

Referencias

1. Plan de Trabajo del Programa de Resultados Electorales Preliminares del Estado de Tabasco 2021.
2. Proceso Técnico Operativo del PREPET 2021.
3. Reglamento de Elecciones:
4. Lineamientos del Programa de Resultados Electorales
5. Plan de seguridad y continuidad del PREPET 2018
6. Recomendaciones adicionales para la emisión de los Planes de seguridad y continuidad. Proceso Electoral Local 2020-2021. UNICOM – INE.
7. Mapa IFETEL: http://www.ift.org.mx/mapa-de-cobertura/telcel-3g-tab