|  |  |
| --- | --- |
|  | A pink dot in the dark  Description automatically generated |

**Plan de Seguridad y Continuidad**

para el Programa de Resultados Electorales Preliminares (PREP) del Proceso Electoral Local Concurrente 2024 en Jalisco

**Marzo 2024**

**Contenido**

[1. Glosario 4](#_Toc161488941)

[2. Introducción 5](#_Toc161488942)

[3. Objetivo 6](#_Toc161488943)

[3.1. Objetivos específicos 6](#_Toc161488944)

[4. Alcance 6](#_Toc161488945)

[5. Sistema informático PREP 7](#_Toc161488946)

[6. Proceso de administración de riesgos 8](#_Toc161488947)

[6.1. Identificación de riesgos 8](#_Toc161488948)

[6.2. Evaluación de riesgos 12](#_Toc161488949)

[6.2.1. Criterios de evaluación de riesgos 12](#_Toc161488950)

[6.2.2. Identificación de activos críticos 13](#_Toc161488951)

[6.2.2.1. Áreas de amenaza 15](#_Toc161488952)

[6.2.3. Evaluación de riesgos 15](#_Toc161488953)

[6.2.4. Priorización de riesgos 20](#_Toc161488954)

[6.3. Respuesta a riesgos 21](#_Toc161488955)

[6.3.1. Plan de Seguridad y Continuidad 21](#_Toc161488956)

[6.3.1.1. Fortalecimiento de la infraestructura tecnológica 21](#_Toc161488957)

[6.3.1.2. Seguridad en la captura 23](#_Toc161488958)

[6.3.1.3. Seguridad en el data center principal y secundario 24](#_Toc161488959)

[6.3.1.4. Seguridad en la transmisión 25](#_Toc161488960)

[6.3.1.5. Seguridad en el procesamiento 26](#_Toc161488961)

[6.3.1.6. Seguridad en la publicación 28](#_Toc161488962)

[6.3.1.7. Robustecimiento de los controles de seguridad física y ambiental 29](#_Toc161488963)

[6.3.1.8. Creación del plan de contingencia 30](#_Toc161488964)

[6.3.1.9. Reporte de incidentes tecnológicos 31](#_Toc161488965)

[6.3.2. Políticas de seguridad informática 31](#_Toc161488966)

[6.3.2.1. Políticas de seguridad sobre usuarios 31](#_Toc161488967)

[6.3.2.2. Políticas de control de accesos 32](#_Toc161488968)

[6.3.2.3. Políticas de seguridad en hardware 33](#_Toc161488969)

[6.3.2.4. Políticas de seguridad en sistemas institucionales y software de terceros 34](#_Toc161488970)

[6.3.2.5. Políticas de seguridad en telecomunicaciones 34](#_Toc161488971)

[6.3.2.6. Políticas de seguridad en Internet y redes sociales 35](#_Toc161488972)

[6.3.2.7. Políticas de acceso a los centros de datos (data centers) 35](#_Toc161488973)

[6.3.2.8. Resguardo de la información 35](#_Toc161488974)

[6.3.2.9. Participación del ente auditor del PREP 36](#_Toc161488975)

[6.3.3. Plan de Continuidad 36](#_Toc161488976)

[6.3.4. Plan de Continuidad del Negocio (BCP) 38](#_Toc161488977)

[6.3.4.1. Replicación de datos 39](#_Toc161488978)

[6.3.4.2. Interrupción de Replicación de Datos 39](#_Toc161488979)

[6.3.4.3. Restablecimiento de Replica de Datos 40](#_Toc161488980)

[6.3.4.4. Información Histórica 41](#_Toc161488981)

[6.3.4.5. Difusión de Resultados 41](#_Toc161488982)

[6.3.4.6. Suministro de Servicios en el Centro de Datos y CATD 42](#_Toc161488983)

[6.3.5. Plan de Recuperación en Caso de Desastres (DRP) 42](#_Toc161488984)

[6.3.5.1. Contingencia en el Centro de Datos Principal 43](#_Toc161488985)

[6.3.5.2. Contingencia en el Centro de Datos Secundario 43](#_Toc161488986)

[6.3.5.3. Contingencia en CATD 43](#_Toc161488987)

[6.3.6. Fin de la Contingencia 44](#_Toc161488988)

[7. Conclusiones 44](#_Toc161488989)

# Glosario

|  |  |
| --- | --- |
| **IEPC Jalisco** | Instituto Electoral y de Participación Ciudadana del Estado de Jalisco |
| **PREP** | Programa de Resultados Electorales Preliminares |
| **Data center** | Centro del procesamiento de datos conformado por servidores informáticos. |
| **CATD** | Centro de Acopio y Transmisión de Datos. |
| **CAE** | Capacitador Asistente Electoral |
| **AEC** | Actas de Escrutinio y Cómputo |
| **Sistema PREP** | Sistema informático o plataforma tecnológica que dará soporte al Programa de Resultados Electorales Preliminares del proceso electoral 2024 y que consiste en distintas aplicaciones informáticas, infraestructura y personal. |
| **ISO 27001:2013** | Norma internacional para los Sistemas de Gestión de la Seguridad de la Información (SGSI) |
| **SGSI** | Sistema de Gestión de la Seguridad de la Información |
| **BCP** | Por sus siglas en inglés (Business Continuity Planning), es el plan de continuidad del negocio consistente en mantener operando los servicios críticos de la institución en caso de una contingencia. |
| **DRP** | Por sus siglas en inglés (Disaster Recovery Planning), es el plan recuperación en caso de desastres. |

# Introducción

El presente plan es elaborado en apego a la normatividad aplicable para los Planes de Seguridad y Continuidad contenida en el Reglamento de Elecciones, en sus artículos 347, numeral 1, y 348, numeral 1. Asimismo, respecto a lo contenido en el Anexo 13: “Lineamientos del Programa de Resultados Electorales Preliminares (PREP)”, del Reglamento de Elecciones, en el Título II, Capítulo III, “De la Auditoría al Sistema Informático”, lineamiento 11; Título II, Capítulo IV, “Consideraciones de Seguridad Operativa”, lineamientos 12 y 13.

Un **Sistema de Seguridad Informática** es un conjunto de medios administrativos, medios técnicos y personal que de manera interrelacionada garantizan niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados.

El **Plan de Seguridad y Continuidad** es la expresión gráfica del Sistema de Seguridad Informática diseñado, y constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en una entidad, y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

Este documento tiene como propósito definir el Plan de Seguridad y Continuidad que se utilizará para el Programa de Resultados Electorales Preliminares (PREP) en el estado de Jalisco.

El Sistema PREP dará soporte al proceso electoral 2024 (PREP 2024), y consta de un conjunto de servicios, dispositivos y aplicaciones que darán soporte a las tareas relativas a la digitalización, captura, verificación y publicación de información.

Con la finalidad de dar cumplimiento a la normatividad, la Dirección de Informática del IEPC Jalisco determinará las acciones que garanticen la confidencialidad, integridad y disponibilidad de la información en los procedimientos de acopio, digitalización, captura, verificación y publicación de ésta.

Para ello, se tomarán como referencia las siguientes normas y metodologías:

* Norma internacional ISO 27001:2013, para definir en este Plan de Seguridad y Continuidad las bases del sistema de gestión de la seguridad de la información del IEPC Jalisco.
* Metodología de Administración de Riesgos del INE.
* Metodología OCTAVE Allegro para la evaluación de riesgos.

# Objetivo

El objetivo de este documento es fortalecer la confidencialidad, integridad y disponibilidad de los activos de información para garantizar la correcta operación del PREP del Proceso Electoral Local Concurrente 2023-2024, desde su preparación, operación y actos posteriores a la jornada electoral.

