PREP 2026 • COAH

IEC Instituto Electoral de Coahuila

Plan
Versión 1.0

Plan de Seguridad y Continuidad PREP 2026

IEC

Febrero 2026

Informática Electoral

Contenido

Tabla de contenido

Tabla de Ilustración

Glosario de Términos

Activo: cualquier ente tangible o intangible que tiene valor para el IEC y para el Tercero Auxiliar del PREP y que requiere protección. Existen diversos tipos de activos, incluyendo:

Activos tangibles

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.
II. **Activos digitales:** balanceadores, servidores de aplicaciones, bases de datos, firewalls, respaldos de S3, aplicaciones para actualizaciones.
III. **Activos de software:** software de aplicación, software del sistema, herramientas de desarrollo.
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.
V. **Activos informáticos:** servidores en nube, equipo de cómputo, equipo de comunicación y medios removibles.
VI. **Personas:** personal directivo, técnico y operativo del PREP con competencias específicas, habilidades, experiencia y roles que desempeñan.

Activos intangibles

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.
II. **Intangibles:** tales como la reputación, percepción de transparencia, la imagen del IEC, confianza de la ciudadanía en el PREP y claridad, certeza y continuidad de la información.

AES 256: Estándar de cifrado simétrico de bloque, aprobado por la NSA para datos ultrasecretos, que utiliza claves de 256 bits para transformar datos, ofreciendo una seguridad extremadamente alta.

Análisis de riesgos: 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.

Baseline: Conjunto de atributos en un tiempo determinado, que sirven como guía de configuración técnica estandarizada basada en las mejores prácticas de seguridad internacional y en los lineamientos de seguridad.

BCP: Plan de Continuidad del Negocio, por sus siglas en inglés "Bussiness Continuity Plan".

CATD: Centro de Acopio y Transmisión de Datos.

CCV: Centro de Captura y Verificación.

CCV Secundario: Centro de Captura y Verificación de respaldo.

Central: Centro de Recepción de Imágenes y Datos.

COPREP: Centro de Operaciones del PREP.

DDoS: 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.

DNS: Sistema de nombres de dominio, encargado de la traducción de direcciones IP en direcciones de dominio.

DRP: Plan de Recuperación de Desastres, por sus siglas en inglés "Disaster Recovery Plan". Estándar Requerimiento mandatorio que soporta a las directrices de seguridad.

FailOver: Es el modo de funcionamiento de respaldo en el que las funciones principales de los dispositivos son preservadas por los componentes secundarios del dispositivo cuando sus componentes principales no están disponibles, ya sea, por una falla o inactividad de estas.

Firewall: Dispositivos de seguridad perimetral de la red, que 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.

Hash o código de integridad: Valor único que permite identificar cada imagen PREP digitalizada y, de este modo corroborar que no haya sido alterada o editada. Ejemplos de función HASH son SHA256 y MD5.

HTTPS: Es la versión segura de HTTP, utilizada para cifrar la comunicación entre un navegador y un sitio web mediante protocolos SSL/TLS.

IDS: Sistema de Detección de Intrusiones, por sus siglas en inglés

IEC: Instituto Electoral de Coahuila.

IMEI: Código único de 15 dígitos que identifica a nivel mundial un teléfono móvil, funcionando como su huella digital.

IPS: Sistema de Prevención de Intrusiones, por sus siglas en inglés "Intrusion Prevention System".

LDAP: Protocolo Ligero de Acceso a Directorios, por sus siglas en inglés "Lightweight Directory Access Protocol".

MCAD: Monitor de Captura de Actas Digitalizadas.

MITM: ("Hombre en el medio" por sus siglas en ingles) es una ciberamenaza donde un atacante intercepta sigilosamente la comunicación entre dos partes (como un usuario y un sitio web) para robar datos confidenciales, espiar o modificar información en tiempo real.

OMS: Organización Mundial de la Salud.

PREP: Programa de Resultados Electorales Preliminares.

Procedimiento: Forma específica para llevar a cabo una actividad determinada, su representación gráfica se realiza mediante diagramas de flujo.

PTO: Proceso Técnico Operativo.

Reglamento: Reglamento de Elecciones Vigente del Instituto Nacional Electoral.

Riesgo Aceptado: Asumir el riesgo siempre con justificación.

Riesgo Mitigado: Atenuar el riesgo con nuevos procedimientos o acciones.

Riesgo Transferido: Transferir el riesgo y sus implicaciones a un tercero.

Sniffer: Aplicación especial para redes informáticas que permite capturar los paquetes que viajan a través de un segmento de red específico.

TCA: Terminal de Captura de Actas.

UPS: (Sistema de Alimentación Ininterrumpida por sus siglas en ingles), es un dispositivo que protege los equipos electrónicos de cortes de luz y variaciones de voltaje.

VLAN: Tecnología que permite crear redes lógicas independientes y aisladas dentro de una misma infraestructura física.

WAF: Firewall de Aplicaciones Web, por sus siglas en inglés "Web Application Firewall".

1 Introducción

El Programa de Resultado Electorales Preliminares (PREP) es el mecanismo de información electoral encargado de proporcionar resultados preliminares, no definitivos y de carácter estrictamente informativo, mediante la digitalización, captura, verificación y publicación de los datos contenidos 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 Electoral de Coahuila (IEC).

El PREP constituye la herramienta mediante la cual se dan a conocer, de forma confiable, rápida y oportuna, los resultados de la votación emitida por la ciudadanía en las diversas casillas electorales que se instalan el día de la Jornada Electoral, sin que dichos resultados constituyan el cómputo final. Asimismo, se trata de un sistema complejo que hace uso de los instrumentos tecnológicos para

procesar grandes volúmenes de datos a alta velocidad, garantizando la certeza de la información, así como su difusión inmediata y simultánea.

La generación y difusión de información oportuna, veraz y pública de los resultados preliminares es una función de carácter nacional que, en el ámbito de sus atribuciones, corresponde al IEC respecto de su implementación y operación. Lo anterior, con fundamento en el artículo 348, numeral 1, del Reglamento de Elecciones del Instituto Nacional Electoral, el cual 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 resulta indispensable para prevenir riesgos, daños, imprevistos o factores no previstos 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.

1.1 Antecedentes y definición de la Seguridad Informática

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 frente a robos o accesos no autorizados.
b) La prevención de la corrupción de la información existente ya sea durante su transmisión a través de redes de datos o directamente en los medios de almacenamiento electrónicos donde se encuentra resguardada.
c) La capacidad de recuperación ante situaciones desastrosas, ya sean de naturaleza fortuita o malintencionada.

Todo lo anterior tiene como finalidad preservar la integridad, disponibilidad, privacidad, control y autenticidad de la información, garantizando al mismo tiempo el acceso a los datos por parte de los usuarios autorizados, y la continuidad operativa de los sistemas.

Con base en esta definición, es importante precisar las políticas, procedimientos y metodologías para asegurar la integridad, disponibilidad y confiabilidad de los datos y sistemas; prevenir y detectar amenazas, así como responder de manera oportuna y adecuada ante cualquier incidente; y proteger y mantener los sistemas en operación continua y de manera ininterrumpida.

Asimismo, es indispensable contar con la certeza de que las propiedades de la información –descritas a continuación– se mantienen y respetan en todo momento durante la operación del sistema y que, en caso de presentarse una brecha de seguridad, la recuperación se lleve a cabo de forma inmediata,

con la menor afectación posible.

1.2 Propiedades de la información

Las propiedades de la información son las siguientes:

- **Confidencialidad:** Garantizar que la información contenida en un sistema de cómputo, así como aquella transmitida a través de medios de comunicación, sea accesible únicamente por personas debidamente autorizadas.
- **Autenticación:** Asegurar 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:** Garantizar que únicamente el personal autorizado pueda modificar la información o los recursos de cómputo.
- **No repudio:** Asegurar que ni el emisor ni el receptor de un mensaje o acción puedan negar la realización de dicha acción.
- **Disponibilidad:** Garantizar que los recursos de un sistema de cómputo, comunicación y almacenamiento se encuentren disponibles en el momento en que sean requeridos.

En este contexto, resulta necesario establecer reglas claras de funcionamiento, así como procedimientos precisos y fácilmente comprensibles, que puedan ser aplicados por todo el personal que participe en la operación del PREP.

2 Objetivo general

Establecer una estrategia para salvaguardar la integridad, disponibilidad y confidencialidad de la información, así como garantizar la continuidad de la operación del Programa de Resultados Electorales Preliminares (PREP), mediante la identificación de los riesgos de seguridad de la información en las diferentes etapas del Programa. Lo anterior abarca procedimientos, servicios e infraestructura de Tecnologías de la Información y Comunicaciones (TIC), recursos humanos y seguridad física, con el propósito de definir e implementar los controles de seguridad adecuados que reduzcan los riesgos a niveles aceptables y aseguren la confiabilidad, continuidad y correcta operación de los sistemas, activos tecnológicos y servicios informáticos.

2.1 Objetivos particulares

A continuación, se describen los objetivos particulares del presente Plan:

a) Elaborar las directrices de seguridad de la información para el PREP, las cuales fungirán como soporte del presente Plan de Seguridad y deberán ser acatadas por las personas servidoras públicas y por los entes externos al IEC que interactúen directa o indirecta con el Programa.
b) Realizar el análisis de riesgos que permita identificar las vulnerabilidades de seguridad de la información a las que se enfrenta el PREP.
c) Identificar e implementar los controles de seguridad en los distintos procesos operativos del PREP, así como en su infraestructura tecnológica.
d) Implantar soluciones de seguridad perimetral con la finalidad de controlar y monitorear el tráfico de la red de datos que soporta al PREP.
e) Fortalecer el desarrollo de las aplicaciones utilizadas para el cumplimiento de los distintos procesos de operación del PREP.
f) Establecer un plan de concientización y capacitación que promueva la cultura de seguridad de la información entre todo el personal que participa en el PREP.
g) Definir el esquema de control de accesos a los diferentes sistemas del PREP, incluyendo los Centros de Acopio y Transmisión de Datos (CATD) y los Centros de Captura y Verificación (CCV), así como la infraestructura destinada a la difusión y publicación de resultados.
h) Establecer el Plan de Continuidad para minimizar el impacto en la operación del PREP, así como el plan de recuperación ante la pérdida de activos de información.
i) Elaborar la documentación necesaria que facilite la evaluación y verificación por parte del ente auditor designado por el IEC.
j) Fortalecer la infraestructura tecnológica mediante la elaboración de guías de configuración técnica estándar (baseline), orientadas a los sistemas operativos y dispositivos de comunicación, así como llevar a cabo pruebas de penetración y revisiones de configuración que permitan detectar y corregir brechas de seguridad en la infraestructura que soportará al PREP.
k) Definir la estrategia de monitoreo, detección y respuesta a incidentes de seguridad, mediante la creación de procedimientos, lineamientos y/o estándares necesarios para tal fin.
l) Coordinar la auditoría externa con la Institución Académica u organismo designado para tal efecto, a fin de llevar a cabo la revisión en materia de seguridad de la infraestructura tecnológica del PREP.

3 Alcance

El presente Plan de Seguridad y Continuidad tiene como objetivo implementar los controles de seguridad aplicables a los procesos de operación del Programa de Resultados Electorales Preliminares (PREP) en sus etapas de acopio, digitalización, captura, verificación, publicación y empaquetado de actas.

Este documento se elabora con fundamento en lo dispuesto en el Anexo 13 del Reglamento de Elecciones del Instituto Nacional Electoral (INE), así como en los Acuerdos que, en el ámbito de sus atribuciones, emita el Consejo General del Instituto Electoral de Coahuila (IEC).

De conformidad con lo establecido en el artículo 347, numeral 1, del Reglamento de Elecciones, el cual señala:

> *"1. El Instituto y los OPL deberán someter su sistema informático a una auditoría técnica 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.*
>
> *Análisis de vulnerabilidades, considerando al menos pruebas de penetración y revisión de las configuraciones de la infraestructura tecnológica del PREP."*

Asimismo, 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.

Por su parte, el numeral 12 del Anexo 13 del Reglamento de Elecciones, que contiene los Lineamientos del PREP, establece 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. 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."

Adicionalmente, se deberá implementar un Plan de Continuidad, cuyo objeto sea determinar las acciones que garanticen la ejecución de los procedimientos correspondientes 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.

El Plan de Seguridad y el Plan de Continuidad deberán ser elaborados por la instancia interna correspondiente y, en su caso, en coordinación con el tercero que auxilie en la implementación y operación del PREP. Ambos planes deberán ser comunicados oportunamente al personal involucrado en su ejecución, de acuerdo con las funciones y responsabilidades asignadas a cada rol operativo, a fin de que formen parte de los ejercicios y simulacros que se realicen.

Todas las medidas y acciones previstas en el presente Plan tendrán carácter obligatorio para el personal que participa en la operación del PREP y serán dadas a conocer a través de las sesiones de capacitación y sensibilización correspondientes.

4 Normatividad aplicable

El presente documento se elabora con base en lo dispuesto en el Anexo 13 del Reglamento de Elecciones del Instituto Nacional Electoral, así como en los acuerdos que emita el Consejo General del mismo y del IEC.

Artículo 347.

1. El Instituto y los OPL deberán someter su sistema informático a una auditoría técnica 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, revisión de las configuraciones de la infraestructura tecnológica del PREP.

Artículo 348.

1. *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.*

5 Desarrollo del Plan de Seguridad

El Plan de Seguridad comprende el conjunto de acciones, directrices, estándares y procedimientos orientados a la prevención, detección y respuesta ante incidentes de seguridad que pudieran afectar la correcta ejecución del Programa de Resultados Electorales Preliminares (PREP).

A través de este Plan, los riesgos asociados a la seguridad de la información y a la infraestructura tecnológica el PREP son identificados, evaluados y mitigados de manera sistemática, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información durante todas las fases de su operación.

6 Directrices de seguridad de la información

Conforme a lo establecido en el artículo 352, numeral 1, inciso f), del Reglamento de Elecciones, se deberá capacitar a todo el personal involucrado en el Proceso Técnico Operativo para la implementación y operación del PREP, en materia de seguridad de la información, manejo de incidentes y cumplimiento de las medidas establecidas en el presente Plan.

Dicha capacitación tendrá como finalidad asegurar que el personal conozca y aplique correctamente las políticas, procedimientos y controles de seguridad definidos, de acuerdo con las funciones y responsabilidad asignadas a cada rol operativo.

7 Análisis de riesgos en materia de seguridad de la información

De acuerdo con el Numeral 12 del Anexo 13 del Reglamento de elecciones, Inciso I que menciona que se deben establecer el conjunto de medidas específicas para evaluar los riesgos con base en su impacto y la probabilidad de ocurrencia, así mismo, de acuerdo con el numeral 6.1.2 de la norma ISO 27001:2022, se debe definir y aplicar un proceso de valoración de riesgos de seguridad de la información, para ello, Informática Electoral propone los siguientes criterios y metodología.

7.1 Definiciones generales

Amenaza. Evento que al llevarse a cabo produce daños de carácter material o inmaterial a los activos de información.

Probabilidad. Es el grado que hace referencia a la probabilidad de que una amenaza se materialice a partir de una vulnerabilidad específica. A mayor número de vulnerabilidades en un activo, mayor será la probabilidad de ocurrencia. Para su estimación se consideran, entre otros factores, la eficacia de los controles aplicados en procesos electorales anteriores. La probabilidad se clasifica en Alta, Media o Baja, conforme a los criterios descritos en el punto 7.2 del presente documento.

Impacto. Es el grado de afectación o consecuencia que genera una amenaza materializada sobre un activo.

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 1 a 25, como se explica en el numeral 7.2.

Responsable. Nombre del responsable de la implementación del plan de mitigación.

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.

7.2 Evaluación

Previo a empezar con la detección de riesgos, se definirá como es que éstos se van a detectar, evaluar y tratar, es por ello por lo que se debe definir una metodología, en este caso, se utiliza una metodología que combina la criticidad, o bien, el impacto de que un riesgo se materialice, en conjunto con la probabilidad de que un riesgo ocurra, para lo cual, se multiplica la probabilidad de ocurrencia por el impacto. Es importante determinar también en qué nivel se tratarán los riesgos en el caso del PREP 2026 se utilizarán las siguientes opciones de tratamiento:

- **Riesgos que en su evaluación resulten mayor o igual que 13:** Mitigarlos o evitarlos mediante la aplicación de controles o eliminación de los riesgos.

- **Riesgos que en su evaluación resulten en un rango de 7 a 12:** Se definirá en conjunto con el IEC cuales riesgos se deberán mitigar o evitar, de acuerdo con las necesidades y expectativas de las partes interesadas y los requisitos contractuales o lineamientos normativos.
- **Riesgos que resulten menor o igual que 6:** Aceptar y monitorear estos riesgos podría ser un tratamiento valido siempre y cuando no se incumpla ningún lineamiento o normatividad vigente, dicho de otra forma, aunque el riesgo sea aceptable, si los lineamientos del INE exigen que el riesgo sea tratado, así se hará.

Para el cálculo de la evaluación se utilizará la siguiente matriz:

		Nivel de impacto				
		1	2	3	4	5
Probabilidad de ocurrencia	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Tabla 1. Matriz de apoyo para la evaluación de riesgos

Para ello, se seguirá el siguiente criterio:

Probabilidad de ocurrencia	
Rango	Descripción
1 – Muy baja	Es improbable que ocurra, por ejemplo, un tsunami.
2 – Baja	Es un evento poco probable, pero puede ocurrir bajo circunstancias especiales.
3 – Moderada	Podría suceder ocasionalmente.
4 – Alta	Es probable que ocurra en el contexto actual.
5 – Muy alta	Es casi seguro que va a ocurrir.

Tabla 2. Criterios para evaluar la probabilidad de ocurrencia

Nivel de impacto	
Rango	Descripción
1 – Muy bajo	Tendría un impacto insignificante en las operaciones, no causaría interrupciones importantes o perdida de datos.
2 – Bajo	Afectaría procesos secundarios, pero no críticos, o bien, moderadamente críticos, pero con una recuperación relativamente rápida.
3 – Moderado	Afecta procesos importantes y causa retrasos costosos para su recuperación.
4 – Alto	Interrumpe procesos críticos y recuperarlo implica muchos recursos.
5 – Muy alto	Compromete la continuidad del proyecto, causa perdidas severas.

Tabla 3. Criterios para evaluar el nivel de impacto

7.3 Identificación de activos críticos

Se deben identificar los activos críticos para la operación del PREP, para ello, Informática Electoral elaborará un listado de los activos que se consideran críticos y no críticos para el proyecto, como se describe a continuación:

- **Activos críticos (AC):** Activo sin el cual las operaciones del proyecto no pueden continuar o que, de no estar disponible, genera una interrupción significativa en los servicios o el

cumplimiento de objetivos clave. Estos activos suelen tener un alto impacto en la seguridad de la información y requieren mayores controles.

- **Activos no críticos (ANC):** Activo cuya interrupción temporal afecta de manera moderada al proyecto y solo genera retrasos en las operaciones, pero no detiene completamente las actividades ni compromete objetivos clave.

Este listado además de clasificarse en activos críticos y no críticos se clasificará por área de la siguiente forma:

- **Hardware:** Haciendo referencia a los equipos e infraestructura del proyecto.
- **Software:** Considerando la operatividad de los sistemas, accesos y todo lo referente a su uso o información que contiene.
- **Recursos humanos:** Haciendo referencia a las personas.
- **Procesos:** Considerando aquellos riesgos que asociados al PTO o lineamientos normativos.
- **Documentación:** Haciendo referencia a los registros físicos y digitales necesarios para respaldar, formalizar y dar seguimiento a las actividades relacionadas con el proceso electoral.
- **Operación:** Haciendo referencia a los inmuebles utilizados para la ejecución de las actividades relacionadas al PREP.

A continuación, se presenta el listado de activos por áreas:

Área	Activo
Hardware	AC - Enlaces de internet
	AC – Firewall
	AC – VPN
	AC – UPS
	AC – NVR
	AC – Switches
	AC – Servidores
	ANC - Conmutadores telefónicos
	AC – Red eléctrica
	AC – Plantas de energía eléctrica
	AC - Equipos de cómputo portátil
	AC – Escáneres
	AC – Impresoras
	ANC – Cámaras de seguridad
	ANC – Sillas y mesas
Software	AC – DSA
	AC – Dispositivos móviles
	AC – Servicios de datos móviles
	AC - Bases de datos en servidores
	AC - Actas digitalizadas
	AC – MCAD
	AC – CVPREP
	AC – PREP Casilla
	AC - Página web portal
	ANC - Chat para comunicación COPREP – CATD – CCV
	AC - Replicador de Base de Datos
	ANC – Difusores oficiales
Recursos humanos	AC – Plantilla operativa completa
Procesos	AC – PTO aprobado
	AC – Material de capacitación

Documentación	AC – Actas (ejercicios, simulacros) AC – Actas (PREP) AC – CATD/CCV
Operación	

Tabla 4. Listado de activos por área

7.3.1 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, tales como movimientos sociales, problemas recurrentes en carreteras o caminos, tormentas eléctricas, lluvias muy frecuentes, problemas constantes de electricidad o de telecomunicaciones.
- Estructura tecnológica propia y contratada, incluyendo infraestructura, servicios y capacidades de soporte
- Ambiente político-electoral, particularmente cuando se identifique una contienda cerrada entre candidaturas, la existencia de escándalos públicos recientes o condiciones que generen una mayor afluencia de observadores del Programa y posibles intentos de sabotaje al PREP.

Considerando los aspectos anteriormente descritos, tendremos oportunidad de planear y tomar las acciones necesarias para mitigar y/o evitar en su totalidad los riesgos identificados. A continuación, se describen los criterios para medir y mitigar dichos riesgos.

7.3.2 Identificación y clasificación de riesgos

Para la identificación de riesgos se establecen cuatro ejes principales de análisis. Estos ejes permiten evaluar las posibles afectaciones al Programa y clasificarlas de acuerdo con el nivel de riesgo que representen.

Ilustración 1. Criterios para medir riesgos

7.3.2.1 Basados en experiencias pasadas

Este criterio resulta especialmente útil cuando existen antecedentes en la implementación del PREP. A partir de experiencias previas, favorables o desfavorables, es posible identificar áreas de oportunidad y establecer medidas preventivas que permitan mitigar riesgos. Si bien la experiencia puede implicar costos, constituye un insumo de alto valor para la adecuada identificación y gestión de riesgos.

7.3.2.2 Basados en condiciones geográficas del Estado

Se identifican riesgos considerando las condiciones geográficas, de infraestructura eléctrica, carreteras, accesos y telecomunicaciones de los Comités Distritales donde se localizan los CATD. Lo anterior tiene como finalidad:

- Establecer rutas de acceso seguras.
- Mitigar o eliminar riesgos asociados a la falta de seguridad o de servicios esenciales.
- Reducir los tiempos de reacción ante contingencias.

7.3.2.3 Basados en ambiente sociopolítico del Proceso Electoral

Se identifican riesgos de carácter sociopolítico que pudieran derivar en marchas, plantones u otras manifestaciones que dificulten o impidan el acceso a los centros de operación del PREP. Asimismo, se evalúa la probabilidad de actos de violencia, amenazas o situaciones de riesgo que puedan afectar la continuidad operativa del Programa.

