GRUPO PROISI S.A DE C.V

PLAN DE SEGURIDAD Y PLAN DE CONTINUIDAD

28 ABRIL 2018

ÍNDICE

Glosario

Activo	Cualquier ente tangible o intangible que tiene valor para el OPLEV y que requiere protección. Existen diversos tipos de activos, incluyendo: a) Activos de información: bases de datos y archivos de datos, hojas electrónicas con datos, contratos y acuerdos, documentación del sistema, información de investigaciones, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad del negocio, 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, gafetes de identificación, uniformes para el personal. d) Servicios: servicios de computación y comunicación, servicios generales; por ejemplo, calefacción, iluminación, energía y aire acondicionado. e) Personas: competencias, habilidades, experiencia y sus roles que desempeñan. f) Intangibles: tales como la reputación y la imagen del OPLEV.
Análisis de riesgos	Proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Baseline	Conjunto de atributos en un tiempo determinado, que sirven como guía de configuración técnica estandarizada basada en las mejores prácticas de seguridad internacional y en los lineamientos de seguridad.
BCP	Plan de Continuidad del Negocio, por sus siglas en inglés “Bussiness Continuity Plan”.
CATD	Centro de Acopio y Transmisión de Datos.
CCV	Centro de Captura y Verificación.
CRID	Centro de Recepción de Imágenes y Datos.
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.
DNS	Sistema de nombres de dominio, encargado de la traducción de direcciones IP en direcciones de dominio.
DRP	Plan de Recuperación de Desastres, por sus siglas en inglés “Disaster Recovery Plan”.
Estándar	Requerimiento mandatorio que soporta a las directrices de seguridad.
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 Intrusiones, por sus siglas en inglés “Intrusion Detection System”.
IPS	Sistema de Prevención de Intrusos, por sus siglas en inglés “Intrusion Prevention System”.
LDAP	Protocolo Ligero de Acceso a Directorios, por sus siglas en inglés “Lightweight Directory Access Protocol”.
MCAD	Monitor de Captura de Actas Digitalizadas.
OPLEV	Organismo Público Local Electoral del Estado de Veracruz.
PREP	Programa de Resultados Electorales Preliminares.
Procedimiento	Forma específica para llevar a cabo una actividad determinada, su representación gráfica se realiza mediante diagramas de flujo.
PTO	Proceso Técnico Operativo.
Sniffer	Aplicación especial para redes informáticas que permite capturar los paquetes que viajan por una red.
TCA	Terminal de Captura de Actas.
WAF	Firewall de Aplicaciones Web, por sus siglas en inglés “Web Application Firewall”.
Reglamento	Reglamento de Elecciones del Instituto Nacional Electoral vigente.

Riesgo Aceptado	Asumir el riesgo siempre con justificación.
Riesgo Mitigado	Atenuar el riesgo con nuevos procedimientos o acciones.
Riesgo Transferido	Transferir el riesgo y sus implicaciones a un tercero.

1. Introducción.

El Programa de Resultados Electorales Preliminares (PREP) es el mecanismo de información electoral, encargado de proveer los resultados preliminares no definitivos, de carácter estrictamente informativo a través de la digitalización, captura, verificación y publicación de los datos plasmados en las actas de escrutinio y cómputo de las casillas que se reciben en los Centros de Acopio y Transmisión de Datos (CATD) autorizados por el OPLEV.

El PREP es la herramienta por la cual se da a conocer en forma confiable, rápida y oportuna los resultados de la votación de los electores en las diversas casillas electorales que se instalarán el día de la Jornada Electoral, sin que ellos constituyan el resultado final. De igual forma es un sistema complejo que hace uso de los instrumentos tecnológicos procesando los datos a una gran velocidad, asegurando la certeza de la información, así como su difusión inmediata y simultánea.

La información oportuna, veraz y pública de los resultados preliminares es una función de carácter nacional, que en el ámbito de sus atribuciones tendrá este OPLEV bajo su responsabilidad, en cuanto a su implementación y operación, esto con base en el artículo 348, numeral 1 del Reglamento que establece: "*El Instituto y los OPL deberán implementar las medidas de seguridad necesarias para la protección, procesamiento y publicación de datos, imágenes y bases de datos. Asimismo, deberán desarrollar en sus respectivos ámbitos de competencia, un análisis de riesgos en materia de seguridad de la información, que permita identificarlos y priorizarlos, así como implementar los controles de seguridad aplicables en los distintos procedimientos del PREP, conforme a las consideraciones mínimas descritas en el Anexo 13.*

La implementación de mecanismos, programas, medidas y políticas de seguridad es indispensable para prevenir riesgos, daños, imprevistos o factores no considerados en cualquier tipo de proceso o trabajo que se lleve a cabo. De esta manera los riesgos de la seguridad son conocidos y minimizados de una forma sistemática, alineada a las normas

de seguridad aplicables y adaptadas a los cambios que se produzcan en el entorno y en las tecnologías utilizadas durante el PREP.

2. Objetivo General.

Identificar, analizar, documentar y mitigar los riesgos de seguridad de las diferentes etapas del PREP Veracruz 2018, a nivel de procedimientos, tecnología y recursos humanos con el fin de establecer los controles de seguridad apropiados que permitan eliminar o reducir el riesgo. Así como, establecer un plan logístico sobre cómo recuperar y restaurar los procesos del PREP en caso de interrupción parcial o total.

2.1 Objetivos Particulares.

- Establecer el plan de concientización para capacitar y transmitir el sentido de la seguridad de la información del PREP.
- Definir el esquema de control de acceso a los diferentes sistemas del PREP.
- Establecer el Plan de Continuidad para minimizar el impacto a la operación, así como el plan de recuperación de pérdidas de activos de información.
- Elaborar los documentos necesarios para favorecer la evaluación del ente auditor designado por el OPLEV.
- Identificar las problemáticas de seguridad que enfrenta el PREP Veracruz 2018.
- Garantizar el tratamiento adecuado de los riesgos identificados.
- Implementar los controles de seguridad en los distintos procesos de operación del PREP Veracruz 2018.

