

**CG/AC-0036/2025**

**ACUERDO DEL CONSEJO GENERAL DEL INSTITUTO ELECTORAL DEL ESTADO, POR EL QUE APRUEBA LOS PLANES DE SEGURIDAD Y CONTINUIDAD DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES DEL PROCESO ELECTORAL LOCAL EXTRAORDINARIO 2025**

**GLOSARIO**

|                             |  |
|-----------------------------|--|
| AEC                         | Acta de Escrutinio y Cómputo.  |
| Acta PREP                   | Primera copia del acta de escrutinio y cómputo destinada para el PREP, o en ausencia de ésta, cualquier copia del acta de escrutinio y cómputo.  |
| CATD                        | Centro de Acopio y Transmisión de Datos.   |
| Coordinación de informática | Coordinación de Informática del Instituto Electoral del Estado.  |
| Código                      | Código de Instituciones y Procesos Electorales del Estado de Puebla.   |
| Comisión Especial           | Comisión Especial para dar seguimiento a la Implementación y Operación del Programa de Resultados Electorales Preliminares.                      |
| COTAPREP                    | Comité Técnico Asesor del Programa de Resultados Electorales Preliminares del Instituto Electoral del Estado.                                    |
| INE                         | Instituto Nacional Electoral.  |
| Instituto                   | Instituto Electoral del Estado.  |
| LGIFE                       | Ley General de Instituciones y Procedimientos Electorales.   |
| Lineamientos                | Lineamientos del Programa de Resultados Electorales Preliminares (PREP), Anexo 13 del Reglamento de Elecciones del Instituto Nacional Electoral. |
| OPLE                        | Organismo (s) Público (s) Local (es) Electoral (es).   |





**CG/AC-0036/2025**

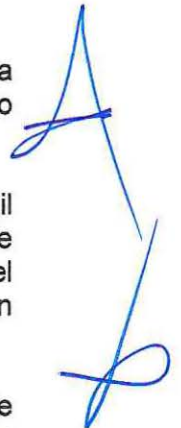
*“Con el fin de aprovechar las Tecnologías de la Información y Comunicación (TIC) para el desarrollo de las actividades a que se refiere el presente Reglamento, las sesiones del Consejo General, se podrán realizar de manera virtual, así como de forma híbrida.*

*Para tal efecto, la Presidencia del Consejo General determinará lo conducente, debiendo informar al respecto a las y los integrantes del mismo en la Convocatoria a la sesión correspondiente”.*

- VI. En sesión ordinaria celebrada el dieciocho de diciembre de dos mil veinticuatro, el Consejo General aprobó el Acuerdo CG/AC-0109/2024, mediante el cual constituyó la Comisión Especial y designó a la Instancia Interna encargada de coordinar el PREP, para el Proceso Extraordinario, recayendo dicha responsabilidad en la Coordinación de Informática.
- VII. En sesión ordinaria celebrada el siete de enero de la presente anualidad, el Consejo General a través del Acuerdo con clave CG/AC-0001/2025, emitió la convocatoria para el Proceso Extraordinario y aprobó el calendario correspondiente; asimismo aprobó el Acuerdo CG/AC-0002/2025, mediante el cual declaró el inicio del Proceso Extraordinario.
- VIII. En la sesión mencionada en el antecedente VII, el Consejo General aprobó el Acuerdo CG/AC-0006/2025, mediante el cual determinó llevar a cabo el PREP de este Organismo, ratificó al COTAPREP del citado programa, así como la realización de auditorías al sistema informático.
- IX. El veintisiete de enero de dos mil veinticinco, el Comité de Adquisiciones del Instituto, aprobó el Acuerdo CA/AC-004/2025, por el que determinó iniciar procedimiento de adjudicación mediante concurso por invitación referente al servicio del diseño, implementación y operación del sistema informático del PREP.
- X. El treinta de enero de dos mil veinticinco, el Consejo General a través del Acuerdo CG/AC-0014/2025, determinó la ubicación de los CATD, así como del Centro de Captura y Verificación de Datos del PREP para el Proceso Extraordinario.

En la misma sesión, mediante el instrumento CG/AC-0017/2025, se aprobó la Carpeta de Documentación y Material Electoral que se utilizarán en el Proceso Extraordinario.

- XI. En la reanudación de la sesión ordinaria de fecha veintisiete de enero de dos mil veinticinco, celebrada en la fecha indicada en el punto anterior, el Comité de Adquisiciones mediante el instrumento CA/AC-005/2025, declaró desierto el procedimiento de adjudicación mediante concurso por invitación mencionado en el antecedente IX.
- XII. En virtud de lo antes referido, el primero de febrero del presente año, el Comité de Adjudicaciones del Instituto, mediante instrumento CA/AC-007/2025, aprobó la



**CG/AC-0036/2025**

adjudicación directa mediante dictamen justificativo con la empresa denominada "GRUPO PROISI S.A. DE C.V.", celebrando el tres de febrero siguiente, contrato de prestación de servicios relativo a la contratación del tercero encargado del diseño, implementación y operación del sistema informático del PREP, para el Proceso Extraordinario.

**XIII.** El veinticuatro de febrero de la anualidad que transcurre, se llevó a cabo la sesión ordinaria del COTAPREP, en la cual, a través del Acuerdo A.28/COTAPREP/240225, las personas integrantes aprobaron dar por visto los planes de seguridad y continuidad.

**XIV.** El veinticinco de febrero del presente año, se llevó a cabo la sesión ordinaria de la Comisión Especial, aprobándose mediante el Acuerdo 01/CEPREP-ORD/25022025 los planes de seguridad y continuidad; asimismo, se facultó al Consejero Presidente del mencionado Órgano Auxiliar a efecto de que los remitiera a la Consejera Presidenta del Instituto, para que por su conducto se sometieran a la consideración y, en su caso, aprobación del Consejo General.

**XV.** En atención a lo anterior, en la misma fecha, el Presidente de la Comisión Especial, a través del Memorándum número IEE/CEPREP-0034/2025, remitió a la Consejera Presidenta del Instituto, los proyectos antes referidos.

En seguimiento a ello, la Consejera Presidenta del Instituto, remitió al Secretario Ejecutivo de este Organismo Electoral, los documentos de mérito a fin de someterlos a la consideración y, en su caso, aprobación del Consejo General; para tal efecto el Secretario Ejecutivo a través del Memorándum IEE/SE-0944/2025, los remitió a la Dirección Técnica del Secretariado del Instituto, para los efectos conducentes.

**XVI.** La Dirección Técnica del Secretariado del Instituto, por instrucciones del Secretario Ejecutivo, el veinticinco de febrero del presente año, remitió vía correo electrónico, a las personas integrantes del Consejo General, para su análisis y posterior discusión, el presente Acuerdo.

**XVII.** Durante el desarrollo de la mesa de trabajo de las personas integrantes del Consejo General, llevada a cabo de manera virtual el veintiséis de febrero del año que transcurre, las y los asistentes a la misma, discutieron el presente documento.

## **CONSIDERANDOS**

### **1. DEL INSTITUTO Y ATRIBUCIONES DEL CONSEJO GENERAL**

El artículo 98 numeral 1 de la LGIPE, establece que los OPLE están dotados de personalidad jurídica y patrimonio propios, gozando de autonomía en su funcionamiento e independencia en sus decisiones, de conformidad con lo previsto en la Constitución Política de los Estados Unidos Mexicanos, la Ley en

**CG/AC-0036/2025**

cita, así como la Constitución Política del Estado Libre y Soberano de Puebla y Leyes Locales, rigiéndose por los principios de certeza, imparcialidad, independencia, legalidad, máxima publicidad y objetividad.

Además, el artículo 3 fracción II de la Constitución Política del Estado Libre y Soberano de Puebla, precisa que el Instituto es el OPLE, dotado de personalidad jurídica y patrimonio propio, gozará de autonomía en su funcionamiento e independencia en sus decisiones y de carácter permanente, al que se le encomendará la función estatal de organizar las elecciones, estableciendo los principios rectores de la función electoral.

Asimismo, los artículos 72 y 73 del Código, indican que el Instituto será autónomo en su funcionamiento, independiente en sus decisiones y profesional en su desempeño y se regirá para su organización, funcionamiento y control por las disposiciones constitucionales y las relativas al mencionado ordenamiento.

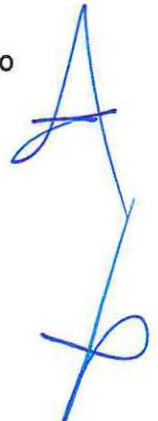
De acuerdo con lo establecido en el artículo 75 fracciones I, II y IV del Código, son fines del Instituto:

- Vigilar en el ámbito electoral el cumplimiento de las disposiciones de la Constitución Local, del Código y demás ordenamientos que garanticen el derecho de organización y participación política de la ciudadanía;
- Contribuir al desarrollo de la vida democrática; y
- Asegurar el ejercicio de los derechos político-electorales de la ciudadanía y de los partidos políticos vigilando el cumplimiento de sus obligaciones.

El artículo 79 del Código, establece que el Consejo General es el Órgano Superior de Dirección del Instituto y el responsable de vigilar el cumplimiento de las disposiciones constitucionales y legales en materia electoral, así como vigilar que los principios rectores de legalidad, imparcialidad, objetividad, certeza, independencia, máxima publicidad y paridad de género, guíen todas las actividades del Instituto, mismas que se realizarán con perspectiva de género.

El artículo 89 fracciones I, II, III, LIII y LX del Código, establece que el Consejo General cuenta, entre otras, con las siguientes atribuciones:

- Determinar las políticas y programas generales del Instituto, para el cumplimiento de sus fines;
- Vigilar el cumplimiento de las disposiciones constitucionales y legales relativas, así como las contenidas en el Código;
- Organizar el Proceso Electoral;
- Dictar los acuerdos necesarios a fin de cumplir sus atribuciones; y
- Las demás que le sean conferidas por el Código y las disposiciones legales aplicables.



**CG/AC-0036/2025**

## **2. MARCO NORMATIVO APLICABLE**

### **2.1 CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS**

El artículo 41 Base V Apartado B inciso a) numeral 5, establece que corresponde al INE, para los procesos electorales federales y locales, establecer las reglas, lineamientos, criterios y formatos en materia resultados electorales preliminares.

Asimismo, conforme lo dispone el artículo en cita en su Apartado C numeral 8, en las entidades federativas, las elecciones locales, estarán a cargo de los OPLE en los términos de la misma, quienes ejercerán funciones en materia de resultados preliminares.

### **2.2 LGIPE**

El artículo 104 numeral 1 inciso k) establece que corresponde a los OPLE, entre otras cosas, implementar y operar el PREP durante las elecciones que se lleven a cabo en la entidad, de conformidad a las reglas, lineamientos, criterios y formato que para tal efecto emita el INE.

A su vez, el artículo 219 numeral 1, establece que el PREP es el mecanismo de información electoral encargado de proveer los resultados preliminares y no definitivos, de carácter estrictamente informativo a través de la captura, digitalización y publicación de los datos asentados en las AEC de las casillas que se reciben en los Centros de Acopio y Transmisión de Datos, autorizados por el INE y por los OPLE; que el INE emitirá las reglas, lineamientos y criterios en materia de resultados preliminares, a los que se sujetarán los OPLE en las elecciones de su competencia; y que su objetivo será el de informar oportunamente bajo los principios de seguridad, transparencia, confiabilidad, credibilidad e integridad de los resultados y la información en todas sus fases al Consejo General, a los OPLE, a los partidos políticos, coaliciones, candidaturas, medios de comunicación y a la ciudadanía.

### **2.3 REGLAMENTO DE ELECCIONES DEL INE**

El Capítulo II del Título III establece las bases y procedimientos generales para la implementación y operación del PREP; mismas que son aplicables para el INE y para los OPLE en sus respectivos ámbitos de competencia, así como para todas las personas que participen en las etapas de diseño, implementación, operación y evaluación de dicho programa.

El artículo 338 numeral 2 inciso b), señala que la implementación y operación del PREP será responsabilidad de los OPLE cuando se trate, entre otros, de:

- Elecciones de las y los miembros de Ayuntamientos; y
- Otras elecciones que por disposición legal o por mandato de autoridad, corresponda al OPLE llevar a cabo.

**CG/AC-0036/2025**

Asimismo, en el numeral 5 de dicho apartado, se señala que los OPLE podrán auxiliarse de terceros conforme a su capacidad técnica y financiera, siempre que los terceros se ajusten a la normatividad aplicable y cumplan con los principios del PREP.

Por su parte el artículo 348 indica que el INE y los OPLE 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 los Lineamientos.

## **2.4 LINEAMIENTOS**

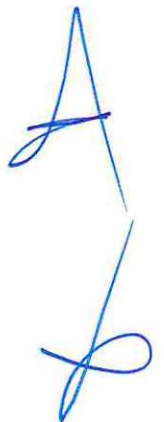
En sus numerales 2 y 3, establece que los OPLE deberán designar una instancia interna responsable de coordinar el desarrollo de las actividades del PREP, la cual deberá asegurar el cumplimiento de lo establecido en el Reglamento de Elecciones del INE, así como en los acuerdos que se emitan en el ámbito de su competencia, garantizando la recopilación de toda la información que debe generarse durante la implementación, operación y evaluación del PREP.

El numeral 4 señala que la implementación y operación del sistema informático del PREP, será responsabilidad de los OPLE.

Por su parte, el numeral 12 señala que la implementación de los controles de seguridad aplicables a los distintos procedimientos del PREP, se considerarán como mínimo los siguientes puntos:

“... ”

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



**CG/AC-0036/2025**

*Tecnologías de la Información y Comunicaciones donde se implemente el PREP. Dicho plan deberá ser elaborado por la instancia interna y, en su caso, en coordinación con el tercero que auxilie en la implementación y operación del PREP.*

...”

Además, en su numeral 13, se señala que se deberá implementar un plan de continuidad para determinar las acciones que garanticen la ejecución de los procedimientos relativos a las fases establecidas en el Proceso Técnico Operativo del INE o de los OPLE, en caso de que se suscite una situación adversa o de contingencia, el cual deberá incluir a los responsables y los medios de contacto para llevar a cabo la resolución de contingencias.

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

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

## **2.5 CÓDIGO**

De acuerdo a lo establecido en el artículo 93 fracción XXXVI, el Secretario Ejecutivo tiene la atribución de sugerir al Consejo General el mecanismo para la difusión inmediata de los resultados preliminares de las elecciones, de conformidad con las reglas, lineamientos, criterios y formatos que para tal efecto emita el INE.

Aunado a lo anterior, el artículo 305 menciona lo siguiente:

“...”

*El Programa de Resultados Electorales Preliminares es el mecanismo de información electoral, encargado de proveer los resultados preliminares y no definitivos, de carácter estrictamente informativo a través de la captura, digitalización 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 autorizados por el Instituto.*

*Su objetivo será el de informar oportunamente garantizando la seguridad, transparencia, confiabilidad, credibilidad e integridad de los resultados y la información en todas sus fases al Consejo General, los partidos políticos, coaliciones, candidatas y candidatos, medios de comunicación y a la ciudadanía.*

*La información oportuna, veraz y pública de los resultados preliminares es una función de carácter nacional que en el ámbito de sus atribuciones,*





**CG/AC-0036/2025**

*tendrá el Instituto bajo su responsabilidad, en cuanto a su implementación y operación, regida por los principios de legalidad, certeza, objetividad, independencia y máxima publicidad.*

*El Programa de Resultados Electorales Preliminares será un programa único cuyas reglas de operación serán emitidas por el Instituto Nacional Electoral.*

*Sólo el Consejo General, a través de los medios electrónicos, y conforme a los avances tecnológicos existentes, dará a conocer la información preliminar de resultados de cada una de las elecciones en la Entidad. La publicación podrá iniciar a las 18:00 horas, quedando prohibido publicar o difundir por cualquier medio los resultados electorales preliminares antes de la hora señalada.*

...”

Por su parte, el artículo 306, señala que los datos consignados en las AEC levantadas en las casillas, constituyen la única fuente de información preliminar de las elecciones.

De este modo, se entiende que el PREP, es un sistema que se abastece de los datos que contienen cada una de las AEC elaboradas por las personas funcionarias de mesa directiva, el día de la jornada electoral, información que debe hacerse del conocimiento de la ciudadanía en forma clara, directa, transparente, fidedigna y oportuna.

### **3. DE LOS PLANES DE SEGURIDAD Y CONTINUIDAD**

El numeral 348 del Reglamento de Elecciones, establece que el INE y los OPLE en sus respectivos ámbitos de competencia, desarrollarán 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 los Lineamientos.

Además, el numeral 13 de los Lineamientos señala que se deberá implementar un plan de continuidad para determinar las acciones que garanticen la ejecución de los procedimientos relativos a las fases establecidas en el Proceso Técnico Operativo del Instituto, en caso de que se suscite una situación adversa o de contingencia, el cual deberá incluir a los responsables y los medios de contacto para llevar a cabo la resolución de contingencias.

Asimismo, señala que dicho plan de continuidad deberá ser elaborado por la Coordinación de Informática en su calidad de instancia interna y ser comunicado al personal involucrado en su ejecución en función de las actividades a desempeñar por cada rol operativo, con la suficiente antelación para formar parte de los ejercicios y simulacros.



## CG/AC-0036/2025

Por lo anterior, con fundamento en el numeral 4 de los Lineamientos, la Coordinación de Informática, como instancia encargada del PREP, en coordinación con la empresa denominada “GRUPO PROISI S.A. DE C.V.” elaboró las propuestas de Planes de Seguridad y Continuidad, documentos que, a través de la Secretaría Ejecutiva se ponen a consideración de este Consejo General, tal y como se refiere en los antecedentes de este Acuerdo.

Los documentos que se analizan y que se denominan “*Plan de Seguridad*” y “*Plan de Continuidad*”, establecen tanto las causas internas como las externas al Instituto y a la empresa que pudieran comprometer en los procesos que integran el PREP, tales como el suministro de energía, telecomunicaciones, personal responsable de la captura y transmisión, suministro de información (Actas PREP) proveniente de los CATD, personal directivo y staff técnico responsable de la operación del PREP, entre otros.

Además, incluye los aspectos generales y específicos que tienen que ver con el personal, el método, el medio ambiente, el equipo e infraestructura y los insumos o material que componen todo el sistema. Las estrategias a considerar respecto a la permanente continuidad de la información, técnicas que procuran evitar los errores humanos o la captura incorrecta de las AEC, así como el material didáctico previsto a usar durante la capacitación para saber las acciones a tomar el día de la Jornada Electoral.