Con base en este análisis, se definen:

- Rutas de acceso alternas.
- Esquemas de redundancia de sedes físicas.
- Medidas de seguridad para el personal.
- Rutas y protocolos de evacuación.

Estas acciones tienen como objetivo garantizar la continuidad operativa del Programa.

7.3.2.4 Basados en la estructura electoral de cada tipo de elección

Se determinan riesgos inherentes a la complejidad de los campos de captura derivados de las distintas

combinaciones posibles en las Actas de Escrutinio y Cómputo (AEC). Para ello, se establecen medidas específicas de capacitación, pruebas funcionales y validaciones, con el fin de prevenir errores o retrasos en la captura de información.

7.3.3 Evaluación de riesgos por probabilidad e impacto

Una vez realizada la evaluación cualitativa de cada uno de los factores de riesgo, los resultados se agrupan conforme a la tipología de riesgos que hemos definido en el numeral 7.2. Para determinar la exposición al riesgo, se agregan los resultados considerando los niveles de probabilidad e impacto.

7.4 Identificación de riesgos

Los riesgos son una combinación de dos factores, como son la vulnerabilidad, las cuales son debilidades internas, y de amenaza, las cuales tienden a ser externas, cuando ambos factores se juntan, se convierten en un riesgo. Por poner un ejemplo, imaginemos que un activo es una laptop, la cual, entre otras amenazas, una de ellas es la de entrar en contacto con agua, y como está laptop tiene la vulnerabilidad de no ser a prueba de agua, se crea el riesgo de daño por contacto con agua, debido a que se juntaron las amenazas con las vulnerabilidades.

En conformidad con el Numeral 12 del Anexo 13 del Reglamento de Elecciones, donde especifica que se deben identificar y describir las amenazas técnicas, legales, económicas, políticas, sociales, entre otras que pueden afectar el PREP, y el inciso IV del mismo numeral, que solicita que se deben identificar los riesgos que se pueden materializar, en la siguiente tabla se muestra la Evaluación de riesgos:

Activo	Riesgo	Responsable del activo	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia (1 - 5)	Impacto (1 - 5)	Control actual	Nivel de riesgo
AC - Enlaces de internet	Falla parcial en el servicio	Departamento de Infraestructura y Seguridad / Proveedor de servicio de internet	Caída del servicio en enlace primario.	Enlace secundario deficiente.	2	3	N/A	6
	Falla en el servicio	Departamento de Infraestructura y Seguridad / Proveedor de servicio de internet	Caída simultanea de ambos enlaces.	Dependencia de dos proveedores.	1	5	Se cuenta con dispositivos móviles habilitados para el envío de las actas	5

	Lentitud del servicio	Departamento de Infraestructura y Seguridad / Proveedor de servicio de internet	Sobre carga de la red interna.	Ancho de banda insuficiente o equipo de red desactualizado	3	2	N/A	6
AC - Firewall	Configuración incorrecta	Departamento de Infraestructura y Seguridad	Configuración errónea o incompleta	Falta de revisión de validación	3	4	N/A	12
	Fallo de hardware	Departamento de Infraestructura y Seguridad	Daño físico	Uso de hardware sin respaldo	2	5	N/A	10
	Ataques externos	Departamento de Infraestructura y Seguridad	Ataques de denegación de servicio (DDoS)	Reglas insuficientes para mitigar ataques avanzados	3	5	N/A	15
AC - VPN	Acceso no autorizado	Departamento de Infraestructura y Seguridad	Robo de credenciales de acceso	Uso de contraseñas débiles	3	4	N/A	12
	Interceptación de datos	Departamento de Infraestructura y Seguridad	Ataques de intermediario (Man-in-the-Middle)	Configuración insegura o cifrado débil	3	5	N/A	15
	Obsolescencia tecnológica	Departamento de Infraestructura y Seguridad	Uso de software o equipos obsoletos	Falta de actualizaciones de seguridad o soporte	2	4	N/A	8
	Saturación de conexiones	Departamento de Infraestructura y Seguridad	Exceso de usuarios o conexiones simultáneas	Falta de monitoreo.	3	4	N/A	12
AC - UPS	Equipos sin energía eléctrica	Departamento de Infraestructura y Seguridad	Falla en el equipo	Mantenimiento inadecuado o desgaste del equipo	3	5	N/A	15
	Obsolescencia tecnológica	Departamento de Infraestructura y Seguridad	Uso de equipos obsoletos	Falta de soporte o cambio de equipos.	2	4	N/A	8
	Tiempo insuficiente de respaldo	Departamento de Infraestructura y Seguridad	Baterías descargadas o dañadas	Uso excesivo	2	4	N/A	8

AC - NVR	Fallo de funcionamiento	Departamento de Infraestructura y Seguridad	Daño físico del disco duro	Desgaste por uso continuo	2	3	N/A	6
	Pérdida de grabaciones de eventos	Departamento de Infraestructura y Seguridad	Eliminación accidental o daño de los archivos	Falta de respaldos	2	5	N/A	10
AC - Switches	Fallo del dispositivo	Departamento de Infraestructura y Seguridad	Daño físico	Sobrecalentamiento y/o desgaste por uso	2	4	N/A	8
	Congestión de la red	Departamento de Infraestructura y Seguridad	Saturación por tráfico no gestionado	Configuración inadecuada	3	4	N/A	12
	Acceso no autorizado	Departamento de Infraestructura y Seguridad	Hackeo o configuraciones maliciosas	Falta de controles de acceso físico y/o lógico.	3	5	N/A	15
	Pérdida de conectividad	Departamento de Infraestructura y Seguridad	Fallo de energía	Falta de respaldo de energía	2	5	N/A	10
AC - Servidores	Fallo de hardware	Departamento de Infraestructura y Seguridad	Daño en componentes críticos	Desgaste por uso, sobrecalentamiento	2	5	N/A	10
	Pérdidas de datos	Departamento de Infraestructura y Seguridad	Corrupción o eliminación de datos	Copias de seguridad insuficientes o no actualizadas	3	5	N/A	15
	Acceso no autorizado	Departamento de Infraestructura y Seguridad	Hackeo o robo de credenciales	Configuración débil de permisos y contraseñas	3	5	N/A	15
	Interrupción del servicio	Departamento de Infraestructura y Seguridad	Fallo de energía o conectividad	Falta de redundancia en energía y red	2	4	N/A	8
ANC – Conmutadores telefónicos	Fallo de equipo	Departamento de Infraestructura y Seguridad	Daño del equipo	Picos de energía que dañen el equipo	2	4	N/A	8
	Interrupción del servicio	Departamento de Infraestructura y	Falla de conexión en la línea telefónica	Mala configuración de conmutador	3	3	N/A	9

		Seguridad / Proveedor de servicio de telefonía						
	Obsolescencia tecnológica	Departamento de Infraestructura y Seguridad	Dispositivos obsoletos funcionalmente	Falta de reemplazo de equipo obsoleto	2	3	N/A	6
AC - Red eléctrica	Interrupción del suministro eléctrico	Departamento de Infraestructura y Seguridad / Proveedor de energía	Corte de energía o fluctuaciones de voltaje	Ausencia de respaldo inmediato	3	4	N/A	12
AC – Plantas de energía eléctrica	Falla en el arranque	Departamento de Infraestructura y Seguridad	Fallo mecánico o eléctrico	Falta de mantenimiento	3	4	N/A	12
	Insuficiencia de combustible	Departamento de Infraestructura y Seguridad	Agotamiento del combustible	Dependencia de suministro externo	2	5	N/A	10
AC – Equipos de cómputo portátil (Personal Operativo)	Robo de equipo	Coordinador de CATD/ CCV	Hurto de equipo	Falta de medidas de seguridad física	3	5	N/A	15
	Daño físico	Coordinador de CATD/ CCV	Golpes, caídas o derrames de líquidos	Manejo inadecuado del equipo	3	4	N/A	12
	Pérdida de información	Coordinador de CATD/ CCV	Robo, sustracción de información	Puertos de USB, bandejas de CD y DVD, Bluetooth habilitados	3	5	N/A	15
	Acceso no autorizado	Coordinador de CATD/ CCV	Robo de credenciales o manipulación	Contraseñas débiles	3	5	N/A	15
	Obsolescencia tecnológica	Departamento de Infraestructura y Seguridad	Equipo desactualizado	Falta de actualización de equipos	2	3	N/A	6
AC – Escáneres	Mal funcionamiento durante la digitalización	Coordinador de CATD/ CCV	Configuración incorrecta	Falta de capacitación en el uso del equipo	2	3	N/A	6
	Daño por sobrecarga de trabajo	Coordinador de CATD/ CCV	Sobrecarga de documentos	Operación fuera de las especificaciones recomendadas	3	4	N/A	12
	Interrupción del servicio	Coordinador de CATD/ CCV	Fallo eléctrico o de conectividad	Falta de respaldo eléctrico o	3	5	N/A	15

				redundancia en dispositivos				
	Pérdida de calidad en digitalizaciones	Coordinador de CATD/ CCV	Ajustes incorrectos	Acomodo inadecuado del Acta PREP	3	3	N/A	9
AC – Impresoras	Falla de equipo	Departamento de Infraestructura y Seguridad	Daño por uso continuo	Falta de mantenimiento	3	4	N/A	12
	Pérdida de documentos impresos	Coordinador de CATD	Documentos extraviados o recolectados por personal no autorizado	Falta de control en la recolección de impresiones.	2	4	N/A	8
	Falta de conectividad	Departamento de Infraestructura y Seguridad	Fallo en la red o configuración incorrecta	Dependencia de la conectividad de red.	2	3	N/A	6
ANC – Cámaras de seguridad	Fallo de equipo	Departamento de Infraestructura y Seguridad	Daño físico	Falta de revisión o protección del equipo	3	4	N/A	12
	Interrupción del servicio	Departamento de Infraestructura y Seguridad	Corte de energía o fallo en la red	Falta de respaldo eléctrico	3	4	N/A	12
ANC – Sillas y mesas	Lesiones al personal	Departamento de Personal y Talento / Coordinador de CATD/CCV	Mobiliario en mal estado	Uso de mobiliario dañado	2	4	N/A	8
	Pérdida o robo	Departamento de Administración y Finanzas / Coordinador de CATD/CCV	Falta de control de inventarios	Falta de registro de los activos	2	2	N/A	4
AC – DSA	Falla en el funcionamiento	Departamento de Infraestructura y Seguridad	Mal funcionamiento o daño mecánico	Falta de revisiones previas	3	4	N/A	12
	Interrupción del servicio	Coordinador de CATD	Fallo eléctrico	Dependencia de suministro eléctrico	2	4	N/A	8
	Pérdida o robo	Coordinador de CATD	Sustitución indebida del equipo	Falta de inventario	2	5	N/A	10

	Daño físico	Coordinador de CATD	Golpes, caídas o manejo inadecuado	Ausencia de protocoles de manejo de equipos	3	3	N/A	9
AC – Dispositivos móviles	Robo o pérdida	Coordinador de CATD	Extracción física o extravío	Falta de seguimiento de los equipos	3	5	N/A	15
	Ataques de malware	Coordinador de CATD	Instalación de aplicaciones no seguras	Falta de políticas para descargas	2	5	N/A	10
	Fallos en la conectividad	Coordinador de CATD	Problemas de red	Dependencia de conexiones de red	3	3	N/A	9
AC – Servicios de datos móviles	Uso no autorizado	Coordinador de CATD	Consumo excesivo por actividades no relacionadas	Fata de restricciones en el uso de datos móviles	3	4	N/A	12
	Sobrecosto en el uso	Departamento de Administración y Finanzas / Coordinador de CATD	Consumo de datos mayor al esperado	Falta de monitoreo o límites de datos contratados	2	4	N/A	8
AC- Bases de datos en servidores	Pérdida de datos	Departamento de Infraestructura y Seguridad	Fallo en el almacenamiento o daño físico del servidor	Falta de respaldo	2	5	N/A	10
	Acceso no autorizado	Departamento de Infraestructura y Seguridad	Robo de credenciales o configuración insegura	Contraseñas débiles y falta de cifrado	3	5	N/A	15
	Ataques cibernéticos	Departamento de Infraestructura y Seguridad	Explotación de vulnerabilidades en infraestructura	Falta de actualizaciones y configuración de seguridad	3	5	N/A	15
	Interrupción del servicio	Departamento de Infraestructura y Seguridad	Sobrecarga del servidor o fallos eléctricos	Falta de escalabilidad y respaldo eléctrico	2	4	N/A	8
AC – Actas digitalizadas	Interrupción de trasmisión de datos	Departamento de Infraestructura y Seguridad	Fallo en la red	Dependencia de la conectividad	4	2	N/A	8
AC – MCAD	Acceso no autorizado	Departamento de Software e Implementación / Coordinador de CATD	Robo de credenciales o configuraciones inseguras	Tener la contraseña a la vista de cualquier persona	3	5	N/A	15

	Alteración de información	Departamento de Software e Implementación / Coordinador de CATD	Identificación errónea del Acta	Falta de capacitación al personal respecto a la identificación de las Actas	4	5	N/A	20
	Interrupción del servicio	Departamento de Infraestructura y Seguridad	Fallo en la red	Dependencia de la conectividad	3	5	N/A	15
AC – CVPREP	Error en la captura de los datos	Departamento de Software e Implementación / Coordinador de CCV	Errores humanos durante la digitalización	Falta de capacitación o supervisión	3	4	N/A	12
	Acceso no autorizado	Departamento de Software e Implementación	Robo de credenciales	Contraseña a la vista del personal.	3	5	N/A	15
	Interrupción del sistema	Departamento de Infraestructura y Seguridad	Fallo en la red	Dependencia de un solo proveedor de servicio.	3	5	N/A	15
AC – PREP Casilla	Error en la digitalización de actas	Departamento de Software e Implementación / CAE	Captura incorrecta o de baja calidad en la imagen	Falta de capacitación o mal uso del dispositivo	3	4	N/A	12
	Bloqueo por intentos falidos de acceso	Departamento de Software e Implementación / CAE	Olvido de contraseñas o uso en dispositivos no autorizados	Asociación de la aplicación con el IMEI y límite de intentos fallidos.	3	4	N/A	12
	Fallo en el envío de actas	Departamento de Software e Implementación	Problemas de conectividad en la casilla	Dependencia de la red móvil	3	4	N/A	12
	Error en la asignación de secciones	Departamento de Software e Implementación / Departamento de Administración de proyecto	Archivo con datos incorrectos o inconsistencias	Validación de asignaciones únicamente cuando se reporta un problema	2	5	N/A	10
AC - Página web portal	Interrupción del servicio	Departamento de Desarrollo / Departamen	Ataque DDoS	Falta de mitigación de tráfico anómalo	2	2	N/A	4

		to de Infraestructura y Seguridad						
AC - Replicador de Base de Datos	Caída de replicación	Departamento de infraestructura y seguridad	Fallo en la red	Falta de redundancia	2	2	N/A	4
ANC - Chat para comunicación COPREP – CATD – CCV	Interrupción de la comunicación	Departamento de Software e Implementación	Fallo en la red	Retraso en la actualización de la información	3	1	N/A	3
	Realización de actividades sin autorización	Coordinador de CATD/ CCV	Retraso de la comunicación	Retrabajo de las tareas asignadas	2	2	N/A	4
ANC – Difusores oficiales	Interrupción de la comunicación	Departamento de Software e Implementación	Fallo en la red	Retraso en la actualización de la información	3	1	N/A	3
	Falla en el servicio de Difusores activos	Departamento de Software e Implementación	Incumplimiento en las capacidades requeridas	Retraso y/o posible interrupción de la replicación de resultados	2	1	N/A	2
AC – Plantilla operativa completa	Retrasó en las actividades del proyecto	Departamento de personal y talento	Actividades estancadas	Dificultades para alcanzar objetivos estratégicos	3	3	N/A	9
	Rotación de personal	Departamento de personal y talento	Capacitación por bloques pequeños	Requerirá una capacitación mucho más segmentada	2	3	N/A	6
AC – PTO aprobado	Falta de transmisión total del PTO		Pasar por alto una necesidad básica para el proceso	Descalificación de actividades por no trasmitir la información requerida	2	4	N/A	8
	Falla en la comprensión de las necesidades		Rechazo de los procesos realizados por incumplimiento	Retrabajo y perdidas considerables durante el proyecto	1	5	N/A	5
AC – Documentos relacionados al proceso PREP	Seguridad en almacenamiento y versionamiento	Departamento de Software e Implementación	Uso y acceso de todo el personal	Documentación obsoleta y/o modificada	3	3	N/A	9
AC – Actas (ejercicios, simulacros)	Retrasó en la entrega de formatos	Coordinador líder	Incumplimiento de las actividades necesarias	No contar con la suficiente ejecución de tareas para una	2	4	N/A	8

				capacitación adecuada				
	Error en la captura de datos	Departamento de personal y talento	Incomprensión de las partes de valor en el proceso	Resultados erróneos y posible falla del sistema	5	2	N/A	10
AC – Actas (PREP)	Daños en las actas	Coordinador líder	Llegada con condiciones que impidan su procesamiento	Imposibilidad de realizar su correcta verificación	5	1	N/A	5
AC – CATD/CCV	Falta de seguridad perimetral	Departamento de personal y talento	Violación de terceros dentro de las instalaciones	Infiltración de información privada	2	4	N/A	8

Tabla 5. Evaluación de riesgos

8 Consideraciones y recomendaciones de seguridad de la información

La seguridad con la cual se maneja la información es uno de los puntos más importantes de esta solución, es por ello, por lo que una vez definida y consensuada con el IEC la evaluación de riesgos, a continuación, se presentan las acciones para la gestión de riesgos.

El presente Plan contempla acciones, directrices, estándares y procedimientos orientados a fortalecer la seguridad de la información, la infraestructura tecnológica y los procesos operativos del PREP.

8.1 Implementación de medidas de capacitación

Con el propósito de instruir y proporcionar al personal contratado las herramientas necesarias para operar correctamente y de manera eficaz el PREP para el proceso electoral 2026, se brindarán los siguientes temas de capacitación:

- Interpretar la estrategia de capacitación.
- Identificar y conocer los cargos de elección popular a renovar.
- Apropiarse del Proceso Técnico Operativo del PREP Coahuila 2026, su ejecución en los CATD y CCV, e identificar el rol y actividades a desempeñar.
- Conocer el programa de trabajo como marco de referencia.
- Identificar y resolver contingencias para la continuidad y operatividad del PREP.
- Conocer y aplicar el objetivo del plan de ejercicios y simulacros, para su eficiente realización.

8.1.1 Materiales de capacitación

En Informática Electoral dependiendo del tipo de capacitación, se proporcionarán los siguientes materiales de capacitación:

- Procedimientos documentados, mismos que podrán encontrarse en un manual de operaciones o en el repositorio utilizado por Informática Electoral.
- Presentaciones en PowerPoint.
- Guías rápidas informativas
- Equipo de cómputo.
- Celulares.
- Acceso a internet y servicios de correo y mensajería.

8.2 Implementación de medidas de arquitectura de seguridad

Los sistemas informáticos por utilizar en el proceso PREP se habilitarán en un sistema de nube híbrida, combinando una nube privada, infraestructura en sitio dentro del COPREP, con seguridad perimetral definida por firewalls, y un servicio de nube pública con seguridad perimetral y otras características de protección basada en nube.

Para la comunicación interna se usarán túneles VPN con encriptación de datos AES de 256 bits. Además, para evitar la saturación de servidores, se utilizarán balanceadores de carga para que distribuyan las peticiones de los usuarios. En los centros de datos internamente se operará con VLAN privadas, y dentro de estas redes habrá firewalls que evitarán que usuarios entren en la red interna de los centros de datos utilizando Intrusion Prevention System (IPS) e Intrusion Detection System (IDS).

Para la publicación del sitio web público se contará con un servicio de protección de ataques DDoS con capacidad mínima de 100 Gbps, capaz de mitigar ataques de denegación de servicio de más de 200Tbps, un firewall de aplicaciones web (WAF por sus siglas en inglés) y una red de entrega de contenidos (CDN, por sus siglas en inglés) con más de 200 puntos de presencia a nivel mundial y capacidad de entregar 50 Gbps de sitio web "limpio". Este servicio mitigará los posibles ataques y enviará las peticiones legítimas a un balanceador de carga redundante con capacidad de 250,000 conexiones únicas.

El balanceador de carga redundante enviará las peticiones a los servidores web necesarios para entregar los contenidos, pudiendo ser desde 2 hasta 10, dependiendo del probable número de visitantes que espere el sitio web público. Siendo el caso particular de Coahuila, el uso de 4 servidores.

8.3 Estructura del modelo de seguridad

Se propone la utilización de dos centros de datos distintos para garantizar la operación de los sistemas en su totalidad, debido a que los datos se guardan inicialmente en el Centro de Datos 1 (CD1) y este, a la vez, replica de manera inmediata los datos capturados a un centro de datos remoto de contingencia (CD2). Esta replicación es en tiempo real para los datos más críticos, tales como bases de datos, actas digitalizadas, sesiones, etcétera, y de 60 segundos en los datos de menor nivel, tales como contenidos estáticos de servidores de publicación, servicios secundarios, etcétera.

Con esta metodología se logrará tener un ambiente de alta disponibilidad con capacidad de continuidad en los procesos principales, tales como servidores de almacenamiento y captura de actas, servidores de bases de datos y servidores de difusión pública de resultados.

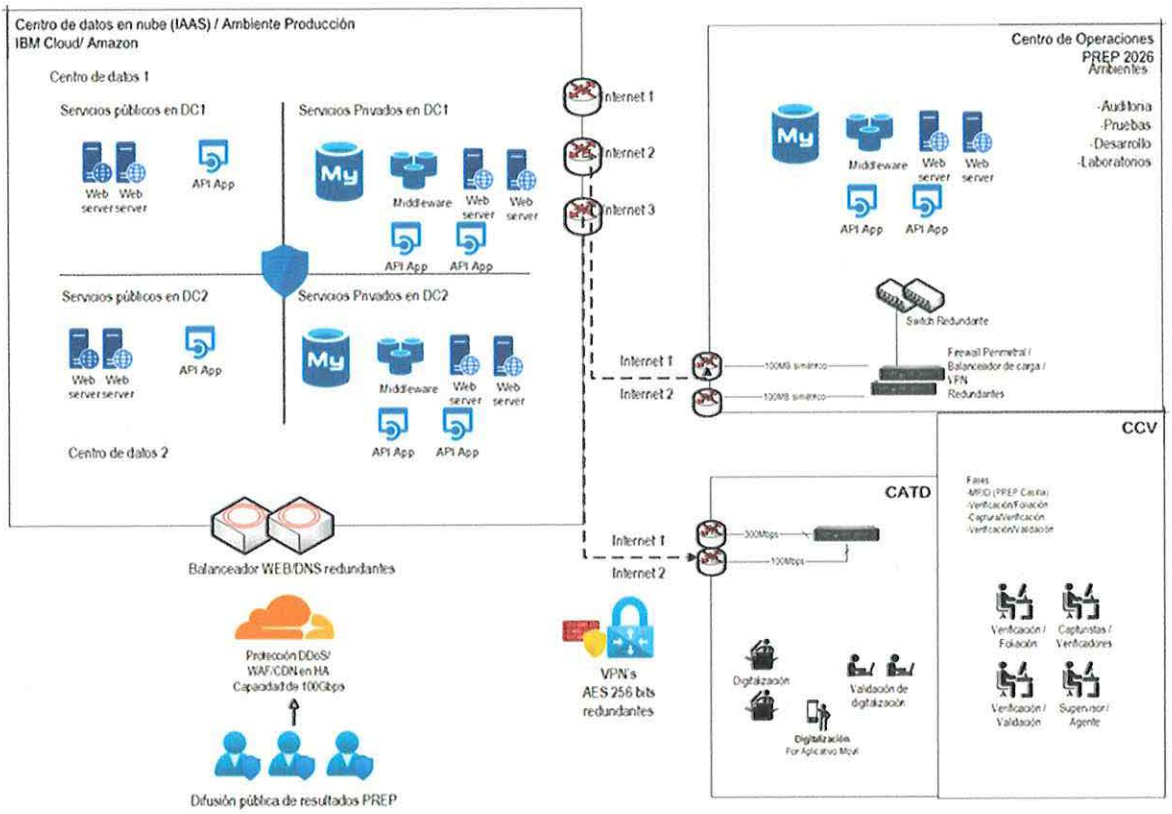


Tabla 6. Diagrama de interconexión y seguridad de red

8.4 Implementación de medidas de seguridad de la información en sistemas informáticos

Para asegurar que existan las adecuadas medidas de seguridad para la protección de la información y de los sistemas, aun previo a la realización de la evaluación de riesgos se realizarán los siguientes controles.