3. Alcance.

El plan de seguridad implementará los controles de seguridad que atenderán los procesos de operación del PREP: Acopio, Digitalización, Captura, Verificación, Publicación, Cotejo y Empaquetado de las Actas.

4. De la Normatividad Aplicable.

Este documento se encuentra elaborado con base en el anexo 13 del Reglamento de Elecciones, así como, con los Acuerdos que emita el Consejo General del Instituto Nacional Electoral y del Organismo Público Local Electoral en la materia.

5. Desarrollo del Plan de Seguridad.

Este plan contiene acciones, directrices, estándares y procedimientos orientados a la prevención, detección y respuesta a incidentes de seguridad que pueden llegar a afectar la correcta ejecución del PREP. De esta manera, los riesgos de la seguridad informática son conocidos y minimizados de forma sistémica.

5.1 Directrices de Seguridad de la Información.

Conforme lo estable el artículo 352, numeral 1, inciso e) del Reglamento de Elecciones, se deberá capacitar a todo el personal y prestador de servicios involucrados en el Proceso Técnico Operativo para la Implementación y Operación del PREP.

5.2 Análisis de Riesgos en Materia de Seguridad de la Información.

5.2.1 Activos Críticos.

Entre los activos críticos que pueden ser comprometidos en algún momento de la operación del PREP se encuentran:

Nombre	Descripción	Responsable	Tipo	Ubicación	Critico
El sistema informático	Programas de computación	Coordinación de desarrollo de software	Programas de computación	En la nube, estaciones de trabajo en los CCV y CATDs	Si
Los sitios de difusión en internet.	Despliegan información del PREP en navegador de Internet	Coordinación de red	Programas de computación	Servidores en la nube	Si
En la seguridad perimetral	Dispositivos para monitorear y detectar intrusos en la red	Coordinación de red	Equipos y programas de computación	En el CCV y los CATDs	Si
Los enlaces de internet del CCV y los CATDs.	Proporcionan conectividad entre el CCV y los CATDs	Coordinación de red y proveedor de servicios de internet	Servicio	En el CCV y los CATDs	Si
La red eléctrica en el CCV y los CATDs.	Proveen energía eléctrica	Coordinación del PREP	Servicio	En el CCV y los CATDs	Si
Los equipos de cómputo y digitalización en el CCV y los CATDs.	Computadoras y equipos de digitalización	Coordinación del PREP y Jefaturas de Zona	Equipo	En el CCV y los CATDs	Si
El personal del CCV y los CATDs.	Personal de coordinación, capturistas y digitalizadores.	Coordinación del PREP y Jefaturas de Zona	Personal	En el CCV y los CATDs	Si
Documentación de los procedimientos de operación	Documentos que describen los procesos y operación del PREP	Coordinación del PREP	Documento	En el CCV y los CATDs	No

En la concientización y capacitación de la seguridad informática	Capacitación de los procesos	Coordinación del PREP y Jefaturas de Zona	Documento	En el CCV y los CATDs	No

Tabla 1. Identificación de activos críticos.

5.2.3 Áreas de amenaza.

Por las implicaciones técnicas, políticas y sociales que existen en las diferentes regiones del estado, se considera que pueden ser susceptibles de afectación al procedimiento para la implementación del PREP, las siguientes áreas:

- El CCV.
- Los CATDs.
- Los enlaces y redes de comunicación.
- El portal del PREP y mecanismos de publicación.

5.2.4 Riesgos Identificados.

Con base en el impacto y la probabilidad de ocurrencia, se consideran los siguientes escenarios:

Riesgo	Responsable	Tratamiento
1. En el control de acceso a las aplicaciones. Controles de acceso poco robustos.	Coordinación del software	Aceptado
2. Por código malicioso. Que el código malicioso infecte al sistema informático.	Coordinación del software	Aceptado
3. En la ausencia de controles criptográficos. Control poco robusto.	Coordinación del software	Aceptado
4. En los dispositivos de seguridad perimetral de la red.	Administrador de la red	Aceptado
5. En la infraestructura de la red. Falta de control y administración de puertos, inadecuado o nulo balanceo de red, cableado o “ponchado” deficiente, no contar con	Administrador de la red	Aceptado

“firewall”, cableado expuesto.		
6. En los enlaces de Internet. Falta de encriptación del enlace, deficiencia en el servicio del proveedor de internet, mala instalación del servicio por parte del proveedor de internet.	Administrador del PREP, Jefe de Zona y Proveedor	Aceptado
7. En suministro y redundancia de energía eléctrica. Red eléctrica mal calculada, falta de un sistema de tierra adecuado, red eléctrica obsoleta.	Coordinación del PREP y Proveedor	Transferido
8. En el mantenimiento de los equipos. Maltrato en la transportación de los equipos, inadecuado manejo, equipos no probados.	Jefatura de Zona CATDs	Mitigado
9. En el personal operativo. Ausencias injustificadas, falta de capacitación, indisciplina en el personal,	Coordinación de personal	Aceptado
10. En la concientización en seguridad de la información. Capacitación inadecuada, selección de personal inadecuado.	Coordinación del PREP	Mitigado
11. En la documentación de procedimientos de operación. Falta de provisión de documentación, capacitación deficiente.	Coordinación del PREP	Mitigado
12. En el control de acceso físico. Controles poco robustos, falta de seguimiento a reglamentaciones.	Coordinación de CATD y CCV	Aceptado

Tabla 2. Riesgos identificados y su tratamiento.

5.3 Implementación del Plan de Tratamiento de Riesgos.

Con base en los riesgos identificados, se implementan los siguientes procedimientos:

Procedimiento 1. Tratamiento del riesgo en el control de acceso a las aplicaciones.

Todas las aplicaciones cuentan con autenticación de usuarios para establecer conexiones confiables, permitiendo que la información que se transfiera desde las aplicaciones de captura hacia la central, viaje de manera segura.