# Objetivos específicos

* Brindar a la ciudadanía la mayor certeza posible sobre la operación del proceso y los resultados de las elecciones a llevarse a cabo.
* Asegurar la correcta operación del PREP mediante el uso de recursos tecnológicos.
* Apoyar al IEPC Jalisco en el cumplimiento de su misión ante un evento electoral.
* Detectar las amenazas y riesgos para el proceso.
* Implementar medidas oportunas que mitiguen dichas amenazas y riesgos.
* Permitir alcanzar la mayor cantidad posible de captura de actas con la mayor precisión posible de forma ininterrumpida durante la ventana de operación del PREP desde todos los CATD disponibles.

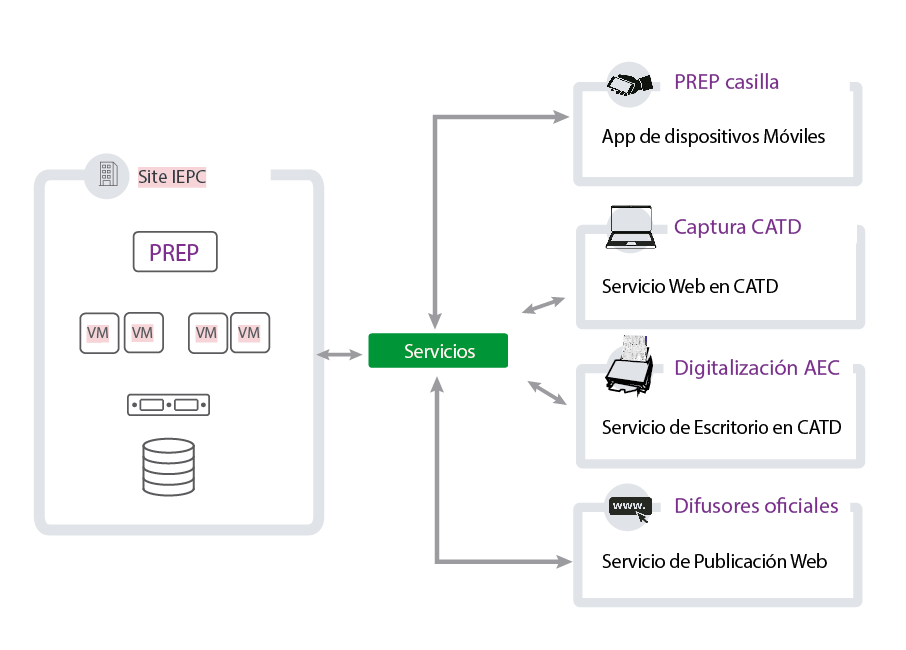
# Alcance

El presente Plan establece los aspectos técnicos y procedimentales que deberán observase para la implementación y priorización de los controles de seguridad que fortalezcan los procesos, procedimientos y recursos humanos involucrados en el PREP Jalisco, considerando al menos:

1. La identificación de riesgos y posibles vulnerabilidades sobre la información generada y contenida en el sistema PREP (sus bases de datos, servidores y dispositivos) en las distintas etapas del modelo de operación para el ejercicio de la votación.
2. La implementación de los controles de seguridad en los distintos procesos y procedimientos electrónicos, a fin de mitigar los riesgos.
3. La confiabilidad y alta disponibilidad del sistema PREP.
4. Verificación de los resultados de la jornada electoral publicados.

# Sistema informático PREP

El sistema PREP es la plataforma tecnológica sobre la cual operará al proceso electoral, la cual consta de distintos servicios de dispositivos y aplicaciones, los que interpelarán para las tareas relativas a la digitalización, captura, verificación y publicación de información.



En caso de una contingencia, se recurrirá al [Plan De Continuidad De Negocio (BCP)](#_Plan_de_Continuidad) o al [Plan Recuperación de Desastres (DRP)](#_Plan_de_Recuperación) según sea la situación que se presente, con el objetivo de determinar las acciones que garanticen la ejecución de los procedimientos de acopio, digitalización, captura, verificación y publicación, derivado de una situación adversa o de una contingencia.

# Proceso de administración de riesgos

El proceso de administración de riesgos contempla **tres fases: identificación, evaluación y respuesta a los riesgos.**  Éstas están divididas en seis actividades principales, como se muestra a continuación:

|  |  |  |
| --- | --- | --- |
| **Identificación de riesgos** | **Evaluación de riesgos** | **Respuesta a riesgos** |
| 1. Identificar riesgos | 1. Criterios de riesgos 2. Evaluación de riesgos 3. Interacción de riesgos 4. Priorizas riesgos | 1. Responder a los riesgos |

Los eventos con impactos negativos representan riesgos, mientras que los eventos con impactos positivos representan oportunidades.

# Identificación de riesgos

El objetivo principal de la identificación de riesgos y posibles vulnerabilidades es implementar un proceso sistemático que permita identificar, evaluar, controlar y dar seguimiento oportunamente a los riesgos que puedan ocurrir antes, durante y después de la jornada electoral.

|  | Factores internos |  |
| --- | --- | --- |
| Eventos/Factores de riesgo | Riesgo | Impacto |
| Falla en la operación del sistema PREP | * No se tiene acceso al sistema. * No se puede hacer el envío y/o recepción de datos. | * No hay procesamiento de datos. * No hay publicación de resultados en tiempo y forma. |
| Falla o alteración maliciosa en los equipos y/o equipos de telefonía móvil | * Falla en su funcionamiento. * Implantación de código malicioso. | * Problemas para operar el sistema PREP. * Provocación de fallas en el sistema. |
| Falla en el escáner | * Imposibilidad de digitalizar los documentos requeridos en tiempo y forma. | * Problemas para la verificación de resultados. |
| Falta de conocimiento sobre la operación del sistema por parte del personal operativo | * Errores durante la captura de resultados. | * Errores en los resultados publicados. |
| Error en la asignación de privilegios de acceso a un usuario en el sistema | * Acceso no autorizado al sistema. * Acceso a información no correspondiente a su perfil y/o funciones. | * Posibilidad de mal uso de los privilegios asignados. * Acceso no autorizado a información, y posibilidad de un mal uso de esa información. |
| Problemas de acceso al sistema por restricciones en la red | * No tener acceso al sistema. | * No se podrían capturar los resultados de las actas. * No habría envío/recepción de datos de las urnas electrónicas. |
| Inasistencia del personal que operará el sistema PREP | * Personal insuficiente para operar el sistema durante el proceso electoral. | * Si se solicita el apoyo de personal no capacitado, esto podría incrementar la cantidad de errores en la captura. * Esto puede ocasionar un retraso en la captura, procesamiento y publicación de resultados. |
| Falla en los respaldos de información | * No contar con una copia de la información a un punto específico en el tiempo | * Posibilidad de pérdida de datos. * Imposibilidad de regresar a un punto específico en el tiempo y consultar dicha información. |
| Extravío de dispositivos de los equipos de cómputo o de telefonía móvil asignados a los CAE (cables, accesorios,  cargadores, etc.) | * No poder utilizar los equipos o celulares durante el PREP. | * Insuficiencia de equipos, lo que puede ocasionar un retraso en la captura, procesamiento y publicación de resultados. |

|  | Factores externos |  |
| --- | --- | --- |
| Eventos/Factores de riesgo | Riesgo | Impacto |
| Corte de energía eléctrica en data center principal | * Suspensión de forma abrupta de todos los servicios tecnológicos. * Daño en la operación de los servidores. * Daño en las bases de datos. * Suspensión del envió de información y replicación hacia el data center secundario. | * Interrupción de recepción, almacenamiento, procesamiento y publicación de la información. * No habría acceso al sistema PREP y su información. * No habría acceso a la información, existiendo pérdida o inconsistencia en los datos. * Afectación en el BCP y DRP en caso de una contingencia. |
| Corte de energía eléctrica en data center secundario | * Suspensión de replicación de información del data center principal, afectando el BCP y DRP. | * En caso de una contingencia en el data center principal, no se contaría con la información actualizada, lo que significaría pérdida o inconsistencia en la información. |
| Corte de energía eléctrica en ubicaciones con urna electrónica, equipos de cómputo y/o escáneres | * Agotamiento de energía de respaldo en No Break. | * No poder utilizar los equipos para el PREP 2024. |
| Ataque malicioso al sistema PREP | * Acceso malicioso al sistema PREP y su información. * Fallas en operación del sistema PREP. | * Alteración y/o pérdida de datos. * Inhabilitación de accesos al sistema. * Problemas para el procesamiento y publicación de resultados. |
| Ataque a los servidores físicos y/o en la nube | * Problemas en la operación de sistema PREP. * Alteración de datos. | * Fallas en la operación del proceso electoral en general y en la publicación de resultados. * Resultados electorales no confiables. |
| Robo o alteración de equipos o dispositivos en  los CATD | * No poder utilizar los equipos o dispositivos durante el PREP. | * Insuficiencia de equipos para el PREP 2024. |
| Robo de equipos de telefonía móvil de los CAE | * No poder enviar la imagen de las actas. | * No poder verificar los resultados de las casillas. |
| Fallas en el servicio de Internet (en las sedes del IEPC Jalisco, CATD y/o casillas) | * Incapacidad de envió de datos al data center principal para su procesamiento. | * Inconsistencia en el procesamiento automatizado de resultados. |