8.4.1 Control de usuarios y contraseñas con privilegios de operación

Al ser el PREP un sistema en línea, es necesario que cuente con un mecanismo de acceso, por lo cual se implementará un estricto control y generación de las cuentas de usuario correspondientes. Como segundo nivel de seguridad en este rubro, es preciso señalar que el PREP contemplará diversos privilegios de operación en las cuentas de usuario que se generen, contemplando diversos aspectos, como, por ejemplo, un usuario de digitalización del CATD del Distrito V no podrá digitalizar e identificar actas e información del CATD del Distrito IV, los usuarios de tipo "consulta", como su nombre lo indica, no podrán capturar información, entre otros.

Cabe destacar que los equipos de cómputo utilizados en PREP, en su totalidad cuentan con actualizaciones diariamente en el sistema operativo, hardware y antivirus, asimismo, se cuenta con

documentos para la administración y configuración de los dispositivos de comunicaciones, servidores y base de datos para evitar vulnerabilidades en su operación.

Para establecer las contraseñas por utilizar, se contará con una longitud y nivel de complejidad mínimo que deberá cumplir dicha contraseña, y se renovará previo al inicio de cada ejercicio, simulacro y Jornada Electoral.

Complementando la seguridad de los equipos de cómputo a utilizarse en el PREP, se inhabilitan los puertos USB de cada uno de los dispositivos, así como la inhabilitación y restricción de las tarjetas de red inalámbrica (Wi-Fi) y Bluetooth y bandejas lectoras de CD/DVD.

Este procedimiento evita filtración de información y protegen al equipo contra la introducción de virus informáticos.

Los usuarios se generarán bajo la siguiente nomenclatura:

[SISTEMA]_[CENTROID]_[NUMERO_USUARIO]

Ejemplo:

Cvprep_40_01

Las contraseñas de dichos usuarios se generarán desde un sistema central, el cual seguirá las siguientes reglas:

- 8 caracteres alfanuméricos (Números, mayúsculas, minúsculas).
- Se generarán contraseñas únicas de manera aleatoria.
- Se realizará una asignación de contraseñas de manera periódica.
- Las contraseñas se resguardarán de forma segura en las oficinas de Informática Electoral.
- Estará estrictamente prohibido registrar contraseñas en cualquier lugar del área de trabajo.

8.4.2 Comunicación cifrada de información

Para fortalecer los mecanismos de envío de la información a través de Internet, se implementarán firewalls con capacidad de encriptación de 256 bits, con esto generando canales seguros entre los CATD's, CCV's y Centro de Operación, además la comunicación a los servidores del sistema será a través de protocolos seguros en específico HTTPS, aunado a esto una doble autenticación de acceso. Dicho protocolo (HTTPS) es el mecanismo estándar a nivel internacional en materia de sistemas de comercio electrónico y servicios bancarios en línea.

8.4.3 Implementación de red segura y estructura de servidores

A la par del uso de protocolos cifrados para el envío de la información, se establecerá una red privada virtual (VPN) con nivel de encriptación de 256 bits entre los equipos de cómputo instalados en los CATD's y en oficinas centrales del COPREP con los servidores que alojen los sistemas del PREP. Cabe señalar que solamente los equipos que estén dados de alta en dicha red privada podrán acceder al sistema, incrementando con ello su nivel de seguridad.

Los firewalls instalados en CATD's / CCV's y Centro de Operación, tendrán reglas que permitirán el acceso únicamente a los equipos de cómputo necesarios y estrictamente a los servicios que se requieren.

Esta red segura contempla el uso de sistemas de protección contra ataques de diversos tipos, tales como: Ataques "Hombre en el Medio" (MITM) que permiten interceptar el tráfico entre un servidor y un equipo de cómputo, ataques de "DNS rebind" que permiten convertir un equipo en un proxy de red, entre otros.

El almacenamiento de la información proveniente de los CATD's, se realizará en al menos dos servidores locales que trabajan en espejo o equivalente, que permite respaldar la información de un servidor a otro en tiempo real, por si alguno de los dos sufriera algún daño, la información seguirá disponible.

8.4.4 Mecanismos de redundancia de información y comunicación

En caso de existir cortes de señal de Internet en algún componente de la red privada, cada CATD, CCV y Centro de Operaciones deberá contar con un enlace alterno, para mantener comunicación con los servidores del sistema.

Ejemplos de servicio de Internet en Centro de Operaciones:

- ISP1 como principal, con ancho de banda suficiente para sostener la operación fluida y al menos un 50% de excedente.
- ISP2 como secundario, con ancho de banda suficiente para sostener la operación fluida y al menos un 50% de excedente.

8.4.5 Bitácora de operaciones

Todo sistema de captura con múltiples usuarios debe contar con un control o bitácora de operaciones realizadas en el sistema, que incluya desde fecha y hora de ingresos y salidas del sistema hasta registro de operaciones de captura y consulta de todos los usuarios que tengan contraseña válida para utilización del sistema.

8.4.6 Protección de sitio web público

Para la publicación del sitio web público, se contará con un servicio de protección de ataques DDoS con capacidad de 100 Gbps, un firewall de aplicaciones web (WAF por sus siglas en inglés) y una red de entrega de contenidos (CDN por sus siglas en inglés) con más de 200 puntos de presencia a nivel mundial y capacidad de entregar al menos 50 Gbps de sitio web "limpio".

Este servicio mitigará los posibles ataques y enviará las peticiones legítimas a un balanceador de carga redundante con capacidad de 250,000 conexiones únicas.

El balanceador de carga redundante enviará las peticiones a los servidores web necesarios para entregar los contenidos, pudiendo ser desde 2 hasta 10, dependiendo del probable número de visitantes que espere el sitio web público.

8.4.7 Listado de verificación de seguridad

Con el fin de fortalecer la gestión y seguimiento de las actividades e infraestructura se recomienda la generación de listas de habilitación de seguridad de los componentes tecnológicos que se utilizarán en los simulacros y el día de la jornada electoral.

8.4.8 Seguridad de los datos

Para realizar el proceso PREP, Informática Electoral suministrará y hará la configuración y pruebas necesarias de los siguientes equipos informáticos en cada CATD y en su caso CCV:

- Equipo para conectividad y seguridad de red: Firewall perimetral, realizará el balanceo de ancho de banda de los internet, habilitación de la red privada virtual.
- Equipo concentrador de red: Se interconectarán los equipos de cómputo y tecnológicos para crear una red LAN.
- Teléfono IP: Equipo configurado con una línea y extensión interna, la cual se comunicará entre CATD's y COPREP mediante VPN.
- Cableado de red: Todos los equipos de cómputo se comunicarán mediante cableado Ethernet categoría 5e con una velocidad de 10/100 Mbps como mínimo en los CATD.
- Y, cableado Ethernet categoría 6 en el caso de los CCV.

8.5 Seguridad física en CATD y CCV

Informática Electoral realizará las adecuaciones pertinentes con el objetivo de lograr que los centros de trabajo designados por el IEC cuenten con las siguientes características:

- El inmueble debe de contar con excelentes condiciones de construcción para evitar posibles filtraciones de aire y agua que dañen el equipo tecnológico. También debe de contar con facilidad para la instalación de servicios externos, tales como telefonía e internet.
- Extintores de CO2, que no dañe el equipo de cómputo al ser usados, distribuidos 1 cada 300 metros cuadrados de acuerdo con lo indicado en la NOM-002-STPS-2010.
- Área libre de ventanas, en caso de existir estas deben de contar con protecciones y cerrojo.
- Es deseable que solo se cuente con una puerta de acceso, la cual debe de contar con cerrojo y acceso biométrico para el control de acceso al personal.
- En el caso de las instalaciones donde vayan a trabajar más de 50 personas, será recomendable que el recinto cuente con salida de emergencia.
- Conexiones eléctricas suficientes para la conexión de los equipos informáticos: Se debe de entregar una conexión de corriente eléctrica regulada y aterrizada a tierra, la cual se conectará al UPS.

- Se verificarán que los espacios de trabajo del PREP se mantengan libres de líquidos y comida. Asimismo, se indicará la prohibición del uso de teléfonos celulares (estos únicamente podrán ser utilizados fuera de las instalaciones del CATD), memorias USB, audífonos u otros dispositivos ajenos a la operación durante el desarrollo del Programa.
- Se contará con una planta de energía de emergencia con capacidad suficiente para garantizar la operación continua de los equipos y dispositivos que forman parte de los CCV. Asimismo, se dispondrá de una planta de energía portátil para asegurar el suministro eléctrico en cada uno de los 16 CATD.
- Cualquier intento de acceso irregular a recintos o equipos (accesos fuera de horario, cantidad de personal diferente del esperado, etc.) debe ser reportado de manera automática mediante alertas oportunas al personal responsable. El acceso al sistema informático fuera de horarios autorizados se encontrará controlado desde la central.
- El IEC contará con el apoyo de la fuerza pública el día de la Jornada Electoral para los espacios destinados a la operación del PREP.
- Se implementará monitoreo mediante circuito cerrado de televisión (CCTV) en los CCV, con acceso permanente para el personal autorizado del IEC, tanto a imágenes en tiempo real como a grabaciones.
- Sistema de ventilación: Con capacidad de abastecimiento para toda el área CATD y CCV.

8.6 Buenas prácticas en el manejo de información sensible

Durante el desarrollo del PREP se observarán buenas prácticas en el manejo de información sensible, tales como:

- Las comunicaciones sobre información sensible no deben llevarse a cabo en lugares donde puedan ser escuchadas.
- Documentos sensibles no deben dejarse a la vista;
- 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;
- Documentos sensibles que ya no son necesarios deben destruirse inmediatamente, o colocados en contenedores apropiados para su posterior destrucción;
- Conversaciones telefónicas sobre temas sensibles deben llevarse a cabo de manera discreta;
- Cuando se trate un tema relativo a una persona en particular, confirmar de quién se está hablando antes de hacerlo;
- Si la persona a quien se quiere localizar no se encuentra, únicamente dejar el nombre y teléfono a donde deberá llamar cuando esté disponible;
- Mantener bajo el volumen del altavoz;
- Evitar colocar información sensible en memorias USB u otros medios de almacenamiento de datos;

- Si un dispositivo móvil es robado o extraviado debe ser reportado inmediatamente al jefe inmediato;
- Tener cuidado al incluir cualquier información que pueda ser considerada como confidencial en un mensaje de correo electrónico;
- Ser particularmente cuidadoso al enviar archivos adjuntos, y tener en cuenta que archivos adjuntos recibidos pueden ser fuente de malware;
- Si la información enviada es confidencial incluir una nota informativa sobre este hecho al final;
- Verificar siempre los destinatarios antes de enviar información confidencial.
- Verificar siempre los campos "para", "cc", "bcc", especialmente cuando se aplica la acción "responder a todos".

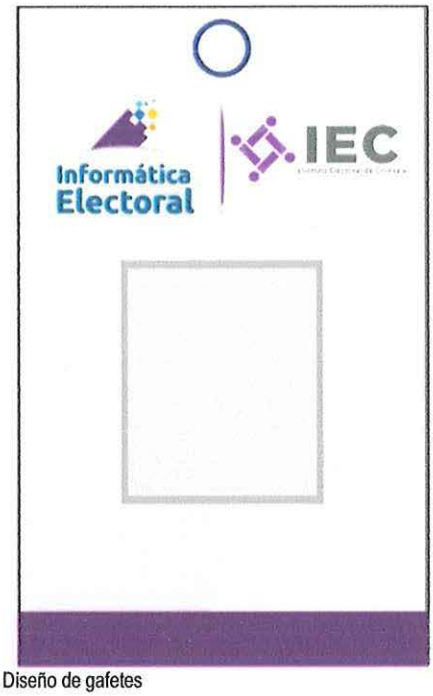
8.7 Seguridad personal

8.7.1 Identificaciones y detección de intrusos

Se implementará una estrategia para asegurar que el acceso a los CATD y CCV's sea restringido a solo el personal autorizado por Informática Electoral y el IEC. Se mantendrá el registro de los accesos.

Para tener una mayor seguridad en los centros, el personal que se encuentre dentro de cada centro deberá portar su identificación oficial, la cual tiene en su diseño: en la parte frontal, el logo de Informática Electoral, fotografía del portador, nombre y puesto; y en la parte trasera de la identificación, la dirección de Informática Electoral, código QR, firma de autorización, clave de elector, tipo de sangre, correo, vigencia de identificación, logo del IEC y logo de IE.

Vista frontal Vista trasera



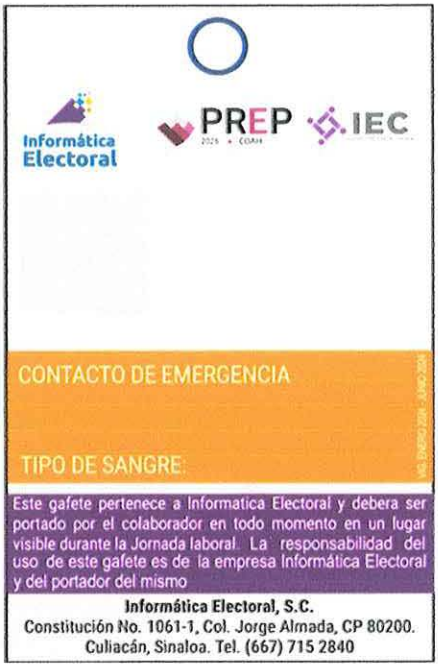


Tabla 7. Diseño de gafetes

8.7.2 Chalecos

Todo el personal deberá portar chalecos oficiales que lo identifiquen como miembro del personal contratado, las cuales deberán tener los colores establecidos por Informática Electoral y el IEC. Los colores serán establecidos de acuerdo con el puesto que funja, para efectos de la presente propuesta se sugieren los siguientes:

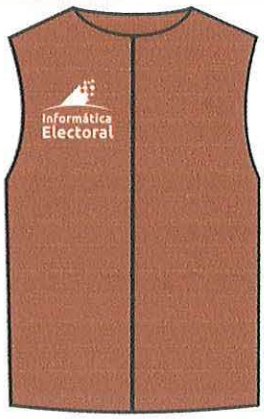
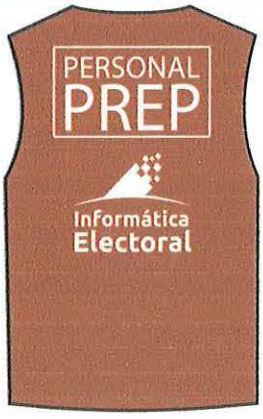
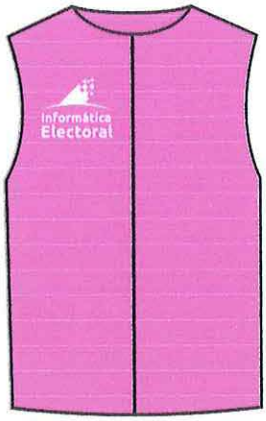
Vista frontal	Vista trasera
	

Tabla 8. Diseño chaleco para coordinador CATD/CCV

Vista frontal	Vista trasera



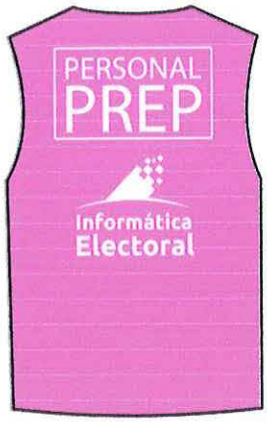


Tabla 9. Diseño chaleco para Capturista / Verificador

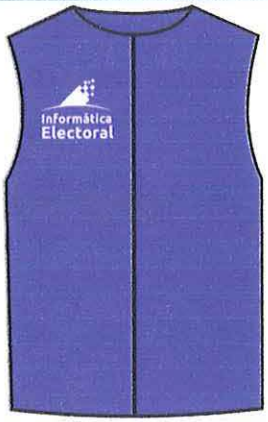
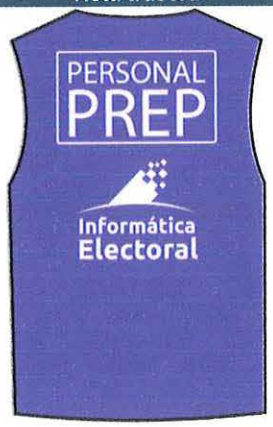
Vista frontal	Vista trasera
	

Tabla 10. Diseño chaleco para digitalizador

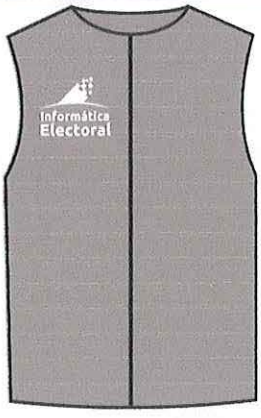
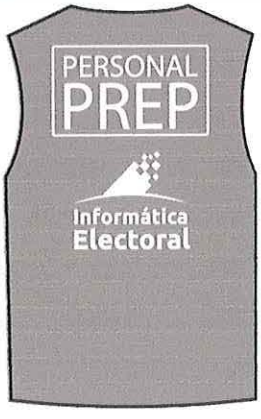
Vista frontal	Vista trasera
	

Tabla 11. Diseño chaleco para acopiador

Vista frontal	Vista trasera

Tabla 12. Diseño chaleco para personal del COPREP

Monitoreo por video CCTV en los CATD y CCV, teniendo acceso en cualquier momento el personal autorizado del IEC, tanto a las imágenes en tiempo real, como a las grabaciones.

No se permitirá el uso de dispositivos móviles de comunicación o fotográficos al interior de las instalaciones, para esto se instalarán 1 línea de Voz IP a las Oficinas de Coordinación.

8.7.3 Seguridad en el acceso a la aplicación móvil

La seguridad en el acceso a aplicación móvil tiene contemplados los siguientes puntos:

- Uso de token (el token tiene una expiración de 2 horas el cual sólo podrá ser utilizado por el usuario al que sea asignado al inicio de la jornada y puede ser configurable con respecto a lineamientos PREP).
  La seguridad en celulares:
  - Los celulares no deben ser root (para PREP Casilla).
  - Las digitalizaciones se guardarán en formato .jpg y esta se almacena en un espacio reservado con acceso único para la aplicación, haciendo que el uso de cualquier otra aplicación de galería no pueda acceder a las digitalizaciones.
  - Las digitalizaciones se encriptarán en SHA: 256 (HASH) el cual se genera al digitalizar el acta desde el dispositivo móvil, al enviarla a MCAD para su identificación se genera otro código el cual se compara con el primero que se generó, si estos son iguales se envía, al llegar al siguiente MCAD para su foliación se genera un 3er HASH que se compara con los primeros, este proceso se realiza para validar que la digitalización no haya sido modificada.
  - Los celulares estarán restringidos para evitar que los usuarios puedan desactivar el servicio de Geolocalización.
  - El uso de geolocalización permite monitorear si el usuario se mueve de la zona en la que se encuentra la casilla donde se le ha asignado, si este se encuentra fuera de la zona asignada la aplicación no permite captura de actas.
  - El personal operativo tendrá el siguiente proceso para:

a) Personal Operativo: Se le asignará un usuario y contraseña, el cual al iniciar sesión se relacionará con el IMEI del celular y generará un token el cual no permitirá que el usuario inicie sesión en otro celular.
b) Al iniciar la jornada la aplicación utilizará la localización para hacer comparación con la localización de la casilla y permitir el uso de este si se encuentra dentro de la zona establecida en la casilla.

- El envío de imágenes será por medio del uso de datos / internet, si no se cuenta con datos la aplicación almacenará una cola de imágenes para que al llegar a una zona con acceso a internet se finalice el envío de imágenes.

Previo a documentar las estrategias de gestión de riesgos resultantes de las evaluaciones, se analizará cuales procedimientos y estrategias no serían riesgosas documentarlas, considerando la naturaleza pública del plan de seguridad, las que resulten aceptables serán documentadas en dicho plan, dicho análisis se realizará en consenso con el IEC.

9 Plan de concientización

El plan de concientización es un programa formal que tiene como propósito capacitar y sensibilizar a los colaboradores de Informática Electoral en materia de las posibles amenazas (principalmente las de amenazas de seguridad de la información) y como gestionarlas.

9.1 Objetivo del plan de concientización

El objetivo es que las y los usuarios que intervienen en el proyecto, de acuerdo con sus atribuciones, puedan conocer los riesgos y las amenazas que enfrenta el PREP, así como saber la forma en que pueden apoyar para minimizar dichos riesgos o prevenir algún incidente de seguridad.

9.2 Alcance del plan de concientización

Abarca desde la definición de la situación actual a través de encuestas y/o pruebas de conocimiento en materia de seguridad de la información, pasando posteriormente por capacitación y concientización hasta la evaluación del personal capacitado con el objetivo de medir la efectividad de la capacitación.
Así mismo, el alcance especifico en la capacitación es el siguiente:

- Sensibilización sobre riesgos de seguridad de la información.
- Promoción de buenas prácticas.
  - Desarrollo seguro.
  - Concientización del SGSI.
  - Herramientas y técnicas de configuración segura de servicios digitales.
  - Gestión de incidentes.
  - Planes de seguridad y continuidad.
- Divulgación de políticas y procedimientos.
- Cumplimiento normativo.

Es importante señalar que no todos los colaboradores llevarán la misma capacitación, ya que, los contenidos por impartir dependerán del rol de cada colaborador en el proyecto.