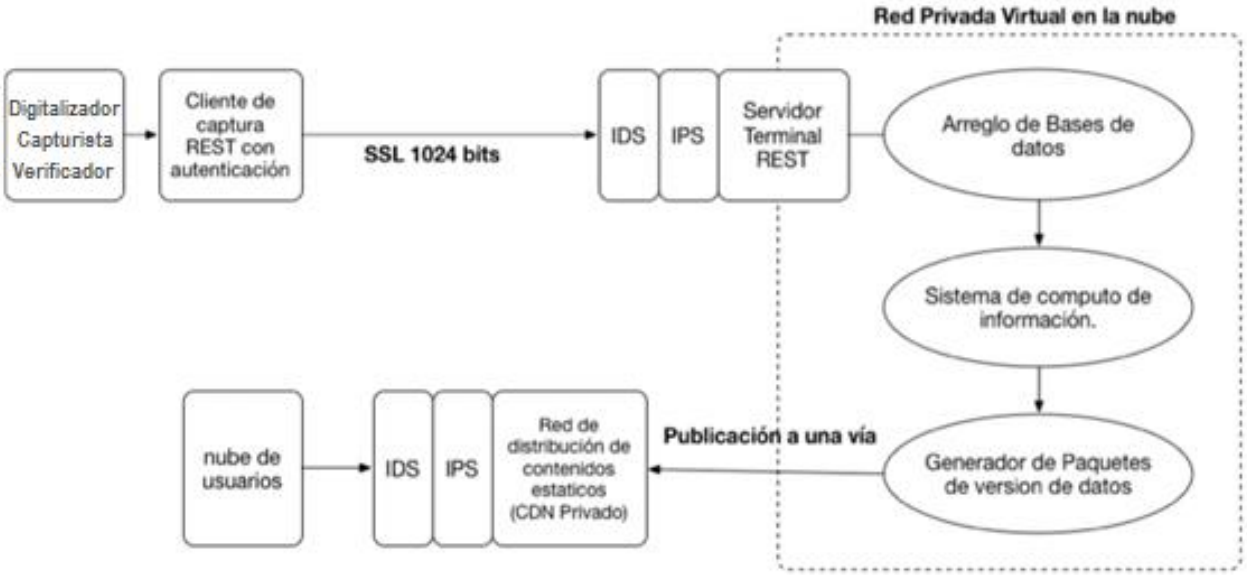

Figura 1. Seguridad en aplicaciones.

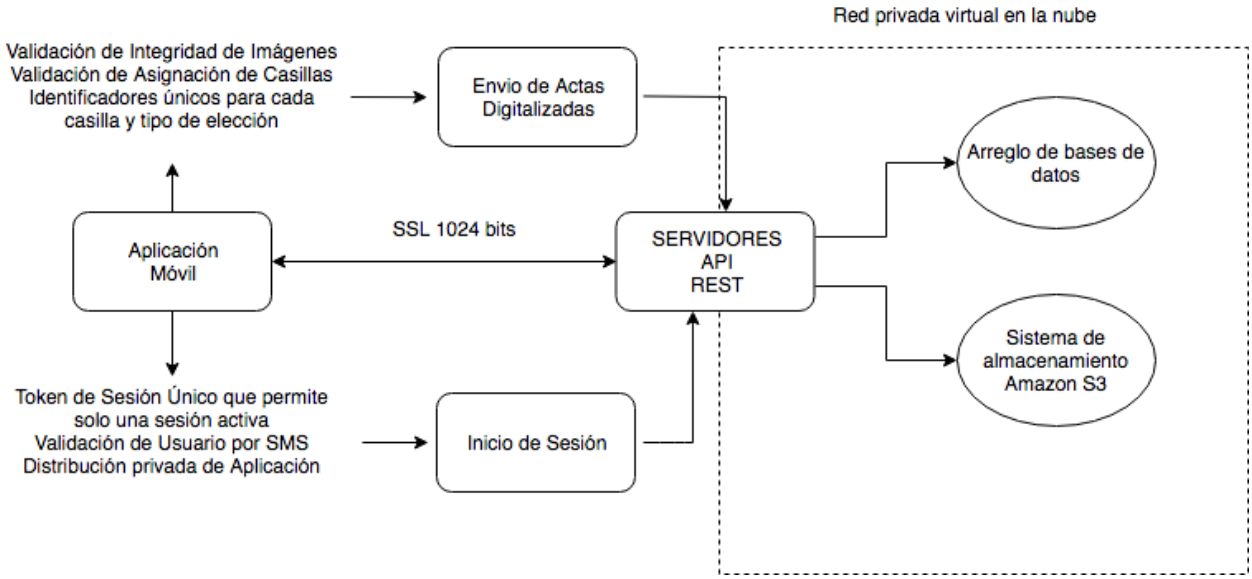

Figura 2. Seguridad en aplicación móvil

Procedimiento 2. Tratamiento del riesgo por código malicioso.

Los equipos de computación de escritorio que intervienen en los procesos cuentan con un paquete de antivirus instalado. Asimismo, los equipos móviles cuentan con bloqueo para evitar descarga de aplicaciones, es decir, que únicamente sea para el uso exclusivo de la aplicación del proceso PREP.

Adicionalmente se mencionan algunas acciones para prevenir que se adquiera algún código malicioso a nivel de usuario:

- No abrir archivos adjuntos en correo electrónicos de procedencia extraña.
- Analizar los archivos con el antivirus instalado antes de abrirlos.
- Analizar medios extraíbles.
- Actualizar el sistema operativo y antivirus constantemente.
- No descargar software de la red.
- No hacer uso de programas de redes sociales.

Procedimiento 3. Tratamiento del riesgo en la ausencia de controles criptográficos.

Todos los equipos de captura, aplicaciones y sitios web cuentan con contraseña de acceso, dichas contraseñas son otorgadas de manera confidencial al personal correspondiente, y éstas cambian de acuerdo con el número de simulacro que se ejecuta y el mismo día de la elección para evitar que personas ajenas puedan acceder a los recursos.

Respecto a la seguridad en la transferencia de los datos, el sistema incluye la encriptación de la información (SSL 1024 bits), el uso de token secreto (contraseña interna del sistema) y claves de usuario.

Referente a la seguridad en la digitalización del acta PREP, el sistema genera un código HASH para cada imagen, con la finalidad de asegurar que ésta no sea manipulada desde su digitalización hasta su publicación.

Procedimiento 4. Tratamiento del riesgo en los dispositivos de seguridad perimetral de la red.