# Evaluación de riesgos

# Criterios de evaluación de riesgos

Para fines de evaluar el efecto de los riesgos en el sistema PREP, empezaremos por identificar los criterios de evaluación de riesgos y su impacto, como se muestra a continuación:

| **Criterio de evaluación del riesgo** | **Área de impacto** | **Nivel de impacto** | | |
| --- | --- | --- | --- | --- |
| **Bajo** | **Medio** | **Alto** |
| **Credibilidad de la ciudadanía en el proceso PREP** | Confianza en los resultados del PREP | Existe una discrepancia en la diferencia de resultados publicado vs las actas no mayor al 1%. | Existe una discrepancia en la diferencia de resultados de entre 1 y 3%. | Existe una discrepancia en la diferencia de resultados mayor al 3%. |
| Publicación de los resultados en el tiempo esperado | La publicación de resultados tiene un retraso no mayor a 5 minutos en su actualización. | Existe un retraso de entre 5 y 30 minutos en la actualización de resultados. | Caída en los sistemas de publicación de los resultados, que no permite hacer la consulta de estos. |
| Afectación de la credibilidad e imagen del PREP | La información relacionada con algún incidente de seguridad es de conocimiento exclusivo de la Dirección de Informática. | La información relacionada con algún incidente de seguridad llega a conocimiento del IEPC Jalisco. | La información relacionada con algún incidente de seguridad es de conocimiento público. |
| **Entorno político** | Consejeros Electorales | El incidente de seguridad es básico, no afecta al PREP y solo es conocido por el personal técnico del PREP. | El incidente de seguridad afecta parcialmente al PREP y es conocido sólo por la presidencia del IEPC Jalisco. | El incidente de seguridad afecta gravemente al PREP y es conocido por la mayoría de los consejeros electorales. |
| Partidos políticos | El incidente de seguridad es básico, no afecta al PREP y solo es conocido por el personal técnico del PREP. | El incidente de seguridad afecta parcialmente al PREP, y es probable que sea del conocimiento de algún partido político. | El incidente de seguridad afecta gravemente al PREP y es conocido por la mayoría de los partidos políticos. |
| INE | El incidente de seguridad es básico, no afecta al PREP y no viola los lineamientos del PREP. | El incidente de seguridad afecta parcialmente al PREP, además de que no se cumple con alguno de los lineamientos del PREP. | El incidente de seguridad afecta gravemente al PREP, y, además, no se cumplen más de tres aspectos de los lineamientos del PREP. |

# Identificación de activos críticos

Como primer paso dentro del análisis de riesgos, nos daremos a la tarea de identificar los activos que deberán ser protegidos para el proceso del PREP 2024; esto, tomando en consideración los riesgos identificados en el punto 7.1 y los criterios de medición de riesgos establecidos en el punto 7.2.1.

Los activos críticos identificados son:

| Activos críticos | |
| --- | --- |
| Tecnológicos | **Hardware:**   * Servidores de red (físicos, virtuales y en la nube) * Equipo de cómputo y sus dispositivos periféricos, para captura de información * Teléfonos móviles y sus cargadores, para envío de imágenes de actas * Escáner para digitalización de actas * Planta de energía eléctrica en data center principal y secundario * Sistemas de Alimentación Ininterrumpida (UPS, por su siglas en inglés) y banco de baterías en data center principal y secundario * No Break de equipos de cómputo y escáneres * *Firewalls* * *Switches, routers* y equipo de telecomunicaciones   **Software:**   * Sistema PREP (software) * Antivirus * Sistema de respaldos de información     **Telecomunicaciones:**   * Enlaces de telecomunicaciones para la captura, procesamiento y publicación de resultados * Esquema de seguridad y telecomunicaciones |
| Data centers | * Data center principal * Data center secundario |
| Humanos | * Personal técnico que desarrollará e implementará el sistema PREP * Personal que operará el sistema PREP * Personal técnico que dará soporte al sistema * Auditores externos |

**Servicios críticos de terceros para el PREP 2024:**

* Servicios en la nube de la publicación
* Servicio de Internet en las sedes del IEPC para la publicación de resultados
* Servicio de Internet en los CATD
* Servicio de Electricidad provisto por la Comisión Federal de Electricidad (CFE)
* Servicio de telefonía móvil
* Sitios web de difusores

# Áreas de amenaza

Se identifican las siguientes **áreas de amenaza para el proceso PREP 2024:**

* Data center principal y secundario
* Centros de Acopio y Transmisión de Datos (CATD)
* Enlaces de telecomunicaciones
* Servicio de Internet
* Mecanismos de difusión

# Evaluación de riesgos

A continuación, se evalúa el riesgo de los eventos o factores de riesgo identificados, iniciando por identificar su impacto y probabilidad, tomando como métricas de evaluación las siguientes:

|  |  |  |
| --- | --- | --- |
| **Impacto** |  | **Probabilidad** |
| Crítico  Vital  Importante  Débil  Marginal |  | Muy alta  Alto  Medio  Bajo  Muy bajo |

Posteriormente, se estima la **exposición al riesgo**, la cual será medida en una escala de **2 a 10** y representada por un semáforo de la siguiente forma:

| **Impacto** | **Probabilidad** | **Exposición al riesgo** | |
| --- | --- | --- | --- |
| Crítico | Muy alta | Muy alta | 10 |
| Crítico | Alta | Muy alta | 9 |
| Vital | Muy alta | Muy alta | 9 |
| Crítico | Media | Muy alta | 8 |
| Vital | Alta | Muy alta | 8 |
| Importante | Muy alta | Muy alta | 8 |
| Crítico | Baja | Alta | 7 |
| Vital | Media | Alta | 7 |
| Importante | Alta | Alta | 7 |
| Débil | Muy alta | Alta | 7 |
| Crítico | Muy baja | Media | 6 |
| Vital | Bajo | Media | 6 |
| Importante | Media | Media | 6 |
| Débil | Alta | Media | 6 |
| Marginal | Muy alta | Media | 6 |
| Vital | Muy baja | Media | 5 |
| Importante | Baja | Media | 5 |
| Débil | Media | Media | 5 |
| Marginal | Alta | Media | 5 |
| Importante | Muy baja | Baja | 4 |
| Débil | Baja | Baja | 4 |
| Marginal | Media | Baja | 4 |
| Débil | Muy baja | Baja | 3 |
| Marginal | Baja | Baja | 3 |
| Marginal | Muy baja | Muy baja | 2 |