Es importante mencionar, que los planes que se proponen mediante este instrumento, detallan el programa informático que se implementará, así como las características con las que cuenta la infraestructura del mismo, el tipo de almacenamiento de la información que se genere integrando, así como las bases de datos, balanceador de cargas, corta fuegos, sistema de monitoreo, que se prevén en su operación para asegurar que su funcionamiento sea continuo y los datos que se ingresen al sistema estén resguardados de manera adecuada.

A su vez, los planes en comento, contemplan las condiciones a las cuales se encuentran sujetos, con la finalidad de dar un cabal cumplimiento al contrato referido en el antecedente XII del presente Acuerdo, mismas que se citan de la forma siguiente:

- Condiciones de calendarización y tiempo;
- Condiciones Geográficas y Climáticas;
- Condiciones de Telecomunicaciones; y
- Condiciones de Seguridad.

Por todo lo anterior, este Consejo General, una vez que analizó los Planes de Seguridad y Continuidad planteados en este instrumento, con fundamento en lo dispuesto por el artículo 89 fracciones III, LIII y LVIII del Código, considera que lo oportuno es aprobarlos toda vez que los referidos documentos establecen de manera puntual los procedimientos a seguir para garantizar la continuidad del

**CG/AC-0036/2025**

sistema, así como los mecanismos de seguridad y las acciones a implementar para garantizar que la información del PREP no corra riesgos por cuestiones derivadas de problemas como cortes en el suministro de energía eléctrica, fallas en el servicio de internet, errores humanos e incluso ataques informáticos que pretendan dañar la base de datos.

#### **4. EFECTOS**

En virtud de lo argumentado en el presente instrumento, y con fundamento en lo dispuesto en el artículo 89 fracciones II, LIII y LX del Código, este Consejo General estima procedente:

- Aprobar los Planes de Seguridad y Continuidad del PREP para el Proceso Extraordinario.

#### **5. COMUNICACIONES**

Con fundamento en lo dispuesto por los artículos 89 fracción LX y 91 fracción XXIX del Código, este Consejo General faculta a la Consejera Presidenta de este Órgano Superior, a efecto de que notifique por el medio que se considere más idóneo y expedito, el contenido del presente Acuerdo:

- a) A la Unidad Técnica de Vinculación con los OPLE del INE, para su conocimiento;
- b) Al Vocal Ejecutivo de la Junta Local del INE con sede en esta Entidad Federativa, para su conocimiento;
- c) Al Consejero Presidente de la Comisión Especial, para su conocimiento; y
- d) A los integrantes del COTAPREP del Instituto, para su conocimiento.

Con fundamento en los artículos 89 fracción LX y 93 fracciones XXIV, XXXI, XXVIII, XL y XLVI del Código, se faculta al Secretario Ejecutivo de este Instituto para notificar el contenido del presente Acuerdo:

- a) A la Coordinación de Informática, adscrita a la Dirección Administrativa del Instituto, para su conocimiento y observancia en el ámbito de su competencia; y
- b) A las Presidencias de los Órganos Transitorios de este Instituto, para su conocimiento y observancia en el ámbito de su competencia.

Por lo anteriormente expuesto y en ejercicio de la facultad establecida por el artículo 89 fracción LIII del Código, el Consejo General tiene a bien emitir el siguiente:



**CG/AC-0036/2025**

## **ACUERDO**

**PRIMERO.** El Consejo General del Instituto Electoral del Estado es competente para conocer y pronunciarse sobre el presente asunto, en términos de lo aducido por los Considerandos 1 y 2 del presente Acuerdo.

**SEGUNDO.** Este Cuerpo Colegiado aprueba los Planes de Seguridad y Continuidad del Programa de Resultados Electorales Preliminares del Proceso Electoral Local Extraordinario 2025; de conformidad con lo narrado en los Considerandos 3 y 4 de este documento.

**TERCERO.** El Consejo General faculta a la Consejera Presidenta y al Secretario Ejecutivo de este Organismo Electoral, para hacer las notificaciones narradas en el Considerando 5 del presente Acuerdo.

**CUARTO.** El presente Acuerdo entrará en vigor a partir de su aprobación.

**QUINTO.** Publíquese el presente Acuerdo en el Periódico Oficial del Estado, a través del formato que para tal efecto se aprobó mediante instrumento CG/AC-004/14.

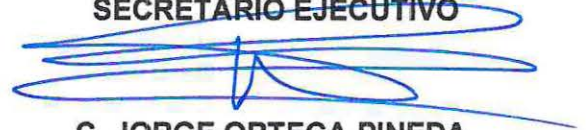
Este Acuerdo fue aprobado por unanimidad de votos de las personas integrantes del Consejo General del Instituto Electoral del Estado, en la sesión ordinaria de fecha veintisiete de febrero de dos mil veinticinco.

**CONSEJERA PRESIDENTA**



**C. BLANCA YASSAHARA CRUZ GARCÍA**

**SECRETARIO EJECUTIVO**



**C. JORGE ORTEGA PINEDA**



# Plan de Seguridad

- | Programa de Resultados Electorales Preliminares del Instituto Electoral del Estado de Puebla
- | Proceso Electoral Local Extraordinario 2025

A

jo

## INDICE

|  |    |
|--|----|
| Glosario .....   | 3  |
| 1. Normatividad Aplicable .....  | 5  |
| 2. Presentación.....   | 6  |
| 1.1 Propiedades de la información.....   | 7  |
| 1.2 Tipos de ataques que pueden presentarse .....  | 8  |
| 3. Objetivos y Alcance .....   | 8  |
| 3.1 Objetivos Generales .....  | 8  |
| 3.2 Objetivos Particulares.....  | 8  |
| 3.3 Alcance .....  | 9  |
| 4. Desarrollo del Plan de Seguridad .....  | 11 |
| 5. Análisis de Riesgos en Materia de Seguridad de la Información .....   | 15 |
| 6. Activos Críticos. ....  | 18 |
| 7. Implementación de los controles necesarios para fortalecer el acceso de las y los usuarios a bases de datos, servidores, equipos de comunicaciones y equipos de cómputo personal..... | 27 |




# Glosario

---

|                                    |   |
|------------------------------------|---|
| <b>Análisis de riesgos</b>         | Proceso que comprende la identificación de activos, 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. |
| <b>Baseline</b>                    | 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.  |
| <b>BCP</b>                         | Plan de Continuidad del Negocio, por sus siglas en inglés "Business Continuity Plan".   |
| <b>CATD</b>                        | Centro de Acopio y Transmisión de Datos.  |
| <b>CCV</b>                         | Centro de Captura y Verificación.   |
| <b>CENTRAL</b>                     | Centro de Recepción de Imágenes y Datos.  |
| <b>DDoS</b>                        | Es un ataque de negación de servicio, también llamado ataque DDoS (por sus siglas en inglés, Distributed Denial of Service), es un ataque masivo a un sistema de computadoras o red, cuyo objetivo es volver un servicio o recurso inaccesible a los usuarios legítimos.                                |
| <b>DNS</b>                         | Sistema de nombres de dominio, encargado de la traducción de direcciones IP en direcciones de dominio.  |
| <b>DRP</b>                         | Plan de Recuperación de Desastres, por sus siglas en inglés "Disaster Recovery Plan". Estándar Requerimiento mandatorio que soporta a las directrices de seguridad.   |
| <b>FailOver</b>                    | 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.                                 |
| <b>Firewall</b>                    | Dispositivos de seguridad perimetral de la red, que puede implementarse tanto en hardware como en software, 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.                           |
| <b>Hash o código de integridad</b> | Es un valor alfanumérico de representación único que permite identificar a cada imagen del Acta PREP digitalizada, con el cual se verifica su integridad. Dicho valor es obtenido a partir de algún algoritmo criptográfico denominado comúnmente función hash. Ejemplo de función hash es sha256.      |
| <b>IPS</b>                         | Sistema de Prevención de Intrusiones, por sus siglas en inglés "Intrusion Prevention System".   |
| <b>LDAP</b>                        | Protocolo Ligero de Acceso a Directorios, por sus siglas en inglés "Lightweight Directory Access Protocol".   |
| <b>MCAD</b>                        | Monitor de Captura de Actas Digitalizadas.  |
| <b>INSTITUTO</b>                   | OPLE.   |
| <b>PREP</b>                        | Programa de Resultados Electorales Preliminares.  |

|                           |  |
|---------------------------|--|
| <b>Procedimiento</b>      | Forma específica para llevar a cabo una actividad determinada, su representación gráfica se realiza mediante diagramas de flujo.   |
| <b>PTO</b>                | Proceso Técnico Operativo.   |
| <b>Sniffer</b>            | Aplicación especial para redes informáticas que permite capturar los paquetes que viajan a través de un segmento de red específico.  |
| <b>TCA</b>                | Terminal de Captura de Actas   |
| <b>WAF</b>                | Firewall de Aplicaciones Web, por sus siglas en inglés "Web Application Firewall".   |
| <b>Reglamento</b>         | Reglamento de Elecciones Vigente del Instituto Nacional Electoral.   |
| <b>Riesgo Aceptado</b>    | Asumir el riesgo siempre con justificación.  |
| <b>Riesgo Mitigado</b>    | Atenuar el riesgo con nuevos procedimientos o acciones.  |
| <b>Riesgo Transferido</b> | Transferir el riesgo y sus implicaciones a un tercero.   |
| <b>Activo</b>             | <p>Cualquier ente tangible o intangible que tiene valor para el INSTITUTO y para el Tercero Auxiliar del PREP y que requiere protección. Existen diversos tipos de activos, incluyendo:</p> <p><b>Activos tangibles</b></p> <ol style="list-style-type: none"> <li>I. Activos de información: Bases de datos y archivos de datos, hojas electrónicas con datos, contratos y acuerdos, documentación del sistema, archivos de usuarios, información de configuraciones, manual de usuario, formatos digitales de identificaciones, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad, acuerdos para contingencias, rastros de auditoría e información archivada.</li> <li>II. Activos digitales: Balanceadores, servidores de aplicaciones, base de datos, firewalls, respaldos de S3, Aplicaciones para actualizaciones.</li> <li>III. Activos de software: Software de aplicación, software del sistema, herramientas de desarrollo.</li> <li>IV. Activos físicos: Lugares operativos PREP CATDS y CCVS, llaves de acceso, gafetes de identificación, uniformes del personal, flotilla vehicular, mobiliario, plantas de luz, pantallas de publicación, sistema de videocámaras.</li> <li>V. Activos informáticos: Servidores en nube, equipo de cómputo, equipo de comunicación y medios removibles.</li> <li>VI. Personas: Personal directivo, técnico y operativo del PREP con competencias específicas, habilidades, experiencia y roles que desempeñan.</li> </ol> <p><b>Activos intangibles</b></p> <ol style="list-style-type: none"> <li>I. Servicios: Servicios de acompañamiento y asesorías en tecnologías de la información, cómputo y comunicaciones, servicios generales; por ejemplo, calefacción, iluminación, energía y aire acondicionado.</li> <li>II. Intangibles: tales como la reputación, percepción de transparencia, la imagen del INSTITUTO, confianza de la ciudadanía en el PREP y claridad, certeza y continuidad de la información.</li> </ol> |





# 1. Normatividad Aplicable

---

Este documento, fue elaborado en conjunto con la Instancia Interna de IEE y el Tercero encargado de auxiliar en el diseño implementación y operación del Programa de Resultados Electorales Preliminares (PREP), de conformidad con lo establecido numeral 13, fracción IV, del Anexo 13 del Reglamento de Elecciones (RE), en el que menciona:

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

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

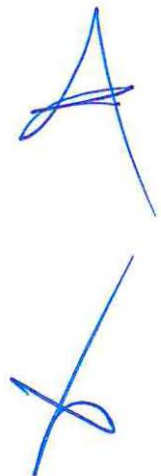
Conforme a lo establecido por el artículo 348, numeral 1 del Reglamento de Elecciones menciona lo siguiente:

*“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”.*

En el Anexo 13, Título II, Capítulo IV del RE, señala en el numeral 12 los puntos que deben tomarse en cuenta al momento de implementar los controles de seguridad en los distintos procedimientos del PREP, los cuales son:

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

- I. **Factores de riesgo:** establecer e identificar el conjunto de medidas específicas para evaluar los riesgos con base en su impacto y la probabilidad de ocurrencia;*
- II. **Activos críticos:** identificar cuáles son los recursos humanos y materiales, servicios e información (en sus diferentes formatos) de valor para los procedimientos del PREP;*
- III. **Identificación, evaluación y gestión de riesgos:** deberá identificarse y describirse la situación o condición –técnica, legal, económica, política, social, entre otros – que pueda afectar los procedimientos del PREP; posteriormente, deberá describirse claramente cuáles son los impactos que se pueden tener en el caso que una amenaza se materialice; finalmente, se deberá definir y documentar la respuesta respecto de cada uno de los riesgos identificados, precisando si los riesgos serán aceptados, mitigados, transferidos o eliminados; y*



- IV. **Plan de seguridad:** se deberá elaborar un plan de seguridad basado en los resultados de un análisis de riesgos, que permita llevar a cabo la implementación de controles en los distintos procedimientos de operación del PREP, así como en la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP. Dicho plan deberá ser elaborado por la instancia interna y, en su caso, en coordinación con el tercero que auxilie en la implementación y operación del PREP.”

De igual manera en el numeral 13 de dicho capítulo antes referido, se determina la elaboración de un Plan de Continuidad tal y como se muestra:

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

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

## 2. Presentación

1. 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 INSTITUTO.

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 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 el INSTITUTO bajo su responsabilidad, en cuanto a su implementación y operación, esto con base en el artículo 348, numeral 1 del Reglamento de Elecciones del Instituto Nacional Electoral 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, en las tecnologías y/o servicios relacionados a la información o comunicación utilizadas durante el PREP.

2. En este sentido, es importante destacar como antecedente que la Seguridad Informática es la rama de las Ciencias de la Computación cuyos objetivos principales son:
  - a. la protección de la información de robos o de acceso no autorizado,
  - b. la prevención de corrupción de la información existente durante su comunicación a través de redes de datos, o directamente en los medios de almacenamiento electrónicos donde ésta se encuentra,
  - c. la recuperación ante situaciones desastrosas, sean de naturaleza fortuita o malintencionada.

Todo esto conlleva a mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información, mientras se garantiza el acceso a los datos por parte de los usuarios autorizados, y se mantiene la continuidad en las operaciones del sistema.

Con base en esta definición, es importante precisar las políticas, procedimientos y metodologías para asegurar la integridad, disponibilidad y confiabilidad de datos y sistemas; prevenir y detectar amenazas respondiendo de forma adecuada y con prontitud ante un incidente; así como, proteger y mantener los sistemas operando de manera ininterrumpida.

3. Es importante tener la certeza de las propiedades de la información, mismas que son mantenidas y respetadas en todo momento de la operación del sistema, y que en caso de que se llegara a presentar una brecha de seguridad, la recuperación se logre de manera inmediata con el mínimo de afectación posible.

## 1.1 Propiedades de la información

- **Confidencialidad:** Asegurarse que la información en un sistema de cómputo y la transmitida por un medio de comunicación, sea accedida solo por las personas autorizadas;
- **Autenticación:** Asegurarse que el origen de un mensaje o documento electrónico está correctamente identificado, con la seguridad que la entidad emisora o receptora no ha sido suplantada;

- **Integridad:** Asegurarse que solo el personal autorizado sea capaz de modificar la información o recursos de cómputo;
- **No repudiación:** Asegurarse que ni el emisor o receptor de un mensaje o acción sea capaz de negar cualquier acción realizada;
- **Disponibilidad:** Requiere que los recursos de un sistema de cómputo, comunicación y almacenamiento estén disponibles en el momento que se necesiten.

## 1.2 Tipos de ataques que pueden presentarse

- **Interrupción:** Es un ataque contra la Disponibilidad en el cual el mensaje no puede llegar a su destino, un recurso del sistema es obstruido o temporalmente inutilizado;
- **Intercepción:** Es un ataque contra la Confidencialidad en el que una persona, computadora o programa sin autorización logra el acceso a un recurso controlado;
- **Modificación:** Es un ataque contra la Integridad donde una persona sin autorización, además de lograr el acceso, modifica el mensaje antes de que sea entregado al destinatario;
- **Fabricación:** Es un ataque contra la Autenticidad donde una persona sin autorización inserta datos en un sistema.

En este orden de ideas, es necesario el establecimiento de reglas claras de funcionamiento, y procedimientos precisos y fácilmente comprensibles, de manera que estos puedan ser aplicados por todo el personal que intervenga en la operación del PREP.

## 3. Objetivos y Alcance

---

### 3.1 Objetivos Generales

Establecer una estrategia para salvaguardar la integridad, disponibilidad y confidencialidad de la Información así como la continuidad de la operación del PREP; identificando los riesgos de seguridad de la información en las diferentes etapas del Programa; en cuanto a procedimientos, Servicios e infraestructura en tecnologías de la información y comunicación, recursos humanos y seguridad física, para así establecer los controles de seguridad apropiados que permitan reducir el riesgo a un nivel tal, que asegure la confiabilidad y continuidad de los sistemas, activos tecnológicos y servicios informáticos.

### 3.2 Objetivos Particulares

- a) Elaborar las directrices de seguridad de la información para el PREP.
- b) Realizar el análisis de riesgos permitiendo identificar las vulnerabilidades de seguridad que enfrenta el PREP.

- c) Identificar e implementar los controles de seguridad en los distintos procesos de operación del PREP y en la infraestructura tecnológica.
- d) Implantar soluciones de seguridad perimetral con la finalidad de controlar y vigilar el tráfico de la red de datos que soporta al PREP.
- e) Fortalecer el desarrollo de las aplicaciones que deriven en el cumplimiento de los distintos procesos de operación del PREP.
- f) Establecer el plan de concientización para capacitar y transmitir el sentido de la seguridad de la información del PREP.
- g) Definir el esquema de control de acceso a los diferentes sistemas del PREP.
- h) Establecer el Plan de Continuidad para minimizar el impacto a la operación, así como el plan de recuperación de pérdidas de activos de información.
- i) Elaborar los documentos necesarios para favorecer la evaluación del ente auditor designado por el INSTITUTO.

### 3.3 Alcance

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

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

Este documento se encuentra elaborado con fundamento en el anexo 13 del Reglamento de Elecciones del Instituto Nacional Electoral, así como, con los Acuerdos que emita el Consejo General del INSTITUTO.