9.3 Situación actual

Para que el plan de concientización tenga la efectividad deseada, es crucial entender las necesidades de capacitación que tienen los colaboradores, mismas que se buscarán comprender a través de la realización de una encuesta de conocimientos en materia del PREP, modelo de servicio y seguridad de la información, a continuación, se puede observar el cuestionario planteado:

1. ¿Qué significa PREP?
    a. Programa de Recuento Electoral Paralelo.
    b. Programa de Resultados Electorales Preliminares.
    c. Proceso de Registro de Electores y Participación.
    d. Ninguna de las anteriores.
2. ¿Alguna vez has sido víctima de algún hackeo en tus dispositivos laborales o personales? De haberlo sido y si está en tus posibilidades, detalla el acontecimiento y si tuvo o no solución y su causa más probable.
    a. Si.
    b. No.
    c. No, pero conozco alguien que sí.
    Explicación de la situación:
3. ¿En tus palabras, como definirías la seguridad de la información?
4. ¿Cuáles son los 3 pilares de seguridad de la información?
    a. Confidencialidad, Disponibilidad e Integridad.
    b. Confidencialidad, Privacidad y Veracidad.
    c. Información, Confidencialidad, Datos.
5. ¿Qué conoces como phishing?
6. ¿Has vivido situaciones en las que hayas tenido que aplicar algún plan de seguridad y continuidad? Si es así y está dentro de tus posibilidades, detalla la situación.
    a. Si.
    b. No.
    c. Detalla la situación:
7. Subraya los equipos que sabes utilizar:
    a. Extintor de incendios.
    b. Cámaras de vigilancia.
    c. Planta generadora de energía eléctrica.
    d. IDS e IPS.
    e. Controles de acceso físico.
    f. Software de antivirus.
    g. Firewall.
    h. Herramientas de criptografía.
    i. Herramientas de gestión de contraseñas.
8. ¿Qué medidas de seguridad de la información has tomado?
9. ¿Qué métodos para la evaluación de riesgos conoces?
10. ¿Estas familiarizado con alguna metodología de gestión de riesgos?

9.4 Materiales de capacitación

Informática Electoral dependiendo del tipo de capacitación, brindará los siguientes materiales de capacitación:

- Procedimientos documentados, mismos que podrán encontrarse en un manual de operaciones o en el repositorio utilizado por Informática Electoral.
- Presentaciones en PowerPoint.
- Equipo de cómputo.
- Celulares.
- Acceso a internet y servicios de correo y mensajería.
- Guías rápidas.

9.5 Plan de trabajo

Personal por capacitar	Contenido	Actividades por desarrollar	Recursos y materiales didácticos	Tiempo	Responsable
Equipo de Desarrollo	-Sensibilización sobre riesgos de seguridad de la información. -Promoción de buenas prácticas. -Desarrollo seguro. -Concientización del SGSI. -Herramientas y técnicas de configuración segura de servicios digitales. -Gestión de incidentes. -Planes de seguridad y continuidad. -Divulgación de políticas y procedimientos. -Cumplimiento normativo.	-Presentación mediante técnica grupal, a elección del facilitador. -Explicación del SGSI de Informática Electoral y del contenido aplicable. -Sesión de preguntas y respuestas. -Aplicación de cuestionario de opción múltiple. -Recapitulación del tema completo.	-PowerPoint con el tema completo. -Prueba objetiva. (cuestionario con 10 ítems, de opción múltiple) -Pantalla para proyección. -Un proyector. -Equipo de cómputo. -Celulares.	10 horas	Gerente de Procesos y Calidad.
COPREP, Agentes de Soporte Técnico, Agentes de Personal y Supervisor Logístico	-Sensibilización sobre riesgos de seguridad de la información. -Promoción de buenas prácticas. -Concientización del SGSI. -Gestión de incidentes. -Planes de seguridad y continuidad. -Divulgación de políticas y procedimientos.	-Presentación mediante técnica grupal, a elección del facilitador. -Explicación del SGSI de Informática Electoral y del contenido aplicable. -Sesión de preguntas y respuestas. -Aplicación de cuestionario de opción múltiple. -Recapitulación del tema completo.	-PowerPoint con el tema completo. -Prueba objetiva. (cuestionario con 10 ítems, de opción múltiple). -Pantalla para proyección. -Un proyector. -Equipo de cómputo. -Celulares.	6 horas	Gerente de Procesos y Calidad.

	-Cumplimiento normativo.				
Personal Operativo (Coordinadores de CATD y en su caso CCV, capturistas / verificadores, acopiadores y digitalizadores)	-Sensibilización sobre riesgos de seguridad de la información. -Promoción de buenas prácticas. -Concientización del SGSI. -Gestión de incidentes. -Planes de seguridad y continuidad. -Divulgación de políticas y procedimientos. -Cumplimiento normativo.	-Presentación mediante técnica grupal, a elección del facilitador. -Explicación del SGSI de Informática Electoral y del contenido aplicable. -Sesión de preguntas y respuestas. -Aplicación de cuestionario de opción múltiple. -Recapitulación del tema completo.	-PowerPoint con el tema completo. -Prueba objetiva. (cuestionario con 10 ítems, de opción múltiple) -Pantalla para proyección. -Un proyector. -Equipo de cómputo. -Celulares.	6 horas	Coordinador de Personal y Talento
Auxiliares de CCV, guardia de seguridad.	-Sensibilización sobre riesgos de seguridad de la información. -Planes de seguridad y continuidad. -Divulgación de políticas y procedimientos. -Cumplimiento normativo.	-Presentación mediante técnica grupal, a elección del facilitador. -Explicación del SGSI de Informática Electoral y del contenido aplicable -Sesión de preguntas y respuestas. -Aplicación de cuestionario de opción múltiple. -Recapitulación del tema completo.	-PowerPoint con el tema completo. -Prueba objetiva. (cuestionario con 10 ítems, de opción múltiple) -Pantalla para proyección. -Un proyector. -Equipo de cómputo. -Celulares.	3 horas	Coordinador de Personal y Talento

Tabla 13. Plan de capacitación

9.6 Modelo de concientización

Ilustración 2. Modelo de concientización

9.7 Evaluación de concientización

Para evaluar la efectividad del plan de concientización se realizará nuevamente una encuesta a los colaboradores que ya fueron capacitados, donde se incluirán los mismos reactivos de la encuesta inicial, más algunos reactivos extra, observándose de la siguiente manera:

1. ¿Qué significa PREP?
    a. Programa de Recuento Electoral Paralelo.
    b. Programa de Resultados Electorales Preliminares.
    c. Proceso de Registro de Electores y Participación.
    d. Ninguna de las anteriores.
2. ¿Alguna vez has sido víctima de algún hackeo en tus dispositivos laborales o personales? De haberlo sido y si está en tus posibilidades, detalla el acontecimiento y si tuvo o no solución y su causa más probable.
    a. Si.
    b. No.
    c. No, pero conozco alguien que sí.

    Explicación de la situación:
3. ¿En tus palabras, como definirías la seguridad de la información?
4. ¿Cuáles son los 3 pilares de seguridad de la información?
    a. Confidencialidad, Disponibilidad e Integridad.
    b. Confidencialidad, Privacidad y Veracidad.
    c. Información, Confidencialidad, Datos.
5. ¿Qué conoces como phishing?
6. ¿Has vivido situaciones en las que hayas tenido que aplicar algún plan de seguridad y continuidad? Si es así y está dentro de tus posibilidades, detalla la situación.
    a. Si.
    b. No.
    c. Detalla la situación:
7. Subraya los equipos que sabes utilizar:
    a. Extintor de incendios.
    b. Cámaras de vigilancia.
    c. Planta generadora de energía eléctrica.
    d. IDS e IPS.
    e. Controles de acceso físico.
    f. Software de antivirus.
    g. Firewall.
    h. Herramientas de criptografía.
    i. Herramientas de gestión de contraseñas.
8. ¿Qué medidas de seguridad de la información has tomado?
9. ¿Qué métodos para la evaluación de riesgos conoces?
10. ¿Estas familiarizado con alguna metodología de gestión de riesgos?
11. ¿Cómo se evalúan los riesgos en Informática Electoral de acuerdo con su nivel de contingencia y su probabilidad de ocurrencia?
12. ¿Cuál es la forma correcta de actuar desde tu rol ante una incidencia de nivel bajo?
13. ¿Cuál es la forma correcta de actuar desde tu rol ante una emergencia?

10 Protocolo de seguridad sanitaria

En concordancia con la notificación de la OMS sobre el término de la emergencia sanitaria a nivel mundial por COVID-19, México realizó una evaluación local que permitió demostrar el fin de la misma, el nueve de mayo de 2023, mediante la publicación en el Diario Oficial de la Federación, se estableció que la vigilancia epidemiológica continuará exclusivamente bajo la estrategia centinela en Unidades de Salud Monitoras de Enfermedad Respiratoria Viral (USMER) y con la confirmación de casos mediante la prueba de RT-PCR.

Se aclara que, sin importar que no se declare una contingencia sanitaria todo el contenido del numeral 10 así como el 11.1 del presente documento es de observancia obligatoria.

Sin embargo, **en caso de nuevamente declararse activa la contingencia sanitaria, Informática Electoral declara lo siguiente**:

Todas las medidas señaladas en el apartado **11** del presente protocolo son de observancia obligatoria para las personas que participen, de manera directa o indirecta, tanto en el desarrollo del Programa de Resultados Electorales Preliminares (PREP), como en sus respectivos simulacros, y tienen por objeto regular su actuación, así como implementar las medidas pertinentes para proteger su salud y prevenir la dispersión y transmisión enfermedades infecciosas respiratorias.

Se limitará el acceso, o en su caso, la permanencia de persona alguna que incurra de manera frecuente con las medidas aquí señaladas; en áreas PREP (COPREP) y, en particular, en los Centros de Acopio y Transmisión de Datos (CATD) y en los Centros de Captura y Verificación (CCV).

El incumplimiento de las disposiciones contenidas en el presente protocolo por parte de colaborador o colaboradora de Informática Electoral es causa de la aplicación de la política de medidas disciplinarias.

Las disposiciones contenidas en este protocolo se aplicarán con un enfoque de derechos humanos.

10.1 Medidas preventivas

Son medidas que se implementan para prevenir un posible contagio dentro de nuestras instalaciones:

- Proveer dispensadores con soluciones a base de alcohol gel al 70% a libre disposición en distintos puntos de los Centros de Acopio y Transmisión de Datos (CATD), en los Centros de Captura y Verificación (CCV), y en las instalaciones de Informática Electoral.
- Tener disponibilidad de cubrebocas en los Centros de Acopio y Transmisión de Datos (CATD), en los Centros de Captura y Verificación (CCV), así como en las instalaciones de Informática Electoral para todo el personal que lo requiera.
- Es de uso obligatorio el cubrebocas cuando algún colaborador presente síntomas de enfermedades respiratorias dentro de los Centros de Acopio y Transmisión de Datos (CATD),

Centros de Captura y Verificación (CCV), o en su defecto, en las instalaciones de Informática Electoral.

11 Estrategias de control durante contingencia

Las siguientes estrategias de control son indispensables y fundamentales para contener la diseminación de enfermedades infecciosas respiratorias, y deberán implementarse en todas las áreas de los Centros de Acopio y Transmisión de Datos (CATD), en los Centros de Captura y Verificación (CCV), y, en general en todos los espacios donde tiene participación el personal de Informática Electoral (COPREP y CENTRAL PREP).

Asimismo, deberán ser observadas en todo momento por toda persona que, de manera directa o indirecta, participe tanto en el PREP como en sus respectivos simulacros, con el fin de apoyar para evitar los riesgos de contagio de enfermedades infecciosas respiratorias, para ello se dará a conocer su contenido durante las capacitaciones que se impartan.

11.1 Promoción de la salud

Implica la orientación y organización de toda persona que participe en las diversas tareas y actividades de Informática Electoral, para prevenir y controlar la propagación de enfermedades infecciosas respiratorias, en actividades que requieran el uso de instalaciones públicas o privadas que impliquen el contacto con personas que presenten síntomas posibles de contagio:

- Información general sobre enfermedades infecciosas respiratorias, los mecanismos de contagio, síntomas que ocasionan y las mejores maneras de prevenir el contagio de otras personas.
- La importancia que tiene el no acudir al trabajo con síntomas compatibles con infecciones respiratorias para no ser un riesgo de potencial contagio para otras personas.
- Sensibilizar al personal involucrado en la necesidad de cumplir con sus funciones con apego a las disposiciones sanitarias, en un ánimo de compromiso y disponibilidad para beneficio de todas y todos.
- Orientar al personal sobre medidas de protección de la salud (lavado frecuente de manos, etiqueta respiratoria, saludo a distancia y recuperación efectiva).
- Lavarse las manos frecuentemente con agua y jabón, o bien, usar soluciones a base de alcohol gel al 70%.
- La práctica de la etiqueta respiratoria: cubrirse nariz y boca al toser o estornudar con un pañuelo desechable o el ángulo interno del brazo.
- No escupir. Si es necesario hacerlo, utilizar un pañuelo desechable y tirarlo a la basura; después lavarse las manos.
- Evitar tocarse la cara con las manos sucias, sobre todo nariz, boca y ojos.
- Limpiar y desinfectar superficies y objetos de uso común en oficinas, sitios cerrados, transporte, centros de reunión, entre otros.

- Procurar, en la medida de lo posible, mantener una sana distancia durante los contactos (este punto en particular recibirá tratamiento como recomendación, ya que solo se aplicará en la medida en la que los inmuebles lo permitan).
- Higienizar: Aplicar un conjunto de procedimientos que tienen por objeto la eliminación de agentes patógenos; realizar la limpieza y desinfección de objetos o lugares, con agua y jabón, además de utilizar toallas desinfectantes, o solución desinfectante. Conforme la recomendación de la autoridad sanitaria, la frecuencia de la limpieza y desinfección se determinará dependiendo del escenario en el que se encuentre el lugar/superficie y el flujo de personas.

Para facilitar las labores de difusión de estas medidas, Informática Electoral, pondrá a disposición del personal que participe en las diversas tareas y actividades del PREP 2026 infografías y material de comunicación elaborado por las autoridades de salud a nivel federal, estatal o municipal y adaptado por la empresa.

11.2 Sana distancia

La sana distancia comprende dos vertientes:

1. Ante la presencia de síntomas como tos y/o fiebre y/o dolor de cabeza; dolor o ardor de garganta, ojos rojos, dolores en músculos o articulaciones (malestar general); y dificultades para respirar o falta de aire en sus pulmones, el personal no deberá asistir a los centros de trabajo; y en su caso acudir a los centros de salud correspondientes.
2. Favorecer una distancia mínima de 1.5 metros, el uso de equipo de protección personal (cubrebocas o caretas) en caso de presentar síntomas y la adecuación de los espacios y áreas de trabajo, para lo cual se deberán establecer las siguientes recomendaciones (mínimas, pero no limitativas):

    a. Garantizar la disponibilidad permanente de agua potable, jabón, papel higiénico, gel con base de alcohol y toallas desechables para el secado de manos.
    b. Establecer horarios alternados de toma de alimentos

11.3 Control de ingreso-egreso

Instrumentación de un control de ingreso-egreso del personal, proveedores o visitantes que permita lo siguiente:

- Establecer un filtro de supervisión en la entrada de las instalaciones de los CATD y/o CCV, consistente en un módulo en el que a cada una de las personas que ingresan se les aplique gel antibacterial. Adicionalmente se deberá contar con un termómetro digital o infrarrojo para la toma de temperatura en casos de sospecha o presencia de síntomas. El filtro deberá ser atendido por las personas que se designen para tal efecto, previa capacitación y dotación de equipo de protección personal para cumplir con esta función.

- Para el personal que se detecta con signos de enfermedades respiratorias y/o temperatura corporal mayor a 37.5 °C, dotarlas de un cubrebocas y remitirlas al domicilio particular y/o servicios médicos.

Proporcionar solución gel base alcohol al 70% para el lavado de manos y verificar el uso apropiado de cubrebocas en presencia de signos de enfermedad respiratoria

11.4 Medidas de prevención de contagios

Son acciones que se realizan para prevenir un posible contagio, es decir, las acciones que lleva a cabo Informática Electoral para prevenir entrada de infecciones respiratorias a los recintos de trabajo. Entre éstas quedan comprendidas cuestiones de higiene, limpieza y sana distancia.

1. Proveer dispensadores con soluciones a base de alcohol gel al 70% a libre disposición en distintos puntos de los Centros de Acopio y Transmisión de Datos (CATD), en los Centros de Captura y Verificación (CCV), y en las instalaciones de Informática Electoral.
2. Concientizar al personal involucrado en el uso cotidiano de productos sanitarios.
3. Contar con depósitos suficientes de productos desechables y de uso personal, procurando la limpieza continua de los mismos.
4. Garantizar que los sanitarios cuenten con lavamanos y con condiciones adecuadas para la limpieza del personal (agua, jabón y toallas de papel desechable).
5. Establecer un programa de limpieza y mantenimiento permanente, utilizando los productos de limpieza adecuados para prevenir la propagación de virus.
6. Uso de acrílicos para la división de lugares de trabajo.

11.5 Equipos de contagio

Se refiere al equipo de protección personal para minimizar el riesgo de infección en el personal en el desempeño de sus actividades.

Durante su permanencia en las instalaciones de los Centros de Acopio y Transmisión de Datos (CATD), en los Centros de Captura y Verificación (CCV), y en general, en todas las áreas PREP, las personas con signos de enfermedades respiratorias deberán de portar de manera obligatoria y adecuada el cubre bocas. El cubre bocas deberá de colocarse de manera tal que cubra el área de la nariz y la boca de la persona.

12 Recomendaciones de atención sanitaria

Informática Electoral garantizará que las siguientes medidas sanitarias se observen en todo momento, con el objetivo de desarrollar las diversas actividades relacionadas con la Operación del Programa de Resultados Electorales Preliminares (PREP), así como sus respectivos simulacros, se realicen en condiciones que permitan mitigar el riesgo de contagios, salvaguardando con ello la salud e integridad del personal y de la ciudadanía involucrada.

12.1 Recomendaciones generales

- Sensibilizar a todo el personal en las recomendaciones sanitarias por implementarse.
- Proporcionar, en todos los accesos a las instalaciones, gel antibacterial.
- Designar al personal necesario para asegurarse del uso de gel antibacterial y la toma de temperatura corporal de las personas que presenten síntomas antes de ingresen a las instalaciones, con un termómetro digital infrarrojo de tipo pistola, para evitar el contacto (únicamente en caso de que se declare una contingencia sanitaria).
- Colocar dispensadores de gel antibacterial en sitios visibles dentro de todos los espacios y áreas de trabajo, para su uso de manera frecuente. De preferencia, colocar señalamientos que ayuden a la fácil localización de estos.
- Colocar carteles de orientación sobre la correcta aplicación de las medidas sanitarias al interior de las instalaciones.
- Lavarse las manos constantemente, con agua y jabón durante por lo menos 20 segundos. En caso de que no sea posible, aplicarse gel antibacterial con la misma frecuencia. Tener en cuenta el lavado en las siguientes situaciones:

  Lave sus manos, antes de:

  - Consumir alimentos o bebidas.
  - Iniciar las actividades de trabajo.

  Después de:

  - Estornudar y toser.
  - Ir al baño.
  - Estar en contacto con personas enfermas.
  - Manejo continuo de objetos de uso común, como teclados de computadora, impresoras, engrapadoras, teléfonos etc.
  - Durante el desarrollo de las actividades se procurará que los espacios se encuentren ventilados adecuadamente.

Se implementarán mecanismos de monitoreo y seguimiento a la salud del personal.

12.2 Medidas específicas durante el desarrollo del PREP y sus simulacros en periodo de contingencia

Adicionalmente a las medidas generales, para la operación y desarrollo del Programa de Resultados Electorales Preliminares (PREP), así como sus respectivos simulacros, se deberán adoptar las siguientes:

- Realizar, durante los días previos a los simulacros del PREP y a la Jornada Electoral, así como al finalizar los mismos, un operativo de limpieza y desinfección de los Centros de Acopio y Transmisión de Datos (CATD), de los Centros de Captura y Verificación (CCV) y Centro de Operaciones del PREP (COPREP).

- Se colocará en las diferentes estaciones y áreas de trabajo gel antibacterial base de alcohol al 70%, la ciudadanía involucrada desinfecte sus manos.
- Exhortar al personal involucrado en PREP a que, en caso de presentar síntomas de enfermedades infecciosas respiratorias, avisar previamente a sus superiores jerárquicos para efectos de tomar las medidas adecuadas y que no se vean afectadas las labores.
- Negar el acceso a las instalaciones de los Centros de Acopio y Transmisión de Datos (CATD), de los Centros de Captura y Verificación (CCV), y, en general, a las instalaciones de áreas PREP a cualquier persona que presente visiblemente uno o varios síntomas de enfermedades infecciosas respiratorias, o bien, con una temperatura superior a 37.5°C. Orientar a la persona en el supuesto, a que acuda una revisión médica.
- Dotar al personal de campo de toallas desinfectantes (un paquete).
- Durante su estancia en las instalaciones de áreas PREP y, en particular, en los Centros de Acopio y Transmisión de Datos (CATD) y en los Centros de Captura y Verificación (CCV), toda persona que presente síntomas de enfermedad respiratoria común deberá de portar de manera permanente y adecuada su cubrebocas.
- Tanto el personal en las oficinas, como el que realice trabajo de campo, en caso de presentar algún síntoma relacionado con enfermedades infecciosas respiratorias, deberá suspender sus actividades, dar aviso de inmediato a su superior jerárquico y acudir a revisión médica. El superior jerárquico deberá dar seguimiento al caso y mantener informado a las instancias superiores.
- Informar a la ciudadanía involucrada en las diversas actividades del PREP sobre las medidas sanitarias implementadas.

Exhortar al personal en PREP que participen, de manera directa o indirecta, tanto en el desarrollo del Programa de Resultados Electorales Preliminares (PREP), como en sus simulacros respectivos, a lavar y desinfectar sus manos constantemente.

13 Vigilancia y supervisión en periodo de contingencia

La Gerencia de Procesos y Calidad de Informática Electoral será responsable de realizar todas las acciones que sean necesarias para constatar la correcta implementación de este protocolo, para ello, podrá designar responsables de Vigilancia en los Centros de Acopio y Transmisión de Datos (CATD) y en los Centros de Captura y Verificación (CCV), cuya labor consistirá en:

- Verificar el establecimiento y seguimiento de las medidas de prevención y protección establecidas en el presente protocolo.
- Verificar la provisión constante de agua, jabón y toallas desechables, y de soluciones a base de alcohol gel al 70% en todas las áreas.
- Implementar y llevar a cabo los mecanismos de monitoreo y seguimiento a la salud del personal involucrado en las diferentes actividades del PREP.

14 Evaluación de riesgos posterior a la implementación de medidas de seguridad

A continuación, se presenta el análisis integral de los riesgos evaluados, una vez implementadas las medidas de seguridad previamente definidas.