La exposición al riesgo de los eventos y/o factores de riesgo identificados para el PREP 2024 es la siguiente:

| **ID** | **Tipo de Factor** | **Eventos/Factores de Riesgo** | **Impacto** | **Probabilidad** | **Exposición al Riesgo** | |
| --- | --- | --- | --- | --- | --- | --- |
| FE-01 | Externo | **Corte de energía**  **eléctrica en data center principal** | Crítico | Media | Muy alta | 8 |
| FE-02 | Externo | **Corte de energía eléctrica en data center secundario** | Crítico | Media | Muy alta | 8 |
| FE-03 | Externo | **Corte de energía eléctrica en ubicaciones con urna electrónica, equipos de cómputo y/o escáneres** | Crítico | Media | Muy alta | 8 |
| FE-04 | Externo | **Ataque malicioso al sistema PREP** | Crítico | Media | Muy alta | 8 |
| FE-05 | Externo | **Ataque a los servidores físicos y/o en la nube** | Crítico | Media | Muy alta | 8 |
| FE-06 | Externo | **Fallas en el servicio de Internet (en las Sedes del IEPC, CATD y/o casillas)** | Crítico | Media | Muy alta | 8 |
| FE-07 | Externo | **Robo o alteración de equipos o dispositivos en los CATD** | Crítico | Alta | Muy alta | 9 |
| FE-08 | Externo | **Robo de equipos de telefonía móvil de los CAE** | Crítico | Alta | Muy alta | 9 |
| FI-01 | Interno | **Falla en la operación del sistema PREP** | Crítico | Media | Muy alta | 8 |
| FI-02 | Interno | **Falla o alteración maliciosa en los equipos y/o equipos de telefonía móvil** | Vital | Baja | Media | 6 |
| FI-03 | Interno | **Error en la asignación de privilegios de acceso a un usuario en el sistema** | Importante | Baja | Media | 5 |
| FI-04 | Interno | **Inasistencia del personal que operará el sistema PREP** | Importante | Baja | Media | 5 |
| FI-05 | Interno | **Extravío de dispositivos de los equipos de cómputo o telefonía móvil asignados a los CAE (cables, accesorios, cargadores, etc.)** | Importante | Baja | Media | 5 |
| FI-06 | Interno | **Problemas de acceso al sistema por restricciones en la red** | Importante | Media | Media | 6 |
| FI-07 | Interno | **Falla en los respaldos de información** | Vital | Baja | Media | 6 |
| FI-08 | Interno | **Falta de conocimiento sobre la operación del sistema por parte del personal operativo** | Importante | Muy baja | Baja | 4 |
| FI-09 | Interno | **Falla en el escáner** | Vital | Media | Alta | 7 |

Los eventos ordenados por la exposición al riesgo, de mayor a menor, quedan de la siguiente manera:

| **ID** | **Tipo de factor** | **Eventos/Factor de riesgo** | **Impacto** | **Probabilidad** | **Exposición al riesgo** | |
| --- | --- | --- | --- | --- | --- | --- |
| FE-07 | Externo | **Robo o alteración de equipos o dispositivos en los CATD** | Crítico | Alta | Muy alta | 9 |
| FE-08 | Externo | **Robo de celulares de los CAE** | Crítico | Alta | Muy alta | 9 |
| FE-01 | Externo | **Corte de energía eléctrica en data center principal** | Crítico | Media | Muy alta | 8 |
| FE-02 | Externo | **Corte de energía eléctrica en data center secundario** | Crítico | Media | Muy alta | 8 |
| FE-03 | Externo | **Corte de energía eléctrica en ubicaciones con urna electrónica, equipos de cómputo y/o escáneres.** | Crítico | Media | Muy alta | 8 |
| FE-04 | Externo | **Ataque malicioso al sistema PREP.** | Crítico | Media | Muy alta | 8 |
| FE-05 | Externo | **Ataque a los servidores físicos y/o en la nube** | Crítico | Media | Muy alta | 8 |
| FE-06 | Externo | **Fallas en el servicio de Internet (en las sedes del IEPC, CATD y/o casillas)** | Crítico | Media | Muy alta | 8 |
| FI-01 | Interno | **Falla en la operación del sistema PREP** | Crítico | Media | Muy alta | 8 |
| FI-09 | Interno | **Falla en el escáner** | Vital | Media | Alta | 7 |
| FI-02 | Interno | **Falla o alteración maliciosa en los equipos y/o celulares.** | Vital | Baja | Media | 6 |
| FI-06 | Interno | **Problemas de acceso al sistema por restricciones en la red.** | Importante | Media | Media | 6 |
| FI-07 | Interno | **Falla en los respaldos de información.** | Vital | Baja | Media | 6 |
| FI-03 | Interno | **Error en la asignación de privilegios de acceso a un usuario en el sistema.** | Importante | Baja | Media | 5 |
| FI-04 | Interno | **Inasistencia del personal que operará el sistema PREP.** | Importante | Baja | Media | 5 |
| FI-05 | Interno | **Extravío de dispositivos de los equipos de cómputo o telefonía móvil asignados a los CAE (cables, accesorios, cargadores, etc.)** | Importante | Baja | Media | 5 |
| FI-08 | Interno | **Falta de conocimiento sobre la operación del sistema por parte del personal operativo.** | Importante | Muy baja | Baja | 4 |

Los resultados anteriores se pueden representar en el siguiente **mapa de riesgo**:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | FE-01, FE-02, FE-03, FE-04, FE-05, FE-06, FI-01 | FE-07, FE-08 |  |
| **Impacto** | Crítico | **6** | **7** | **8** | **9** | **10** |
|  |  | FI-02, FI-07 | FI-09 |  |  |
| Vital | **5** | **6** | **7** | **8** | **9** |
|  | FI-08 | FI-03, FI-04, FI-05 | FI-06 |  |  |
| Importante | **4** | **5** | **6** | **7** | **8** |
|  |  |  |  |  |  |
| Débil | **3** | **4** | **5** | **6** | **7** |
|  |  |  |  |  |  |
| Marginal | **2** | **3** | **4** | **5** | **6** |
|  |  | Muy Bajo | Bajo | Medio | Alto | Muy alta |
|  |  | **Probabilidad** | | | | |

# Priorización de riesgos

La priorización de riesgos es el proceso por el cual se determinan las preferencias para la administración de riesgos mediante la comparación de la exposición de los riesgos obtenida como resultante de la evaluación de riesgos con los criterios aceptados a continuación:

| **Exposición al riesgo** | **Criterio de priorización** |
| --- | --- |
| Muy alta | Requiere de un plan de mitigación o control inmediato |
| Alta | Se requiere asegurar que se está preparado para el riesgo |
| Media | Dar seguimiento al impacto acumulado de los riesgos |
| Baja | Requiere poco monitoreo |
| Muy baja | Operación normal |

# Respuesta a riesgos

Los riesgos identificados y evaluados en los puntos anteriores serán mitigados mediante la implementación del Plan de Seguridad y Continuidad y las políticas de seguridad informática.

# Plan de Seguridad y Continuidad

De acuerdo con los riesgos identificados y evaluados en los puntos 7.1 y 7.2, el Plan de Seguridad y Continuidad se enfocará en los siguientes rubros:

## **Fortalecimiento de la infraestructura tecnológica**

Se sugiere tomar las siguientes acciones, además de apegarse a las políticas de seguridad mencionadas en este plan:

| Categoría | Subcategoría | Acciones |
| --- | --- | --- |
| Hardware | Servidores de red | Al ser este uno de los factores más críticos para el PREP 2024, se optará por la contratación de servicios en la nube (servidores virtuales), a fin de asegurar la alta disponibilidad de los servicios durante el proceso electoral. |
| Equipo de cómputo | Se solicitará el apoyo a la Secretaría de Administración del Gobierno del Estado de Jalisco para el préstamo en comodato de equipos de cómputo nuevos para el proceso. |
| Teléfonos móviles | Se llevará a cabo la contratación de servicios de telefonía móvil que incluyan aparatos con las características indispensables para su interacción con el sistema PREP. |
| Escáner para digitalización de actas | Se contará con equipos de escaneo de documentos de alto volumen durante el PREP. |
| No Break | Se probará cada equipo, buscando asegurar que estos provean de un tiempo de respaldo suficiente para que se active la planta de energía (en las ubicaciones que cuenten con una) o que permitan al usuario llevar a cabo el apagado ordenado de su equipo en caso de un corte de energía eléctrica.  Para las sedes distritales, se cuenta con un convenio con la CFE para dar atención con prioridad alta en caso de una falla en el servicio de energía eléctrica.  **IMPORTANTE**: En las ubicaciones que no cuentan con planta de respaldo, los UPS proveerán de un limitado tiempo de operación. En cuanto la falta de energía consuma el respaldo disponible para el Servidor CATD, este se trasladará a una sede alterna para enviar la información almacenada, y las actas que se reciban posteriormente en el CATD se procesaran por PREP Casilla y capturaran en el CATD alterno. |
| Software | Sistema PREP | De acuerdo con el análisis previo realizado por la Dirección de Informática del IEPC Jalisco, se decidió que el sistema informático que dará soporte al PREP 2024 será desarrollado por la Coordinación de Software (desarrollo interno), así como todos los aplicativos relacionados con este. |
| Antivirus | Los equipos de cómputo, servidores y celulares contarán con un antivirus instalado y actualizado. |
|  | Licenciamiento de Software | Los servidores y equipos de cómputo deberán contar con licenciamientos de software vigentes (sistemas operativos, aplicaciones, etc.), los cuales cuenten con soporte técnico por parte de los fabricantes. |
| Telecomunicaciones | Enlaces de telecomunicaciones | Se contará con redundancia en enlaces, ampliación de ancho de banda durante la operación PREP, entre otras medidas. |
|  | Servicio de internet | Se ampliará el ancho de banda temporalmente para fines de contar con la capacidad requerida durante el PREP 2024, en el *site* ubicado en la bodega. |
| Seguridad Informática | Esquema de seguridad y telecomunicaciones | Se revisará, actualizará y fortalecerá el esquema de seguridad en sus diferentes capas. |

## **Seguridad en la captura**

Se establecerán los controles necesarios para brindar un alto grado de seguridad al proceso de captura de las Actas PREP, además de apegarse a las Políticas de Seguridad mencionadas en este plan, tales como:

* **El acceso a los equipos de cómputo será controlado mediante el uso de usuarios y contraseñas personalizadas.** Dichos accesos serán controlados por el Coordinador en el sitio y asignados al capturista. Se tendrá un registro con los datos de cada capturista.
* **Se deberán inhabilitar los puertos innecesarios (USB, HDMI, etc.) en los equipos de cómputo, así como el acceso a la unidad de DVD.**
* **El sistema informático deberá de considerar una doble captura de los datos, reduciendo así la posibilidad de errores humanos.** Adicionalmente, un verificador deberá de cotejar que los datos capturados en el sistema informático coincidan con la información plasmada en el AEC, además de verificar que la imagen publicada del AEC corresponda a la casilla en cuestión haciendo una revisión del encabezado del AEC con respecto a la imagen publicada.
* **Los equipos que serán utilizados para la captura de información deberán contar con las capacidades necesarias para almacenar todas las transacciones que se generarán en dicha computadora.** Esto permitirá tener la posibilidad de hacer una retransmisión de todo lo registrado y/o capturado en caso de una contingencia en el data center principal, y, por otro lado, que las transacciones queden almacenadas para posibles auditorías posteriores al día de la jornada electoral.

## **Seguridad en el data center principal y secundario**

Se contará con las siguientes medidas de seguridad en los data center del IEPC, además de apegarse a las políticas de seguridad mencionadas en este plan:

* **Ubicación:** contamos con dos *sites* geográficamente separados. En ambos se cuenta con personal capacitado para su monitoreo, mantenimiento y servicio.
* **Contar con un** **enlace de telecomunicaciones adicional al actual** durante el proceso electoral (redundancia).
* **Se contará con** **servidores de alto desempeño con una configuración en paralelo con el data center secundario**, de tal forma que, en caso de una falla, se activen de inmediato los servicios desde el data center secundario.
* **Planta de energía eléctrica:** esta deberá contar con la capacidad para soportar la carga de energía de todo el equipamiento en su interior (servidores y equipo de telecomunicaciones), equipo de cómputo, iluminación interna y otros servicios críticos que requieran de energía eléctrica. Se solicitará la programación de mantenimientos preventivos en forma periódica a las plantas de energía eléctrica ubicadas en las sedes del IEPC Jalisco. También se llevarán a cabo pruebas programadas de corte del suministro de energía para asegurar su correcto funcionamiento.
* **Sistema de respaldos de información:** se actualizará el esquema y calendario de respaldos para fines de asegurar que estos se lleven a cabo con la frecuencia y características adecuadas para el PREP 2024. Dichos respaldos serán probados en forma aleatoria para fines de asegurar su correcto funcionamiento en caso de requerir la restauración de información, lo cual está contemplado como parte del Plan de Continuidad. El respaldo de la infraestructura de servidores ser realiza automáticamente en línea manteniendo una copia con hasta 10 segundos de diferencia entre nuestro site principal y nuestro site de respaldo.
* **UPS y banco de baterías:** se solicitará la programación de mantenimientos preventivos en forma periódica a los UPS y sus bancos de baterías ubicados en las sedes del IEPC Jalisco. También se llevarán a cabo pruebas programadas de corte del suministro de energía y apagado de la planta de energía eléctrica para asegurar su correcto funcionamiento.
* **Sistema de aire acondicionado:** se cuenta con un sistema de enfriamiento redundante (aire acondicionado) en ambos *sites*. Ambos *sites* cuentan con un sistema primario de alto rendimiento y especializado para instalaciones de este tipo. El equipo redundante en ambos *sites* lo constituye una unidad *mini-split* de 1 tonelada de capacidad y serán activados manualmente en cuanto un equipo principal falle en cualquiera de los sites.
* **Se reforzarán las medidas de seguridad mediante el apego a las políticas respectivas.**

## **Seguridad en la transmisión**

Para reforzar la seguridad en la transmisión de datos, se implementarán las siguientes acciones, además de apegarse a las políticas de seguridad mencionadas en este plan:

| Categoría | Acciones |
| --- | --- |
| Equipos y Dispositivos | * El envío de datos se realizará de forma segura mediante paquetes codificados. * Durante el PREP 2024, las redes internas (alámbricas e inalámbricas) permanecerán restringidas al mínimo indispensable (perímetro seguro). * Se aplicarán medidas para la detección de intrusos a nivel red acorde con el volumen de tráfico esperado. * Uso de dispositivos de filtrado de paquetes de red (*firewalls*) para proteger el perímetro de la infraestructura tecnológica del data center principal y secundario. * Se establecerá una política restrictiva para configurar los dispositivos de filtrado, restringiendo todo el acceso de tráfico a la red del data center principal; solamente se deberá de habilitar el acceso a aquellos puertos que sean estrictamente necesarios. * Se debe de contar con equipos redundantes para los dos casos señalados en los puntos anteriores, del tal forma que se tenga un esquema de redundancia para garantizar que el tráfico estará siendo analizado por los dispositivos mencionados. |
| Conectividad | * La topología de la red estará enfocada en un esquema de alta disponibilidad. * Se debe de hacer una segmentación del tráfico de las diferentes capas de procesamiento de la información usando redes virtuales. * La información solamente debe de viajar desde los CATD hacia el data center principal y no a la inversa. Por lo tanto, la configuración de reglas de acceso en todos los dispositivos de comunicaciones debe de seguir este principio. * Se propone contar con un esquema de monitoreo proactivo de todos los enlaces de red. El centro de monitoreo podrá estar ubicado dentro del data center y/o el centro de operaciones del IEPC Jalisco. * La configuración de todos los dispositivos de comunicaciones involucrados (*switches, routers, y firewalls*) deberán de tomar como base las recomendaciones de seguridad de organismos reconocidos internacionalmente en la materia, como el Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés). |