El artículo 347, numeral 1 del Reglamento de Elecciones, establece que el Instituto y los OPL deberán someter su sistema informático a una auditoría técnica de verificación y análisis, para lo cual se deberá designar un ente auditor. El alcance de la auditoría deberá cubrir, como mínimo, los puntos siguientes:

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

El artículo 348, numeral 1, del Reglamento de Elecciones, dispone que, 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.

El numeral 12 del Anexo 13 del Reglamento de Elecciones que contiene los Lineamientos del PREP, señala que 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: deberán 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 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.

El numeral 13 de los lineamientos del PREP, establece que 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 será comunicado al personal directivo, técnico y operativo del Programa, y será de observancia para todos los involucrados en su ejecución y formará parte de los ejercicios y simulacros.

Todas las medidas y acciones a tomar serán de carácter obligatorio para todo el personal que trabaja en la operación de PREP y se les dará a conocer en las sesiones de capacitación y sensibilización.

## 4. 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.

### Respuesta a incidentes.

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.

Se considerará el marco temporal con el que se dispone para llevar a cabo la implementación de los siguientes puntos:

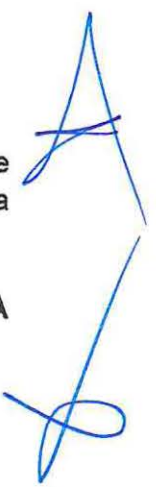
- Se generará, aprobará y difundirán las Directrices de seguridad de la información para el PREP.
- Se realizará un análisis de riesgos en materia de seguridad de la información mediante el apoyo de alguna Metodología de Administración de Riesgos.
- Se desarrolló y se implementará el plan de tratamiento de riesgos para fortalecer la seguridad física, de recursos humanos, de procesos operativos y de infraestructura tecnológica del PREP.
- Se fortalecerá y complementarán los programas de capacitación y concientización en materia de seguridad de la información.
- Se llevarán a cabo auditorías internas de los controles de seguridad aplicados a nivel tecnológico y de proceso o procedimiento.
- Se generarán los esquemas de prevención, detección y respuesta a incidentes de seguridad.
- Se desarrollaron los mecanismos de continuidad y de recuperación ante casos de desastre.
- Se coordinan en conjunto con personal del ente auditor externo, las actividades de auditoría al sistema informático y a la infraestructura del PREP.

### 1. DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

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

### 2. CONSIDERACIONES Y RECOMENDACIONES DE SEGURIDAD DE LA INFORMACIÓN

Respecto a la Seguridad Física se siguen las siguientes recomendaciones:



#### **a) Diseño del ambiente de control**

- I. La instalación eléctrica de los CCV y CATD cuentan con tierra física apropiadamente instalada, y verificar que la asignación de la polaridad de los contactos sea correcta para evitar contratiempos relacionados con el suministro eléctrico;
- II. Se instalan fuentes de alimentación ininterrumpida (UPS o No Break) con regulador integrado, de manera que, ante una posible variación en el suministro eléctrico, el equipo de cómputo esté debidamente protegido y pueda continuar su operación en lo que el corte se resuelve, o se implementa alguna alternativa de operación;
- III. Se cuenta con una planta de energía de emergencia con las características y capacidad suficiente para que los equipos y dispositivos conectados, que forman parte del CCV continúen en operación.
- IV. Colocar extintores basados en CO<sub>2</sub>, que no dañan el equipo de cómputo al ser usados, distribuidos estratégicamente en todos los recintos donde se vaya a llevar a cabo la operación del PREP.
- V. Realizar actividades de supervisión para evaluar los problemas y corregir las deficiencias

#### **b) Controles de acceso electrónicos, procedimentales y mecánicos**

- I. El acceso tanto a recintos como a equipos debe ser controlado de manera estricta, por personal de seguridad, tanto en recintos como a equipos, y registrados en bitácoras que sean analizables en cualquier momento por el personal autorizado del OPLE;
- II. Definir, preferentemente, contraseña a nivel de BIOS/CMOS para aquellos equipos cruciales para la operación del PREP, de manera que no sea posible acceder a las opciones de configuración a nivel de equipo;
- III. Se establece el bloqueo automático de pantalla en todas las computadoras al tiempo mínimo posible, instruyendo al personal que deben bloquear manualmente sus terminales de trabajo al alejarse de estas, aún si el tiempo de ausencia es mínimo.

#### **c) Detección de intrusiones**

- I. Acceso restringido en el centro de datos principal y controles de seguridad físicos sobre los activos y bienes vulnerables
- II. Cualquier acción de acceso irregular, tanto a recintos como a equipos, (accesos fuera de horario, cantidad de personal diferente del esperado, etc.) debe ser debidamente reportada de manera automática bajo la forma de una alerta de manera oportuna al personal responsable.
- III. Monitoreo por video CCTV en los CCV, teniendo acceso en cualquier momento el personal autorizado del INSTITUTO, tanto a las imágenes en tiempo real, como a las grabaciones.

En cuanto a la Integridad de los datos, se siguen las siguientes recomendaciones:



- a) Debe existir un programa verificable de realización de respaldos de la información crucial para la operación del PREP por parte del proveedor de los servicios de operación del PREP;
- b) Buscar minimizar el riesgo de infección por virus computacionales, de preferencia haciendo uso de un sistema operativo con bajo riesgo de ser afectado por programas perniciosos, o instalando programas antivirus con licencias y firmas actualizadas, y asegurando que los equipos tengan instaladas las últimas actualizaciones del sistema operativo.
- c) Se utilizan comunicaciones cifradas utilizando protocolo TLS versión 1.3.
- d) Actualmente se configura el servicio de monitoreo de infraestructuras y aplicaciones de AWS Amazon CloudWatch <https://aws.amazon.com/es/cloudwatch/>

Respecto de la Seguridad de los datos, se siguen las siguientes recomendaciones:

- a) Hacer uso de contraseñas fuertes, pudiendo verificarse la fortaleza de estas a través de aplicaciones como: <https://www.security.org/how-secure-is-my-password/>
- b) Algunas sugerencias para la definición de contraseñas seguras y que se siguen por protocolo son: su longitud debe ser de al menos ocho caracteres; se usa la combinación de letras mayúsculas y minúsculas, así como el uso de caracteres numéricos y signos de puntuación; no usar palabras contenidas en un diccionario en cualquier idioma, ni información personal o basada en el contexto; asimismo es importante seleccionar una contraseña que sea fácil de recordar, de forma tal que no sea necesario escribirla, pero que al mismo tiempo sea difícil de imaginar; cada contraseña debe ser de uso estrictamente personal y no debe ser compartida con nadie. Las contraseñas se almacenan hasheadas en la base de datos.
- c) Los servidores donde se almacenen programas y datos, y donde sean ejecutados los programas del Sistema PREP, deben contar con medidas de seguridad especialmente estrictas, como lo es el uso de contraseñas robustas, estar detrás de un firewall definiendo claramente la lista de usuarios que tienen derecho a acceder a este;
- d) Las cuentas de usuario deben tener el mínimo de privilegios disponible en el sistema operativo que se use para la operación del PREP, teniendo en particular restringida la instalación de software, estando preferentemente en un segmento de red aislado, verificando la correcta asignación de permisos de acceso y uso a los diversos sistemas de archivos, de preferencia a través de algún estándar basado en RBAC (Role-Based Access Control);
- e) Se debe contar con firewall físico en las áreas de importancia crucial para la correcta operación del PREP, y se debe habilitar el firewall del sistema operativo en todas las terminales de operación del PREP;
- f) Toda transmisión de datos debe hacerse de manera encriptada haciendo uso de algoritmos fuertes basados en SSL/TLS versión 1.3 para tal efecto;
- g) Se debe deshabilitar la cuenta de superusuario en todas las terminales.
- h) Se debe deshabilitar en las terminales de trabajo el acceso a todo sitio que no esté directamente relacionado con la operación del PREP (filtrado MAC y por dirección IP), de preferencia dando única y exclusivamente acceso a los equipos autorizados (mapeo uno a uno);

- i) Se debe deshabilitar en todas las computadoras destinadas a la operación del PREP el uso de medios de arranque externos, como memorias USB o CD;
- j) Se debe deshabilitar el uso de cualquier medio externo de almacenamiento de datos, salvo con la autorización, a través de acceso directo a la terminal de trabajo, de un coordinador;
- k) Se debe entrenar al personal operativo para reconocer adecuada y oportunamente cualquier tipo de ataque, siendo los más comunes de éstos la suplantación de identidad a través de mensajes de correo electrónico, y el conocido como Phishing, de manera que sean capaces de identificar las características de este tipo de ataques, y poder actuar en consecuencia ante la presencia de uno;
- l) Se debe deshabilitar el acceso inalámbrico, tanto vía Wifi como Bluetooth, a todos los equipos de operación del PREP, así como en todos los puntos de acceso de red, usándose única y exclusivamente comunicación vía cable UTP, o tecnología alámbrica equivalente.

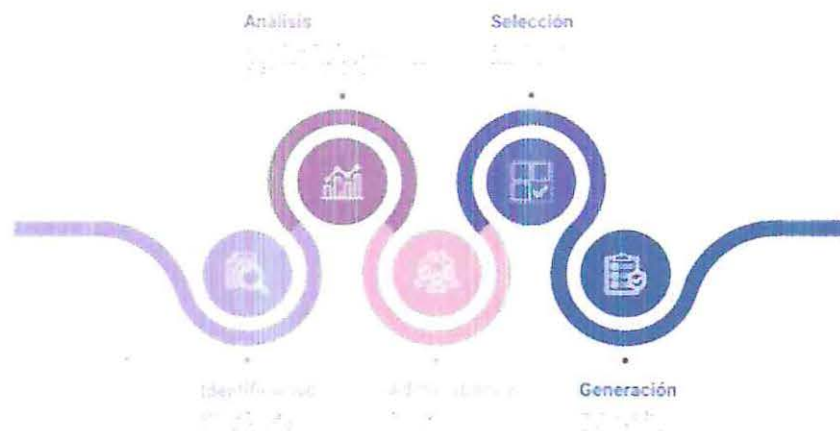
Además de las anteriores consideraciones, es importante tener en cuenta que, durante el desarrollo del Programa, se pondrán en práctica los buenos usos y prácticas en términos de la gestión de seguridad de toda documentación de naturaleza sensible, como las que se presentan a continuación:

- a) Las comunicaciones sobre información sensible no deben llevarse a cabo en lugares donde puedan ser escuchadas;
- b) Información que pueda llevar a la identificación de individuos deberá ser evitada en las conversaciones;
- c) La comunicación oral de información sensible debe hacerse en áreas seguras;
- d) Documentos sensibles no deben ser dejados sobre impresoras, copiadoras, escritorios, etcétera;
- e) Documentos sensibles no deben dejarse a la vista de posibles visitantes externos;
- f) Si es necesario dejar documentos sensibles en áreas donde puede haber visitantes, deben colocarse con el contenido hacia abajo, o eventualmente cubiertos con una hoja;
- g) Documentos sensibles que ya no son necesarios deben destruirse inmediatamente, o colocados en contenedores apropiados para su posterior destrucción;
- h) Conversaciones telefónicas sobre temas sensibles deben llevarse a cabo de manera discreta;
- i) Cuando se trate un tema relativo a una persona en particular, confirmar de quién se está hablando antes de hacerlo;
- j) Si la persona a quien se quiere localizar no se encuentra, únicamente dejar el nombre y teléfono a donde deberá llamar cuando esté disponible;
- k) Mantener bajo el volumen del altavoz;
- l) Evitar colocar información sensible en memorias USB u otros medios de almacenamiento de datos;
- m) Si un dispositivo móvil es robado o extraviado debe ser reportado inmediatamente;
- n) Tener cuidado al incluir cualquier información que pueda ser considerada como confidencial en un mensaje de correo electrónico;

- o) Ser particularmente cuidadoso al enviar archivos adjuntos, y tener en cuenta que archivos adjuntos recibidos pueden ser fuente de malware;
- p) Si la información enviada es confidencial incluir una nota informativa sobre este hecho al final;
- q) Releer un mensaje antes de enviarlo con la finalidad de corroborar que los destinatarios son correctos; y
- r) Verificar siempre los campos "para", "cc" y "bcc", especialmente cuando se aplica la acción "responder a todos"

## 5. Análisis de Riesgos en Materia de Seguridad de la Información

Se cuenta con una Metodología de Administración de Riesgos para el análisis y evaluación de riesgos en materia de seguridad de la información para así detectar posibles riesgos y poder aplicar controles con la finalidad de administrar los riesgos identificados.



La Administración de Riesgos está basada en los principios de la Metodología NIST SP 800-30 el cual establece como procesos en la gestión de riesgos los siguientes:

- a) **Estructura:** definiendo los activos o áreas donde se pueden identificar posibles amenazas
- b) **Evaluación:** Clasificar el grado de criticidad
- c) **Respuesta:** el procedimiento a ejecutar al detectarse
- d) **Seguimiento:** el tratamiento para mitigar el riesgo

### Criterios de Evaluación de Riesgos

Para evaluar los riesgos se tomará como referencia:

- I. Activos. Recursos relacionados con la ejecución del PREP para el Proceso Electoral Local Extraordinario 2025.
- II. Criticidad de Activo. Valor que se determina evaluando los criterios a cada activo de:
  - a) **Confidencialidad:** Información debe ser accedida sólo por las personas autorizadas.
  - b) **Disponibilidad:** Acceso a la información cuando se necesita.
  - c) **Integridad:** Exactitud y totalidad de la información.

**Nivel de Criticidad = Confidencialidad + Integridad + Disponibilidad**

Para obtener el nivel de criticidad se establecen los siguientes niveles seleccionados en la Confidencialidad, Integridad y Disponibilidad:

| <b>Confidencialidad</b> | La información debe ser accesible solo a las personas debidamente autorizadas: |
|-------------------------|--|
| Pública                 | 1  |
| Uso interno             | 2  |
| Confidencial            | 3  |
| Reservada               | 4  |

| <b>Integridad</b>   | La información debe ser completa, exacta y válida. La información no debe ser alterada. Si el activo o información contiene errores: |
|---|--|
| Afecta la operación                                       | 4  |
| Afecta moderadamente la operación                         | 3  |
| Los errores o cambios no afectan su sentido principal     | 2  |
| Pueden tener errores sin tener un impacto en la operación | 1  |
| <b>Disponibilidad</b>                                     | La información o el activo debe estar disponible cuando se le necesita, en forma organizada para las personas autorizadas:           |
| Muy Alta  | 4  |



|       |   |
|-------|---|
| Alta  | 3 |
| Media | 2 |
| Baja  | 1 |

Según el valor promedio que se registra en cada pilar de la información, se realiza la tasación final correspondiente al valor de criticidad, como se muestra en la siguiente tabla y solamente cuando dos de los tres pilares de seguridad tiene el valor de 4, se le asignará al activo un valor de 4.4 de Muy Alto.

| Valoración del Activo | Criticidad |
|-----------------------|------------|
| Muy Alto              | 4.4        |
| Alto                  | 4          |
| Medio                 | 3          |
| Bajo                  | 2          |

- I. **Amenaza.** Evento que al llevarse a cabo produce daños de carácter material o inmaterial a los activos.
- II. **Probabilidad.** Es el grado que hace referencia a la probabilidad de que una amenaza se materialice por una vulnerabilidad específica, es decir, mientras que un activo posee más vulnerabilidades, la probabilidad de ocurrencia es mayor, para lo cual se debe tener en cuenta el nivel eficacia de los controles utilizados en pasados procesos electorales, la estimación de la probabilidad se realiza, mediante la escala, Alto, Bajo y Medio..
- III. **Impacto.** Es el grado de consecuencia que deja una amenaza materializada sobre un activo.
- IV. **Riesgo.** Es el grado o estimación de que una amenaza se materialice sobre un activo y produzca daños en la operación. Para la determinación del nivel de riesgo se usa una escala de Alto, medio y bajo.
- V. **Responsable.** Nombre del responsable de la implementación del plan de mitigación.
- VI. **Tratamiento del riesgo.** Define las acciones para gestionar los riesgos de seguridad de la información, valora el nivel de riesgo o aquellos a los que se les ha implementado controles efectivos, en la etapa de valoración de riesgos. Para ello nos remitimos a analizar cada uno de ellos:
  - a) **Aceptar o Asumir el Riesgo:** Se acepta el riesgo, bien porque está debajo del umbral aceptable de riesgo o porque no hay necesidad de implementar controles adicionales y se puede retener el riesgo.
  - b) **Mitigar el Riesgo:** El nivel de riesgo debe ser gestionado introduciendo, alterando o eliminando controles para que el riesgo pueda ser reevaluado como aceptable. En esos casos lo que hay que hacer es ampliar o mejorar el conjunto de salvaguardas

tomando las medidas oportunas para que el nivel de riesgo se sitúe por debajo del umbral.

- c) **Transferir o compartir el Riesgo:** Se lleva a cabo cuando se decide transferir el riesgo a partes externas. La transferencia se puede realizar mediante subcontratación, o contratación de seguros, etc.
- d) **Evitar o eliminar el riesgo:** Cuando los riesgos identificados se consideran demasiado altos otras opciones de tratamiento de riesgos que exceden los beneficios, es tomar la decisión de evitar el riesgo por completo, retirándose de una actividad o conjunto de actividades planificadas o existentes, o cambiando las condiciones bajo el cual se opera la actividad.
- e) **Exposición del riesgo:** La combinación de valores de importancia, probabilidad y cobertura de los controles asignados a cada factor de riesgo de la forma que se ha descrito anteriormente, determina su clasificación en uno de los niveles de riesgo definidos. Esta información puede sintetizarse en un mapa semántico, construido con la combinación de un gráfico con un código de color basado en el porcentaje de impacto y la probabilidad de ocurrencia para determinar la exposición a cada uno de esos factores y determinar un valor de prioridad de monitoreo.