A través de un sistema de detección de intrusos (IDS) que previene sobrecargas de recursos a causa de ataques como denegación de servicio (DoS) y controles de acceso mediante rangos IP permitidas, se mantiene la seguridad y disponibilidad de los elementos que conforman el módulo de publicación y evita posibles “caídas” del sitio web, y para validar que la información que entre al sistema provenga de una fuente no autorizada tanto en los servicios destinados a la recepción de datos provenientes de la captura, como en los destinados a la entrega de información para la publicación en el sitio web. La empresa cuenta con 3 métodos o técnicas para bloquear intrusos, que tienen que ver con el cambio y patrón de comportamiento de las conexiones:

1. Control por número de peticiones. Utilizamos parámetros limitados de conexiones por IP que se pueden conectar al servicio, un escudo o PROXY que analiza el comportamiento de conexiones, si el número de conexiones de una misma IP excede un límite establecido (1 conexión por IP), entonces ocurre un bloqueo temporal a nuestro sitio, si llegara a manifestar insistencia de esa misma IP, entonces el bloqueo será definitivo puesto que es indicativo de un comportamiento anormal. Se reporta al administrador del sistema.

2. Utilización de ancho de banda. El ancho de banda empleado para las conexiones tiene un límite, si alguien manda una petición más allá de nuestro límite y excede por mucho nuestro ancho de banda ocurre un “Overflow” o sobre saturación de nuestra infraestructura de conectividad, si llegara a ocurrir, sería un intento de ataque a nuestro sistema. Se procede del mismo modo

descrito anteriormente, es decir, se bloquea temporalmente la solicitud de petición del servicio y cuando ocurre tres veces seguidas, entonces bloquearemos permanentemente. Lo anterior, se reporta al administrador del sistema.

3. Validación de “headers”. Esto es validación mediante un “token” que genera nuestro validador en el IDS, un “header” especial que genera nuestro controlador, para cuando se realice la conexión a través del túnel de SSL, evaluamos y vemos si existe ese token y aceptamos la conexión, si alguien realiza un ataque masivo en cualquier lenguaje, no generará este “token” y será una conexión no válida. Se bloquea y se reporta al administrados del sistema.

Procedimiento 5. Tratamiento del riesgo en la infraestructura de la red.

Para garantizar la disponibilidad del sitio en todo momento, sin interrupciones, se incorpora un sistema de redundancia a través del DNS en donde además de tener físicamente balanceadas las cargas entre servidores por zonas, se tiene un DNS en particular que detecta la disponibilidad de todas las demás zonas geográficas, para que, en caso de que alguna falle, se pueda redirigir automáticamente a otra zona diferente, de la cual se tenga previamente la certeza que se encuentra disponible.

Existe un balanceo geográfico para asegurar el redireccionamiento automático en caso de posible falla. En el siguiente URL se muestra el contrato establecido con la empresa Amazon (Service Level Agreement) que contiene el acuerdo de nivel de servicio de las unidades de servicio contratadas con Amazon.

https://d1.awsstatic.com/legal/amazon-ec2-sla/Amazon_EC2_Service_Level_Agreement_es.pdf

El DNS funciona de la siguiente manera: para ambientes multizona, es posible revisar las zonas de operación, tiene la capacidad adicional de balancear las cargas

entre servidores de destino, puede resolver la IP contra el nombre, entre varios puntos de destino, es decir, si tenemos 5 servidores, nosotros establecemos un protocolo de HTTP o HTTPS, siempre tiene que obtener una respuesta de un código, pudiendo ser respuesta exitosa o respuesta no-exitosa, adicionalmente las peticiones regresan un contenido de la petición de respuesta y deshabilita la petición. Básicamente podemos deshabilitar una petición por contenido de información, balancea y nos da una verificación del código de respuesta, se utiliza para ambiente de alta disponibilidad, es decir, balanceo de DNS.

Procedimiento 6. Tratamiento del riesgo en los enlaces de internet.

Para el caso de la caída del enlace principal del CCV, se cuenta con dos proveedores de internet distintos, y mediante equipos de balanceo se regulan las cargas para administrar la red, asimismo, a través de firewalls se establecen los parámetros de seguridad necesarios para evitar accesos no permitidos o mal intencionados hacia la red de información del PREP. Los enlaces de respaldo están conectados al equipo de balanceo, en caso de que el principal falle, el enlace de respaldo se habilita de manera automática.

El día de la jornada, personal técnico y administrativo que proveen el suministro de los enlaces de internet de ambas compañías, se encuentran desde las 6:00 horas hasta que se declare la conclusión del PREP para atender cualquier situación de contingencia.

Si en el CCV existiera alguna contingencia, la captura de información de las Actas PREP no se suspende, continúa desde los CATDs porque los servicios están en la nube, de tal manera que la ejecución del PREP no se detiene pues existen capturistas/verificadores que continuarían sus tareas, adicional a ello, si el problema se prolongara por más de 30 minutos, el personal que labora en los CATD´s está capacitado para realizar todas las actividades del PTO por lo que realizando un

balance en las cargas de trabajo, los digitalizadores podrán sumarse a las actividades de Captura y Verificación.

En caso de perder conectividad en las aplicaciones de los CATDs debido a problemas con la red de internet, el sistema está preparado para continuar trabajando fuera de línea (off-line), que asegura la captura ininterrumpida de información, guardando toda la información en una base de datos local, hasta que el equipo vuelva a tener conectividad y sea posible transmitir la información a la central.

Procedimiento 7. Tratamiento del riesgo en la insuficiencia del suministro de energía eléctrica.

- *Falla en la red eléctrica de los CATDs.*

En cada uno de los equipos se cuenta con una unidad de corriente ininterrumpida con capacidad de 20 minutos para evitar pérdida de información debido a problemas de suministro eléctrico. Además, se cuenta con una unidad de suministro eléctrico (planta de energía eléctrica móvil) con suficiente capacidad para proveer a todos los equipos del CATD´s. Como una medida extrema, si el suministro de energía eléctrica se ve interrumpido por causas externas al CATD de forma permanente, se deberá implementar el mecanismo para el traslado de actas de forma parcial al CATD más cercano la unidad de captura debe trasladarse al CATD más cercano al lugar.