Activo	Riesgo	Responsable del activo	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia (1 - 5)	Impacto (1 - 5)	Control actual	Nivel de riesgo
AC - Enlaces de internet	Falla parcial en el servicio	Departamento de Infraestructura y Seguridad / Proveedor de servicio de internet	Caída del servicio en enlace primario.	Enlace secundario deficiente.	2	3	Equipo perimetral realiza balancea el internet automático	6
	Falla en el servicio	Departamento de Infraestructura y Seguridad / Proveedor de servicio de internet	Caída simultanea de ambos enlaces.	Dependencia de dos proveedores.	1	5	Se cuenta con dispositivos móviles habilitados para el envío de las actas	5
	Lentitud del servicio	Departamento de Infraestructura y Seguridad / Proveedor de servicio de internet	Sobre carga de la red interna.	Ancho de banda insuficiente o equipo de red desactualizado	3	2	Monitoreo de tráfico y configuración de equipos según las necesidades	6
AC – Firewall	Configuración incorrecta	Departamento de Infraestructura y Seguridad	Configuración errónea o incompleta	Falta de revisión de validación	3	2	Agentes de Soporte Técnico capacitados y con guías rápidas de las configuraciones correspondientes.	6
	Fallo de hardware	Departamento de Infraestructura y Seguridad	Daño físico	Uso de hardware sin respaldo	2	3	Remplazo de equipo cuando se presenta la falla.	6
	Ataques externos	Departamento de Infraestructura y Seguridad	Ataques de denegación de servicio (DDoS)	Reglas insuficientes para mitigar ataques avanzados	2	3	Monitoreo constante, actualización de reglas.	6

AC – VPN	Acceso no autorizado	Departamento de Infraestructura y Seguridad	Robo de credenciales de acceso	Uso de contraseñas débiles	2	2	Implementación de contraseñas robustas	4
	Interceptación de datos	Departamento de Infraestructura y Seguridad	Ataques de intermediario (Man-in-the-Middle)	Configuración insegura o cifrado débil	2	3	Uso de protocolos de seguridad y redes aisladas.	6
	Saturación de conexiones	Departamento de Infraestructura y Seguridad	Exceso de usuarios o conexiones simultáneas	Falta de monitoreo.	2	2	Monitoreo en tiempo real del tráfico VPN sin acceso a usuarios externos	4
AC – UPS	Equipos sin energía eléctrica	Departamento de Infraestructura y Seguridad	Falla en el equipo	Mantenimiento inadecuado o desgaste del equipo	2	2	Capacitación y guías rápidas al personal para uso adecuado	4
	Obsolescencia tecnológica	Departamento de Infraestructura y Seguridad	Uso de equipos obsoletos	Falta de soporte o cambio de equipos.	1	4	Identificación de equipos obsoletos y sustitución de equipos.	4
	Tiempo insuficiente de respaldo	Departamento de Infraestructura y Seguridad	Baterías descargadas o dañadas	Uso excesivo	2	2	Reposición de batería.	4
AC – NVR	Fallo de funcionamiento	Departamento de Infraestructura y Seguridad	Daño físico del disco duro	Desgaste por uso continuo	1	3	Remplazo de disco duro	3
	Pérdida de grabaciones de eventos	Departamento de Infraestructura y Seguridad	Eliminación accidental o daño de los archivos	Falta de respaldos	1	5	Respaldo de grabaciones de eventos	5
AC – Switches	Fallo del dispositivo	Departamento de Infraestructura y Seguridad	Daño físico	Sobrecalentamiento y/o desgaste por uso	2	2	Ubicación en áreas ventilados y revisiones previas, así como Agentes de Soporte Técnico capacitados para reemplazarlos	4
	Congestión de la red	Departamento de Infraestruct	Saturación por tráfico no gestionado	Configuración inadecuada	2	3	Configuración de VLAN's para la	6

		ura y Seguridad					segmentación de tráfico.	
	Acceso no autorizado	Departamento de Infraestructura y Seguridad	Hackeo o configuraciones maliciosas	Falta de controles de acceso físico y/o lógico.	2	2	Implementación de protocolos de seguridad lógica y accesos físicos controlados.	4
	Pérdida de conectividad	Departamento de Infraestructura y Seguridad	Fallo de energía	Falta de respaldo de energía	2	3	Uso de enlaces y fuentes de alimentación redundantes	6
AC – Servidores	Fallo de hardware	Departamento de Infraestructura y Seguridad	Daño en componentes críticos	Desgaste por uso, sobrecalentamiento	2	3	Hardware instalado en un área climatizada y con componentes disponibles para cambiarlos	6
	Pérdidas de datos	Departamento de Infraestructura y Seguridad	Corrupción o eliminación de datos	Copias de seguridad insuficientes o no actualizadas	2	2	Implementación de políticas de respaldo	4
	Acceso no autorizado	Departamento de Infraestructura y Seguridad	Hackeo o robo de credenciales	Configuración débil de permisos y contraseñas	2	1	Uso de contraseñas robustas.	2
	Interrupción del servicio	Departamento de Infraestructura y Seguridad	Fallo de energía o conectividad	Falta de redundancia en energía y red	2	1	Uso de UPS, generadores de respaldo y redundancia en UPS.	2
ANC – Conmutadores telefónicos	Fallo de equipo	Departamento de Infraestructura y Seguridad	Daño del equipo	Picos de energía que dañen el equipo	2	1	Uso de UPS para proteger el equipo	2
	Interrupción del servicio	Departamento de Infraestructura y Seguridad / Proveedor de servicio de telefonía	Falla de conexión en la línea telefónica	Mala configuración de conmutador	1	3	Agentes de Soporte técnico realizarán configuraciones en el conmutador conforme sea necesario.	3
	Obsolescencia tecnológica	Departamento de Infraestructura y Seguridad	Dispositivos obsoletos funcionalmente	Falta de reemplazo de equipo obsoleto	1	3	Revisión previa de los equipos y sustitución de equipos obsoletos	3

AC - Red eléctrica	Interrupción del suministro eléctrico	Departamento de Infraestructura y Seguridad / Proveedor de energía	Corte de energía o fluctuaciones de voltaje	Ausencia de respaldo inmediato	2	2	Uso de UPS y generadores de respaldo de energía.	4
AC – Plantas de energía eléctrica	Falla en el arranque	Departamento de Infraestructura y Seguridad	Fallo mecánico o eléctrico	Falta de mantenimiento	2	2	Realización de pruebas de funcionamiento con capacitación	4
	Insuficiencia de combustible	Departamento de Infraestructura y Seguridad	Agotamiento del combustible	Dependencia de suministro externo	1	4	Disposición de combustible	4
AC – Equipos de cómputo portátil (Personal Operativo)	Robo de equipo	Coordinador de CATD/ CCV	Hurto de equipo	Falta de medidas de seguridad física	2	1	Implementación de candados de seguridad física	2
	Daño físico	Coordinador de CATD/ CCV	Golpes, caídas o derrames de líquidos	Manejo inadecuado del equipo	3	2	Capacitación y guías rápidas al personal para uso adecuado	6
	Pérdida de información	Coordinador de CATD/ CCV	Robo, sustracción de información	Puertos de USB, bandejas de CD y DVD, Bluetooth habilitados	2	2	Deshabilitación de puertos de USB, Bluetooth e inhabilitación de internet	4
	Acceso no autorizado	Coordinador de CATD/ CCV	Robo de credenciales o manipulación	Contraseñas débiles	2	2	Credenciales de administrador no proporcionadas a usuario final	4
AC – Escáneres	Mal funcionamiento durante la digitalización	Coordinador de CATD/ CCV	Configuración incorrecta	Falta de capacitación en el uso del equipo	2	3	Capacitación al personal sobre el manejo del equipo	6
	Daño por sobrecarga de trabajo	Coordinador de CATD/ CCV	Sobrecarga de documentos	Operación fuera de las especificaciones recomendadas	2	2	Capacitación y guías rápidas al personal para uso adecuado	4
	Interrupción del servicio	Coordinador de CATD/ CCV	Fallo eléctrico o de conectividad	Falta de respaldo eléctrico o redundancia en dispositivos	2	1	Uso de UPS y capacitación disponibilidad de equipos de respaldo.	2

	Pérdida de calidad en digitalizaciones	Coordinador de CATD/ CCV	Ajustes incorrectos	Acomodo inadecuado del Acta PREP	2	1	Capacitación y guías rápidas para digitalizaciones previas al envío	3
AC – Impresoras	Falla de equipo	Departamento de Infraestructura y Seguridad	Daño por uso continuo	Falta de mantenimiento	2	1	Mantenimiento preventivo y guías rápidas al personal para limpieza periódica	3
	Pérdida de documentos impresos	Coordinador de CATD	Documentos extraviados o recolectados por personal no autorizado	Falta de control en la recolección de impresiones.	2	1	Uso exclusivo de impresoras por coordinador	2
	Falta de conectividad	Departamento de Infraestructura y Seguridad	Fallo en la red o configuración incorrecta	Dependencia de la conectividad de red.	2	1	Pruebas de conectividad.	2
ANC – Cámaras de seguridad	Fallo de equipo	Departamento de Infraestructura y Seguridad	Daño físico	Falta de revisión o protección del equipo	2	2	Agente de soporte técnico capacitado para solucionar fallas o cambiar equipo	4
	Interrupción del servicio	Departamento de Infraestructura y Seguridad	Corte de energía o fallo en la red	Falta de respaldo eléctrico	2	3	Uso de planta de energía con guía de uso para su rápida implementación	6
ANC – Sillas y mesas	Lesiones al personal	Departamento de Personal y Talento / Coordinador de CATD/CCV	Mobiliario en mal estado	Uso de mobiliario dañado	2	2	Revisión y sustitución de mobiliario dañado	4
	Pérdida o robo	Departamento de Administración y Finanzas / Coordinador de CATD/CCV	Falta de control de inventarios	Falta de registro de los activos	2	2	Implementación de sistema de inventario	4
AC – DSA	Falla en el funcionamiento	Departamento de Infraestruct	Mal funcionamiento o daño mecánico	Falta de revisiones previas	2	3	Revisiones y pruebas del dispositivo antes de su	6

		ura y Seguridad					uso, así como capacitación y guías rápidas al personal para uso adecuado	
	Interrupción del servicio	Coordinador de CATD	Fallo eléctrico	Dependencia de suministro eléctrico	2	2	Uso de respaldo eléctrico (UPS)	4
	Pérdida o robo	Coordinador de CATD	Sustitución indebida del equipo	Falta de inventario	2	3	Registro de los equipos ubicados en cada CATD y cámaras de seguridad	6
	Daño físico	Coordinador de CATD	Golpes, caídas o manejo inadecuado	Ausencia de protocoles de manejo de equipos	2	1	Capacitación y guías rápidas al personal para uso adecuado	3
AC – Dispositivos móviles	Robo o pérdida	Coordinador de CATD	Extracción física o extravío	Falta de seguimiento de los equipos	2	2	Registro detallado, etiquetado de los equipos y protocolos de seguridad y cámaras de seguridad	4
	Ataques de malware	Coordinador de CATD	Instalación de aplicaciones no seguras	Falta de políticas para descargas	2	2	Deshabilitación de funcionabilidad para descargar o instalar aplicaciones	4
	Fallos en la conectividad	Coordinador de CATD	Problemas de red	Dependencia de conexiones de red	2	1	Disponibilidad de redes alternativas	2
AC – Servicios de datos móviles	Uso no autorizado	Coordinador de CATD	Consumo excesivo por actividades no relacionadas	Fata de restricciones en el uso de datos móviles	2	2	Políticas de uso de datos móviles y restricción	4
	Sobrecosto en el uso de datos	Departamento de Administración y Finanzas / Coordinador de CATD	Consumo de datos mayor al esperado	Falta de monitoreo o límites de datos contratados	2	3	Monitoreo de consumo y ajustes de planes de datos	6
AC- Bases de datos en servidores	Pérdida de datos	Departamento de Infraestructura y Seguridad	Fallo en el almacenamiento o daño físico del servidor	Falta de respaldo	1	3	Implementación de copias de seguridad automáticas y redundancia en	3

							almacenamiento	
	Acceso no autorizado	Departamento de Infraestructura y Seguridad	Robo de credenciales o configuración insegura	Contraseñas débiles y falta de cifrado	2	2	Uso de contraseñas robustas y cifrado de datos	4
	Ataques cibernéticos	Departamento de Infraestructura y Seguridad	Explotación de vulnerabilidades en infraestructura	Falta de actualizaciones y configuración de seguridad	2	2	Actualizaciones regulares, implementación de mecanismos de protección perimetral e interna.	4
	Interrupción del servicio	Departamento de Infraestructura y Seguridad	Sobrecarga del servidor o fallos eléctricos	Falta de escalabilidad y respaldo eléctrico	2	3	Uso de balanceadores de carga, planta eléctrica y monitoreo del servidor	6
AC – Actas digitalizadas	Interrupción de trasmisión de datos	Departamento de Infraestructura y Seguridad	Fallo en la red	Dependencia de la conectividad	2	1	Disponibilidad de redes alternativas	2
AC – MCAD	Acceso no autorizado	Departamento de Software e Implementación / Coordinador de CATD	Robo de credenciales o configuraciones inseguras	Tener la contraseña a la vista de cualquier persona	2	2	Asignación de permisos según roles y concientización al personal respecto al manejo de las contraseñas	4
	Alteración de información	Departamento de Software e Implementación / Coordinador de CATD	Identificación errónea del Acta	Falta de capacitación al personal respecto a la identificación de las Actas	2	3	Capacitación y guías rápidas al personal operativo para la identificación y foliación	6
	Interrupción del servicio	Departamento de Infraestructura y Seguridad	Fallo en la red	Dependencia de la conectividad	3	2	Monitoreo de red. Enlace alterno	6
AC – CVPREP	Error en la captura de los datos	Departamento de Software e Implementación / Coordinador de CCV	Errores humanos durante la digitalización	Falta de capacitación o supervisión	2	2	Capacitación al personal operativo, guías rápidas, dobles capturas y validaciones previas a la publicación.	4

	Acceso no autorizado	Departamento de Software e Implementación	Robo de credenciales	Contraseña a la vista del personal.	2	2	Concientización al personal de la importancia de la seguridad de la información	4
	Interrupción del servicio	Departamento de Infraestructura y Seguridad	Fallo en la red	Dependencia de la conectividad	3	2	Monitoreo de red. Enlace alterno	6
AC – PREP Casilla	Error en la digitalización de actas	Departamento de Software e Implementación / CAE	Captura incorrecta o de baja calidad en la imagen	Falta de capacitación o mal uso del dispositivo	2	2	Capacitación previa a los CAE y proporción de guías rápidas	4
	Bloqueo por intentos falidos de acceso	Departamento de Software e Implementación / CAE	Olvido de contraseñas o uso en dispositivos no autorizados	Asociación de la aplicación con el IMEI y límite de intentos fallidos.	3	2	Revisión y restablecimiento rápido de accesos por parte del Departamento de Software e Implementación.	6
	Fallo en el envío de actas	Departamento de Software e Implementación	Problemas de conectividad en la casilla	Dependencia de la red móvil	2	2	Almacenamiento local temporal con envío automático una vez que se recupere la conectividad	4
	Error en la asignación de secciones	Departamento de Software e Implementación / Departamento de Administración de proyecto	Archivo con datos incorrectos o inconsistencias	Validación de asignaciones únicamente cuando se reporta un problema	2	3	Corrección de las asignaciones tras notificación de inconsistencia	6
AC - Página web portal	Interrupción del servicio	Departamento de Desarrollo / Departamento de Infraestructura y Seguridad	Ataque DDoS	Falta de mitigación de tráfico anómalo	2	2	Firewall con limitación, así como protección ante DDoS	4
AC - Replicador de Base de Datos	Caída de replicación	Departamento de infraestructura y seguridad	Fallo en la red	Falta de redundancia	2	2	Se tienen contemplados servicios de red redundantes	4

ANC - Chat para comunicación COPREP – CATD – CCV	Interrupción de la comunicación	Departamento de Software e Implementación	Fallo en la red	Retraso en la actualización de la información	3	1	Opciones de comunicación alternativa	3
	Realización de actividades sin autorización	Coordinador de CATD/ CCV	Retraso de la comunicación	Retrabajo de las tareas asignadas	2	2	Definición de las actividades y capacitación	4
ANC – Difusores oficiales	Interrupción de la comunicación	Departamento de Software e Implementación	Fallo en la red	Retraso en la actualización de la información	3	1	Tener más de un proveedor de internet	3
	Falla en el servicio de Difusores activos	Departamento de Software e Implementación	Incumplimiento en las capacidades requeridas	Retraso y/o posible interrupción de la replicación de resultados	2	1	Investigación de las capacidades instaladas con anterioridad	2
AC – Plantilla operativa completa	Retrasó en las actividades del proyecto	Departamento de personal y talento	Actividades estancadas	Dificultades para alcanzar objetivos estratégicos	2	2	Opciones de más posibles candidatos en espera	4
	Rotación de personal	Departamento de personal y talento	Capacitación por bloques pequeños	Requerirá una capacitación mucho más segmentada	2	3	Contratación de personal con formación adecuada para las actividades	6
AC – PTO aprobado	Falta de transmisión total del PTO		Pasar por alto una necesidad básica para el proceso	Descalificación de actividades por no trasmitir la información requerida	2	2	El equipo de cuenta con un proceso de verificación y autorización	4
	Falla en la comprensión de las necesidades		Rechazo de los procesos realizados por incumplimiento	Retrabajo y perdidas considerables durante el proyecto	2	3	Procesos de verificación continua y autorización segmentada	6
AC – Documentos relacionados al proceso PREP	Seguridad en almacenamiento y versionamiento	Departamento de Software e Implementación	Uso y acceso de todo el personal	Documentación obsoleta y/o modificada	2	3	Control de usuarios y contraseñas con privilegios de edición	6
AC – Actas (ejercicios, simulacros)	Retrasó en la entrega de formatos	Coordinador líder	Incumplimiento de las actividades necesarias	No contar con la suficiente ejecución de tareas para una capacitación adecuada	2	2	Ejecución de ejercicios previo a los simulacros	4
	Error en la captura de datos	Departamento de	Incomprensión de las partes de	Resultados erróneos y	2	2	Capacitación e implementaci	4

		personal y talento	valor en el proceso	posible falla del sistema			ón de ejercicios de reforzamiento	
AC – Actas (PREP)	Daños en las actas	Coordinador líder	Llegada con condiciones que impidan su procesamiento	Imposibilidad de realizar su correcta verificación	5	1	Capacitación al personal operativo para la ejecución de procesos de contingencia	5
AC – CATD/CCV	Falta de seguridad perimetral	Departamento de personal y talento	Violación de terceros dentro de las instalaciones	Infiltración de información privada	2	1	Acceso limitado de las instalaciones con identificación	2

Tabla 14. Evaluación de riesgos posterior a la implementación de medidas de seguridad

15 Remanentes posteriores a la implementación de medidas de seguridad

La implementación de medidas de seguridad es un proceso continuo que requiere evaluación y mejora constante. Tras la adopción de controles, protocolos, políticas y capacitaciones los remanentes de riesgo representan aquellos puntos que, aunque mitigados, aún podrían ser vulnerabilidades latentes en el sistema. Identificar y gestionar estos remanentes es crucial para garantizar que el plan de seguridad cumpla con todos los puntos críticos que representan un riesgo en los procesos de la organización.

Para demostrar la efectividad del plan de seguridad, es fundamental realizar auditorías periódicas, asegurando así que las amenazas emergentes sean abordadas de manera proactiva. Además, la capacitación del personal y la actualización de los controles de seguridad refuerzan la resiliencia de la organización frente a nuevos desafíos. En conclusión, un plan de seguridad no solo debe cumplir con los estándares actuales, sino que debe evolucionar continuamente para enfrentar los riesgos cambiantes del entorno tecnológico.

16 Respuesta a incidentes

Se cuenta con un procedimiento formal para la atención y seguimiento de los incidentes detectados durante las revisiones al sistema realizadas por el IEC, el COTAPREP y el Ente Auditor. Dicho procedimiento contempla:

Se proporcionará el procedimiento para que la instancia interna encargada en la supervisión del PREP del IEC pueda reportar los incidentes que se presenten durante las revisiones que realice el Ente Auditor designado por El IEC 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.

16.1.1 Tiempos de respuesta para la atención de incidentes

a) Tiempos de atención en periodos normales

- Horarios de atención: lunes a viernes de 09:00 a 21:00 horas; sábados y domingos de 10:00 a 18:00 horas.

b) Tiempo de atención en periodos críticos

I. Pruebas de funcionalidad

Se procesará la cantidad de actas necesarias 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. Se cubrirá un horario de atención de 8:00 a 20:00 horas, o en su defecto hasta que se termine la actividad.

II. Durante la realización de ejercicios previos

Se realizarán ejercicios antes del primer y segundo simulacro, así como previo a la Jornada Electoral, y cuando menos dos ejercicios que cumplan todas las fases del Proceso Técnico Operativo. Se cubrirá 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 oficiales

Conforme a lo establecido en el artículo 349, numeral 3 del Reglamento de Elecciones, se realizarán 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 debe de realizarse 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

La operación iniciará al cierre de casillas el día de la Jornada Electoral y se mantendrá durante 24 horas, es decir, de las 18:00 horas del día de la Jornada Electoral a las 18:00 horas del día siguiente, o antes, en caso de alcanzar el 100% del registro de las actas PREP esperadas y/o agotarse los mecanismos de recuperación de estas.

16.1.2 Niveles de servicio por tipo de falla

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.

	Del sistema			
	Periodo normal		Periodo de contingencia	
	Desde la solicitud hasta la generación del reporte (ya sea 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 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 15. Acuerdos nivel de servicio (Sistema).

	De la generación y entrega de información. Información relativa al sistema o cualquier otra información prevista en el contrato.	
	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.
Periodo normal	2 horas	10 días naturales

Tabla 16. tiempo de solicitud hasta generación del reporte

16.2 Modelo de trabajo de respuesta de incidentes

El modelo de trabajo es un esquema que se elabora para el usuario, con la finalidad de llevar a cabo las actividades entre usuario y el equipo de soporte de manera eficiente.

Ilustración 3. Modelo de trabajo

16.3 Clasificación de solicitudes

El agente de soporte de primer nivel clasifica en Service Desk todas las solicitudes recibidas. Una vez registrada la solicitud, esta pasa al estado de ticket, el cual genera un número de registro único, el nivel de atención de solicitud (bajo, medio o alto) y el estado correspondiente.

La siguiente tabla muestra la clasificación de los tickets de acuerdo con el nivel de atención y el perfil del personal que los atiende.

Clasificación de solicitudes	Nivel de atención	Perfil
Soporte	Nivel medio	Agente de soporte
Mantenimiento	Nivel bajo	Agente de desarrollo

Tabla 17. Clasificaciones de solicitudes

Posibles estados a considerarse para cada ticket son:

- **Abierto:** Es cuando un ticket se encuentra registrado por un problema de soporte y se asignó a un responsable, el ticket cuenta con un nivel de clasificación, lo que determina el tiempo de atención para otorgar su solución. El estado es cambiado hasta que el responsable da solución al problema presentado por el usuario para que este sea validado.
- **En progreso:** Es cuando el personal de soporte está trabajando en la solución al problema presentado en el ticket, este se cambia de estado a "En Progreso".
- **Resolver incidencia:** Es cuando se entrega la solución del problema al usuario, este validó que la solución fue la correcta y quedó satisfecho con la misma, el ticket cambia su estado a "Resuelto".
- **Cerrar incidencia:** Es cuando se cancela un ticket duplicado, este cambia su estado a "Cerrado".

16.4 Descripción de clasificaciones de solicitudes

16.4.1 Soporte (primer nivel)

El primer nivel de soporte está enfocado en la atención de solicitudes referentes a la aclaración o uso del sistema PREP, así como de la funcionalidad de cada una de las opciones de este en cada uno de sus módulos.