## 6. Activos Críticos.

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

|    | Tipo    | Nombre                     | Descripción   | Responsable                            | Tipo                                 | Ubicación   | Criticidad |
|----|---------|----------------------------|---|--|--------------------------------------|---|------------|
| A1 | Digital | Sistema informático        | Programas de computación  | Coordinación de desarrollo de software | Programas de computación             | En la nube, estaciones de trabajo en los CCV y CATD | Muy Alto   |
| A2 | Digital | Infraestructura en la nube | Servidores de procesamiento de información                          | Coordinador de Desarrollo de software  | Programas de computación             | Servidores en la nube                               | Alto       |
| A3 | Digital | Aplicativo móvil           | APK desarrollada para móviles y la foto de fotografía en la casilla | Coordinador de Desarrollo de software  | Aplicaciones de dispositivos móviles | Servidores en la nube, dispositivos móviles         | Medio      |

|     |             |  |   |  |                                    |  |                   |
|-----|-------------|--|---|--|------------------------------------|--|-------------------|
| A4  | Digital     | Sitios de difusión en internet.        | Despliegan información del PREP en navegador de Internet          | Coordinación de red                                      | Programas de computación           | Servidores en la nube                        | Bajo              |
| A5  | Mixto       | Seguridad perimetral                   | Dispositivos para monitorear y detectar intrusos en la red        | Coordinación de red                                      | Equipos y programas de computación | En los CCV y los CATD                        | Alto              |
| A6  | Mixto       | Enlaces de internet del CCV y los CATD | Proporcionan conectividad entre el CCV, los CATD y los Servidores | Coordinación de red y proveedor de servicios de internet | Servicio                           | En los CCV, los CATD y Servidores en la nube | Alto              |
| A7  | Físico      | La red eléctrica en el CCV y los CATD  | Provee energía eléctrica a los equipos e infraestructura de red   | Coordinación del PREP                                    | Servicio                           | En los CCV y los CATD                        | Medio             |
|     | <b>Tipo</b> | <b>Nombre</b>                          | <b>Descripción</b>  | <b>Responsable</b>                                       | <b>Tipo</b>                        | <b>Ubicación</b>                             | <b>Criticidad</b> |
| A8  | Físico      | Los equipos de cómputo en los CCV      | Computadoras y componentes externos                               | Coordinación del PREP                                    | Equipo                             | En los CCV y los CATD                        | Alto              |
| A9  | Físico      | Enlaces de telefonía fija              | Enlaces de comunicación a través del Teléfono fijo                | Proveedor de telefonía                                   | Servicio                           | En los CCV                                   | Bajo              |
| A10 | Mixto       | Servicio de datos Móviles              | Servicios de datos  | Proveedor de datos                                       | Servicio                           | CAE y CATD                                   | Alto              |

|     |        |                                     |  |                       |           |                               |          |
|-----|--------|-------------------------------------|--|-----------------------|-----------|-------------------------------|----------|
| A11 | Físico | Equipo móvil para la digitalización | Celulares distribuidos a los CAE y en los CATD                 | Coordinación del PREP | Equipo    | CAE y CATD                    | Alto     |
| A12 | Humano | El personal Operativo               | Personal involucrado en el desarrollo del PREP                 | Coordinación del PREP | Personal  | En los CCV, los CATD y CAE    | Muy Alto |
| A13 | Físico | Acta PREP                           | Fuente de información del PREP Acta de Escrutinio y Cómputo    | Acopiador             | Documento | En las Casillas y en los CATD | Alto     |
| A14 | Mixto  | Plantas de Energía                  | Planta generadora de luz para asegurar la operatividad del CCV | Personal Operativo    | Equipo    | CCV Central                   | Medio    |
| A15 | Mixto  | Documentos internos                 | Documentos que describen los procesos y operación del PREP     | Coordinación del PREP | Documento | En los CCV y los CATD         | Bajo     |

|     | Tipo   | Nombre   | Descripción                  | Responsable           | Tipo      | Ubicación             | Criticidad |
|-----|--------|--|------------------------------|-----------------------|-----------|-----------------------|------------|
| A16 | Humano | Concientización y capacitación de la seguridad informática | Capacitación de los procesos | Coordinación del PREP | Documento | En los CCV y los CATD | Medio      |



## ÁREAS DE AMENAZA

Por las implicaciones técnicas, políticas y sociales que existen en las diferentes regiones del Estado, y en específico la experiencia resultante de los Procesos Electorales anteriores, se considera que pueden ser susceptibles de afectación al procedimiento para la implementación del PREP, las siguientes áreas:

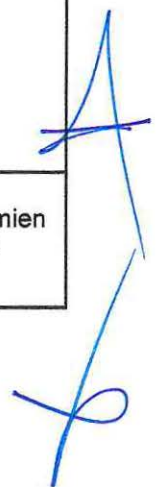
- El CCV Central
- Los CATD
- Los celulares PREP Casilla
- Los enlaces y redes de comunicación
- El portal del PREP y mecanismos de publicación

## RIESGOS IDENTIFICADOS

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

| RESULTADOS DE ANÁLISIS DE RIESGOS  |   |              |         |        |                         |                       |                 |
|------------------------------------|---|--------------|---------|--------|-------------------------|-----------------------|-----------------|
| DURANTE LA OPERACIÓN DEL PREP 2025 |   |              |         |        |                         |                       |                 |
| NÚM                                | AMENAZA   | PROBABILIDAD | IMPACTO | RIESGO | RESPONSABLE             | TRATAMIENTO DE RIESGO | PROCEDIMIENTO   |
| 1                                  | Acceso no autorizado a las aplicaciones                       | Bajo         | Alto    | Bajo   | Coordinador de software | ACEPTADO              | Procedimiento 1 |
| 2                                  | Virus informáticos o código malicioso.                        | Bajo         | Alto    | Bajo   | Coordinador de software | ACEPTADO              | Procedimiento 2 |
| 3                                  | Fuga de información por ausencia de controles criptográficos. | Bajo         | Medio   | Bajo   | Coordinador de software | ACEPTADO              | Procedimiento 3 |
| 4                                  | Inadecuada seguridad de los dispositivos de seguridad         | Bajo         | Alto    | Bajo   | Administrador de la red | ACEPTADO              | Procedimiento 4 |

|    |   |       |       |       |                         |          |                 |
|----|---|-------|-------|-------|-------------------------|----------|-----------------|
|    | perimetral de la red.   |       |       |       |                         |          |                 |
| 5  | Caída de Servidores o no disponibilidad del sitio de publicación                      | Medio | Alto  | Medio | Administrador de la red | MITIGAR  | Procedimiento 5 |
| 6  | Falla en los servicios de Internet y servicios de datos                               | Medio | Medio | Medio | Administrador de la red | MITIGAR  | Procedimiento 6 |
| 7  | Insuficiencia del suministro de energía eléctrica                                     | Bajo  | Alto  | Bajo  | Coordinación del PREP   | ACEPTADO | Procedimiento 7 |
| 8  | CATD o CCV no puede operar en el lugar  | Bajo  | Alto  | Bajo  | Coordinador del PREP    | ACEPTADO | Procedimiento 7 |
| 9  | Falla o ausencia en los equipos de cómputo y para la realización de la digitalización | Bajo  | Alto  | Bajo  | Coordinador del PREP    | ACEPTADO | Procedimiento 8 |
| 10 | Ausencia del personal   | Alto  | Alto  | Alto  | Coordinador de personal | MITIGAR  | Procedimiento 9 |



|    |  |       |       |       |                            |          |                  |
|----|--|-------|-------|-------|----------------------------|----------|------------------|
| 11 | Falta de Conciencia y capacitación en los requerimientos de seguridad y las necesidades de control | Medio | Alto  | Medio | Coordinador del PREP       | MITIGAR  | Procedimiento 11 |
| 12 | Falta de provisión de documentación de operación   | Medio | Medio | Medio | Coordinador del PREP       | MITIGAR  | Procedimiento 10 |
| 13 | Ausencia de control de acceso físico a los CCV y CATD  | Bajo  | Alto  | Bajo  | Coordinación de CATD y CCV | ACEPTADO | Procedimiento 12 |

## Criterios para medir riesgos

Para establecer una línea o base de criterios de medición de riesgos, se deberán tomar en consideración aspectos como los enlistados a continuación:

- Experiencia en la implementación del Programa
- Circunstancias ambientales y geográficas
- Estructura tecnológica propia y contratada
- Ambiente político electoral

Considerando los aspectos anteriormente descritos, tendremos oportunidad de planear y tomar las acciones necesarias para mitigar y/o evitar en su totalidad los riesgos per se. Los criterios para medir y en dado caso mitigar estos riesgos, los enlistamos a continuación:

## Basados en experiencias pasadas

Este criterio, resulta ser muy útil cuando aplica, pues de acuerdo con las experiencias pasadas, ya sean favorables o desfavorables en la implementación del PREP, es posible establecer medidas preventivas para mitigar los riesgos, es decir, la experiencia, resulta ser algunas veces costosa y de gran ayuda, pero sin duda debe ser tomada en cuenta.



## Basados en condiciones geográficas del Estado

Identificamos riesgos de acuerdo con las condiciones geográficas, eléctricas, carreteras, accesos y de telecomunicaciones de los Consejos Distritales donde se localizan los CATD, para establecer rutas seguras tendientes a lograr mitigar o eliminar los riesgos asociados con la falta de seguridad o de algún servicio necesario o los tiempos de reacción para imprevistos.

## Basados en ambiente sociopolítico del Proceso Electoral

Identificamos riesgos sociopolíticos que pudieran tener como consecuencia marchas o plantones que pudieran evitar accesos a los lugares de trabajos del PREP, violencia o amenaza para continuar con las labores del programa a fin de establecer rutas de accesos alternos, redundancia de lugares físicos para continuar con las labores y medidas de seguridad personal y rutas de evacuación.

## Basados en la estructura electoral de cada tipo de elección

Identificamos riesgos basados en la complejidad de campos de captura por distintas y variadas combinaciones en las AEC a fin de establecer medidas pertinentes de capacitación y pruebas y evitar errores o retrasos en la captura.

Para establecer los criterios de identificación de los riesgos, nos basamos en cuatro consideraciones:



Tomando en consideración los anteriores aspectos, se podrá tener una visión clara de las afectaciones que pudieran tener sobre los diferentes aspectos del Programa y así clasificarlos de acuerdo con el nivel de riesgo que representen.



## Evaluación de riesgos por probabilidad e impacto

Efectuada la evaluación cualitativa de cada uno de los factores de riesgo, hay que agrupar los resultados según la tipología de riesgos definidos para determinar la exposición de cada uno de los factores (manteniendo el mismo criterio de simplicidad que se ha utilizado hasta ahora), se realizó la agregación de los resultados para determinar la exposición al riesgo y se determinaron intervalos en función del número de factores de riesgo que se han calificado en cada uno de los niveles. Finalmente, para obtener el resultado se multiplican entre sí los valores determinados para obtener la Probabilidad y el Impacto, como a continuación se muestra:

| Probabilidad de ocurrencia de una Amenaza | Impacto                      |                               |                                |
|---|------------------------------|-------------------------------|--------------------------------|
|   | Bajo (10)                    | Medio (50)                    | Alto (100)                     |
| Alta (1.0)                                | Bajo<br>$10 \times 1.0 = 10$ | Medio<br>$50 \times 1.0 = 50$ | Alto<br>$100 \times 1.0 = 100$ |
| Media (0.5)                               | Bajo<br>$10 \times 0.5 = 5$  | Medio<br>$50 \times 0.5 = 25$ | Alto<br>$100 \times 0.5 = 50$  |
| Baja (0.1)                                | Bajo<br>$10 \times 0.1 = 1$  | Medio<br>$50 \times 0.1 = 5$  | Alto<br>$100 \times 0.1 = 10$  |

Dependiendo del valor que resulte al hacer la multiplicación mencionada se determina el riesgo

| NIVEL | VALORES ENTRE |
|-------|---------------|
| ALTO  | 51 y 100      |
| MEDIO | 11 y 50       |
| BAJO  | 1 y 10        |

En general priorizaremos mediante este criterio:

- A. **Baja probabilidad y bajo impacto:** serán normalmente ignorados.
- B. **Baja probabilidad y alto impacto:** reduciremos su impacto o estableceremos los procedimientos del plan de seguridad y continuidad, si se presentan.
- C. **Alta probabilidad y bajo impacto:** reduciremos la probabilidad.
- D. **Alta probabilidad y alto impacto:** se actuará inmediatamente.

Cada intervalo viene definido por el cumplimiento de la condición numérica establecida. Los umbrales para evaluar cada intervalo se pueden determinar de la siguiente forma:

| Nivel de exposición | Porcentaje de factores de riesgo |
|---------------------|----------------------------------|
| Alto                | 50% al 100%                      |
| Medio               | 10 % al 49%                      |

|      |          |
|------|----------|
| Bajo | 1% al 9% |
|------|----------|

| Puntaje de impacto (basado en las medidas de Criticidad, efectividad de los controles e impacto) |       | Escala de Impacto |       |      |
|--|-------|-------------------|-------|------|
|  |       | Bajo              | Medio | Alto |
| Probabilidad   | Alta  | 10%               | 50%   | 100% |
|  | Medio | 5%                | 25%   | 50%  |
|  | Bajo  | 1%                | 5%    | 10%  |

| Amenaza   | Exposición al Riesgo | Amenaza   | Exposición al Riesgo |
|---|----------------------|---|----------------------|
| Acceso no autorizado al sistema.  | 10                   | CATD o CCV no puede operar en el lugar  | 10                   |
| Virus informáticos o código malicioso.                                      | 10                   | Falla o ausencia en los equipos de cómputo y para la realización de la digitalización | 10                   |
| Fuga de información por ausencia de controles criptográficos.               | 5                    | Ausencia del personal   | 100                  |
| Inadecuada seguridad de los dispositivos de seguridad perimetral de la red. | 10                   | Falta de conciencia en los requerimientos de seguridad y las necesidades de control   | 50                   |
| Caída de servidores o no disponibilidad del sitio de publicación            | 50                   | Falta de provisión de documentación de operación                                      | 25                   |
| Falla en los servicios de Internet y servicios de datos                     | 25                   | Ausencia de control de acceso físico a los CCV y CATD                                 | 10                   |

|   |    |
|---|----|
| Insuficiencia del suministro de energía eléctrica | 10 |
|---|----|

## 7. Implementación de los controles necesarios para fortalecer el acceso de las y los usuarios a bases de datos, servidores, equipos de comunicaciones y equipos de cómputo personal.

Los controles a implementar para fortalecer la seguridad en el acceso a servidores, base de datos, equipos de comunicaciones y cómputo personal son los siguientes:

- Se implementarán controles necesarios para detectar cualquier actividad sospechosa en el tráfico generado en la red donde se encuentran los equipos, con la instalación de dispositivos para el monitoreo y control de tráfico.
- Los equipos de cómputo tendrán los parches de seguridad instalados y firmas de antivirus actualizadas.
- Se implementarán restricciones por IP para las conexiones realizadas en el periodo de pruebas.
- Se implementarán sistemas de detección y prevención de intrusos en la central donde se encuentran los servidores web, bases de datos, sistema de cómputo y servicios de publicación

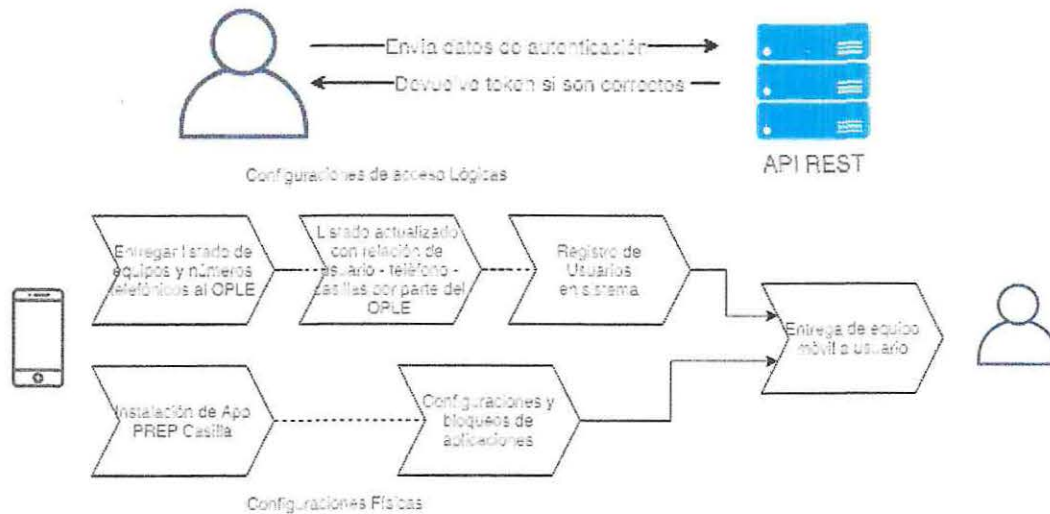
### Emisión de lineamientos para control de acceso lógico.

Lineamientos para controlar el acceso lógico a las aplicaciones que debe seguir el personal que requiera acceso a la red, recursos y aplicaciones es el siguiente:

- Todo acceso debe ser autorizado por el área correspondiente.
- Cada equipo instalado en los CCV para las actividades de captura y verificación deben estar conectados a la red local.
- El uso de usuarios y contraseñas de los aplicativos es responsabilidad de cada usuario, toda actividad realizada en las aplicaciones quedará registrada con el usuario que la realizó. Esta bitácora deberá tener la característica de que sólo se podrán agregar registros, y no modificar ni eliminar, de manera que no se pueda borrar o modificar el rastro de alguna acción realizada, eliminándose así evidencia que pudiera implicar responsabilidad.
- Las solicitudes de usuarios a aplicaciones serán distribuidas por el área de coordinación, quienes llevarán un registro del personal autorizado para el uso de cada aplicación.
- El acceso o conexión a la red local de equipo de cómputo o dispositivos debe ser autorizado por el administrador de red.

## Arquitectura para la autenticación desde los dispositivos móviles y desde los MCAD y TCA.

- Para las aplicaciones involucradas en las tareas de digitalización, captura y verificación se utiliza el modelo de autenticación API REST con token y cifrado SSL.
- Los datos de autenticación requeridos para los usuarios de las aplicaciones son usuario y contraseña, a excepción de la app PREP casilla la cual utiliza la autenticación mediante número telefónico y código de acceso enviado al teléfono móvil por mensaje de texto SMS.
- El API REST valida los datos de autenticación del usuario, si son correctos éste genera y devuelve un token.