Para la implementación de los mecanismos de traslado se deberá realizar lo siguiente:

1.- La Coordinación del CATD, informará la situación inmediatamente a su Coordinación del CCV Xalapa, así como, a la Presidencia del Consejo Distrital de que se trate, quienes a su vez informarán a la Instancia Interna Encargada de la Implementación y Operación del PREP (es decir, la UTSI), detallando las

circunstancias en las que se encuentra y los motivos por los cuales se considera imposible solucionar el problema por otra vía.

2.- La instancia interna, con base en las comunicaciones informará a la Comisión Temporal del Programa de Resultados Electorales Preliminares, Conteo Rápido y Encuestas, quien determinará la ejecución o no del mecanismo de traslado.

3.- De resultar procedente, la presidencia de la Comisión del PREP, informará de inmediato al Consejo General que se realizará dicho procedimiento.

4.- La instancia interna notificará la decisión en primer término al Consejo Distrital para que brinde las facilidades necesarias a la empresa Grupo PROISI S.A. de C.V. y a su vez, informe en el pleno de dicho Consejo.

5.- Asimismo, la instancia interna notificará la decisión a la empresa Grupo PROISI S.A. de C.V., con la finalidad de que inicien los preparativos para el traslado controlado de las Actas de Escrutinio y Cómputo que no puedan digitalizarse en el CATD. En dicha comunicación se indicará también, a cuál de los Consejos se deberán trasladar las Actas PREP.

6.- El personal de la empresa Grupo PROISI S.A. de C.V. determinará el número de actas esperadas faltantes por digitalizar, y una vez recibido el 50% de las mismas, se realizará el primer envío.

7.- La Coordinación del CATD con apoyo de su personal acomodará las Actas de Escrutinio y Cómputo de forma ascendente con base en la fecha y hora de acopio.

8.- La Coordinación del CATD introducirá las Actas PREP en un sobre y procederá a sellarlo, posteriormente designará de entre su personal a dos figuras que realizarán el traslado y pegará donde se apertura el sobre una etiqueta de identificación que deberá contener los siguientes datos:

- Distrito Electoral.
- Cantidad de Actas PREP que contiene el sobre.
- Nombre completo y firma de quien Coordina el CATD.
- Nombre completo del personal designado para trasladar las Actas PREP.
- Fecha y hora del inicio de traslado de las Actas PREP.

- Firma de quien preside el Consejo Distrital, o en su caso, la Vocalía de Capacitación.

9.- En el vehículo proporcionado por la empresa, se realizará el traslado del personal designado para ello, en dicho vehículo, no podrá viajar personal distinto al designado. Esta limitante abarca a representantes de partidos políticos.

10.- A la llegada del personal de traslado a la sede del CATD designada, se procederá de la siguiente manera:

a) El personal de traslado entregará a la Coordinación del CATD el sobre y sus identificaciones oficiales para constatar que es el personal designado para ello y que va plasmado en la etiqueta de identificación.

b) Una vez corroborada la información, procederá a abrir el sobre y contar el número de Actas PREP, las cuales deberán coincidir con el número de Actas especificadas en la etiqueta de identificación.

c) Hecho lo anterior, procederá a distribuir las Actas PREP del CATD huésped a dos de sus digitalizadores, posteriormente, el personal de Traslado deberá regresar a su CATD para realizar el segundo envió, quien deberá repetir el procedimiento desde el numeral 7 del presente procedimiento de traslado.

d) El personal designado para la digitalización de las Actas PREP del CATD huésped, una vez terminada la actividad procederán a devolverlas nuevamente al sobre donde llegaron y la Coordinación, sellará el sobre y le pegará una etiqueta de identificación que contendrá los siguientes datos:

- Nombre completo y firma de quien coordina el CATD sede.
- Numero de Actas PREP.

11.- Cuando se reciba el segundo envió de Actas PREP del CATD huésped, se realizarán las actividades establecidas en el numeral 10 de este procedimiento.

12.- El personal de traslado del CATD huésped, en el segundo envío, permanecerá en el CATD sede, hasta que se concluya la digitalización de estas, pues una vez terminada la digitalización, recibirán por parte de la Coordinación del CATD sede, el total de Actas PREP.

13.- El personal de traslado regresa a su CATD y entregará las Actas PREP a la Coordinación, para iniciar con la fase de Empaquetado de Actas, conforme a lo establecido en el PTO.

14.- Las Coordinaciones, tanto del CATD sede (CATD que llevará a cabo la digitalización de las Actas) como del CATD huésped (CATD que realizara el traslado de sus Actas PREP), deberán dejar constancia de los actos en sus bitácoras correspondientes.

- *Fallas en la red eléctrica del CCV.*

En cada uno de los equipos se cuenta con unidad de corriente ininterrumpida durante 20 minutos para evitar perdida de información debido a problemas de suministro eléctrico. Además, se cuenta con una unidad de suministro eléctrico (planta de energía eléctrica móvil) con suficiente capacidad para proveer a todos los equipos del CCV.

Procedimiento 8. Tratamiento del riesgo en el mantenimiento de los equipos.

- *Falla en equipo de cómputo y digitalizadores.*

En el caso de suscitarse un problema en el funcionamiento de cualquiera de los equipos, el digitalizador o Capturista/Verificador de contingencia deberá reportarlo a la Coordinación del CATD y ésta a su vez a la jefatura de zona, quién cambiará el equipo en cuestión. En caso de agotar todas las opciones posibles para resolver el problema, se planteará la posibilidad de iniciar el mecanismo de traslado descrito en el Procedimiento 7 del presente documento.

En caso de violencia y eventos extremos, se priorizará siempre la seguridad del personal, teniendo como indicación resguardar su integridad física y las AEC y en segundo lugar los equipos. En caso de que el lugar se vea comprometido por factores externos o causas de fuerza mayor, y éstas no permitan la operación en el

lugar, se planteará la posibilidad de iniciar el mecanismo de traslado descrito en el Procedimiento 7 del presente documento.

Procedimiento 9. Tratamiento del riesgo en el personal de los CCV y CATDs.