16.4.2 Mantenimiento (segundo nivel)

Este nivel se encarga de atender las solicitudes para las correcciones de código fuente de la aplicación cuando se ha detectado algún mal funcionamiento en cualquiera de sus componentes (aplicaciones, bases de datos). Una vez se corrigen las fallas detectadas, se libera una nueva versión.

16.5 Funciones y responsabilidades del personal de soporte

Gerente de Software e Implementación: Encargado del funcionamiento de soporte.

Principales actividades:

- Supervisar el desarrollo y avance de las correcciones de fallas, nuevos requerimientos o mejoras realizadas.
- Reportar el estado del funcionamiento y tickets de la mesa de ayuda.

Coordinador líder: Documentar soluciones.

Principales actividades:

- Reportar avances en solución de incidentes.
- Documentar soluciones en Service Desk.
- Auxiliar de soporte en dudas y asignación de tickets.

Agente de Soporte de Primer Nivel: Encargado de dar atención a usuarios.

Principales actividades:

- Responsable de recibir las solicitudes de los usuarios por cualquiera de los medios anteriormente mencionados.
- Registrar los tickets en Service Desk, clasificarlos, asignarlos y, en caso de 1er nivel de atención, resolverlos.
- Comunicar al Gerente de Software e Implementación sobre las solicitudes de carácter urgente o dudas que se presenten.
- Validación de soluciones resueltas por 2do nivel de atención (pruebas).
- Elaborar reporte de total de solicitudes.
- Realizar pruebas antes de una liberación.

Agente de Desarrollo: Encargado de dar atención a las solicitudes de segundo nivel.

Principales actividades:

- Soluciona tickets de 2do. nivel.
- Da soporte al sistema.

16.6 Procedimiento de soporte de incidentes

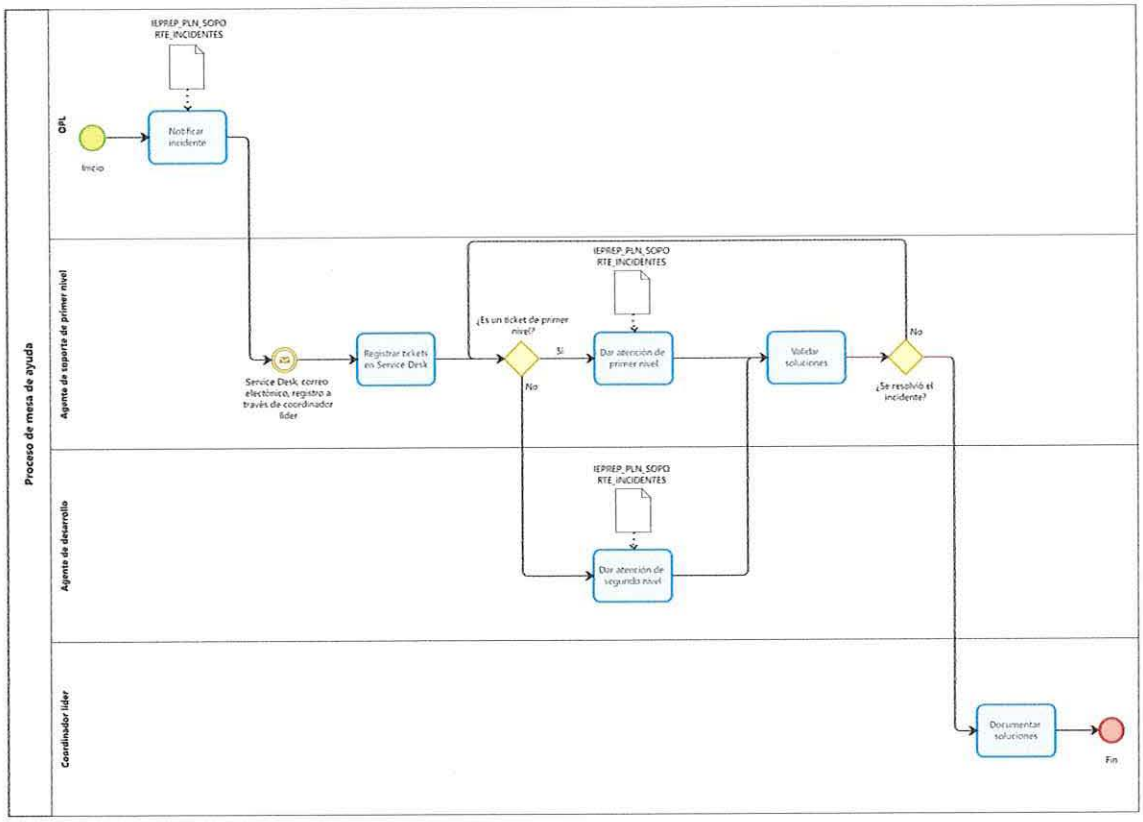


Tabla 18. Procedimiento de soporte de incidentes

17 Recursos humanos

La estructura organizacional, esencialmente, define cómo se organiza una empresa en términos de jerarquía, roles y relaciones entre diferentes áreas, departamentos o unidades. Esta estructura proporciona un marco para la toma de decisiones, la comunicación, la asignación de tareas y la coordinación de actividades dentro de la organización.

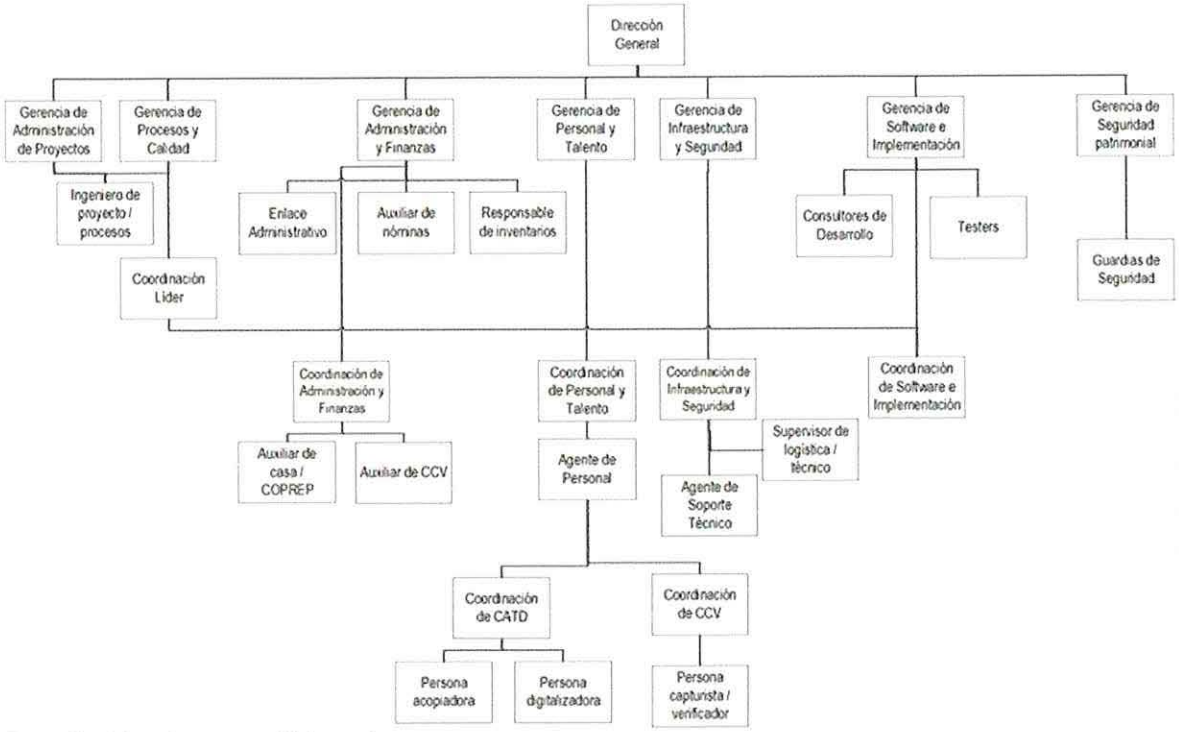


Ilustración 4. Organigrama general del proyecto

17.1 Líneas de autoridad

En este apartado se describe el nivel jerárquico que debe seguirse en la toma de decisiones dentro de la organización, definiendo esto, se identifica quién es la persona adecuada para solucionar cualquier situación que se presente de acuerdo con el área donde exista algo que resolver.

17.2 Flujo de comunicación

El flujo de comunicación define cómo se debe dar la comunicación entre el personal de las distintas áreas, de acuerdo con sus responsabilidades, para que en caso de que exista una situación, se pueda solventar de la mejor manera posible sin que afecte el proceso PREP ni las líneas de autoridad establecidas.

Al igual que sucede con las líneas de autoridad, la comunicación debe ser con el siguiente nivel jerárquico, sólo en caso de que este no pueda solucionar la situación que se presente, deberá ser comunicado al siguiente nivel, y así sucesivamente, hasta llegar a quien pueda dar solución a la situación. Si lo que se presenta requiere de una decisión entonces se deberán ver las líneas de autoridad y dirigirse a ellas para que den pronta decisión, y así evitar que se presente el paro o lentitud del proceso PREP.

17.2.1 CATD y CCV

Puesto	Se comunica con
Coordinaciones de CATD.	– Consejo Distrital. – Personas acopiadoras. – Personas digitalizadoras de actas. – Área de bandejas de acomodo de actas.
Personas acopiadoras.	– Funcionario de casilla que traslada los paquetes electorales. – Personas digitalizadoras.
Personas digitalizadoras.	– Coordinación de CATD. – Personas acopiadoras.
Coordinaciones de CCV.	– Personas capturistas. – Personas verificadoras.
Personas capturistas.	– Personas verificadoras. – Coordinación de CCV.
Personas verificadoras.	– Coordinador de CCV. – Personas capturistas. – Página web.

Tabla 19. Flujo de comunicación CATD y CCV

17.2.2 Oficinas centrales

Puesto	Se comunica con
Dirección de IE.	– Coordinación Líder – Gerencia de Administración de Proyecto. – Gerencia de Administración y Finanzas. – Gerencia de Personal y Talento. – Gerencia de Procesos y Calidad. – Gerencia de Software e Implementación. – Gerencia de Infraestructura y Seguridad. – Gerencia de Seguridad Patrimonial.
Gerencia de Personal y Talento.	– Dirección de IE. – Gerencia de Administración de Proyecto. – Gerencia de Administración y Finanzas. – Gerencia de Procesos y Calidad. – Gerencia de Software e Implementación. – Gerencia de Infraestructura y Seguridad. – Gerencia de Seguridad Patrimonial. – Coordinaciones de Personal y Talento de cada una de las plazas.
Gerencia de Infraestructura y Seguridad.	– Dirección de IE. – Gerencia de Administración de Proyecto. – Gerencia de Administración y Finanzas. – Gerencia de Personal y Talento. – Gerencia de Procesos y Calidad. – Gerencia de Software e Implementación. – Gerencia de Seguridad Patrimonial. – Coordinaciones de Infraestructura y Seguridad de cada una de las plazas. – Supervisor técnico.
Gerencia de Administración y Finanzas.	– Dirección de IE. – Gerencia de Administración de Proyecto. – Gerencia de Personal y Talento. – Gerencia de Procesos y Calidad. – Gerencia de Software e Implementación.

	– Gerencia de Infraestructura y Seguridad. – Gerencia de Seguridad Patrimonial – Coordinaciones de Administración y Finanzas de cada una de las plazas.
Gerencia de Software e Implementación.	– Dirección IE. – Gerencia de Administración de Proyecto. – Gerencia de Administración y Finanzas. – Gerencia de Personal y Talento. – Gerencia de Procesos y Calidad. – Gerencia de Infraestructura y Seguridad. – Coordinaciones de Software e Implementación de cada una de las plazas. – Gerencia de Seguridad Patrimonial. – Soporte Técnico de Informática Electoral.
Gerencia de Administración de Proyecto.	– Dirección de IE. – Gerencia de Administración y Finanzas. – Gerencia de Personal y Talento. – Gerencia de Procesos y Calidad. – Gerencia de Software e Implementación. – Gerencia de Infraestructura y Seguridad. – Gerencia de Seguridad Patrimonial. – Coordinación Líder.
Gerencia de Procesos y Calidad.	– Director de IE. – Gerencia de Administración de Proyecto. – Gerencia de Administración y Finanzas. – Gerencia de Personal y Talento. – Gerencia de Software e Implementación. – Gerencia de Infraestructura y Seguridad. – Gerencia de Seguridad Patrimonial – Coordinación Líder.
Gerencia de Seguridad Patrimonial	– Director de IE. – Gerencia de Administración de Proyecto. – Gerencia de Administración y Finanzas. – Gerencia de Personal y Talento. – Gerencia de Software e Implementación. – Gerencia de Infraestructura y Seguridad. – Gerencia de Procesos y Calidad.

Tabla 20. Flujo de comunicación en oficinas centrales

17.2.3 COPREP

Puesto	Se comunica con
Coordinación Líder	– Dirección IE. – Gerencias. – Supervisión de Logística. – Coordinación de Administración y Finanzas. – Coordinación de Infraestructura y Seguridad. – Coordinación de Personal y Talento. – Coordinación de Software e Implementación. – Coordinación de Administración de Proyecto. – Coordinación de Procesos y Calidad.
Supervisión de Logística.	– Gerencia de Infraestructura y Seguridad. – Coordinación Líder. – Coordinación de Administración y Finanzas. – Coordinación de Infraestructura y Seguridad. – Coordinación de Personal y Talento.

	– Coordinación de Software e Implementación.
Coordinación de Administración y Finanzas	– Gerencia de Administración y Finanzas. – Coordinación Líder. – Coordinación de Administración y Finanzas de otras plazas. – Coordinación de Infraestructura y Seguridad. – Coordinación de Personal y Talento. – Coordinación de Software e Implementación. – Auxiliar de casa/COPREP. – Auxiliar de CCV.
Coordinación de Infraestructura y Seguridad	– Gerencia de Infraestructura y Seguridad. – Coordinación Líder. – Supervisión de Logística. – Coordinación de Administración y Finanzas. – Coordinación de Infraestructura y Seguridad de otras plazas. – Coordinación de Personal y Talento. – Coordinación de Software e Implementación. – Agentes de Soporte Técnico. – Supervisor técnico.
Coordinación de Personal y Talento	– Gerencia de Personal y Talento. – Coordinación Líder. – Coordinación de Administración de Proyecto. – Coordinación de Administración y Finanzas. – Coordinación de Infraestructura y Seguridad. – Coordinación de Personal y Talento de otras plazas. – Coordinación de Software e Implementación. – Agentes de Personal. – Coordinador de CATD. – Coordinador de CCV.
Coordinación de Software e Implementación	– Gerencia de Software e Implementación. – Coordinación Líder. – Supervisión de Logística. – Coordinación de Administración de Proyecto. – Coordinación de Administración y Finanzas. – Coordinación de Infraestructura y Seguridad. – Coordinación de Personal y Talento. – Coordinación de Software e Implementación de otras plazas.
Supervisor Técnico/Logístico	– Gerencia de Infraestructura y Seguridad. – Coordinación de Infraestructura y Seguridad. – Agentes de Soporte Técnico.
Agentes de Soporte Técnico	– Coordinador de Infraestructura y Seguridad. – Agentes de Soporte Técnico de otras plazas. – Supervisor técnico.
Agentes de Personal.	– Coordinación de Personal y Talento. – Agentes de personal de otras plazas. – Coordinación de CCV. – Supervisión de CCV. – Coordinación de CATD.
Enlace **IEC**	– Coordinación Líder.

Tabla 21. Flujo de comunicación COPREP

17.3 Grupos de respuesta

Si bien Informática Electoral, ya cuenta con líneas de comunicación y jerarquías bien definidas, las cuales contribuyen a una efectiva toma de decisiones y correcta gestión de incidentes, también se han generado grupos de respuesta para situaciones de emergencia, su principal función es la de gestionar y coordinar la respuesta inmediata a cualquier emergencia que frene la operación normal y cualquier actividad posterior a la recuperación de las operaciones.

Grupos de respuesta	Integrantes	Objetivo
Grupo coordinador	Coordinación Líder Gerencia de Administración de Proyecto Gerencia de Procesos y Calidad	El grupo coordinador es el encargado de evaluar las emergencias, movilizar al o los equipos correspondientes y documentar los incidentes y sus soluciones una vez se hayan resuelto.
Grupo de respuesta de infraestructura	Gerencia de Infraestructura y Seguridad Coordinación de Infraestructura y Seguridad Agentes de Soporte Técnico Supervisor Logístico	Este grupo se encarga de dar respuesta a todas las emergencias cuya afectación sea a equipos, telecomunicaciones, inmuebles, vehículos y problemas logísticos en general.
Grupo de respuesta de sistemas	Gerencia de Software e Implementación Coordinación de Personal y Talento Consultores de Desarrollo	Da respuesta a cualquier emergencia referente a los sistemas, y los ambientes que habitan.
Grupo de respuesta de personal	Gerencia de Personal y Talento Coordinación de Personal y Talento Agentes de Personal	Atiende problemas relacionados a la capacitación del personal, faltas, y en general, seguimiento al recurso humano.

Tabla 22. Grupos de respuesta

18 Procesos de solución de contingencias CATD/CCV

Es necesario establecer los procesos que permitan a las personas involucradas en el proceso PREP Coahuila 2026 conocer la forma de actuar ante la presencia de situaciones, desastres o problemas que se pudieran presentar durante la operación del PREP.

18.1 Proceso de solución de contingencias de bajo nivel en CATD/CCV

El proceso de solución de contingencias de nivel bajo, o bien, las contingencias que tienen un nivel de impacto 3 o inferior de acuerdo con la evaluación de riesgos, describe las actividades iniciales en la detección de la contingencia por parte del personal ubicado en el CATD y/o en el CCV.

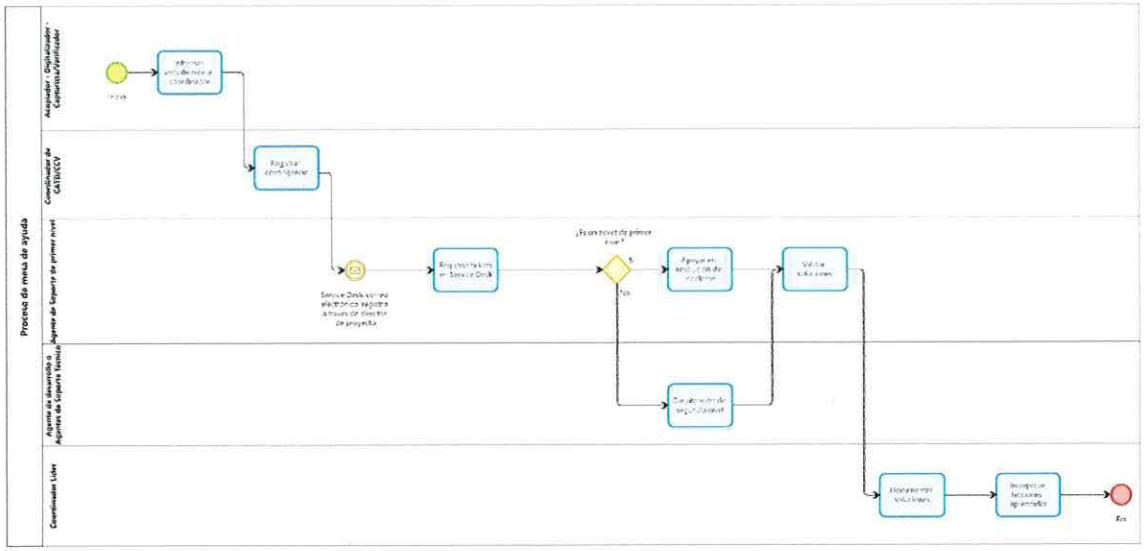


Ilustración 5. Proceso de solución de contingencias de bajo nivel

18.2 Proceso de solución de contingencias en COPREP

El proceso de solución a contingencias de nivel bajo, o bien, las contingencias que tienen un nivel de impacto 3 o inferior de acuerdo con la evaluación de riesgos, describe las actividades iniciales en la detección de la contingencia por parte del personal ubicado en el COPREP.