### Políticas de seguridad para el aplicativo PREP Casilla

- El equipo telefónico móvil proporcionado a la o el CAE debe tener precargada la aplicación PREP Casilla, el equipo será configurado por el personal técnico, el cual realizará también los bloqueos de ejecución o descarga de aplicaciones innecesarias para la actividad de digitalización en el equipo.
- Se debe contar con registro de cada teléfono celular: nombre de usuario, número de teléfono asignado, IMEI para tener un control en la asignación de los equipos.
- Cada usuario debe tener los permisos en cuanto a las casillas que le corresponden, la relación usuario casillas corresponde al listado de casillas instaladas proporcionado por el INE.
- Los usuarios deben recibir capacitación acerca del uso de la aplicación.
- Cada vez que se inicie sesión se realizará la autenticación mediante envío de código por SMS al número telefónico que solicita iniciar sesión, validando que esté registrado en la base de datos del sistema.
- Los equipos tendrán geolocalización para validar la procedencia de las imágenes. Cada equipo, así como su uso es responsabilidad del digitalizador/CAE al cual se le asignó, cada actividad realizada será registrada con su número telefónico y usuario correspondiente.
- Uso de cifrado de datos SSL



- Generación de código HASH o código de integridad para imágenes digitalizadas.
- La aplicación PREP Casilla permitirá la digitalización off-line, en caso de fallas en la red que impidan en algún momento la transferencia hacia la central de datos, los usuarios
- Digitalizadores podrán continuar realizando las actividades de digitalización y el envío se realizará al restablecerse la conectividad.

#### **Políticas de seguridad para la aplicación de digitalización desde CCV.**

- a) El equipo de cómputo debe ser proporcionado por el personal técnico, el equipo contará con los programas necesarios para el funcionamiento de la aplicación, así como con los parches de seguridad, antivirus y bloqueos tanto de software como de hardware que no sea necesario para realizar la actividad de digitalización y/o represente un riesgo para la integridad y seguridad de la información que se procese.
- b) Se debe tener registro de los datos personales de cada Digitalizador, así mismo deberá haber pasado por los filtros de selección requeridos para su contratación.
- c) Los digitalizadores deberán recibir la capacitación acerca del uso de la aplicación, así como conocer el estándar de calidad deseado de las imágenes de PREP Casilla, ya que tendrá la decisión de rechazar o enviar las imágenes digitalizadas desde la casilla. Cualquier error del sistema o del equipo de cómputo asignado deberá ser reportado al supervisor del CCV para recibir instrucciones de la forma de proceder ante la falla.
- d) Cada digitalizador deberá tener su propio usuario y contraseña.
- e) La aplicación de digitalización contará con las validaciones necesarias en cuanto a la información requerida, de manera que no se pueda enviar imágenes digitalizadas sin tener datos de identificación del acta, así como de la información de acopio, fecha y hora, mecanismo de traslado y tipo de documento.
- f) Las contraseñas usadas el día de la Jornada Electoral serán distintas a las usadas en los simulacros internos y oficiales, y siempre serán proporcionadas por el supervisor del CCV
- g) La información transmitida hacia la central de datos contará con mecanismos de seguridad como el uso de tokens y encriptación de datos SSL, aunados a la autenticación de usuarios y contraseñas. La central contará con validación de patrones de recepción de datos desde la aplicación de manera que cualquier patrón de recepción fuera de lo normal será bloqueado.
- h) La aplicación realizará el bloqueo de identificación de acta una vez realizado el envío de imagen, para que el digitalizador no pueda volver a mandar una imagen de acta previamente enviada a la central.
- i) Restricción de descarga y actualización de base de datos local mediante IP durante el período de pruebas.
- j) Generación de código HASH o código de integridad para imágenes digitalizadas.

#### **Políticas de seguridad para la aplicación de captura**

- a) El equipo de cómputo debe ser proporcionado por el personal técnico, el equipo contará con los programas necesarios para el funcionamiento de la aplicación, así como con los parches de seguridad, antivirus y bloqueos tanto de software como de hardware que no sea necesario para realizar la actividad de digitalización y/o represente un riesgo para la integridad y seguridad de la información que se procese.



- b) Se debe tener registro de datos personales de cada Capturista, así mismo deberá haber pasado por los filtros de selección requeridos para su contratación.
- c) Los Capturistas deberán recibir la capacitación acerca del uso de la aplicación, así como de aprender a clasificar correctamente las inconsistencias de las actas PREP en el sistema.
- d) Cualquier error del sistema o del equipo de cómputo asignado deberá ser reportado al supervisor del CCV Central, para recibir instrucciones de la forma de proceder ante la falla.
- e) La aplicación validará el tipo de dato permitido para cada campo de captura de datos.
- f) Cada capturista deberá tener su propio usuario y contraseña.
- g) Las contraseñas usadas el día de la Jornada Electoral serán distintas a las usadas en los simulacros internos y oficiales, y siempre serán proporcionadas por el supervisor del CCV Central.
- h) La información transmitida hacia la central de datos contará con mecanismos de seguridad como el uso de tokens y encriptación de datos SSL, aunados a la autenticación de usuarios y contraseñas.
- i) Restricción de descarga y actualización de base de datos local mediante IP durante el período de pruebas.

#### **Políticas de seguridad para la aplicación de verificación.**

- a) El equipo de cómputo debe ser proporcionado por el personal técnico, el equipo contará con los programas necesarios para el funcionamiento de la aplicación, así como con los parches de seguridad, antivirus y bloqueos tanto de software como de hardware que no sea necesario para realizar la actividad de digitalización y/o represente un riesgo para la integridad y seguridad de la información que se procese.
- b) Se debe tener registro de datos personales de cada usuario Verificador, así mismo deberá haber pasado por los filtros de selección requeridos para su contratación.
- c) Los Verificadores deberán recibir la capacitación acerca del uso de la aplicación, así como de aprender a clasificar correctamente las inconsistencias posibles del acta PREP PUEBLA en el sistema, el perfil del usuario de verificación es parecido al de captura, sin embargo los usuarios de verificación deberán mostrar una mayor capacidad de análisis y cuidado en su actividad, ya que tendrán la decisión final en la captura de información de actas donde 3 capturistas previamente no coincidieron en la información capturada.
- d) Cualquier error del sistema o del equipo de cómputo asignado deberá ser reportado al supervisor del CCV Central, para recibir instrucciones de la forma de proceder ante la falla.
- e) Cada Verificador contará con su propio usuario y contraseña.
- f) Las contraseñas usadas el día de la Jornada Electoral serán distintas a las usadas en los simulacros internos y oficiales, y siempre serán proporcionadas por el supervisor del CCV Central.
- g) La información transmitida hacia la central de datos contará con mecanismos de seguridad como el uso de tokens y encriptación de datos SSL, aunados a la autenticación de usuarios y contraseñas.
- h) El Verificador contará con la liga de acceso a la aplicación guardada en el navegador para su rápido y fácil acceso.



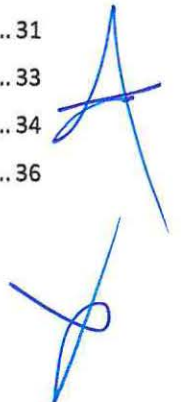
# Plan de Continuidad

- | Programa de Resultados Electorales Preliminares del Instituto Electoral del Estado de Puebla
- | **Proceso Electoral Local Extraordinario 2025**

A  
B

## INDICE


|   |    |
|---|----|
| Glosario .....  | 3  |
| 1. Normatividad Aplicable .....   | 5  |
| 2. Presentación.....  | 6  |
| 1.1 Propiedades de la información.....  | 7  |
| 1.2 Tipos de ataques que pueden presentarse .....   | 8  |
| 3. Objetivos y Alcance .....  | 8  |
| 3.1 Objetivos Generales .....   | 8  |
| 3.2 Objetivos Particulares.....   | 8  |
| 3.3 Alcance .....   | 9  |
| 4. Desarrollo del Plan de Continuidad.....  | 10 |
| 5. Recursos humanos .....   | 13 |
| 6. Implementación del plan de tratamiento de Riesgos .....  | 15 |
| 7. Implementación del Plan de Tratamiento de Riesgos.....   | 25 |
| 8. Control de Accesos y Políticas de Seguridad .....  | 26 |
| 9. Definición de esquema de trabajo a seguir para el control de acceso al aplicativo central, a la aplicación móvil, a la base de datos, servidores y demás infraestructura que den soporte al PREP. .... | 27 |
| 10. Plan de Concientización .....   | 28 |
| 11. Monitoreo Respuesta a los Incidentes de Seguridad.....  | 31 |
| 12. Plan de Continuidad y Recuperación de Desastres.....  | 33 |
| 13. Plan de Comunicación.....   | 34 |
| 14. Auditoría externa en materia de seguridad .....   | 36 |



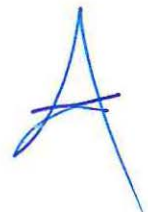
# Glosario

---

|                                    |   |
|------------------------------------|---|
| <b>Análisis de riesgos</b>         | Proceso que comprende la identificación de activos, 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. |
| <b>Baseline</b>                    | 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.  |
| <b>BCP</b>                         | Plan de Continuidad del Negocio, por sus siglas en inglés "Business Continuity Plan".   |
| <b>CATD</b>                        | Centro de Acopio y Transmisión de Datos.  |
| <b>CCV</b>                         | Centro de Captura y Verificación.   |
| <b>CENTRAL</b>                     | Centro de Recepción de Imágenes y Datos.  |
| <b>DDoS</b>                        | Es un ataque de negación de servicio, también llamado ataque DDoS (por sus siglas en inglés, Distributed Denial of Service), es un ataque masivo a un sistema de computadoras o red, cuyo objetivo es volver un servicio o recurso inaccesible a los usuarios legítimos.                                |
| <b>DNS</b>                         | Sistema de nombres de dominio, encargado de la traducción de direcciones IP en direcciones de dominio.  |
| <b>DRP</b>                         | Plan de Recuperación de Desastres, por sus siglas en inglés "Disaster Recovery Plan". Estándar Requerimiento mandatorio que soporta a las directrices de seguridad.   |
| <b>Failover</b>                    | 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.                                 |
| <b>Firewall</b>                    | Dispositivos de seguridad perimetral de la red, que puede implementarse tanto en hardware como en software, 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.                           |
| <b>Hash o código de integridad</b> | Es un valor alfanumérico de representación único que permite identificar a cada imagen del Acta PREP digitalizada, con el cual se verifica su integridad. Dicho valor es obtenido a partir de algún algoritmo criptográfico denominado comúnmente función hash. Ejemplo de función hash es sha256.      |
| <b>IPS</b>                         | Sistema de Prevención de Intrusiones, por sus siglas en inglés "Intrusion Prevention System".   |
| <b>IEE</b>                         | Instituto Electoral del Estado de Puebla  |
| <b>LDAP</b>                        | Protocolo Ligero de Acceso a Directorios, por sus siglas en inglés "Lightweight Directory Access Protocol".   |
| <b>MCAD</b>                        | Monitor de Captura de Actas Digitalizadas.  |



|                           |   |
|---------------------------|---|
| <b>INSTITUTO</b>          | OPLE.   |
| <b>PREP</b>               | Programa de Resultados Electorales Preliminares.  |
| <b>Procedimiento</b>      | Forma específica para llevar a cabo una actividad determinada, su representación gráfica se realiza mediante diagramas de flujo.  |
| <b>PTO</b>                | Proceso Técnico Operativo.  |
| <b>Sniffer</b>            | Aplicación especial para redes informáticas que permite capturar los paquetes que viajan a través de un segmento de red específico.   |
| <b>TCA</b>                | Terminal de Captura de Actas  |
| <b>WAF</b>                | Firewall de Aplicaciones Web, por sus siglas en inglés "Web Application Firewall".  |
| <b>Reglamento</b>         | Reglamento de Elecciones Vigente del Instituto Nacional Electoral.  |
| <b>Riesgo Aceptado</b>    | Asumir el riesgo siempre con justificación.   |
| <b>Riesgo Mitigado</b>    | Atenuar el riesgo con nuevos procedimientos o acciones.   |
| <b>Riesgo Transferido</b> | Transferir el riesgo y sus implicaciones a un tercero.  |
|                           | Cualquier ente tangible o intangible que tiene valor para el INSTITUTO y para el Tercero Auxiliar del PREP y que requiere protección. Existen diversos tipos de activos, incluyendo:  |
|                           | <b>Activos tangibles</b>  |
|                           | <ul style="list-style-type: none"> <li>I. Activos de información: Bases de datos y archivos de datos, hojas electrónicas con datos, contratos y acuerdos, documentación del sistema, archivos de usuarios, información de configuraciones, manual de usuario, formatos digitales de identificaciones, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad, acuerdos para contingencias, rastros de auditoría e información archivada.</li> <li>II. Activos digitales: Balanceadores, servidores de aplicaciones, base de datos, firewalls, respaldos de S3, Aplicaciones para actualizaciones.</li> <li>III. Activos de software: Software de aplicación, software del sistema, herramientas de desarrollo.</li> <li>IV. Activos físicos: Lugares operativos PREP CATDS y CCVS, llaves de acceso, gafetes de identificación, uniformes del personal, flotilla vehicular, mobiliario, plantas de luz, pantallas de publicación, sistema de videocámaras.</li> <li>V. Activos informáticos: Servidores en nube, equipo de cómputo, equipo de comunicación y medios removibles.</li> <li>VI. Personas: Personal directivo, técnico y operativo del PREP con competencias específicas, habilidades, experiencia y roles que desempeñan.</li> </ul> |
| <b>Activo</b>             |   |
|                           | <b>Activos intangibles</b>  |
|                           | <ul style="list-style-type: none"> <li>I. Servicios: Servicios de acompañamiento y asesorías en tecnologías de la información, cómputo y comunicaciones, servicios generales; por ejemplo, calefacción, iluminación, energía y aire acondicionado.</li> <li>II. Intangibles: tales como la reputación, percepción de transparencia, la imagen del INSTITUTO, confianza de la ciudadanía en el PREP y claridad, certeza y continuidad de la información.</li> </ul>  |




# 1. Normatividad Aplicable

Este documento fue elaborado por la Instancia Interna del IEE en conjunto con la empresa Grupo PROISI S.A. de C.V. encargada de auxiliar en el diseño implementación y operación del Programa de Resultados Electorales Preliminares (PREP), de conformidad con lo establecido numeral 13, fracción IV, del Anexo 13 del Reglamento de Elecciones (RE), en el que menciona:

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

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

Conforme a lo establecido por el artículo 348, numeral 1 del Reglamento de Elecciones menciona lo siguiente:

*“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”.*

En el Anexo 13, Título II, Capítulo IV del RE, señala en el numeral 12 los puntos que deben tomarse en cuenta al momento de implementar los controles de seguridad en los distintos procedimientos del PREP, los cuales son:

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

- I. **Factores de riesgo:** establecer e identificar el conjunto de medidas específicas para evaluar los riesgos con base en su impacto y la probabilidad de ocurrencia;*
- II. **Activos críticos:** identificar cuáles son los recursos humanos y materiales, servicios e información (en sus diferentes formatos) de valor para los procedimientos del PREP;*
- III. **Identificación, evaluación y gestión de riesgos:** deberá identificarse y describirse la situación o condición –técnica, legal, económica, política, social, entre otros – que pueda afectar los procedimientos del PREP; posteriormente, deberá describirse claramente cuáles son los impactos que se pueden tener en el caso que una amenaza se materialice; finalmente, se deberá definir y documentar la respuesta respecto de*



*cada uno de los riesgos identificados, precisando si los riesgos serán aceptados, mitigados, transferidos o eliminados; y*

- IV. **Plan de seguridad:** *se deberá elaborar un plan de seguridad basado en los resultados de un análisis de riesgos, que permita llevar a cabo la implementación de controles en los distintos procedimientos de operación del PREP, así como en la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP. Dicho plan deberá ser elaborado por la instancia interna y, en su caso, en coordinación con el tercero que auxilie en la implementación y operación del PREP."*

De igual manera en el numeral 13 de dicho capítulo antes referido, se determina la elaboración de un Plan de Continuidad tal y como se muestra:

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

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

## 2. Presentación

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 IEE.

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 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 el IEE bajo su responsabilidad, en cuanto a su implementación y operación, esto con base en el artículo 348, numeral 1 del Reglamento de Elecciones del Instituto Nacional Electoral 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, en las tecnologías y/o servicios relacionados a la información o comunicación utilizadas durante el PREP.

En este sentido, es importante destacar como antecedente que la Seguridad Informática es la rama de las Ciencias de la Computación cuyos objetivos principales son:

- a) Protección de la información de robos o de acceso no autorizado,
- b) Prevención de corrupción de la información existente durante su comunicación a través de redes de datos, o directamente en los medios de almacenamiento electrónicos donde ésta se encuentra,
- c) Recuperación ante situaciones desastrosas, sean de naturaleza fortuita o malintencionada.

Todo esto conlleva a mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información, mientras se garantiza el acceso a los datos por parte de los usuarios autorizados, y se mantiene la continuidad en las operaciones del sistema.

Con base en esta definición, es importante precisar las políticas, procedimientos y metodologías para asegurar la integridad, disponibilidad y confiabilidad de datos y sistemas; prevenir y detectar amenazas respondiendo de forma adecuada y con prontitud ante un incidente; así como, proteger y mantener los sistemas operando de manera ininterrumpida.

Es importante tener la certeza de las propiedades de la información, mismas que son mantenidas y respetadas en todo momento de la operación del sistema, y que en caso de que se llegara a presentar una brecha de seguridad, la recuperación se logre de manera inmediata con el mínimo de afectación posible.

## 1.1 Propiedades de la información

- **Confidencialidad:** Asegurarse que la información en un sistema de cómputo y la transmitida por un medio de comunicación, sea accedida solo por las personas autorizadas;
- **Autenticación:** Asegurarse que el origen de un mensaje o documento electrónico está correctamente identificado, con la seguridad que la entidad emisora o receptora no ha sido suplantada;
- **Integridad:** Asegurarse que solo el personal autorizado sea capaz de modificar la información o recursos de cómputo;

- **No repudiación:** Asegurarse que ni el emisor o receptor de un mensaje o acción sea capaz de negar cualquier acción realizada;
- **Disponibilidad:** Requiere que los recursos de un sistema de cómputo, comunicación y almacenamiento estén disponibles en el momento que se necesiten.

## 1.2 Tipos de ataques que pueden presentarse

- **Interrupción:** Ataque contra la Disponibilidad en el cual el mensaje no puede llegar a su destino, un recurso del sistema es obstruido o temporalmente inutilizado;
- **Intercepción:** Ataque contra la Confidencialidad en el que una persona, computadora o programa sin autorización logra el acceso a un recurso controlado;
- **Modificación:** Ataque contra la Integridad donde una persona sin autorización, además de lograr el acceso, modifica el mensaje antes de que sea entregado al destinatario;
- **Fabricación:** Es un ataque contra la Autenticidad donde una persona sin autorización inserta datos en un sistema.