- *Ausencia del personal destinado a la digitalización y captura en los CATDs.*

El equipo de Coordinaciones y Jefaturas de soporte tienen los horarios de trabajo de cada capturista y digitalizador de imágenes en el CCV y los CATD; además, cuentan con las instrucciones necesarias en caso de retrasos o contratiempos del mismo personal.

Los perfiles para cada CATD son cuatro:

- La coordinación del CATD;
- El acopiador o acopiadora;
- El digitalizador o la digitalizadora; y,
- El o la capturista

Sin embargo, todos están capacitados para realizar el trabajo de acopio, digitalización, captura, verificación, cotejo y empaquetado de actas, en caso de que alguno de ellos tenga un imprevisto, el otro puede realizar la tarea de la persona ausente, de igual manera la jefatura de zona está capacitada para desempeñar ambas labores en lo que llega el reemplazo de la persona ausente. Asimismo, la empresa cuenta con personal de emergencia para sustituir a la o las figuras que no acudan a laborar durante la jornada electoral. Como medida de prevención a lo anterior, Grupo PROISI S.A. de C.V. cuidará que el personal contratado sea responsable y diligente en sus actividades.

Toda persona contratada para la operación del PREP cuenta con gafete de identificación y uniforme, y es seleccionada cuidadosamente pasando por varios filtros de selección, de esta manera se asegura que no sea una persona que cause

un riesgo o amenaza para la operación. Adicionalmente, para causas de fuerza mayor, la empresa contará con insumos extras para la identificación de su personal.

Procedimiento 10. Tratamiento del riesgo en la documentación de procedimientos de operación.

La documentación de los procesos deja constancia de los pasos a seguir, las entradas y salidas y los entes que interactúan en los mismos. Sirve como evidencia para los controles de auditoría, elimina o reduce ambigüedades, confusión o desconocimiento del proceso entre el personal.

Los manuales del usuario PREP, las listas de verificación, registros de personal, son documentos que soportan la operación del PREP. La documentación del software es de carácter privado por ser propiedad intelectual de la empresa, sin embargo, Grupo PROISI S.A de C.V. se encuentra obligado a compartir con el OPLE Veracruz y el Ente Auditor la documentación necesaria para la correcta implementación y operación del PREP.

Procedimiento 11. Tratamiento del riesgo en la concientización, educación y capacitación en seguridad de la información.

Las personas son el elemento de falla más común en un sistema de seguridad. La falta de conciencia en los requerimientos de seguridad y las necesidades de control por parte de los administradores de sistemas, operadores, programadores y usuarios pueden representar el riesgo más importante para la organización.

Este procedimiento incluye la capacitación de los usuarios PREP para concientizar que los atacantes e intrusos pueden hacer uso de técnicas de ingeniería social y aprovechar la falta de conciencia de usuarios y operadores, para obtener información confidencial, tales como encontrar passwords escritos en papel de

notas, debajo de los teclados, sobre el monitor del usuario, respaldos de información incompletos, errores de configuración en equipos, etc.

Se incluyen temas como:

- Internet y sus riesgos.
- ¿Qué hacer para protegerse en redes Wifi?.
- Uso de Dispositivos móviles.
- Uso de Redes sociales
- Incidentes de seguridad.

Procedimiento 12. Tratamiento del riesgo en el control de acceso físico al CCV y CATDs.

- *CCV*

Para prevenir el acceso no autorizado a las instalaciones del CCV se implementan las siguientes acciones:

- Circuito cerrado de televisión.
- Identificación con fotografía.
- Chapa de seguridad.

El cumplimiento de que las medidas de seguridad sean observadas es responsabilidad de las Coordinaciones del CCV.

- *CATD*

Para el caso de los CATDs se utilizan gafetes de identificación con fotografía. El cumplimiento de que las medidas de seguridad sean observadas es responsabilidad de la Coordinación del CATD.

5.3.1 Fortalecimiento de las Actividades Operativas.

La operación de los procesos se ven favorecidas con las siguientes listas de verificación:

- Inicio de operaciones en simulacros y el día de la jornada en el CCV y los CATDs.
- Inventario de equipo en los CATDs y CCV.

Registro de datos:

- Entradas y salidas del personal al CCV y los CATDs.
- Pase de asistencia del personal.
- Inventario de equipos en el CCV y los CATDs.
- Entrega/Recibo de equipos en el CCV y los CATDs.
- Entrega/Recibo de informes de avance y documentación.
- Entrega/Recibo de reportes de datos del día de la jornada.

5.3.2 Robustecimiento de los Controles de Seguridad Física y Ambiental.

Para fortalecer la continuidad durante el proceso del PREP. Se consideran los siguientes aspectos fundamentales:

- *Seguridad en el edificio que alberga al CCV y los CATDs*, el OPLE Veracruz estableció en el acuerdo OPLEV/CG078/2018, que el CCV, así como los 30 CATDs, se instalarán dentro de las instalaciones del mismo Organismo, por lo que en primer término el acceso a las instalaciones del OPLEV es controlado por su personal de vigilancia, adicionalmente a ello, los espacios que ocupan los CATDs se encuentran en espacios cerrados cuyo acceso solo es permitido por las respectivas Coordinaciones.

- *Sistema de control de acceso a cada uno de los CATDs y el CCV*. El acceso es controlado por la identificación (gafete otorgado por la empresa) que en todo momento debe ser visible, que lo identifique como personal de Grupo PROISI S.A. de C.V. o como personal del OPLE Veracruz facultado por coadyuvar o supervisar en las actividades del PREP.

- Controles Ambientales para los recintos con aire acondicionado.

- *Registro del personal que accede al CCV y a los CATDs*. Las coordinaciones del CCV o CATD, según corresponda, deberán supervisar que la entrada de cualquier persona al CATD o CCV quede asentada en una libreta de registro.

- Establecer medidas preventivas de contingencia ambiental como sensores detectores de humo, inundación del sitio, sensores de humedad. Esta actividad dentro del CCV o CATD es responsabilidad de la empresa.

- Separar adecuadamente los cables de datos de los cables de energía eléctrica en los CATDs y el CCV.