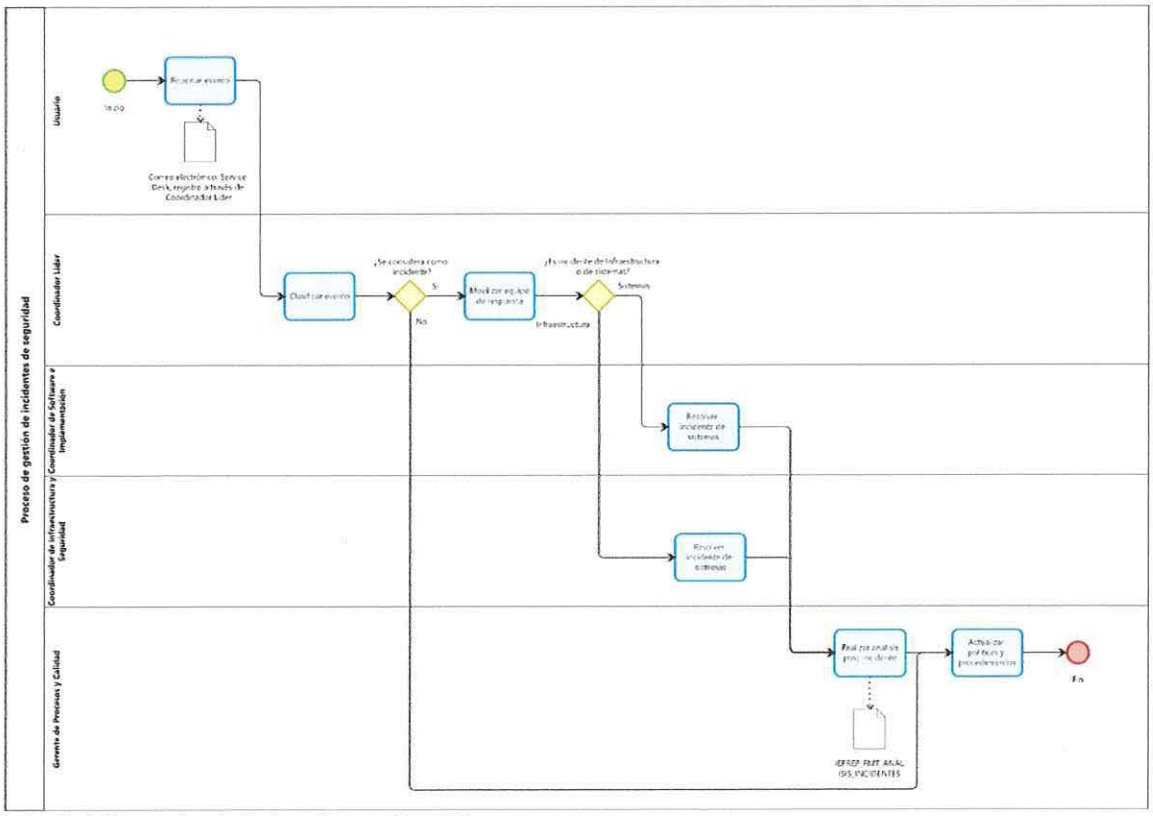


Ilustración 6. Proceso de solución de contingencia COPREP

19 Resolución de emergencias

Se considerará como una emergencia, cualquier contingencia que en su evaluación de riesgos haya salido con un nivel de impacto 4 o superior, o bien, los que se acuerden con el **IEC** y para su tratamiento entrarán en acción los grupos de respuesta anteriormente mencionados, siguiendo el siguiente procedimiento:

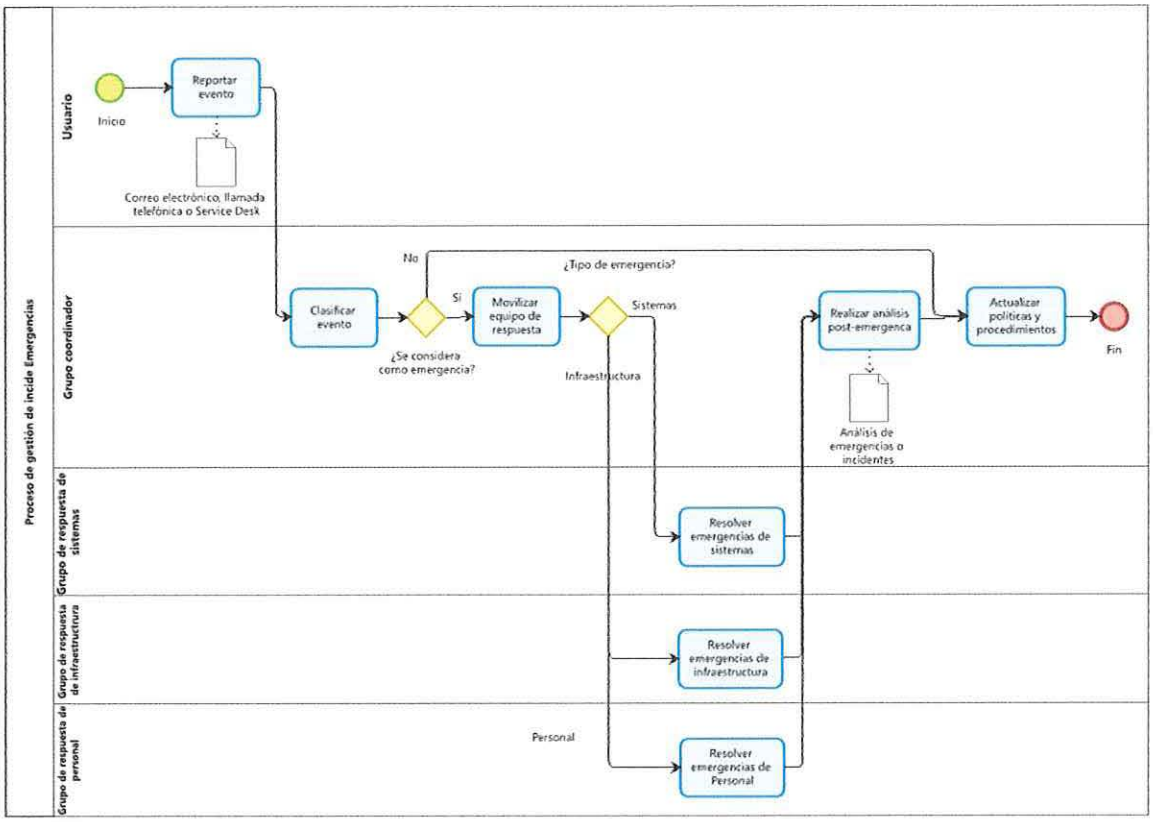


Ilustración 7. Procedimiento de resolución de emergencia

Responsable	Responsabilidades
Usuario	Reportar cualquier emergencia que detecte.
Grupo coordinador	Clasificar los eventos ocurridos. Gestionar la respuesta y resolución de las posibles contingencias cuyo nivel de impacto sea igual o superior a 4 de acuerdo con la evaluación de riesgos (emergencias). Registro de lecciones aprendidas y mejora continua de los procesos o medidas de seguridad.
Grupo de respuesta de infraestructura	Gestionar la resolución de cualquier emergencia a nivel de equipos, telecomunicaciones, inmuebles, vehículos y problemas logísticos en general.
Grupo de respuesta de sistemas	Gestionar la resolución de cualquier emergencia a nivel de software o sistemas.
Grupo de respuesta de personal	Gestionar la resolución de cualquier emergencia a nivel de personal.

Tabla 23. Responsabilidades del procedimiento de resolución de emergencias

No.	Responsable	Procedimiento
1	Usuario	**Reportar evento** Un evento podría ocurrir durante cualquier etapa del servicio PREP, es por ello que cualquier persona que se encuentre utilizando o monitoreando el proyecto, así como sus sistemas y se percate de que está ocurriendo un evento, deberá notificar al Grupo coordinador para la clasificación del mismo, esto mediante un correo electrónico en el que se describa la situación, llamada telefónica, o bien, por Service Desk.
2	Grupo Coordinador	**Clasificar evento** Una vez recibido la notificación del evento, deberá analizarlo para comprender la naturaleza del mismo y proceder, determinar si es una emergencia o no. ¿Se considera como emergencia? **Si:** Ejecutar actividad 3 **No:** Ejecutar actividad 8 **Nota:** Sin importar si se tratará como evento o como incidente, se debe responder al usuario que notifico el evento para hacer de su conocimiento que se le dará seguimiento al evento presentado.
3	Grupo Coordinador	**Movilizar equipo de respuesta** Una vez que se ha determinado el evento como emergencia o contingencia de nivel alto se debe determinar qué equipo de respuesta es necesario movilizar y hacérselo saber por el medio que considere más conveniente, ya sea llamada telefónica, correo electrónico o Service Desk. **Tipo de emergencia** **De sistemas:** Ejecutar actividad 4. **De infraestructura:** Ejecutar actividad 5. **De personal:** Ejecutar actividad 6.
4	Grupo de respuesta de sistemas	**Resolver emergencias de sistemas** Debe ejecutar cualquier acción de acuerdo con sus experiencia técnica, documentación existente y situaciones similares ocurridas con anterioridad, resolver la emergencia y comunicárselo al Grupo coordinador.
5	Grupo de respuesta de infraestructura	**Resolver emergencias de infraestructura** Debe ejecutar cualquier acción de acuerdo con sus experiencia técnica, documentación existente y situaciones similares ocurridas con anterioridad, resolver la emergencia y comunicárselo al Grupo coordinador.
6	Grupo de respuesta de personal	**Resolver emergencias de personal** Debe ejecutar cualquier acción de acuerdo con sus experiencia técnica, documentación existente y situaciones similares ocurridas con anterioridad, resolver la emergencia y comunicárselo al Grupo coordinador.
7	Grupo coordinador	**Realizar análisis post-emergencia** Una vez resuelta la emergencia, se deben documentar las lecciones aprendidas, para ello se debe llenar el **formato de análisis de emergencias o incidentes** y resguardarlo, ya que servirá como evidencia de lo sucedido.
8	Grupo coordinador	**Actualizar políticas y procedimientos**

	Sin importar si lo ocurrido fue un incidente o emergencia, se deberá analizar la documentación existente que tenga relación con lo ocurrido y actualizarlo para fortalecer el Sistema de Gestión de Seguridad de la Información, así mismo, si no existe documentación relacionada con lo ocurrido, deberá crearla.

Tabla 24. Descripción de las actividades del procedimiento de resolución de emergencias

20 Continuidad ante incidentes

A lo largo de la operación del PREP, hay numerosos incidentes que pudieran manifestarse a pesar de que se implementen las medidas preventivas razonables, para enfrentar estos incidentes se han documentado procedimientos específicos y guías operativas para cada uno de estos incidentes recurrentes, así mismo, a lo largo de las capacitaciones se adiestra al personal contratado en la aplicación de las mismas y se refuerza su comprensión y entendimiento durante ejercicios, laboratorios y simulacros.

En esta sección se detallan algunos de los incidentes más comunes identificados para los cuales ya se tiene un marco de acción predefinido que minimizan los tiempos de respuesta y refuerzan la continuidad operativa del PREP.

20.1 Contingencia de fallo de energía eléctrica

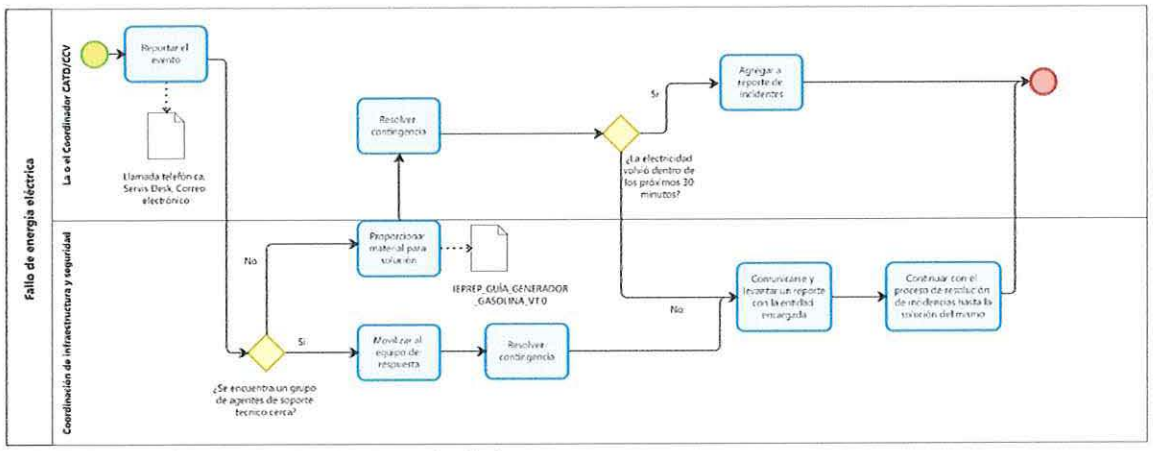


Ilustración 8. Procedimiento de resolución fallo de energía eléctrica

20.2 Contingencia de ausencia de internet

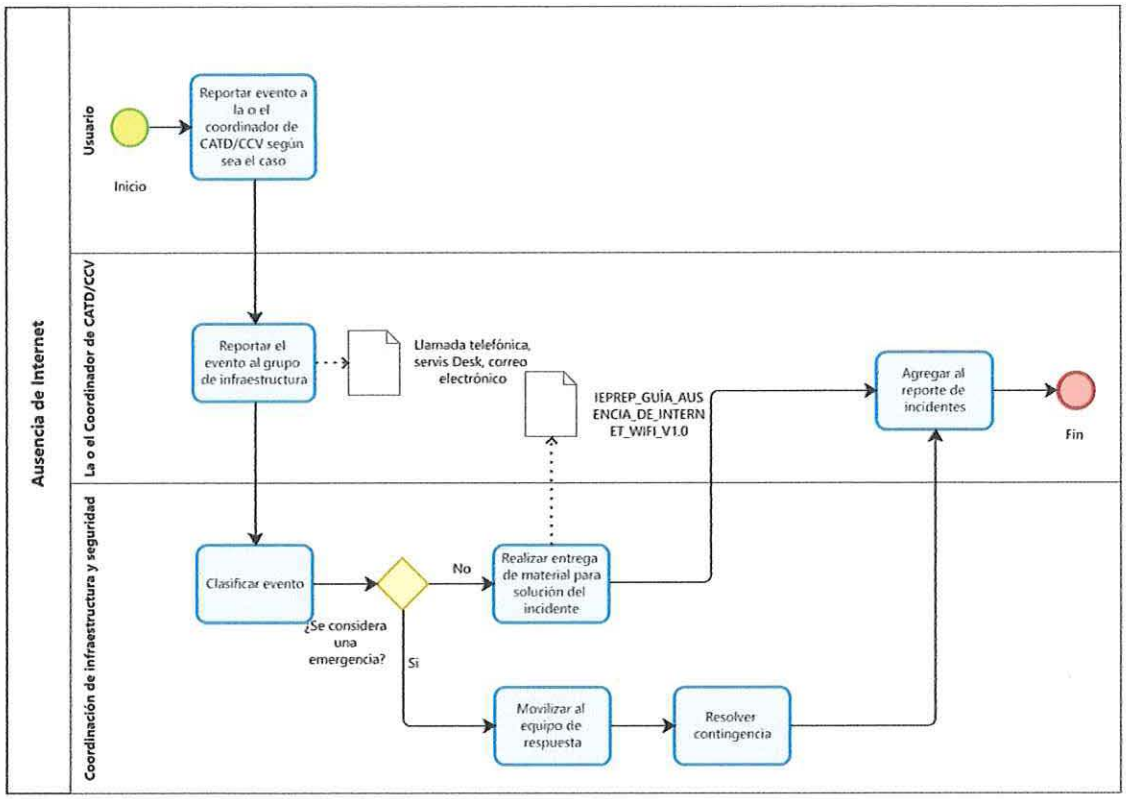


Ilustración 9. Procedimiento de resolución ausencia de internet

20.3 Contingencia multifuncionales

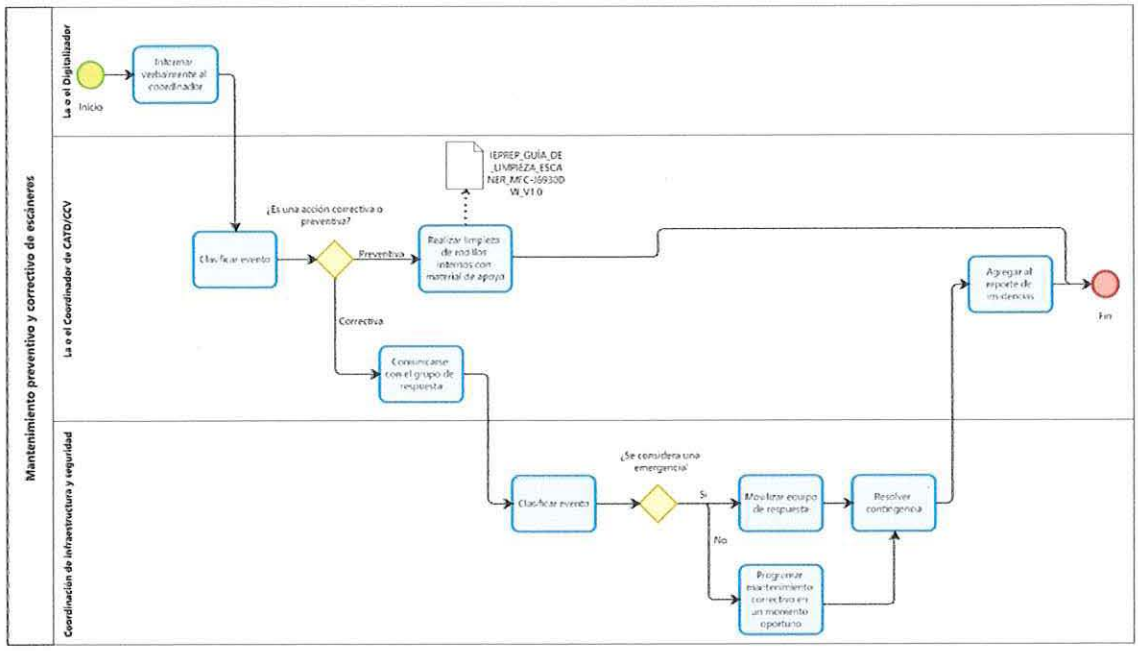


Ilustración 10. Procedimiento de resolución Mantenimiento preventivo y correctivo de escáneres

20.4 Contingencia de ausencia de personal

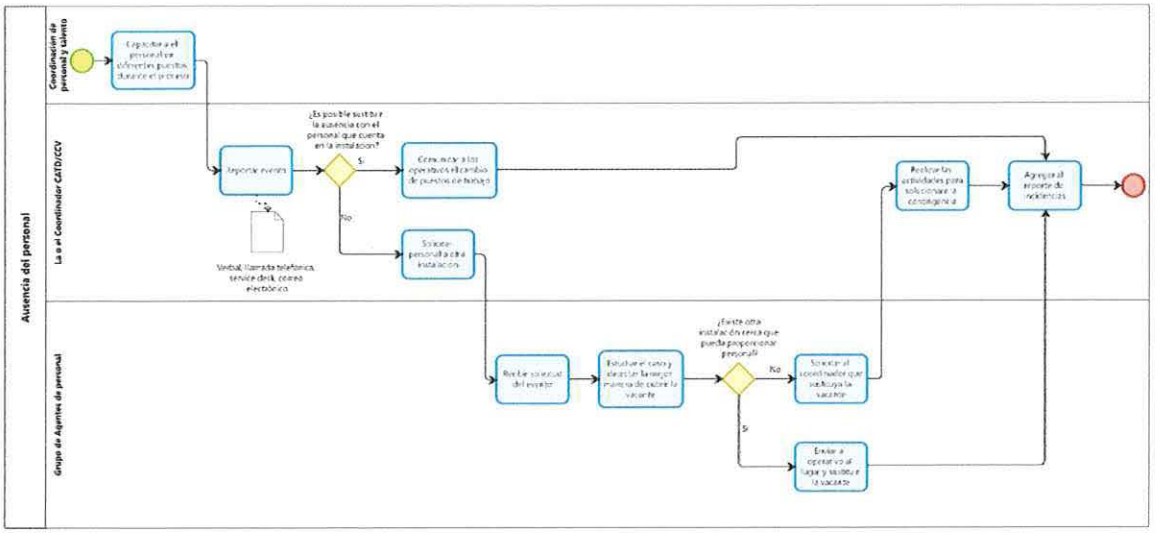


Ilustración 11. Procedimiento de resolución de ausencia de personal

21 Simplificación e ilustración de contingencias

Para garantizar la continuidad operativa y minimizar el impacto de fallas o emergencias en proceso críticos, se implementará una solución de contingencia basada en la capacitación del personal y la entrega de guías rápidas que faciliten la ejecución de procedimientos esenciales.

21.1 Capacitación de personal

Se realizarán sesiones de formación teórico-prácticas dirigidas al equipo y usuarios clave, abordando los siguientes temas:

- Uso adecuado e inspección
- Mantenimiento preventivo
- Procedimientos de reemplazo
- Actualización o restricciones del sistema

21.2 Entrega de guías rápidas

Se desarrollarán y distribuirán guías rápidas en formato digital, estructuradas de manera sencilla y visual para facilitar su consulta. Estas guías incluirán:

- Instrucciones claras de uso e inspección de equipos.
- Procedimientos paso a paso para el mantenimiento preventivo.
- Protocolos de respuesta ante fallas específicas.

Informática Electoral

Guía rápida - Primeros auxilios PREP

Limpieza de Escáner MFC-J6940DW

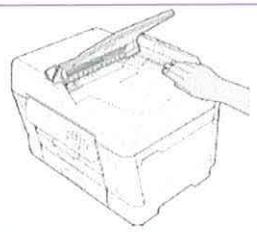
Este documento tiene como finalidad dar a conocer cómo mantener limpio y en óptimas condiciones de funcionamiento el equipo y eliminar residuos que puedan afectar la calidad de las imágenes escaneadas o incluso dañar el equipo a largo plazo.

Medidas Preventivas

- **Utilizar productos de limpieza adecuados**: Emplea únicamente productos de limpieza recomendados por el fabricante del escáner. Evita el uso de líquidos corrosivos o abrasivos que puedan dañar los componentes delicados del dispositivo.
- **Limpiar regularmente**: Establece una rutina de limpieza regular para mantener el escáner en óptimas condiciones de funcionamiento. La frecuencia de limpieza puede variar según el entorno de uso y la cantidad de documentos escaneados.
- **Evitar el exceso de líquido**: Al limpiar el escáner, evita el exceso de líquido para prevenir daños por humedad. Siempre asegúrate de que los componentes estén completamente secos antes de volver a encender el escáner.
- **Evitar el uso de aire comprimido**: Aunque puede ser tentador, evita el uso de aire comprimido para limpiar el escáner, ya que puede introducir humedad y partículas de polvo en el interior del equipo, causando daños.

Contingencias Comunes

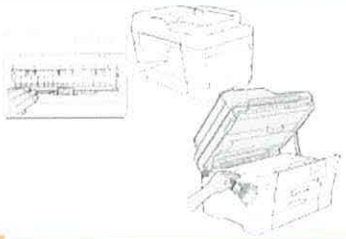
1 Sobrecarga de actas



- Al intentar escanear demasiadas hojas a la vez, es probable que el escáner tenga dificultades para alimentarlas correctamente a través del mecanismo de escaneo, por lo tanto, es necesario que solo **10 actas** sean colocadas en el alimentador.
- Los rodillos de alimentación de papel del escáner están diseñados para procesar una cantidad específica de hojas a la vez. Si se sobrecargan con un número excesivo de hojas, los rodillos pueden dañarse.
- Al intentar escanear un gran número de hojas a la vez, es posible que algunas hojas se deslicen o se desalineen durante el proceso de escaneo. Esto puede resultar en imágenes escaneadas, borrosas, distorsionadas o incompletas.

2 Limpieza de los rodillos de alimentación de papel

- Después de cada **50 actas** digitalizadas debe hacerse una limpieza.
- Abre la cubierta del escáner para acceder a los rodillos de alimentación. Están ubicados en la parte superior del escáner y en la bandeja de documentos.
- Selecciona una brocha suave, preferiblemente una brocha de cerdas finas diseñada para la limpieza de equipos electrónicos. Asegúrate de que la brocha esté limpia y seca antes de comenzar.
- Pasa suavemente la brocha a lo largo de los rodillos de alimentación para eliminar cualquier suciedad, polvo o residuos acumulados. Es importante hacerlo con cuidado para no dañar los rodillos.
- Después de limpiarlos con la brocha, gira manualmente los rodillos para asegurarte de que estén limpios y para verificar que giran correctamente.
- Una vez que hayas limpiado los rodillos de alimentación, cierra la cubierta del escáner de manera segura.



3 Falla de alimentador y utilización de láser

- Organiza las actas que deseas escanear y asegúrate de que estén en buen estado y sin arrugas ni dobleces que puedan afectar la calidad del escaneo.
- Levanta la tapa del escáner para acceder a la superficie de vidrio. Esta es el área donde colocarás manualmente cada documento para escanearlo.
- Una vez que hayas colocado el documento en la superficie de vidrio, cierra la tapa del escáner para evitar la entrada de luz externa y mantener la calidad del escaneo.

1

Ilustración 12. Guía rápida multifuncional

Informática Electoral

Guía rápida - Primeros auxilios PREP

DSA TP-50

Este documento tiene como finalidad dar a conocer cómo usar el dispositivo de sellado automático de manera correcta y eficiente, desde el encendido y apagado hasta la configuración de parámetros y la carga de materiales.

Medidas Preventivas

- Asegúrate de que todo el personal que operará el dispositivo esté debidamente capacitado en su uso seguro y eficiente.
- En primera instancia asegurarse de contar con la llave para poder abrir el dispositivo.
- Realiza inspecciones periódicas para identificar cualquier desgaste o daño en el dispositivo que pueda afectar su seguridad o rendimiento.

Configuración de dispositivo de sellado DSA

1 Inicio

- Introducir la llave y girar de manera que se pueda retirar la tapa gris.
- Presionar el botón de engrane

2 Desplazamiento

- Con los botones A y B desplazarte de arriba abajo en el menú C para seleccionar y D para cancelar o regresar.

3 Reloj

- Desplazarte hacia abajo y seleccionar la opción RELOJ.
- En este apartado seleccionar lo que se desea modificar ya sea la hora o la fecha.