## **Seguridad en el procesamiento**

Se sugiere implementar las siguientes acciones, además de apegarse a las políticas de seguridad mencionadas en este plan:

| Categoría | Acciones |
| --- | --- |
| Servidores de aplicaciones | * Para garantizar la alta disponibilidad del aplicativo, se debe implantar una arquitectura paralela distribuida de servidores interconectados entre sí. Mediante un mecanismo de balanceo de carga, cada servidor debe de tener la posibilidad de atender peticiones por parte de los CATD. * Cada servidor deberá contar con un sistema operativo especialmente diseñado para servidores de aplicaciones, como puede ser: Windows Server Enterprise Edition, Linux RedHat AS 4.0, entre otros. De manera adicional, se propone que se habiliten opciones para reforzar la seguridad a nivel del núcleo del sistema * Respecto al control de acceso, cabe mencionar que las reglas de control de tráfico que fueron aplicadas a nivel de dispositivos de comunicaciones fueron también configuradas a nivel de sistema operativo. Cada servidor procesó única y exclusivamente el tráfico que se consideró esperado. * Los servidores deberán contar con todas las actualizaciones en sistema operativo y paquetería necesarios y aplicables. |
| Servidores de bases de datos | Esta capa es de vital importancia, pues el primer paso en la estrategia de recuperación en caso de desastres consistirá en la correcta replicación de los datos entre el servidor de base de datos primario y el secundario, mismos que estarán instalados en el data center principal y secundario, respectivamente. Por esta razón, se deberán tomar las siguientes previsiones:   * Uso de tecnología de manejadores de base de datos (SQL Server, Oracle, etc.) para garantizar la alta disponibilidad y la correcta réplica de información entre los servidores de bases de datos del centro de cómputo. * Se sugiere el uso de tecnología de virtualización VMWare para facilitar el aprovisionamiento de escenarios de desarrollo y pruebas del sistema. * Adicional al control de acceso a nivel de sistema operativo, se deberán de aplicar los ajustes necesarios para que el manejador de la base de datos restrinja el acceso solamente a los usuarios autorizados. * Se debe de contar con un sistema de monitoreo proactivo, que permita conocer en todo momento el estado de la base de datos. * Los servidores deberán contar con todas las actualizaciones en sistema operativo y paquetería necesarios y aplicables. |
| Almacenamiento de datos | Este tema es crítico para el correcto funcionamiento de todo el sistema, por lo que se debe de considerar una red de almacenamiento SAN (Storage Area Network, por sus siglas en inglés) para brindar el nivel de certeza requerido. La configuración de la SAN debe considerar también elementos de seguridad informática, como los que se proponen a continuación:   * Red independiente, dedicada al almacenamiento, basada en la tecnología Fibre Channel. * Redundancia de los *switches*, asegurando así alta disponibilidad. * Balanceo de carga a nivel de servidor. * La configuración de la SAN debe de contemplar las mejores prácticas de seguridad referidas por organismos a nivel mundial. |
| Contratación de SOC | * Adicionalmente a los elementos mencionados, se sugiere la contratación e implantación de un Security Operation Center (SOC), el cual estaría conformado por un equipo de monitoreo-respuesta que esté integrado por personal especializado que lleve a cabo en tiempo real el análisis de los posibles incidentes de seguridad informática que llegaran a presentarse. Éste deberá de estar de manera constante en coordinación con áreas internas y externas para tomar las acciones pertinentes. |

## **Seguridad en la publicación**

La publicación de los resultados preliminares se llevará a cabo a través de los sitios web de los difusores oficiales. Dichos resultados serán enviados desde los servidores del IEPC Jalisco.

Los mecanismos de seguridad informática que se deberán implantar en este rubro consistirán en *firewalls* para protección del perímetro y la definición de un protocolo de transferencia de información en un solo sentido: del IEPC Jalisco hacia los diversos medios.

Se propone realizar la conexión con los medios a través de enlaces de comunicación dedicados, mediante los cuales se depositarán archivos en un equipo dedicado del difusor.

En adición a lo anterior, deberán apegarse a las políticas de seguridad mencionadas en este plan.

## **Robustecimiento de los controles de seguridad física y ambiental**

Se deberán implementar las siguientes medidas, además de apegarse a las políticas de seguridad mencionadas en este plan:

|  |  |
| --- | --- |
| Categoría | Acciones |
| Seguridad física | * Se deberá contar con personal de seguridad (pública o privada) para el resguardo de las instalaciones del IEPC Jalisco, sobre todo para aquellas en las que se encuentran los data center principal y secundario. * Se deberá contar con un control de acceso a las instalaciones, el cual consistirá en:   + Tener una bitácora para el registro de quienes ingresan y salen del edificio.   + Los empleados del IEPC Jalisco, especialmente quienes participarán en el PREP, deberán portar el gafete oficial de la institución, siempre a la vista.   + Revisión de pertenencias de los visitantes y empleados, asegurando la no portación de armas o dispositivos que impliquen un riesgo para las personas o el PREP. * Monitoreo permanente mediante equipo de CCTV (Circuito Cerrado de Televisión) en las instalaciones del IEPC Jalisco y en los data center. De ser posible, se sugiere lo mismo para los CATD. * Protección de equipo e Información sensible. * Seguridad perimetral en el centro de cómputo, así como en cada uno de los CATD. * Sistema de detección de intrusos en el centro de cómputo. * Se deberá contar con suministros de energía redundantes dentro del centro de cómputo para activos críticos durante el PREP 2024. * Separación adecuada de los cables de datos con los cables de energía eléctrica en los data center y, de preferencia, en todas las ubicaciones que participen en el PREP 2024. * Identificación del personal de mantenimiento de los servidores y equipos dentro del Centro de Cómputo autorizados. |
| Seguridad ambiental | Se deben tomar las siguientes medidas:   * Analizar las condiciones de humedad de los sitios en donde operarán los equipos de cómputo y servidores. * Mantener una temperatura adecuada para los equipos mediante equipo de aire acondicionado. * Contar con filtros de polvo. * Revisar las condiciones de las instalaciones de alimentación eléctrica. |

## **Creación del plan de contingencia**

La Dirección de Informática y sus coordinaciones definirán los planes de contingencia para el PREP 2024, siendo estos el **Plan de Continuidad del Negocio (BCP)** y el **Plan de Recuperación de Desastres (DRP)**.

El Plan de Continuidad del Negocio definirá las acciones que garanticen la ejecución de los procesos críticos del PREP 2024 para el acopio, digitalización, captura, verificación y publicación en caso de que se suscite una situación adversa o una contingencia, mientras que el Plan de Recuperación de Desastres (DRP) se enfocará en la recuperación de los servicios en caso de una situación de daños mayores o desastres.

Los objetivos de estos planes son:

* Asegurar la correcta operación del sistema PREP durante la jornada electoral.
* Minimizar el riesgo de fallas durante el PREP 2024.
* La recuperación de servicios tecnológicos soportados en el data center principal y secundario en el menor tiempo posible.
* Detectar oportunamente cualquier falla o interrupción en los servicios.
* Definir la estrategia para la recuperación de servicios en forma oportuna.
* Minimizar el riesgo de inconsistencia, pérdida o daños en la información y servicios.

## **Reporte de incidentes tecnológicos**

Se definirá un esquema de atención y escalamiento de los incidentes tecnológicos que se puedan presentar durante el desarrollo del PREP.

# Políticas de seguridad informática

## **Políticas de seguridad sobre usuarios**

Todo usuario de los servicios tecnológicos (voz, datos, video, Internet, etc.) deberá apegarse a estas políticas de seguridad informática.