En este orden de ideas, es necesario el establecimiento de reglas claras de funcionamiento, procedimientos precisos y fácilmente comprensibles, de manera que estos puedan ser aplicados por todo el personal que intervenga en la operación del PREP.

## 3. Objetivos y Alcance

---

### 3.1 Objetivos Generales

Establecer una estrategia para salvaguardar la integridad, disponibilidad y confidencialidad de la Información así como la continuidad de la operación del PREP; identificando los riesgos de seguridad de la información en las diferentes etapas del Programa; en cuanto a procedimientos, Servicios e infraestructura en tecnologías de la información y comunicación, recursos humanos y seguridad física, para así establecer los controles de seguridad apropiados que permitan reducir el riesgo a un nivel tal, que asegure la confiabilidad y continuidad de los sistemas, activos tecnológicos y servicios informáticos.

### 3.2 Objetivos Particulares

- a) Elaborar las directrices de seguridad de la información para el PREP.
- b) Realizar el análisis de riesgos permitiendo identificar las vulnerabilidades de seguridad que enfrenta el PREP.
- c) Identificar e implementar los controles de seguridad en los distintos procesos de operación del PREP y en la infraestructura tecnológica.
- d) Implantar soluciones de seguridad perimetral con la finalidad de controlar y vigilar el tráfico de la red de datos que soporta al PREP.



- e) Fortalecer el desarrollo de las aplicaciones que deriven en el cumplimiento de los distintos procesos de operación del PREP.
- f) Establecer el plan de concientización para capacitar y transmitir el sentido de la seguridad de la información del PREP.
- g) Definir el esquema de control de acceso a los diferentes sistemas del PREP.
- h) Establecer el Plan de Continuidad para minimizar el impacto a la operación, así como el plan de recuperación de pérdidas de activos de información.
- i) Elaborar los documentos necesarios para favorecer la evaluación del ente auditor designado por el IEE.

### 3.3 Alcance

Este plan implementará los controles de seguridad que atenderán los procesos de operación del PREP, tales como son Acopio, Digitalización, Captura, Verificación, Publicación y Empaquetado de las Actas, con fundamento en el anexo 13 del Reglamento de Elecciones del Instituto Nacional Electoral, así como, con los Acuerdos que emita el Consejo General del IEE.

El artículo 347, numeral 1 del Reglamento de Elecciones, establece que el Instituto y los OPL deberán someter su sistema informático a una auditoría técnica de verificación y análisis, para lo cual se deberá designar un ente auditor. El alcance de la auditoría deberá cubrir, como mínimo, los puntos siguientes:

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

El artículo 348, numeral 1, del Reglamento de Elecciones, dispone que, 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.

El numeral 12 del Anexo 13 del Reglamento de Elecciones que contiene los Lineamientos del PREP, señala que 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:** Deberán 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 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.

El numeral 13 de los lineamientos del PREP, establece que 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 será comunicado al personal directivo, técnico y operativo del Programa, y será de observancia para todos los involucrados en su ejecución y formará parte de los ejercicios y simulacros.

Todas las medidas y acciones a tomar serán de carácter obligatorio para todo el personal que trabaja en la operación de PREP y se les dará a conocer en las sesiones de capacitación y sensibilización.

## 4. Desarrollo del Plan de Continuidad

---

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.

### Respuesta a incidentes.

Se utiliza un procedimiento para dar respuesta a los incidentes que se presenten en las revisiones al sistema por parte del IEE, del COTAPREP y del ente auditor, dando seguimiento correspondiente a cada uno de ellos.

Se proporcionará el procedimiento para que la instancia interna encargada en la supervisión del PREP del IEE pueda reportar los incidentes que se presenten durante las revisiones que realice el Ente Auditor designado por el IEE conforme a su plan de trabajo. El procedimiento se remitirá por correo electrónico, a la cuenta que se establezca para el efecto.

Se incluirá, por lo menos, los niveles de servicio, cuentas de correo, números telefónicos locales, nombres de contactos, y procedimientos para distribuir los reportes en cuestión, así como los medios de contacto para los reportes que provengan de PREP casilla.

Los tiempos de respuesta para la atención de incidentes es el siguiente:

**a) Tiempos de atención en períodos normales**

Los días y horarios de atención serán de lunes a viernes de 09:00 a 21:00 horas y los sábados y domingos de 10:00 a 18:00 horas.

**b) Tiempo de atención en periodos críticos**

**I. Durante las pruebas de funcionalidad**

Se procesará la cantidad de actas que permita verificar los distintos flujos del funcionamiento integral del sistema informático del PREP, si como resultado de la prueba no fuera posible verificar el correcto funcionamiento del sistema, se deberán ejecutar las pruebas necesarias hasta cumplir con el objetivo de estas. Se atenderán todas las características aplicables al Anexo 13 del Reglamento de Elecciones.

**II. Durante la realización de ejercicios**

Se realizarán ejercicios previos al primer, segundo y tercer simulacro, se realizarán cumpliendo todas las fases del Proceso Técnico Operativo y su anexo técnico, durante un horario de atención de 8:00 a 20:00 horas, o en su defecto hasta que se termine la actividad.

**III. Durante la realización de los simulacros**

Conforme a lo establecido en el artículo 349, numeral 3 del Reglamento de Elecciones, se realizarán como mínimo tres simulacros oficiales previos a la Jornada Electoral, durante este periodo se cubrirá un horario de atención de 24 horas que contarán a partir del inicio del simulacro. Dentro de los simulacros se realizará al menos un simulacro de tipo Failover, ya que esta medida permitirá optimizar el tiempo de recuperación y reducir el impacto en la operación general del PREP ante un fallo de esta naturaleza, así como acordar con proveedores de los servicios que se contratan (telefonía, internet, energía eléctrica, etc.) se cuente con la presencia de personal de soporte para resolver eventualidades.

**IV. Durante la operación del PREP**

Se operará el Programa a partir de las 20:00 hrs del Día de la Jornada Electoral y hasta las 20:00 hrs del día siguiente, o bien antes, en caso de que se logre el 100% del registro de las actas PREP esperadas y/o se hayan agotado los recursos de recuperación de las mismas.

**c) Descripción de los niveles de servicio atribuibles a errores o fallas del Sistema:**

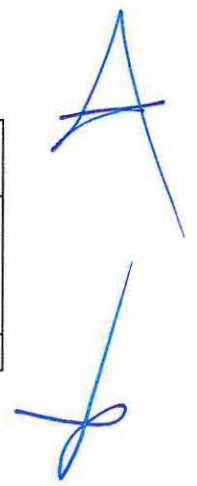
- **Nivel Alto:** Cuando no se pueda operar el Sistema ni la Aplicación móvil.
- **Nivel Medio:** Cuando se presente una falla que afecte la funcionalidad del Sistema o Aplicación móvil.
- **Nivel Bajo:** Cuando se presente una falla que no impide operar el Sistema o la Aplicación móvil, pero impide su administración.

TABLA 1 ATENCIÓN A FALLOS

|             | PERÍODO DE ATENCIÓN ANTE FALLAS DEL SISTEMA Y/O APLICACIÓN MÓVIL   |   |  |   |
|-------------|--|---|--|---|
|             | Período normal   |   | Período crítico  |   |
|             | Desde la solicitud hasta la generación del reporte (ya sea que la solicitud se reciba por Internet, teléfono o correo) | Desde la generación del reporte (ya sea por Internet, teléfono o correo) hasta la resolución de la incidencia | Desde la solicitud hasta la generación del reporte (ya sea que la solicitud se reciba por Internet, teléfono o correo) | Desde la generación del reporte (ya sea por Internet, teléfono o correo) hasta la resolución de la incidencia |
| Nivel alto  | 15 min   | 60 min  | 10 min   | 30 min  |
| Nivel medio | 15 min   | 3 horas   | 10 min   | 60 min  |
| Nivel bajo  | 15 min   | 8 horas   | 10 min   | 90 min  |

TABLA 2 ENTREGA DE INFORMACIÓN

| De la generación y entrega de información relativa al Sistema o cualquier otra información prevista en el contrato |  |  |
|--|--|--|
| Período normal   | Desde la solicitud hasta la generación del reporte (ya sea que la solicitud se reciba por Internet, teléfono o correo) | Desde la generación del reporte hasta la entrega de la información |
|  | 2 horas  | 10 días naturales  |



## 5. Recursos humanos

---

En este rubro se encuentra el personal involucrado de la empresa Grupo PROISI S.A. de C.V. en las distintas actividades relacionadas con el PREP en los centros de operación que se instalarán.

### PERSONAL DIRECTIVO

#### Coordinador General del PREP

- Coadyuvar con el IEE para la implementación completa del programa.
- Coordinar las actividades de planeación y ejecución del proyecto.
- Coordinar las actividades de definición de los aspectos tecnológicos y logísticos.
- Ser el vínculo con el personal del Organismo y los miembros del COTAPREP para informar respecto a los avances y atender sugerencias.

#### Dirección de operaciones

- Coordinar los procesos para la adquisición de equipos de procesamiento, almacenamiento y comunicaciones, así como la contratación de diversos servicios asociados.
- Coordinar las actividades vinculadas con la instalación y configuración de la infraestructura informática y de soporte (suministro eléctrico y aire acondicionado) del CCV y los CATD.
- Coordinar las actividades de instalación y configuración de la infraestructura informática y de proyección de la Sala de Consejo.
- Coordinar las actividades de acondicionamiento y equipamiento del CCV, CATD y Sala de Difusión.

#### Dirección general de desarrollo de software

- Administrar el desarrollo de los aplicativos
- Realizar el levantamiento e integración de los requerimientos para la definición del PREP.
- Coordinar el desarrollo de los diversos módulos e interfaces que integran el Programa.
- Rediseñar los procesos operativos y casos de uso.
- Codificar los cambios y nuevos módulos de los subsistemas.
- Liberar los aplicativos.
- Desarrollar pruebas de calidad.
- Coordinar la estrategia de seguridad en materia informática.
- Definir los requerimientos necesarios para difusores externos y coordinación de las actividades necesarias para su conexión.
- Administrar, monitorear y dar asistencia técnica referente a la infraestructura informática y soporte del CCV y los CATD.
- Coordinar los planes de continuidad de la operación del PREP (en caso necesario)
- Monitorear la operación de los difusores externos
- Participar en la ejecución de los Simulacros.



- Ejecutar los procedimientos de arranque en el CCV.
- Monitorear los diversos aplicativos y operación de difusores.

### **Coordinación de Vinculación y difusión**

- Definir la estrategia de comunicación del Programa
- Coordinar la logística de interacción con los medios de comunicación.
- Generar informes y comunicados respecto a los avances y operación del PREP.

### **Coordinación Administrativa**

- Gestionar los procedimientos administrativos para la adquisición de bienes y la contratación de servicios, así como para la contratación de personal.
- Administrar el presupuesto del Programa.
- Llevar el control de resguardo de los bienes adquiridos.
- Coordinar las actividades de contratación de personal a nivel estatal.

### **Planeación y Administración de Proyecto**

- Coordinar las actividades de integración y definición de proyecto.
- Dar seguimiento a los avances.
- Integrar informes.
- Elaborar e integrar información administrativa y operativa.

## **PERSONAL TÉCNICO**

### **Coordinador o coordinadora del CCV**

- Da seguimiento a las tareas necesarias para la instalación, adecuación y operación del CCV; en lo que se refiere a: personal, equipo, materiales, capacitación y realización de pruebas, ejercicios y simulacros
- Atiende y pone en práctica cada requerimiento e instrucción que reciba de la Instancia Interna encargada de coordinar el desarrollo de las actividades del PREP y es el vínculo con las oficinas de esta.
- Mantiene en todo momento informada a la Instancia Interna encargada de coordinar el desarrollo de las actividades del PREP, sobre los avances de instalación, habilitación y operación del CCV.
- Realiza un informe final de los avances de instalación, habilitación y operación del CCV, de la ejecución de los simulacros, así como de lo acontecido durante la operación del PREP, y
- Toma decisiones en el ámbito de operación del CCV

### **Coordinador o coordinadora de CATD.**

- Da seguimiento a las tareas necesarias para la instalación, adecuación y operación del CATD; en lo que se refiere a: personal, equipo, materiales, capacitación y realización de pruebas, ejercicios y simulacros



- Atiende y pone en práctica cada requerimiento e instrucción que reciba de la Instancia Interna encargada de coordinar el desarrollo de las actividades del PREP y es el vínculo con las oficinas de esta.
- Mantiene en todo momento informada a la Instancia Interna encargada de coordinar el desarrollo de las actividades del PREP, sobre los avances de instalación, habilitación y operación del CATD.
- Realiza un informe final de los avances de instalación, habilitación y operación de los CATD, de la ejecución de los simulacros, así como de lo acontecido durante la operación del PREP, y
- Toma decisiones en el ámbito de operación del CATD

### **Supervisor de CCV**

- Supervisa al personal adscrito al CATD o, en su caso CCV;
- Controla la distribución de las cargas de trabajo durante la operación del PREP;
- Ejecuta las acciones necesarias para asegurar la continuidad de la operación del CATD o, en su caso CCV;
- Apoya a la o el coordinador en el desarrollo de otras actividades, como la evaluación de los procesos, procedimientos y actividades a su cargo;
- Verifica el correcto funcionamiento de los equipos del CATD o, en su caso CCV;
- Supervisa la capacitación al personal operativo;
- Vigila la seguridad del personal, del equipo de cómputo, de los materiales y de la información, y
- En ausencia de la o el coordinador, le suplirá en sus funciones.

La siguiente lista corresponde al personal operativo, con el que se contará para la operación del PREP 2025, cuyas funciones están descritas dentro del Proceso Técnico Operativo

### **Personal Operativo**

- Capturistas/ Verificadores
- Acopiadores / Digitalizadores

## **6. Implementación del plan de tratamiento de Riesgos**

---

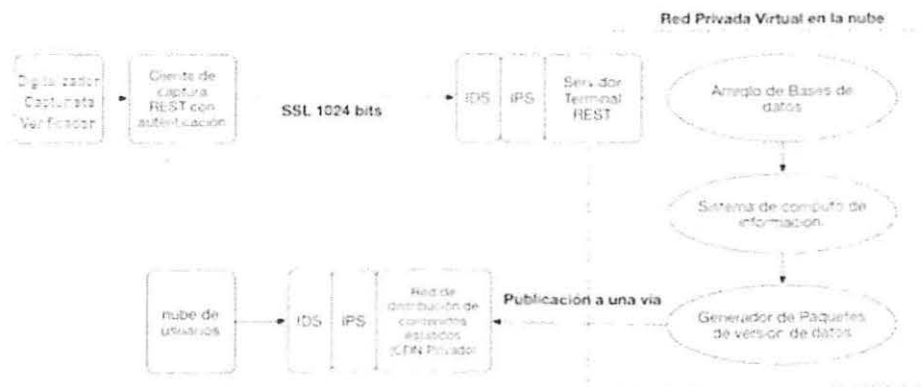
Con base en los riesgos identificados, se implementan los siguientes procedimientos:

### **PROCEDIMIENTO 1**

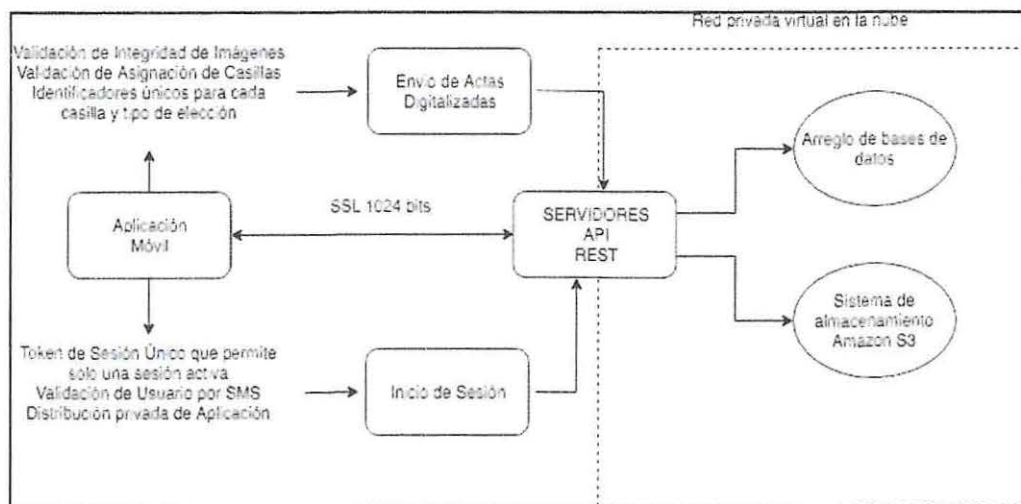
#### **Tratamiento del riesgo en el control de acceso a las aplicaciones:**

Todas las aplicaciones operativas cuentan con autenticación doble factor mediante SMS para que los usuarios establezcan conexiones confiables, permitiendo que la información que se transfiera desde las aplicaciones de captura hacia la central, viaje de manera segura.

### Seguridad en aplicaciones



### Seguridad en aplicación Móvil



## PROCEDIMIENTO 2

### Tratamiento del riesgo por Virus informático o código malicioso:

Los equipos de computación de escritorio que intervienen en los procesos deberán contar con un paquete de antivirus instalado, cuyas bases de datos de firmas deberán garantizarse permanentemente actualizadas. Asimismo, los equipos móviles deberán contar con un sistema de bloqueo para evitar descarga de aplicaciones, es decir, que únicamente sea para el uso exclusivo de la aplicación denominada PREP PUEBLA.

Adicionalmente se mencionan algunas acciones para prevenir que llegara a ocurrir una infección por algún código malicioso a nivel de usuario:

- a) No abrir archivos adjuntos en correos electrónicos de procedencia extraña.
- b) Analizar los archivos con el antivirus instalado antes de abrirlos.
- c) Analizar medios extraíbles.
- d) Actualizar el sistema operativo y antivirus constantemente.
- e) No descargar software de la red.
- f) No hacer uso de programas de redes sociales.