4 Impresión

- Para configurar el lado de impresión.
  - Seguir el paso 2
- Seleccionar la opción IMPRESIÓN
- Desplazarte hacia abajo
- Seleccionar lado
  - Cambiar a IZQUIERDO.

1

Ilustración 13. Guía rápida DSA

Informática Electoral

Guía rápida - Primeros auxilios PREP

Equipos de cómputo y Comunicaciones

Este documento tiene como finalidad dar a conocer la información básica de los equipos de cómputo y comunicaciones utilizados durante el proceso PREP, así como también explicar las medidas preventivas y correctivas que deberán seguirse para minimizar el mal funcionamiento de estos equipos.

Medidas Preventivas

- Encienda y apague el equipo de cómputo de manera adecuada, según el procedimiento del sistema operativo.
- No acerque al equipo de cómputo bebidas ni alimentos, ya que un descuido podría ocasionar que se derramen sobre el teclado y ocasionarle daño.
- En caso de requerir conectar más dispositivos de los necesarios en el UPS, o en la barra de contactos del equipo de cómputo, consúltelo con el COPREP.
- Utilice el equipo de cómputo solo para los fines que le fueron indicados, ya que el uso indebido puede inhabilitar por completo el funcionamiento del mismo, ocasionando así fallas en el flujo de la información.
- En caso de un problema eléctrico en su lugar de trabajo, apague y desconecte las barras de contacto y los equipos UPS. No mueva los equipos del lugar al que fueron destinados, a menos de que haya una instrucción contraria. Avise al COPREP.
- Evite desconectar componentes de los equipos, en caso de que cualquier componente falle y tenga que ser reemplazado repórtelo al COPREP y recibirá instrucciones.
- Evite usar equipos de cómputo personales en su oficina de trabajo, ya que el uso de otros equipos no autorizados puede ocasionar un contagio de virus informático, así como lentitud en los enlaces de comunicación.

Contingencias Comunes

1 Equipo de cómputo no enciende


No break o UPS


Cable de corriente


Extención

- Verifique cables de corriente.
- Reinicie el equipo si es necesario.
- Verifique que el cable de corriente esté bien conectado.
- Verifique que haya energía eléctrica.
- Verifique cables de corriente.

2 Teclado o PAD numérico dejan de responder

- Verifique que la tecla NumLock esté encendida.
- Reiniciar el equipo en caso de ser necesario.


Teclado

3 Fallo de conexión a los sistemas PREP


Switch


Firewall


Explorador


Módem

- Verificar que los equipos de Internet (módem) estén encendidos.
  - Debe tener las cuatro luces en verde.
- Checar equipo SONICWALL esté encendido.
  - Debe tener al menos las luces de X0 y X1 encendidas.
- Verificar que el cable que viene del módem Telmex esté en el puerto X1 (WAN).
- Verificar que el switch Cisco esté encendido y que las luces donde están los cables conectados estén encendidas, de igual manera verificar que llegue el cable de SONICWALL.
- Verificar que el cable de red que se encuentra conectado en la laptop de la computadora esté conectado correctamente.
- Verificar que el navegador sea Google Chrome.

1

Ilustración 14. Guía rápida Equipo de cómputo y telecomunicaciones

Informática Electoral

Guía de uso - Primeros auxilios PREP

Generador a gasolina con arranque manual y eléctrico

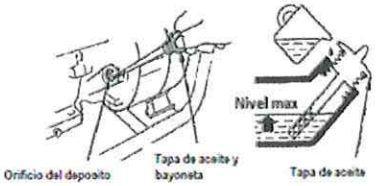
Proporcionar a los usuarios una guía detallada y fácil de entender que les permita familiarizarse con el funcionamiento, mantenimiento y medidas de seguridad necesarias para operar de manera eficiente y segura un generador a gasolina con arranque tanto manual como eléctrico. Esta guía busca capacitar a los usuarios para maximizar la vida útil del generador, minimizar el riesgo de accidentes y asegurar un suministro confiable de energía en situaciones donde se requiera su uso.

Consideraciones iniciales

- **Ubicación segura:** Se debe colocar el generador en un área bien ventilada al aire libre, lejos de áreas congestionadas o espacios cerrados para evitar la acumulación de gases nocivos como monóxido de carbono.
- **Nivelación y estabilidad:** Asegurarse de que el generador esté colocado sobre una superficie nivelada y estable para prevenir caídas o vuelcos durante su funcionamiento.
- **Mantenimiento regular:** Mantener un programa de mantenimiento regular según las recomendaciones del fabricante, que incluya la revisión periódica de niveles de aceite, combustible y filtros, así como la limpieza de componentes esenciales.
- **Conexión segura:** Conectar correctamente los dispositivos al generador utilizando cables y enchufes en buen estado para prevenir cortocircuitos y descargas eléctricas.
- **Aceite:** Verificar que se use aceite de 4 tiempos con el nivel indicado antes de usar el generador.

Contingencias Comunes

1 Aceite



El aceite es el factor más importante que puede afectar el desempeño y vida del generador, no usar aceites de 2 tiempos ya que dañara el motor.
Use aceite de 4 tiempos, se recomienda el SAE40.
Verifique el nivel de aceite antes de usar el generador, siempre con el motor apagado. (Aproximadamente ½ litro de aceite).

1. Retire el tapón de aceite y limpie la bayoneta.
2. Verifique el nivel de aceite, insertando la bayoneta dentro del cuello del tanque sin enroscarlo en él.
3. Si el nivel es bajo, añada aceite de 4 tiempos hasta la marca.
4. Retire el tapón de aceite y limpie la bayoneta.

2 Gasolina

1. Verifique el nivel de gasolina con el medidor del tanque.
2. Rellene el tanque si el nivel es bajo. No sobrecargue el tanque más allá del brazo del filtro.

AVISO

- La gasolina es extremadamente inflamable y explosiva en ciertas condiciones.
- Recargue en algún lugar bien ventilado con el motor apagado. No fume, no permita que haya flamas o chispas en el lugar donde se recarga el combustible o donde se almacena.
- No cargue de más el tanque. No debe haber combustible en el cuello de llenado del tanque. Después de recargar, asegúrese que la tapa del tanque está cerrada apropiadamente y bien.
- Sea cuidadoso de no derramar gasolina cuando recargue. Los derrames y vapores pueden encenderse. Si hay derrame, por favor, séquelos y límpielos antes de arrancar el motor.
- Evite el contacto prolongado de vapor con la piel, y no lo respire.
- Mantenga alejados a los niños
- Capacidad del tanque de gasolina: 17L
- Se recomienda usar gasolina sin plomo.
- Nunca usar gasolina contaminada, ni mezclar con aceite.
- Evite que entre agua al tanque de gasolina.

1

Ilustración 15. Guía rápida planta eléctrica A

Ilustración 16. Guía rápida planta eléctrica B

Informática Electoral

Guia de uso - Primeros auxilios PREP

6 Encendido con Jalón Manual

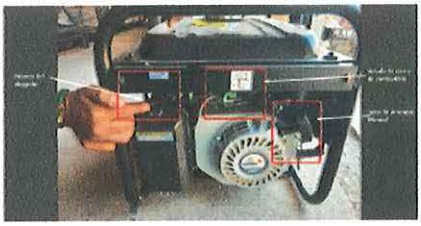
1. Abrir la palanca de la gasolina en la posición de encender.
2. Girar el interruptor (se encuentre en posición de encendido).
3. Tomar el jalón y jalar a menos de 1 metro.
4. Al encender el generador mover, la palanca del ahogador a la derecha.
5. Listo el generador debe quedar encendido listo para utilizar.

https://youtu.be/nr6BscZLiX4

7 Apagado de Generador

https://youtu.be/osq7qxYSqbY

1. Girar interruptor o llave a la izquierda.
2. Cerrar palanca de gasolina a la posición de APAGAR.
3. Mover la palanca del ahogador a la izquierda.



3

Ilustración 17. Guía rápida planta eléctrica C

Informática Electoral

Guía rápida - Primeros auxilios PREP

No hay luz

Este documento tiene como finalidad garantizar la continuidad de las operaciones críticas y la protección de los datos durante un corte de energía.

Medidas Preventivas

- **Sistemas de respaldo de energía:** Se instalaron sistemas de respaldo de energía, generadores de gasolina y UPS.
- **Planificación de la capacidad:** Asegurarse de que la capacidad del sistema de respaldo de energía sea suficiente para mantener en funcionamiento los equipos críticos.
- **Protección contra sobretensiones:** Se instalaron dispositivos de protección contra sobretensiones para evitar daños en los equipos sensibles debido a fluctuaciones de energía.
- **Entrenamiento del personal:** Capacitar al personal sobre cómo responder adecuadamente ante un corte de energía, incluyendo la identificación de procedimientos de emergencia, el uso de equipos de respaldo y la minimización del riesgo de pérdida de datos.

Contingencias Comunes

1 Activación de sistemas de respaldo

- **Inicio de UPS:** Estos sistemas deben activarse automáticamente en caso de un corte de energía para proporcionar una fuente de energía inmediata durante 15 a 20 minutos y proteger los equipos críticos contra picos de voltaje y fluctuaciones. Más información en *IEPREP_GUIA_UPS_V1.0*
- **Arranque del generador de gasolina:** Si el corte de energía es prolongado o si los UPS no pueden mantener la carga durante mucho tiempo, activa el generador gasolina para proporcionar una fuente de energía continua y sostenible. Más información en *IEPREP_GUÍA_GENERADOR_GASOLINA_V1.0*
- **Lampara de emergencia:** Debe activarse automáticamente en caso de un corte de energía para proporcionar una fuente de luz durante 15 a 20 minutos.

2 Priorización de operaciones críticas

- **Priorización del generador de gasolina:** Dictaminar si es necesario mantener prendido el generador en el caso donde no se encuentren actas.
- **Identificación:** Evalúa y documenta las operaciones y sistemas que dependen directamente de la energía eléctrica y que son críticos para la continuidad de las operaciones.
- **Asignación de recursos limitados:** Si los recursos de respaldo, como la energía de emergencia y el personal disponible, son limitados, asigna estos recursos de manera estratégica para apoyar las operaciones críticas más importantes primero

3 Apagado seguro de sistemas no esenciales

- **Identificación de sistemas no esenciales:** Determine qué sistemas y equipos no son críticos para las operaciones inmediatas. Prioriza el apagado en función de su importancia y su impacto en las operaciones.
- **Cierre de aplicaciones y archivos:** Antes de apagar los sistemas, asegúrate de que todas las aplicaciones estén cerradas adecuadamente y que los archivos estén guardados correctamente para evitar pérdidas de datos.

4 Comunicación interna y externa

- **Alerta de emergencia:** Notificar a todo el personal sobre el corte de energía y las medidas que se están tomando.
- **Recopilación de información:** Obtén detalles sobre el área afectada por el apagón, incluyendo el tamaño del territorio afectado podría ser solo el inmueble o consejo, el área PREP o la colonia.
- **Causa del apagón:** Identifica la causa del apagón, como fallos en la red eléctrica, condiciones climáticas extremas, problemas en la infraestructura de energía como pastillas botadas o extensiones dañadas y/o acciones humanas.
- **Solicitud:** Si el territorio del apagón es demasiado amplio, una localidad o colonia debe notificarse al OPL para que levante un reporte directamente con CFE.

Nota: Solicitar el consejo utilizar extensiones hablar a soporte técnico para dictaminar la falla

1

Ilustración 18. Guía rápida no hay luz

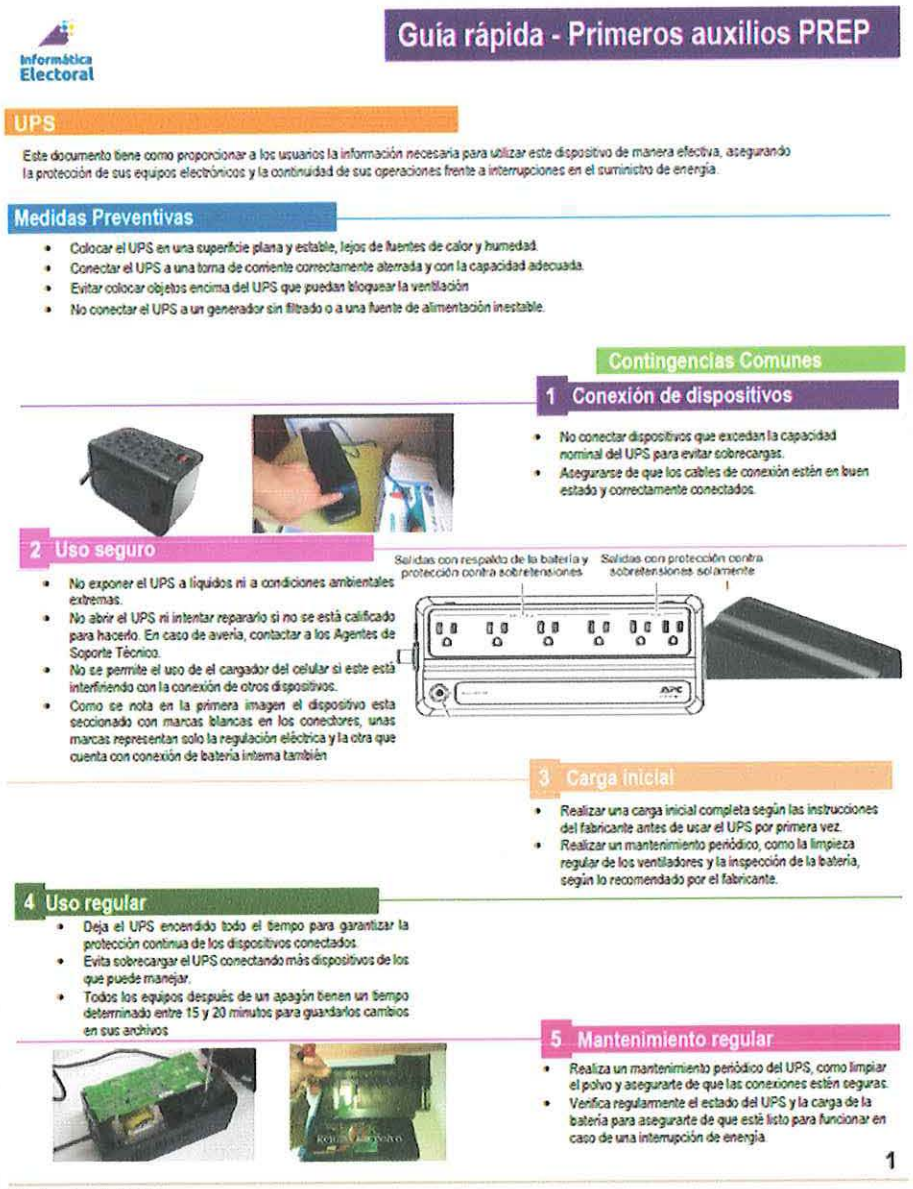


Ilustración 19. Guía rápida UPS

22 Robustecimiento de los controles de seguridad física y ambiental

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

a. El acceso a los edificios que albergan los CCV y los CATD está controlado por el personal de vigilancia del IEC, y adicionalmente, los espacios ocupados por los CATD y los CCV se encuentran en áreas cerradas cuyo acceso solo está permitido mediante autorización de las respectivas Coordinaciones.

b. Cada CATD y CCV cuenta con un sistema de control de acceso mediante identificación visible, otorgada a través de gafetes y chalecos que acreditan al personal como autorizado para operar, supervisar o coadyuvar en las actividades del PREP.
c. Los recintos cuentan con controles ambientales, incluyendo aire acondicionado y medidas de prevención ante contingencias, tales como sensores de humo, inundación y humedad.
d. Todo el personal que accede a los CCV y CATD queda registrado en libros o sistemas de control administrados por las Coordinaciones correspondientes.
e. Los cables de datos y de energía se encuentran correctamente separados y protegidos contra interferencias o descargas estáticas, y los medios de almacenamiento removibles se resguardan de manera segura.
f. Asimismo, se contemplan medidas de protección para las áreas de carga y descarga de equipos en los CCV.

23 Control de accesos y políticas de seguridad

El acceso a los recursos del PREP, tanto físicos como informáticos, se realiza bajo controles estrictos definidos en políticas de seguridad previamente establecidas. Estos controles cubren todo el ciclo de vida del usuario, desde su registro inicial hasta la cancelación de accesos cuando ya no requiere utilizar los recursos.

23.1 Control de acceso a bienes informáticos

a. El control de acceso a los bienes informáticos sigue el principio de mínimos privilegios. En las aplicaciones se implementa mediante usuario y contraseña, asignando roles y características que determinan los recursos a los que el usuario puede acceder.
b. Para el acceso físico a los CCV y a los CATD, se cuenta con identificación fotográfica mediante gafete de presentación y chaleco.

Para proteger el acceso a servidores, bases de datos, equipos de comunicaciones y estaciones de trabajo son los siguientes:

a) 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. Esta función la realiza la dirección general de desarrollo de software.
b) Los equipos de cómputo tendrán los parches de seguridad instalados y firmas de antivirus actualizadas.
c) Se implementarán restricciones por IP para las conexiones realizadas en el periodo de pruebas.
d) Se implementarán sistemas de detección y prevención de intrusos en la central donde se encuentran los servidores web, bases de datos, sistema de cómputo yservicios de publicación.

23.2 Políticas de seguridad para el aplicativo PREP Casilla

23.2.1 Control de acceso y autenticación

a) Cada usuario contará únicamente con permisos para operar las casillas que le hayan sido asignadas, conforme al listado oficial proporcionado por el INE.
b) Los usuarios deberán recibir capacitación previa sobre el uso adecuado de la aplicación.

23.3 Políticas de seguridad para la aplicación de digitalización (CATD)

23.3.1 Equipamiento

El equipo de cómputo será proporcionado y configurado por personal técnico autorizado, contará con los programas necesarios para el funcionamiento de la aplicación, así como con los parches de seguridad actualizados, antivirus y bloqueos tantode software y hardware que no sea necesario para realizar la actividadde digitalización y/o represente un riesgo para la integridad y seguridad de la información que se procese.

23.3.2 Personal

a. Se contará con registro de datos personales de cada Digitalizador, quien deberá haber cumplido con los filtros de selección requeridos para su contratación.
b. Los Digitalizadores deberán recibir la capacitación sobre:
    - Uso de la aplicación.
    - Estándares de calidad de las imágenes
    - Procedimiento de aceptación o rechazo de imágenes digitalizadas desde la casilla.
c. Cada digitalizador contará con usuario y contraseña individuales.
d. Las contraseñas utilizadas el día de la Jornada Electoral serán distintas a las empleadas en los simulacros internos y oficiales, y siempre serán proporcionadas por el supervisor de los CCV.

23.3.3 Controles técnicos

a. La aplicación de digitalización incorporará validaciones obligatorias para impedir el envío de imágenes sin datos completos de identificación del acta, información de acopio, fecha, hora, mecanismo de traslado y tipo de documento.
b. 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.
c. Restricción de descarga y actualización de base de datos local mediante IP durante el período

de pruebas.

d. Generación de código HASH o código de integridad para imágenes digitalizadas.

Cualquier error del sistema o del equipo de cómputo asignado deberá ser reportado al supervisor de los CATD para recibir instrucciones de la forma de proceder ante la falla.

23.4 Políticas de seguridad para la aplicación de captura y verificación

a. El equipo de cómputo será proporcionado y configurado por personal técnico autorizado, contará con los programas necesarios para el funcionamiento de la aplicación, así como con los parches de seguridad actualizados, antivirus y bloqueos tanto de software y hardware que no sea necesario para realizar la actividad captura y/o represente un riesgo para la integridad y seguridad de lainformación que se procese.
b. Se contará con registro del personal Capturista/Verificador, quien deberá haber aprobado los filtros de selección requeridos para su contratación.
c. Los Capturistas/Verificadores recibirán capacitación sobre:
    - Uso de la aplicación.
    - Clasificación de inconsistencias de las actas PREP en el sistema.
    - Las descritas en el punto 9.5
d. La aplicación validará el tipo de dato permitido para cada campo de captura de datos.
e. Cada capturista deberá tener su propio usuario y contraseña individuales.
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 personal de coordinación.
g. Se implementará restricción de descarga y actualización de base de datos local mediante control de IP durante el período de pruebas.

24 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 serán los siguientes:

a) Verificación de la captura de datos.
b) Validación de 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) Revisión del manejo de inconsistencias y contabilización de los datos.

d) Revisar que el sistema realiza el manejo de inconsistencias y contabilización delos resultados de las actas de acuerdo con lo descrito en el numeral 31 del Anexo13 del Reglamento de Elecciones.

24.1 Funciones mínimas del sistema

a) 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.

24.2 Integridad en el registro de la información

a) Revisar que el sistema informático mantiene los datos libres de modificaciones,es decir, sin alteración.

24.3 Imparcialidad en el tratamiento de la información

a) 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.

24.4 Precisión en resultados

a) 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 deElecciones.

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

- Propósito, tipo y alcance de la prueba.
- Entrega de información necesaria (aplicaciones, usuarios, credenciales temporales, restricciones tecnológicas y contactos).
- Reglas del contrato:
    I. Acuerdo formal entre el auditor (hacker ético) y los administradores del PREP.
    II. Identificación del tráfico generado por el auditor.
    III. Definición de duración y horarios.
    IV. Planificación de comunicaciones seguras: contactos diversos y protegidos para la comunicación.
    V. Elaboración de resumen ejecutivo con hallazgos y recomendaciones.
    VI. Descripción detallada de la metodología aplicada.

25 Requisitos de contratación de personal

Todos los aspirantes por colaborar en el Proceso Operativo del PREP deben cumplir con los Requisitos Legales estipulados en el Artículo 351, Numeral 2 del Reglamento de Elecciones vigente, expedido por el Instituto Nacional Electoral; así como, los que establece el presente documento.

Las personas interesadas en desempeñar las actividades establecidas en las funciones de cualquier puesto del CATD y/o CCV, así como Agentes, deberán cumplir todos los requisitos legales y administrativos que contendrá el expediente y que a continuación se describen:

Requisitos legales y administrativos:

a) Tener la ciudadanía mexicana y tener el pleno ejercicio de sus derechos civiles y políticos.
b) Estar inscrito en el Registro Federal de Electores y contar con credencial para votar vigente.
c) No haber sido registrado como candidata o candidato ni haber desempeñado cargo alguno de elección popular en los cuatro años anteriores a la designación.
d) No ser ni haber sido miembro de dirigencias nacionales, estatales o municipales de partido político alguno en los últimos cuatro años.
e) No ser consejera o consejero ciudadano, propietario o suplente, ante algún consejo electoral local, distrital, estatal o municipal.
f) Ser ciudadano residente de la entidad federativa en que se presta el servicio del PREP.
g) No estar inhabilitado para ocupar cargo o puesto público o no haber sido destituido por el Instituto Nacional Electoral o cualquier Organismo Público Local.
h) No ser miembro de los cuerpos de seguridad, ni ministro de culto religioso.
i) No ser, ni haber sido militante, adherente, o cualquier otra figura que reconozca algún partido político en término de sus estatutos, en los últimos 4 años anteriores a la fecha de la designación.
j) Tener completa disponibilidad de horario para llevar a cabo sus actividades.
k) Cumplir con el perfil requerido para cada cargo.