* Los empleados que requieran acceso a los servicios y sistemas institucionales deberán:
  + Pertenecer oficialmente al IEPC Jalisco, es decir, haber firmado su contrato.
  + Sus accesos y/o la asignación de equipo de cómputo deberán ser definidos y solicitados a la Dirección de Informática por su jefe inmediato.
* Se impartirá un curso de inducción al personal de nuevo ingreso, en el cual se dará a conocer al nuevo servidor público las políticas de seguridad a las que debe apegarse.
* El usuario firmará un resguardo a través del cual acepta que se hace responsable del cuidado y buen uso del equipo asignado.
* El usuario recibirá su usuario y contraseña para el acceso a la red y su equipo de cómputo a través de personal de la Coordinación de Hardware.
* El usuario recibirá sus usuarios y contraseñas para el acceso a sistemas y aplicaciones institucionales a través del correo electrónico institucional.
* El usuario será el único responsable del uso que se dé a sus usuarios y contraseñas, por lo cual deberá:
  + No compartir su usuario y contraseña con otra persona.
  + Hacer un buen uso de sus privilegios de acceso a sistemas y aplicaciones.
  + No registrar sus usuarios y contraseñas en papeles o medios que permanezcan a la vista o sean de fácil acceso para otras personas.
  + Cerrar su sesión siempre al terminar sus actividades.
  + Cerrar su sesión siempre que requiera separarse o moverse del sitio en donde se encuentra su equipo de cómputo.

## **Políticas de control de accesos**

* El acceso a los servicios tecnológicos, sistemas y equipos de cómputo se llevará a cabo mediante el uso de usuarios y contraseñas.
* Los accesos serán asignados por las siguientes áreas:

|  |  |
| --- | --- |
| Área responsable | Permisos y/o privilegios a asignar |
| Coordinación de Software | * Sistemas institucionales * Servicios web |
| Coordinación de Hardware | * Equipos de cómputo * Correo electrónico * Servicios de red local |
| Coordinación de Redes y Comunicaciones | * Servicio de Internet * Conexión a sitios externos * Conexión desde sitios externos |

* + Para la generación de usuario:
    - Entregar de forma personalizada cada usuario y contraseña (un correo para cada usuario y solicitar su firma de recibido en documento).
    - Compartir estas políticas de seguridad a sus usuarios.
    - No enviar usuarios y contraseñas a correos electrónicos no institucionales.
    - Solicitar confirmación de recepción.
* Como medida de seguridad adicional, se considerará implementar una de las siguientes soluciones tecnológicas: servicios de gestión de identidades, software de doble factor de autenticación, directorio activo o Protocolo Ligero de Acceso a Directorios (LDAP por sus siglas en inglés), token en software y/o hardware para enrolamiento, con el fin de poder definir el esquema a implantar para el control de acceso lógico a los activos del PREP.

## **Políticas de seguridad en hardware**

* Los equipos cuentan sólo con el software indispensable para la jornada electoral y estos son configurados por la Coordinación de Hardware.
* Los equipos de cómputo cuentan con un antivirus instalado.
* Se contempla el control de acceso a equipos mediante uso de usuario y contraseña.
* Los usuarios y contraseñas son administrados en forma centralizada por la Coordinación de Hardware del IEPC Jalisco.
* Como medida de seguridad adicional, se considerará implementar una de las siguientes soluciones tecnológicas: servicios de gestión de identidades, software de doble factor de autenticación, directorio activo o Protocolo Ligero de Acceso a Directorios (LDAP por sus siglas en inglés), token en software y/o hardware para enrolamiento, con el fin de poder definir el esquema a implantar para el control de acceso lógico a los activos del PREP.
* Estarán inhabilitados los accesos a la navegación en sitios web.
* Se cuenta con un inventario de todos los equipos y dispositivos tecnológicos del IEPC Jalisco, el cual es actualizado una vez al año.
* Toda información generada como producto de las funciones de un servidor público (usuario) del IEPC Jalisco es propiedad del IEPC Jalisco, y responsabilidad del usuario almacenar dicha información en las unidades de red.
* La información almacenada en los equipos de cómputo personal no es respaldada por personal de la Dirección de Informática, por lo cual el usuario deberá apegarse al punto anterior.
* Queda prohibido el uso del equipo de cómputo asignado por el IEPC Jalisco para fines personales.

## **Políticas de seguridad en sistemas institucionales y software de terceros**

* El desarrollo de software para el IEPC Jalisco deberá realizarse bajo las siguientes políticas de la Coordinación de Software:
  + Apegarse a los lenguajes de programación estándar del área.
  + Utilizar los motores de base de datos estándar en el IEPC.
  + Deberá desarrollarse para plataformas Windows.
  + Las aplicaciones móviles deberán operar en plataformas iOS y Android.
  + El nuevo sistema desarrollado deberá apegarse a la infraestructura tecnológica existente.
* Los usuarios cuentan con acceso restringidos a los sistemas y servicios tecnológicos.
* La asignación de privilegio es de acuerdo con sus funciones y/o perfiles definidos.
* Cada usuario es responsable del buen uso de sus cuentas de acceso y contraseñas.
* Diariamente, a primera hora, se lleva a cabo un *checklist* para la verificación del correcto funcionamiento y operación de:
  + Servicios de red
  + Servicios de telefonía
  + Sistemas informáticos institucionales
* Se cuenta con un calendario anual para el pago de licenciamientos de software.

## **Políticas de seguridad en telecomunicaciones**

* Se cuenta con un esquema de seguridad en diferentes capas.
* Diariamente se lleva a cabo un *checklist* para verificar el correcto funcionamiento de:
  + Enlaces de telecomunicaciones en cada una de las sedes del IEPC.
  + Enlace de Internet.

## **Políticas de seguridad en Internet y redes sociales**

* El área normativa interna para la publicación de información en redes sociales e Internet es la Dirección de Comunicación Social.
* Toda publicación requerida por las diferentes áreas deberá ser validada por dicha área.
* La administración del sitio web principal del IEPC Jalisco (<https://iepcjalisco.org.mx>) es responsabilidad de la Dirección de Informática. No obstante, la Dirección no es responsable de los contenidos publicados en él. Los contenidos publicados serán responsabilidad del área solicitante de estos.

## **Políticas de acceso a los centros de datos (data centers)**

* El acceso a los centros de datos es restringido y sólo para personal autorizado.
* El acceso a los centros de datos deberá ser avalado por el director de Informática y/o el coordinador de Telecomunicaciones.
* Se cuenta con una bitácora junto a la puerta de cada data center, en la cual se registra cada una de las personas quienes ingresan, señalando el motivo de su visita y quién autorizó su acceso.
* Queda prohibido el acceso con alimentos, bebidas y demás líquidos a los centros de datos.
* Diariamente se lleva a cabo un *checklist*, el cual contempla la verificación de la operación de los siguientes elementos:
  + Servidores físicos
  + Servidores virtuales
  + UPS y su banco de baterías
  + Iluminación interna
  + Aire acondicionado
* Se contará con un data center secundario, el cual soportará los servicios, procesos electrónicos y sistemas críticos del IEPC Jalisco.

## **Resguardo de la información**

* Se cuenta con un esquema de respaldos de la información.
* Toda información institucional deberá ser almacenada en las unidades de red correspondientes.

## **Participación del ente auditor del PREP**

A efecto de constituir un mecanismo que permita realizar una evaluación objetiva del nivel de seguridad alcanzado con la aplicación de los controles y salvaguardas derivados del análisis de riesgos, se incluye en el presente Plan de Seguridad la participación del ente auditor del PREP para reducir vulnerabilidades en la infraestructura tecnológica; en este sentido, el ente auditor llevará a cabo pruebas de negación de servicio al sitio principal del Instituto y a los sitios del PREP para comprobar que la mitigación y los controles de seguridad funcionen adecuadamente.

# Plan de Continuidad

El objetivo del Plan de Continuidad es determinar las acciones que garanticen la ejecución de los procedimientos de acopio, digitalización, captura, verificación y publicación, derivado de una situación adversa o de contingencia.

Este plan de continuidad para el Programa de Resultados Electorales Preliminares se implementa como estrategia para salvaguardar la confidencialidad, integridad y disponibilidad de la información y servicios relacionados con dicho proceso, previo, durante y posteriormente al día de la Jornada Electoral. La Dirección de Informática cuenta con planes de contingencia que permiten garantizar la continuidad de los servicios críticos (BCP) y la recuperación de la operación en caso de desastres (DRP).