- Protección contra intercepción y estática del cableado de los datos y energía eléctrica.

- Almacenamiento adecuado de la información y medios removibles de forma segura.

- Protección para las áreas de carga y descarga en el CCV.

5.4 Control de acceso.

El acceso a los recursos del PREP requieren de controles de acceso a ejecución de aplicaciones y unidades físicas de acuerdo con las políticas previamente establecidas.

Los controles cubren las etapas del ciclo de vida desde inicio de registro hasta la cancelación del final del usuario que no requiere más acceso a los recursos.

- *Identificación de los usuarios:*

Se lleva a cabo mediante la presentación de la identificación fotográfica, la verificación de autorización del usuario, la firma de declaraciones y políticas en los que asume las condiciones de acceso, conservar el registro impreso, verificar periódicamente la validez del usuario para bloquear o continuar permitiendo el acceso.

- *La autenticación del usuario:*

Se lleva a cabo una inspección visual de la identificación presentada con los registros de usuarios permitidos y la confrontación de una identificación oficial por parte del usuario.

- *Control de acceso a bienes informáticos:*

El control de acceso tiene la política de mínimos privilegios, en las aplicaciones está implementado a través de un nombre de usuario y su contraseña. El usuario tiene asignado una serie de características y roles que le permite el acceso a los diferentes recursos del sistema informático.

El usuario de un equipo cuenta con contraseña del BIOS de la máquina, para el sistema operativo y para acceder a la aplicación.

Para el acceso físico al CCV y a los CATDs, se cuenta con identificación fotográfica mediante gafete de presentación y registro manual de las entradas y salidas.

5.5 Plan de concientización.

Consiste en fomentar la cultura informática a través de una breve capacitación que ayuda a comprender la importancia de la información del PREP a los usuarios de este. Esta capacitación comprende los siguientes aspectos:

- Importancia de la seguridad de los sistemas informáticos. Breve explicación de principios, ética y políticas de protección a la infraestructura e información.
- Amenazas para la seguridad de la información. Se explica la diferencia entre amenazas y vulnerabilidades.
- Código malicioso. Métodos, impacto y medidas de prevención.

- Seguridad en el equipo personal. Móvil, redes sociales, robo de identidad.

5.6 Monitoreo respuesta a los incidentes de seguridad.

Se tiene implementado el registro de las actividades de los módulos y servicios en una bitácora de auditoría, así como en bitácoras (registro secuencial de eventos o acciones de un sistema), para monitorear el comportamiento de los distintos procesos del sistema y detectar o dar seguimiento a cualquier problema que pueda presentarse.

La figura 3 muestra como todos los componentes del sistema dejan evidencia en bitácoras y logs para llevar a cabo el seguimiento de las actividades mediante una API de auditoría y la implementación de RES WEB Services para obtener mejor ejecución de los procesos de transmisión y adquisición de datos a través de los métodos nativos del protocolo http.

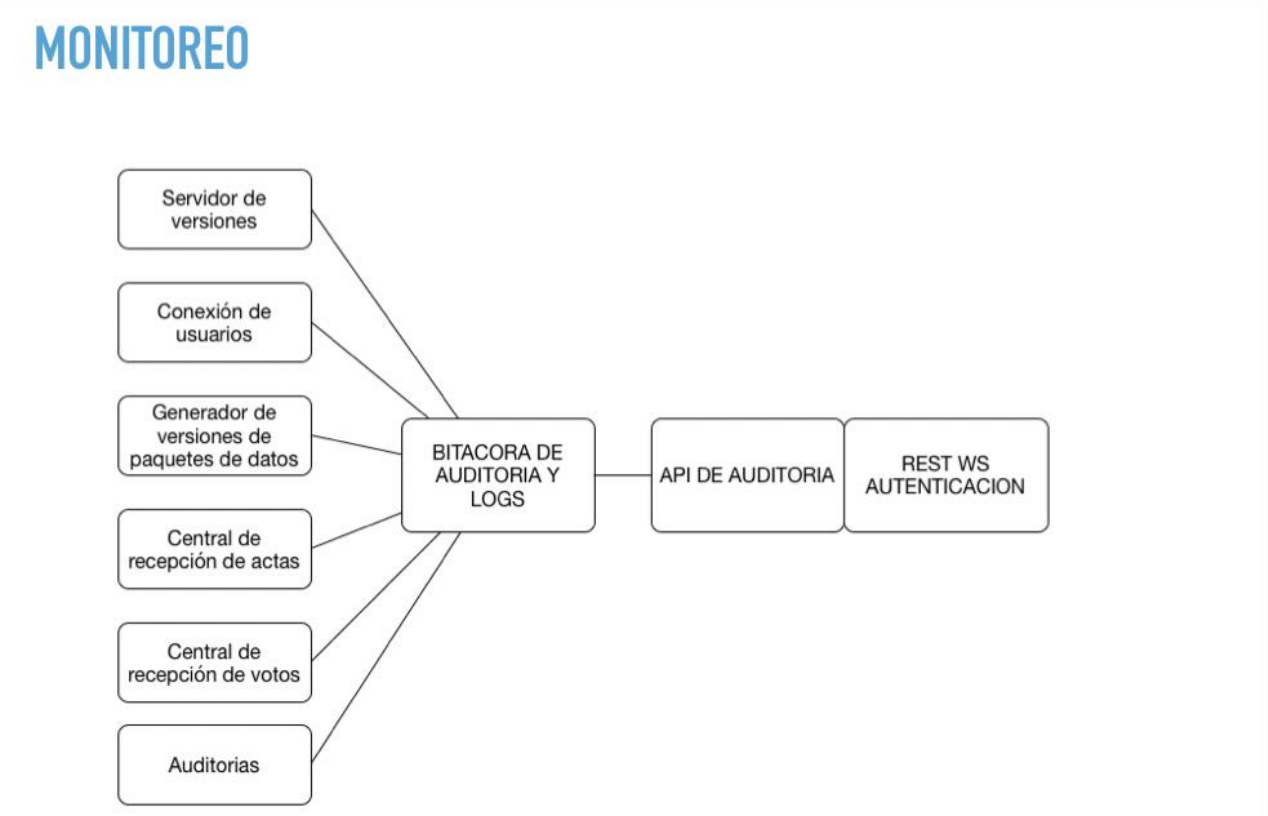

Figura 3. Sistema de Monitoreo.