### **PROCEDIMIENTO 3**

#### **Tratamiento del riesgo en la ausencia de controles criptográficos**

- a) Todos los equipos de captura, aplicaciones y sitios web deberán contar con contraseña de acceso, mismas que deben ser otorgadas de manera confidencial al personal correspondiente de forma personal y presencial en sobre cerrado, y estas 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.
- b) Respecto a la seguridad en la transferencia de los datos, el sistema incluye la encriptación de la información (SSL/ TSL v 1.3 1024 bits), el uso de token secreto (contraseña interna del sistema), claves de usuario y doble autenticación.
- c) Referente a la seguridad en la digitalización del acta PREP, el sistema genera un código HASH utilizando sha256 para cada imagen, con la finalidad de asegurar que esta 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. Contando con 3 métodos o técnicas para bloquear intrusos, que tienen que ver con el cambio y patrón de comportamiento de las conexiones:

- a) Control por número de peticiones. Se utilizarán parámetros limitados de conexiones por IP que se pueden conectar al servicio, un escudo o PROXY que analizará 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 en el sitio, si llegara a manifestar insistencia de esa misma IP, entonces el bloqueo será definitivo, puesto que es indicativo de un comportamiento anormal. Se reportará al administrador del sistema.
- b) Utilización de ancho de banda. El ancho de banda empleado para las conexiones tiene un límite, si alguien manda una petición más allá del límite y excede por mucho el ancho

de banda ocurre un "Overflow" o sobresaturación de la infraestructura de conectividad, si llegara a ocurrir, sería un intento de ataque al sistema. Se procede del mismo modo, 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.

- c) Validación de "headers". Esto es validación mediante un "token" que genera el validador en el IDS, un "header" especial que genera el controlador, para cuando se realice la conexión a través del túnel de SSL, se evalúa y determina si existe ese token y se acepta la conexión, si alguien realiza un ataque masivo en cualquier lenguaje, no se generará este "token" y será una conexión no válida. Se bloqueará y se reportará al administrador del sistema.

## PROCEDIMIENTO 5

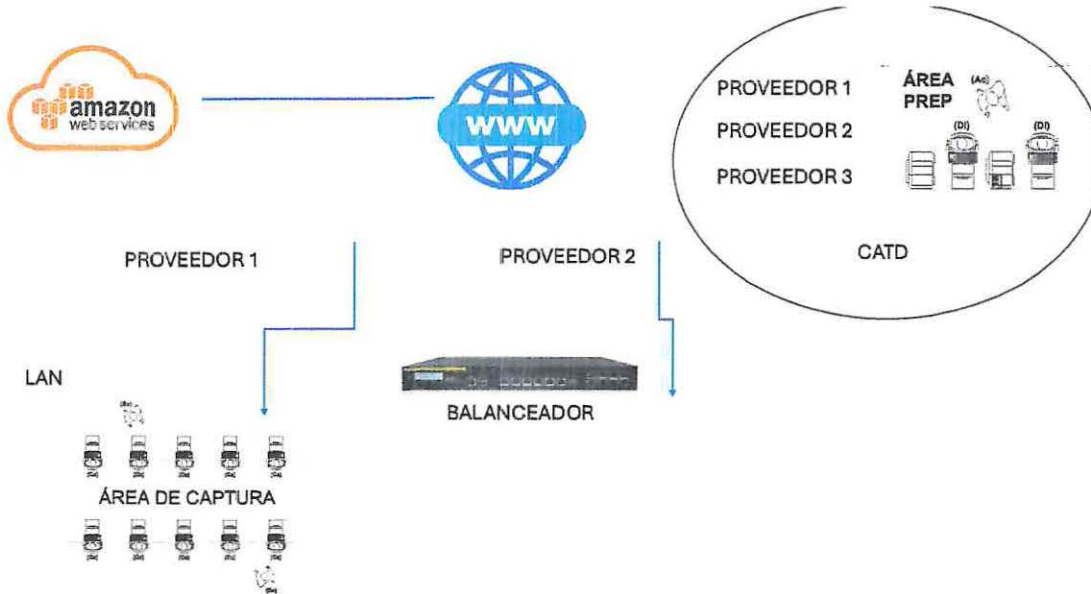
### Tratamiento del riesgo en la infraestructura de la red:

- a) 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.
- b) Los servicios alojados en los servidores de la empresa Amazon Web Services asegura un porcentaje de Tiempo de Actividad Mensual de al menos 99.99%, por lo que la tolerancia a fallas es mínima.

El DNS funciona 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, se cuenta con 5 servidores, en los cuales se establece 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 y en los servicios de datos:



### Para el CCV

En el CCV se contará con tres enlaces de internet de proveedores distintos conectados a un balanceador el cual distribuye el ancho de banda efectivo a cada una de las estaciones de trabajo de los capturistas, en caso de falla de uno de los enlaces de internet, el equipo balanceador asigna el ancho de banda del enlace del proveedor activo a la totalidad de las estaciones de trabajo. Una vez que el enlace que pudiese haber fallado se restablece, el balanceador normaliza la operación distribuyendo la carga de los dos enlaces a internet hacia todas las estaciones de trabajo.

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

Si en el CCV central existiera alguna contingencia, la captura de información de las Actas PREP no se suspende, ya que los servicios están en la nube, de tal manera que la ejecución del PREP no se detiene pues existen capturistas/verificadores que continuarán sus tareas. Adicional a ello, si el problema se prolongara por más de 30 minutos, el personal que labora en los CCV está capacitado para realizar todas las actividades del PTO por lo que realizando un balance en las cargas de trabajo.

## Para los CATD

En los CATD se tiene un enlace principal y uno secundario de servicios de datos, en caso de falla del enlace principal, el Coordinador del CATD deberá realizar la interconexión del enlace secundario, ya sea de proveedor fijo o de datos móviles para proporcionar conectividad temporal para el envío de las actas al CCV. Una vez que se normalice el enlace principal el Coordinador del CATD realizará la conexión nuevamente del equipo. En cada uno de los CATD se deberá privilegiar el enlace que otorgue las mejores prestaciones para la conexión, por lo que se podrá dar el supuesto que, en caso de contingencia, se cambia del servicio de datos al enlace principal (fijo).

## Para PREP Casilla

En caso de perder conectividad en las aplicaciones PREP Casilla, tanto en los dispositivos de los CAE como en los de los CATD, el sistema deberá estar preparado para continuar trabajando fuera de línea (offline), que asegure 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

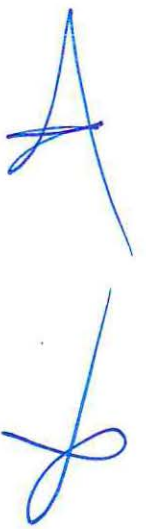
Cada equipo de cómputo instalado en los CCV debe contar con UPS con capacidad de suministrar de energía al menos por 20 minutos, para el caso de que el corte de energía se prolongue en los CCV. Se deberá contar con una planta eléctrica de gasolina o diésel con las características y capacidad suficiente para que los equipos y dispositivos conectados, que forman parte del CCV continúen en operación, quedando a visto bueno de la Instancia Interna y de la opinión técnica de Comisión Federal de Electricidad, el modelo a utilizar que se encuentre interconectada a un switch de doble tiro para su activación en caso de que se prolongue el corte de energía.

### **Falla en la red eléctrica de los CATD:**

En cada uno de los equipos se debe contar con una unidad de corriente ininterrumpida (UPS) con capacidad de 20 minutos para evitar pérdida de información debido a problemas de suministro eléctrico.

En cada Consejo Municipal Electoral con CATD se contará con una planta de energía eléctrica portátil a gasolina que estará previamente preparada para que los equipos del CATD se conecten y continúen con el trabajo asignado.

Si la planta de luz no funcionara de manera correcta, el digitalizador podrá continuar con los trabajos mediante el aplicativo PREP Casilla que estará dispuesto en el lugar, instalado en un teléfono celular de la empresa con datos de internet y disponible para casos de emergencia y contará con la asignación previa de las casillas que se deban recibir en cada Consejo Municipal Electoral.



Como una medida extrema, si el suministro de energía eléctrica se ve interrumpido por causas externas al CATD de forma permanente o en caso de la imposibilidad de continuar con la digitalización porque la planta no funcionará de manera correcta o el celular PREP Casilla no pudiera enviar las Actas correspondientes, se deberá implementar el mecanismo para el traslado de actas al centro más cercano.

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

1. La Coordinación del CATD, informará la situación inmediatamente al coordinador del CCV, así como, a la Presidencia del Consejo Municipal Electoral del que se trate, quienes a su vez informarán a la Instancia Interna Encargada de la Implementación y Operación del PREP, 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 Comisión Especial para dar Seguimiento a la Implementación y Operación del Programa de Resultados Electorales Preliminares (PREP), 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 Municipal Electoral para que brinde las facilidades necesarias al personal del PREP, e informe al pleno de dicho Consejo.
5. Asimismo, la Instancia Interna notificará la decisión a la coordinación del CATD, 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 mismo. En dicha comunicación se indicará también, a cuál de los Consejos se deberán trasladar las Actas PREP.
6. La coordinación del CATD determinará el número de actas esperadas faltantes por digitalizar, y una vez recibido el 100% de las mismas, se realizará el 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 realizará procedimiento tal, que evite toda posibilidad de abrir el sobre durante su traslado; dicho procedimiento será como sigue: se designará a dos figuras de entre su personal que realizarán el traslado, se pegará una etiqueta donde se abrirá el sobre, después de realizar el sellado, se rubricará con las firmas de las y los presentes (entre las que deben estar, la presidencia del Consejo, titular de la vocalía de capacitación electoral, alguna consejería electoral, la coordinación del CATD, en su caso, representaciones de los partidos políticos), se procederá a sellar mediante cinta transparente autoadherible con al menos tres vueltas, asegurando el perfecto sellado y finalmente tomando fotografía con dispositivo celular inteligente, enviando la imagen por alguna red social, al supervisor del CCV central en ;
9. 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 o candidaturas independientes, sin embargo, se permitirá que en vehículo aparte sigan el traslado.

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

- a) El personal de traslado entregará a la Coordinación del Centro Sede 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 por la Coordinación del Centro Sede y asegurando que el sobre contenga los sellos, firmas y después de evaluar cuidadosamente que permanezca la cinta y se compruebe que el proceso de sellado no fue violentado, se procederá a abrir el sobre haciendo constancia de las condiciones en las que fue recibido y contar el número de Actas PREP, las cuales deberán coincidir con el número de Actas especificadas en la etiqueta de identificación.

Hecho lo anterior, la Coordinación del Centro Sede procederá a distribuir las Actas PREP del CATD huésped al personal de digitalización.

El personal designado para la digitalización de las Actas PREP del CATD huésped o la sede correspondiente, una vez terminada la actividad procederán a meter al sobre donde llegaron las actas y la Coordinación del centro sede, sellará el sobre y le pegará una etiqueta de identificación que contendrá los siguientes datos:

- Nombre completo y firma de quien coordina el Centro sede.
- Número de Actas PREP.

Una vez terminada la digitalización, recibirán por parte de la Coordinación del Centro sede, el total de Actas PREP.

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.

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

### **Fallas en la red eléctrica de los CCV**

En cada uno de los equipos se cuenta con unidad de corriente ininterrumpida durante 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 de los CCV), en caso de falla permanente, los trabajos de este centro podrán continuar en el CCV alterno.

En caso de falla permanente de red eléctrica de los dos CCV se podrá continuar con los trabajos de captura y verificación en alguno o algunos de los CATD instalados, aunque será más tardado por la cantidad de equipos, se podrá continuar con el Programa pues los equipos de cómputo ahí



instalados podrán ser utilizados por personal de captura y verificación con los permisos respectivos.

## PROCEDIMIENTO 8

### Tratamiento del riesgo por falla o ausencia en los equipos de cómputo para la realización de la digitalización

Falla en equipo de cómputo y digitalizadores

- A. En el caso de suscitarse un problema en el funcionamiento de cualquiera de los equipos, el digitalizador o Capturista/Verificador deberá reportarlo a la Coordinación del CATD y/o al del CCV y este a su vez al supervisor del CCV, quién autorizará cambiar el equipo en cuestión, ya que se tiene considerado equipos de respaldo, mínimo uno extra en cada CATD y en el CCV los necesarios para restablecer el 100% de los equipos móviles y de escritorio dispuestos a la operación del PREP. Este mismo proceso, será considerado para la situación de robo de uno o más de estos equipos. En caso de agotar todas las opciones posibles para resolver el problema, se planteará la posibilidad de digitalización mediante el aplicativo PREP Casilla con celulares dispuestos para tal efecto y en caso de no funcionar por alguna situación, se podrá iniciar el mecanismo de traslado descrito en el Procedimiento 7 del presente documento.
  
- B. En caso de violencia y eventos extremos, se priorizará siempre la seguridad del personal, teniendo como indicación resguardar su integridad física, en segundo término, las AEC y por último 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 seguirán las indicaciones del Consejo General del IEE y/o se planteará la posibilidad de iniciar el mecanismo de traslado descrito en el Procedimiento 7 del presente documento.

## PROCEDIMIENTO 9

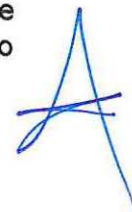
### Tratamiento del riesgo en el personal de los CCV y CATD

En caso de ausencia del personal destinado a la digitalización y/o captura en los CCV y CATD, las coordinaciones de los CCV tienen los horarios de trabajo de cada capturista y digitalizador de imágenes en los CCV; además, cuentan con las instrucciones necesarias en caso de retrasos o contratiempos del mismo personal.

Los perfiles para cada CCV son los siguientes:

- La coordinación del CCV;
- El digitalizador o la digitalizadora; y,
- El o la capturista.

Sin embargo, todos están capacitados para realizar el trabajo de digitalización, captura, verificación, cotejo, en caso de que alguno de ellos tenga un imprevisto, el otro puede realizar la tarea de la persona ausente.



Toda persona contratada para la operación del PREP cuenta con gafete de identificación, uniforme y es escogida 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

## **PROCEDIMIENTO 10**

### **Tratamiento del riesgo en la documentación 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, por lo que la reducción de este riesgo consiste en la implementación y desarrollo del plan de capacitación.

Así como, la distribución manual del usuario PREP, las listas de verificación, registros de personal, son documentos que soportan la operación del PREP.

Lo que corresponde a la documentación del software es de carácter privado, sin embargo, la empresa Grupo PROISI S.A. de C.V. el IEE, compartirá con 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**

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

Se incluyen los siguientes temas dentro de a capacitación del personal operativo:

- 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 a los CCV y CATD**

#### **CCV**

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

- Circuito cerrado de video
- Identificación con gafete oficial con fotografía
- Chapa de seguridad

El cumplimiento de que las medidas de seguridad sean observadas es responsabilidad de la Coordinación del CCV Central.

### **CATD**

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

## **7. Implementación del Plan de Tratamiento de Riesgos**

---

### **Fortalecimiento de las Actividades Operativas**

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

- Inicio y cierre de operaciones en simulacros y el día de la jornada en los CCV y los CATD
- Inventario de equipo en los CATD y CCV's
- Reporte de Incidentes durante el tiempo de captura y transmisión de datos.

### **Registro de datos:**

- Entradas y salidas del personal a los CCV y los CATD.
- Pase de asistencia del personal.
- Hora de inicio de la digitalización, captura, verificación de datos y empaquetado de Actas PREP
- Hora de cierre de captura
- Entrega/Recibo de equipos en los CCV y los CATD.
- Entrega/Recibo de informes de avance y documentación.
- Entrega/Recibo de reportes de datos del día de la jornada.
- Registro y explicación de las AEC no capturadas o de no contabilización de resultados

### **Robustecimiento de los Controles de Seguridad Física y Ambiental.**

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

- a) Seguridad en el edificio que alberga a los CCV y los CATD, por lo que en primer término el acceso a las instalaciones del IEE es controlado por su personal de vigilancia, adicionalmente a ello, los espacios que ocupan los CATD y los CCV se encuentran en espacios cerrados cuyo acceso solo es permitido por las respectivas Coordinaciones.
- b) Sistema de control de acceso a cada uno de los CATD y los 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 del IEE facultado para coadyuvar, operar o supervisar las actividades del PREP.
- c) Controles Ambientales para los recintos con aire acondicionado.
  - d) Registro del personal que accede a los CCV y a los CATD. La coordinación de los CCV o CATD, según corresponda, deberán supervisar que la entrada de cualquier persona al CATD o los CCV quede asentada en una libreta de registro.
  - e) Establecer medidas preventivas de contingencia ambiental como sensores detectores de humo, inundación del sitio, sensores de humedad. Esta actividad dentro de los CCV o CATD.
  - f) Separar adecuadamente los cables de datos de los cables de energía eléctrica en los CATD y los CCV.
  - g) Protección contra interceptación y estática del cableado de los datos y energía eléctrica.
  - h) Almacenamiento adecuado de la información y medios removibles de forma segura.
  - i) Protección para las áreas de carga y descarga en los CCV.

## 8. Control de Accesos y Políticas de Seguridad

El acceso a los recursos del PREP PUEBLA 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.

### **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 a los CCV y a los CATD, se cuenta con identificación fotográfica mediante gafete de presentación y registro manual de las entradas y salidas.

## 9. Definición de esquema de trabajo a seguir para el control de acceso al aplicativo central, a la aplicación móvil, a la base de datos, servidores y demás infraestructura que den soporte al PREP.

---

El esquema para seguir para el control de acceso a las aplicaciones es el siguiente:

### Para la aplicación PREP casilla

- Se registrarán en la base de datos de la aplicación los usuarios, con la información correspondiente a nombre, número de teléfono asignado y permisos.
- Se proporcionará el equipo móvil a los CAEs con la aplicación instalada y configuraciones de seguridad establecidas.
- Todo usuario registrado podrá tener acceso a la aplicación iniciando sesión con su número de teléfono y un mensaje de texto SMS con el código de activación que recibirá al autenticar con su número.

### Para la digitalización, captura y verificación

- Se tendrá registro de datos personales de cada usuario de las aplicaciones, sus teléfonos celulares a los cuales les llegará la doble autenticación por SMS, mismos que debieron haber pasado los filtros de selección requeridos para su contratación.
- Cada usuario recibirá su estación de trabajo configurada por el equipo de soporte técnico.
- Cada usuario contará con su propia contraseña las cuales serán proporcionadas por la coordinación.

### Desarrolladores y administradores de aplicaciones

- El equipo de TI que requiera realizar conexiones a base de datos y servidores, mismas que se realizarán mediante conexiones VPN cifradas con Ipsec u Open SSL.

Implementación de los controles necesarios para fortalecer el acceso de las y los usuarios al aplicativo central y a la aplicación móvil.