5.7 Plan de Continuidad y Recuperación de Desastres.

El propósito es garantizar las ejecuciones de los procesos de acopio, digitalización, captura, verificación y publicación en caso de que se suscite una situación adversa o de contingencia. Se plantea como objetivo detectar los riesgos presentes, analiza su probabilidad de ocurrencia, establece su criticidad según cómo afectan la continuidad de los servicios, considerando los escenarios de contingencia (desastre total o desastre parcial) que pudieran afectar a los servicios informáticos a nivel nacional.

Las metas para la recuperación en caso de desastre deberán incluir los siguientes puntos:

- La recuperación de los servicios soportados por el CCV.
- Proporcionar los elementos para restablecer los servicios informáticos durante la vida del PREP.
- Monitoreo para detectar interrupciones de los sistemas de manera oportuna.
- Responder y recuperar oportunamente para asegurar la continuidad de los servicios.
- Minimizar las pérdidas y daños inmediatos mediante estrategias, procedimientos, herramientas de software, controles de copia/recuperación de información y actualización de versiones que ayuden en su momento a recuperar los bienes.
- Establecer los tiempos de recuperación y tolerancia de la aplicación, para validar que estos tiempos sean acordes a los requerimientos de operación del PREP.
- En caso de una falla en el suministro de la corriente eléctrica, cada equipo dentro del CATD y CCV cuenta con el soporte de una unidad de corriente ininterrumpida (NO-BREAK), que le permita proteger la información y la continuidad de operación. Si la interrupción de la energía fuese prolongada (más de 5 minutos) o permanente, la Coordinación del CATD deberá instruir a su personal para que proceda a realizar el encendido de la planta de energía de emergencia, así como

la conexión de la línea de energía de todos los equipos hacia la planta.

- En los CATDs y CCV se cuenta con enlaces de internet primarios y de respaldo de proveedores distintos, que puedan proveer del servicio en caso de falla del enlace principal. En caso de una interrupción en el servicio de internet, la coordinación del CATD y, en su caso CCV, habilitará el internet de respaldo, con ayuda del personal realizará las conexiones necesarias para ello. En caso de una interrupción permanente en el servicio de internet, la aplicación MCAD tiene una opción para exportar las actas digitalizadas a un archivo comprimido para poder trasladarlo al CATD más cercano para realizar su envío al CRID, o en su defecto al lugar más cercano con conexión a internet para su envío por otro medio alterno.
- Si en los CATDs y, en su caso CCV, se viera comprometida la seguridad de las instalaciones, siempre se privilegiará la seguridad del personal que se encuentre dentro de las mismas, se deberá informar a la Coordinación de Operaciones de la situación y se procederá a abandonar el edificio.
- Si existiera una falla extrema en el equipo de cómputo o que las condiciones de comunicación se colapsen en su totalidad, la Coordinación del CATD deberá comunicarse vía telefónica con la Coordinación de Operaciones, para que sea suministrado conectado el equipo de cómputo de respaldo, ubicado en los lugares estratégicos definidos por el proveedor.
- En caso de que se suspenda, se limite o se entorpezca la entrega de actas en los CATD, su Coordinación, hará del conocimiento a la Coordinación de Operaciones, a fin de que se informe a la Comisión del Programa de Resultados Electorales Preliminares, Conteo Rápido y Encuestas del OPLE Veracruz respecto a esta situación y se tomen las medidas conducentes.
- En caso de que el CCV dejara de funcionar temporalmente o quedara fuera de línea permanentemente por causas ajenas (Toma de las instalaciones o desastre natural), las fases de Captura y Verificación seguirán realizándose de manera continua, pues como medida de seguridad se contara con 120 capturistas distribuidos en los 30 Centros de Acopio y Transmisión de Datos del Estado.

5.8 Auditoría externa en materia de seguridad.

Los criterios para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares mediante pruebas de la caja negra son los siguientes:

- Captura de datos.
    - Verificar que el sistema informático; captura, calcula y publica los datos conforme a lo establecido en el numeral 30 del Anexo 13 del Reglamento de Elecciones.
- Manejo de inconsistencias y contabilización de los datos.

  Revisar que el sistema realiza el manejo de inconsistencias y contabilización de los resultados de las actas de acuerdo con lo descrito en el numeral 31 del Anexo 13 del Reglamento de Elecciones.
- Funciones mínimas del sistema.

  Verificar que el sistema informático integra los procedimientos mínimos y considerar los roles de los Centros de Acopio y Transmisión de Datos relacionados con la operación del sistema numeral 21 del mismo ordenamiento.
- Integridad en el registro de la información.

  Revisar que el sistema informático mantiene los datos libres de modificaciones, es decir, sin alteración.
- Imparcialidad en el tratamiento de la información.

Verificar que el sistema informático permite que la información se registre bajo las mismas reglas y conforme al momento en que es capturada, evitando algún tratamiento parcial injustificado.

- Precisión en resultados.

  Elaborar una batería de actas de pruebas, introducir esos datos y verificar que los resultados presentados son numéricamente precisos y se expresan conforme a lo señalado en el numeral 27 y 30 del Anexo 13 del Reglamento de Elecciones.

Continuando con las mismas directrices del reglamento, se consideran dos pruebas de penetración y revisión de configuraciones a la infraestructura del PREP, para detectar vulnerabilidades con los siguientes criterios:

- Propósito, tipo y alcance de la prueba.
- Entregar información requerida para la prueba: aplicaciones, nombres de usuario y contraseñas, restricciones tecnológicas, información de contacto.
- Reglas del Contrato:
  - Ambas partes deben estar de acuerdo (hacker ético y los administradores del PREP).
  - Identificar Tráfico del “Hacker Ético” y Datos en la Aplicación.
  - Acordar Duración y Horarios.
- Planificar las Comunicaciones: Contactos diversos y protegidos para la comunicación.
- Elaborar un resumen ejecutivo de hallazgos y recomendaciones.
- Describir la metodología paso a paso.