Los controles de acceso a implementar para fortalecer el acceso de los usuarios a las aplicaciones son los siguientes:

- Contraseñas robustas
- Contraseñas a nivel sistema operativo de los equipos
- Usuarios y contraseñas en las aplicaciones
- Cambios frecuentes de contraseñas para los accesos a las aplicaciones
- Cifrado SSL en las conexiones.
- Así como implementación de controles físicos como es el uso de casacas con el logo del IEE e identificación con gafete que los empleados deben tener visible en todo momento



## **Implementación de los controles necesarios para fortalecer el acceso de las y los usuarios a bases de datos, servidores, equipos de comunicaciones y equipos de cómputo personal.**

Los controles para implementar y fortalecer la seguridad en el acceso a servidores, base de datos, equipos de comunicaciones y cómputo personal son los siguientes:

- Se implementarán controles necesarios para detectar cualquier actividad sospechosa en el tráfico generado en la red donde se encuentran los equipos, con la instalación de dispositivos para el monitoreo y control de tráfico.
- Los equipos de cómputo tendrán los parches de seguridad instalados y firmas de antivirus actualizadas.
- Se implementarán restricciones por IP para las conexiones realizadas en el periodo de pruebas.
- Se implementarán sistemas de detección y prevención de intrusos en la central donde se encuentran los servidores web, bases de datos, sistema de cómputo y servicios de publicación

## **Emisión de lineamientos para control de acceso lógico.**

Lineamientos para controlar el acceso lógico a las aplicaciones que debe seguir el personal que requiera acceso a la red, recursos y aplicaciones es el siguiente:

- Todo acceso debe ser autorizado por el área correspondiente.
- Cada equipo instalado en los CCV para las actividades de captura y verificación deben estar conectados a la red local.
- El uso de usuarios y contraseñas de los aplicativos es responsabilidad de cada usuario, toda actividad realizada en las aplicaciones quedará registrada con el usuario que la realizó. Esta bitácora deberá tener la característica de que sólo se podrán agregar registros, y no modificar ni eliminar, de manera que no se pueda borrar o modificar el rastro de alguna acción realizada, eliminándose así evidencia que pudiera implicar responsabilidad.
- Las solicitudes de usuarios a aplicaciones serán distribuidas por el área de coordinación, quienes llevarán un registro del personal autorizado para el uso de cada aplicación.
- El acceso o conexión a la red local de equipo de cómputo o dispositivos debe ser autorizado por el administrador de red.

# 10. Plan de Concientización

---

## **Objetivo**

Establecer una estrategia a implementar para el personal que opera el PREP, el cual permita generar una conciencia de grupo donde quede clara la importancia de la información que se va a manejar y las consecuencias que puede tener un mal uso o manejo de ella, definiendo los factores tanto internos como externos que pudiesen representar un riesgo para la integridad, disponibilidad y confidencialidad de esta.

## Alcance

El plan de concientización implementará las herramientas necesarias para la capacitación del personal que operará en todo el proceso del PREP: coordinadores, jefes de equipo, supervisores, acopiadores, digitalizadores, capturistas y verificadores.

## Plan de Trabajo

Se llevará a cabo la capacitación del personal de los CATD y de los CCV, en cuanto al personal que utilizará la aplicación PREP Casilla, las y los Capacitadores- Asistentes Electorales, llevará a cabo su capacitación en forma y fechas que el INE determine. Sin embargo, contemplando los casos Ordinarios, si se contrata nuevo personal, se impartirá de forma personalizada la capacitación al personal de nuevo ingreso, pues se cuenta con una herramienta que permite llevar a cabo videoconferencias, con lo cual en cualquier momento se puede reforzar la capacitación a todo el personal en los CATD o en los CCV. Esta capacitación se llevará a cabo mediante documentos en físico entregados a las figuras operativas, así como, a través de TICs mediante vídeos didácticos, que comprenderán los siguientes aspectos: Las figuras operativas del PREP. Descripción y funciones de cada una.

- Importancia de la seguridad de los sistemas informáticos, principios, ética y políticas de protección a la infraestructura e información.
- Amenazas para la seguridad de la información, diferencia entre amenazas y vulnerabilidades.
- Código malicioso. Métodos, impacto y medidas de prevención.
- Seguridad en el equipo personal, móvil, redes sociales y robo de identidad.
- El sistema de digitalización captura y verificación.

Las capacitaciones se harán en un horario en coordinación con los consejos intentado que el mismo quede comprendido en una franja horaria entre las 9:00h y 16:00h, para que se lleven a cabo en un horario seguro.

En este Plan de Concientización se incluye los simulacros oficiales, debido a que si se presentan áreas de oportunidad se realizarán las mejoras para disminuir los riesgos.

A pesar del esfuerzo en cuanto a la selección para la contratación de personal en las actividades que los CCV y CATD del Programa de Resultados Electorales Preliminares se tiene el enorme reto de capacitar y concientizar acerca de la importancia del PREP para la democracia, transparencia del proceso electoral y estabilidad social, los riesgos y amenazas que puedan presentarse durante la jornada electoral, la necesidad de garantizar la continuidad del programa, la importancia de su presencia y actividad, así como de su compromiso y profesionalismo con las actividades que se le han encomendado.

La capacitación en cuanto a los diferentes requerimientos de seguridad, procesos, sistemas y control que serán primordiales para el desempeño de sus actividades y funciones. Esto implica una capacitación detallada para el entendimiento y comprensión sus actividades designadas; para evitar y disminuir los riesgos se implementa la herramienta de Plan de Concientización, la cual se concentra en los siguientes cuestionamientos que son indispensables para poder operar en la Jornada Electoral:

Cuestionario inicial y final (se procederá a comparar ambos documentos antes y después de la capacitación)

- ¿Sabes qué es el PREP?
- ¿Has trabajado previamente en un CATD o un CCV del PREP?
- ¿Qué fases de desarrollo tiene?
- ¿Sabes qué figuras están presentes en el PREP?
- ¿Qué es para ti la seguridad informática?
- Enlista 5 acciones que consideras que pueden causar problemas a nivel de seguridad informática en el Proceso Electoral.
- ¿Qué se debe hacer en caso de interrupción en el suministro de energía eléctrica durante tus labores?
- ¿Qué harías si se pierde la conectividad cuando estás trabajando?
- ¿Sabes cómo instalar un equipo de cómputo?

Para el final de la capacitación, se volverá a solicitar que rellenen este cuestionario (1-9) y además:

- ¿Cuáles son los pasos en el proceso de acopio de acta PREP?
- ¿Cuáles son los pasos en el proceso de digitalización?
- ¿Cuáles son los pasos en el proceso de captura de los datos del Acta PREP?
- Ante cualquier problema durante los ensayos, simulacros y el día de la jornada, ¿a quién acudirías?

#### **Diseño y contenido de formatos y materiales para la capacitación:**

- Manuales de usuario
- Equipo de Cómputo
- Complementos y accesorios al equipo de cómputo
- Equipo de Escáner
- Teléfono
- Presentación PowerPoint – PDF - Video

**El material de presentación será transmitido por las coordinaciones de los CATD y los CCV.**

Con la presentación del Plan de Concientización que se incluye en el presente plan se espera tener óptimos resultados para la disminución de riesgos y/o amenazas para lograr el objetivo del Programa de Resultados Electorales Preliminares para el Proceso Electoral Local Extraordinario 2025.



## 11. Monitoreo Respuesta a los Incidentes de Seguridad

---

### Requerimientos y planeación del proyecto de monitoreo

Una parte importante para el manejo de incidentes es tener las herramientas necesarias para poder detectarlos, es por eso que se tiene un sistema de monitoreo <https://aws.amazon.com/es/cloudwatch/> para que directamente el encargado del grupo de desarrollo de la empresa o en su ausencia el segundo a bordo tome la responsabilidad de revisar en todo momento los diferentes componentes de la solución tecnológica y de sistemas que va a estar operando para cumplir con el desarrollo del PREP PUEBLA el día de la Jornada Electoral.

Al tener la arquitectura de TI en la nube, se tiene también, previa configuración, de la misma, una plataforma de monitoreo inteligente que permite analizar no solo los datos, sino el performance de las aplicaciones y de la infraestructura, permitiendo tener un tiempo de respuesta rápido ante cualquier contingencia que se presente.

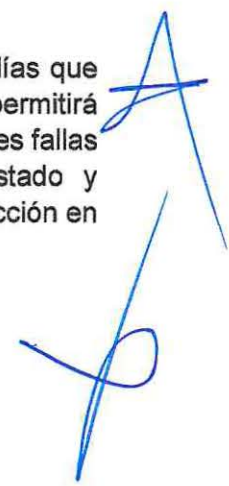
El plan para seguir para la implementación del sistema de monitoreo consta de:

#### A. Realizar análisis de la arquitectura PREP PUEBLA

Los elementos para monitorear son servidor de versiones, conexiones de usuario, generador de versiones, central de recepción de datos y el módulo de auditorías, registrando la actividad en bitácoras y logs para llevar a cabo el seguimiento de las actividades mediante una API de auditoría y la implementación de REST WEBServices para obtener mejor ejecución de los procesos de transmisión y adquisición de datos a través de los métodos nativos el protocolo http.

#### B. Monitoreo y análisis del tráfico de la red

Monitoreo de la infraestructura en la nube utilizando procesos de detección de anomalías que afecten el performance de los servicios mediante la configuración de un sistema que nos permitirá tener una visión clara de la situación que guarda cada componente, alertará sobre posibles fallas o incrementos de carga en los diversos servicios y en general indicarán el estado y comportamiento del tráfico en los servicios de publicación de resultados a fin de tomar acción en caso de requerirlo para garantizar la continuidad del Programa.



**MONITOREO**

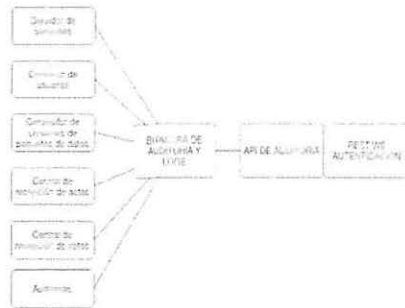


ILUSTRACIÓN 1 DIAGRAMA DE MONITOREO

**C. Instalación y configuración de equipos de monitoreo:**

La instalación y configuración del sistema de monitoreo será realizada por el personal de la empresa GRUPO PROISI S.A. de C.V. siguiendo las siguientes actividades:

- Cubrir los requerimientos del sistema de monitoreo para su instalación en la nube.
- Realizar la instalación del sistema de monitoreo
- Configurar el ambiente o consola de administración, configuraciones iniciales, certificados SSL, alertamientos, etc.

**Configuración de monitoreo para:**

- Transacciones y servicios
- Bases de datos
- Monitoreo de logs
- Tráfico de redes

**D. Pruebas de Funcionalidad:**

Se realizarán pruebas una vez que el sistema de monitoreo esté instalado y configurado para validar su funcionalidad validando que quede cubierto cada módulo especificado en el diagrama de arquitectura.

**E. Monitoreo y generación de reportes o vistas:**

El sistema permite generar vistas de los estados de los módulos que se incluyen en el monitoreo, de forma sencilla, de manera que se puede tener un panorama claro de cada elemento verificando tiempos de respuesta, número de peticiones, problemas o errores, monitoreo de logs, gráficas de desempeño, entre otros.

Se deberá presentar un informe sobre las amenazas presentadas en este documento, especificando si se materializó, porque causa y qué controles se utilizaron, para realizar el seguimiento en

ILUSTRACIÓN 2 MONITOREO

*[Firma manuscrita]*

futuros procesos electorales sobre la efectividad de los procedimientos y controles implementados.



## 12. Recuperación de Desastres

El propósito es garantizar al IEE 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 nivel de gravedad 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 los 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 los 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 CCV 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.

- g) En los 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 de los CCV, habilitará el internet de respaldo (FailOver), con ayuda del personal realizará las conexiones necesarias para ello.
- h) Si en los CATD y, en su caso en los 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 al supervisor del CCV de la situación y se procederá a abandonar el edificio.
- i) Si existiera una falla extrema en el equipo Móvil o que las condiciones de comunicación colapsen en su totalidad, la Coordinación del CATD deberá comunicarse vía telefónica con el Supervisor del CCV, para tener conocimiento de la situación e inmediatamente comenzar a implementar alguno de los procedimientos establecidos para solucionar la situación.
- j) En caso de que se suspenda, se limite o se entorpezca la entrega de actas en los CATD, su Coordinación, hará del conocimiento al coordinador del CCV, a fin de que se informe a la Comisión Especial para dar Seguimiento a la Implementación y Operación del Programa de Resultados Electorales Preliminares (PREP) del EE respecto a esta situación y se tomen las medidas apropiadas.
- k) 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 contingencia, la captura y verificación se realiza en ambos, por otra parte si algunos de los CATD dejara de operar por cuestiones ajenas (toma de las instalaciones o desastre natural), se activaría el mecanismo de traslado hacia la sede PREP más cercano para continuar con la digitalización de las Actas de Escrutinio y Cómputo del PREP que estuvieran pendientes, conforme a lo establecido en el Procedimiento 7 de este Plan de Continuidad. Durante los simulacros establecidos en las fechas 2, 9 y 16 de marzo, se realizará la aplicación del presente plan de continuidad, con la finalidad de probar estos procedimientos. La auditoría deberá ejecutarse sobre todos los módulos del sistema informático previo al inicio de simulacros. Si de las pruebas y simulacros resultará necesario realizar ajustes al sistema, esto deberá hacerse del conocimiento del ente auditor para contar con un margen de tiempo que permita aplicar las medidas que resulten necesarias y se garantice que el sistema auditado sea el que se opere para el PREP.

## 13. Plan de Comunicación

Durante la Jornada del Proceso Electoral el Personal de los CATD y los CCV cuando ocurra algún incidente los canales de comunicación para la solución de incidencias deberá estar atendida a través de la siguiente manera:

Para los CATD si se cuenta con una incidencia por parte de los Acopiadores, Digitalizadores, se debe acudir directamente con su Coordinador del CATD.

En caso de que el Coordinador del CATD no tenga manera de solventar la incidencia, se deberá informar al Supervisor del CCV para su resolución. A su vez el Supervisor en caso de no poder dar solución a la incidencia, deberá reportar a la Instancia Interna del IEE para su atención.

Para los CCV si se cuenta con una incidencia por parte de los Capturista y Verificadores, se debe acudir directamente con el coordinador del CCV.

En caso de que el Coordinador del CCV no esté en posibilidades de solventar la incidencia, deberá ser atendida la incidencia por el supervisor del CCV.

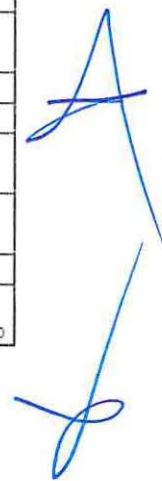
Finalmente, si el supervisor del CCV, no puede solventar el problema, deberá solicitar la intervención de la Instancia Interna del IEE.

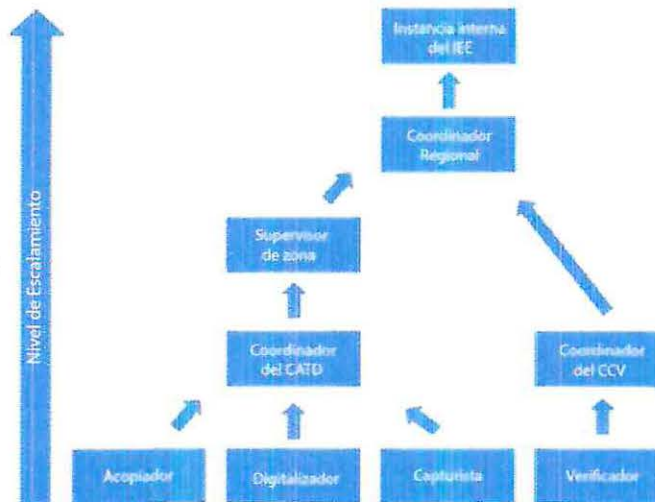
A continuación, se detalla la matriz de comunicación:

Matriz de comunicación

| Quien se comunica | Quien lo comunica    | A quien lo comunica                      | Cómo lo comunica                   |
|-------------------|----------------------|--|------------------------------------|
| Incidencias       | Acopiador            | Coordinador del CATD                     | Verbal en sitio                    |
|                   | Digitalizador        | Coordinador del CATD/CCV                 | Verbal en sitio                    |
|                   | Capturista           | Coordinador del CATD                     | Verbal en sitio                    |
|                   | Verificador          | Coordinador del CCV                      | Verbal en sitio                    |
|                   | Coordinador del CATD | Supervisor de Zona                       | Verbal en sitio                    |
|                   | Coordinador del CCV  | Coordinador Regional                     | Verbal en sitio                    |
|                   | Supervisor de zona   | Coordinación Regional                    | Verbal en sitio                    |
|                   | Coordinador Regional | Unidad Técnica de Servicios Informáticos | Vía telefónica/ correo electrónico |

ILUSTRACIÓN 3 MATRIZ DE COMUNICACIÓN





Se deberá realizar un documento en donde se incluirá, por lo menos, los niveles de servicio, medios de contacto, nombres de los responsables, para llevar a cabo la resolución de contingencias o en caso de que se suscite una situación adversa, para dar cumplimiento a los dispuesto en el numeral 13 del Anexo 13 del Reglamento de Elecciones.

## 14. 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:

- a) Captura de datos.
- b) 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.
- c) Manejo de inconsistencias y contabilización de los datos.
- d) 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.
- e) Funciones mínimas del sistema.
- f) 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.
- g) Integridad en el registro de la información.
- h) Revisar que el sistema informático mantiene los datos libres de modificaciones, es decir, sin alteración.
- i) Imparcialidad en el tratamiento de la información.

- j) 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.
- k) Precisión en resultados.
- l) 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.
- m) 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:
  - n) Propósito, tipo y alcance de la prueba
  - o) Entregar información requerida para la prueba: aplicaciones, nombres de usuario y contraseñas, restricciones tecnológicas, información de contacto.
  - p) Reglas del Contrato:
    - I. Ambas partes deben estar de acuerdo (hacker ético y los administradores del PREP).
    - II. Identificar Tráfico del "Hacker Ético" y Datos en la Aplicación.
    - III. Acordar Duración y Horarios.
    - IV. Planificar las Comunicaciones: Contactos diversos y protegidos para la comunicación.
    - V. Elaborar un resumen ejecutivo de hallazgos y recomendaciones.
    - VI. Describir la metodología paso a paso.