Es importante señalar también que, los CATD operan servidores locales con un sistema de *contenedores* que garantizan una operación continua independientes unos de otros y que permite el ciclo completo de digitalización y captura localmente.

En este esquema, es el servidor del CATD el único que se conecta, vía VPN, a nuestra infraestructura *on-premise* para enviar la información de las capturas, y lo hace de forma asíncrona, es decir, mantiene un canal de conexión al site principal a través del cuál va enviando información, y si por alguna razón se interrumpe dicho canal (falla de Internet, falla en site principal, etc.), el servidor del CATD continuará recibiendo y procesando sus capturas locales para enviarlas al *site* principal en cuanto la conexión se reestablezca.

Además, con base en los análisis de riesgos previos, se toman las siguientes consideraciones generales de continuidad:

| **Evento** | **Nivel de Riesgo** | **Impacto** | **Efecto** | **Plan de Continuidad** | **Tiempo de Respuesta** | **Responsable** |
| --- | --- | --- | --- | --- | --- | --- |
| **Falla en TCA, Servidor CATD, VPN** | Crítico | Alto | Imposibilidad de captura | Reemplazo de TCA, rehabilitación de servidor CATD o rehabilitación de VPN. | 30 – 50 min. | Coordinador de Informática en CATD |
| **Falla en site principal (*On-Premise*)** | Crítico | Alto | Imposibilidad de recibir datos desde todos los CATD y CVV | Evaluación rápida, restauración y/o activación de *site* alterno. | 10-30 min. | Dirección de Informática |
| **Falla eléctrica en *site* principal** | Crítico | Alto | Imposibilidad de mantener los servidores operando | Se cuenta con un *site* alterno. El *site* cuenta con un banco de baterías de alta capacidad que proveen hasta 5 horas de operación continua, además de una planta de energía a diésel de activación automática. | Menos de 1 min. | Dirección de Recursos |
| **Falla eléctrica en *site* secundario** | Crítico | Alto | Imposibilidad de mantener *site* alterno | El site cuenta con un banco de baterías de alta capacidad que proveen hasta 5 horas de operación continua además de planta de energía a gasolina (activación manual) | 20 min. (*site* secundario) | Dirección de Informática |
| **Falla eléctrica en CATD** | Crítico | Alto | Interrupción de captura de datos focalizada | Uso de UPS, plantas de energía o migración de CATD | 45-120 min. | Coordinador de Informática en CATD / Dirección de Informática |
| **Falla en red celular** | Importante | Medio | En fallo durante las primeras horas, falta de actas para captura adelantada | Uso de Wifi público (Red Jalisco) | 5-30 min. | CAEL |
| **Falta de personal** | Crítico | Medio | Reducción de capacidad de captura o ausencia focalizada | Movilización de personal | 5 min. - 2 horas | Dirección de Informática |
| **Falla en proveedor de nube** | Crítico | Alto | Publicación fuera de línea | Activación de clúster alterno | 5-20 min. | Dirección de Informática |
| **CATD sin Internet** | Importante | Alto | Información focalizada no publicada | En caso extremo, el equipo servidor puede trasladarse a otra sede para transmitir su información | 20 min. – 2 horas | Coordinador de Informática en CATD |

# Plan de Continuidad del Negocio (BCP)

El BCP es un plan que permite garantizar la no interrupción en la operación de los servicios críticos de la institución, y en este caso, del PREP.

Al presentarse una contingencia, ésta es identificada y se toman medidas inmediatas para que la continuidad de la operación en los sistemas protegidos no se vea afectados o interrumpidos en el tiempo que la contingencia es solucionada.

* El director de Informática deberá declarar la contingencia y dar luz verde para la ejecución de este plan.

## **Replicación de datos**

El sistema contemplado para esta protección se basa en la replicación y recuperación entre los dos centros de datos que se tienen en el Instituto: Centro de Datos Principal (IEPC - Unidad de Informática) y Centro de Datos Secundario (Bodega Electoral), independientemente de la tecnología en Hardware y Software y de entornos virtuales que se tiene en uno u otro centro de datos.

Diagrama

Descripción generada automáticamente

La replicación entre los centros de datos garantiza que la información contenida en el Centro de Datos Principal sea la misma contenida en el Centro de Datos Secundario, simultáneamente y en tiempo real, así que al momento de que por una contingencia el centro de datos principal tenga algún tipo de interrupción, el Centro de Datos replicado (secundario) entra en funciones de una manera transparente para las aplicaciones y los usuarios que utilizan los servicios y base de datos.

## **Interrupción de Replicación de Datos**

Al momento de ser declarada una contingencia, las funciones principales son asumidas por el centro de datos secundario (FAILOVER), y éste asume el control de las operaciones. Técnicamente el servicio de replicación se interrumpe y se queda en espera de que el centro de datos principal sea restablecido.

Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamente

Un FAILOVER puede ser determinado por problemas en el centro de datos principal, por fallas de hardware, problemas eléctricos, fallas lógicas en la base de datos o sistemas operativos, por fallas provocadas por virus o por actualizaciones defectuosas de aplicaciones.

## **Restablecimiento de Replica de Datos**

Una vez restablecido el centro de datos principal, la replicación se restablece y la integridad de ambos centros de datos deja de estar comprometida.

Diagrama

Descripción generada automáticamente

## **Información Histórica**

Para los casos en los cuales se requiera recuperar información a un punto específico en el tiempo, se realizan respaldos periódicos de los datos.

## **Difusión de Resultados**

Se cuenta con empresas y medios de comunicación que serán difusores de la página del PREP.

El servidor central remitirá cada una de las peticiones a cada uno de los difusores activos, y verificará en todo momento que todos los sitios de difusión cuenten con el mismo paquete de datos.

En el caso de que las empresas que funjan como difusores no resuelvan, se contará con un servidor extra de contingencia para realizar la difusión de los resultados por parte del IEPC Jalisco.

## **Suministro de Servicios en el Centro de Datos y CATD**

Se cuenta con equipos de respaldo ininterrumpido de energía eléctrica en los centros de datos, los cuales dan un tiempo de respaldo de energía suficiente para, en caso de ser necesario, activar los generadores de energía con los que se cuenta.

En los consejos distritales se cuenta con generadores de energía eléctrica, los cuales pueden ser utilizados para brindar servicio de electricidad en los CATD en caso de ser necesario.

Servicios para la conexión de los CATD al Sistema Informático del PREP, en los Consejos Distritales: se cuenta con 2 servicios de Internet, cada uno con distinto proveedor, lo que nos permite contar con una salida alterna en caso de alguna contingencia. En los consejos municipales se contará con un servicio de Internet, y en caso de ser necesario, se procederá a recurrir a una sede alterna para la conexión con los sistemas del PREP.

# Plan de Recuperación en Caso de Desastres (DRP)

El DRP se enfoca en la rehabilitación de los servicios críticos en caso de una contingencia mayor, la cual impida la operación del Centro de Datos Principal o la de alguna(s) sede(s) esenciales para la operación del PREP.

Algunas situaciones de este tipo son: un terremoto, inundación, incendio, colapso del edificio del Centro de Datos Principal, actos terroristas, etc.

En caso de presentarse una situación de esta magnitud, el IEPC Jalisco cuenta con estrategias que permitan la no interrupción de los servicios, los cuales son mencionados en el punto 6.3.4.

## **Contingencia en el Centro de Datos Principal**

Si el sitio en contingencia es el Centro de Datos Principal:

1. El Consejo General y/o la Secretaría Ejecutiva deberá declarar la contingencia y dará luz verde para la ejecución de este plan, notificando a los directores de las distintas áreas sobre la situación.
2. Se solicitará al personal del IEPC Jalisco que realice actividades críticas en ese momento y no cuenten con un equipo de cómputo que se traslade al Centro de Datos Secundario a fin de continuar operando desde ahí.
3. Al personal crítico que cuente con un equipo de cómputo y acceso a Internet se le pedirá que se retire del sitio y opere desde su casa, manteniéndose en comunicación constante con su área.
4. Al resto del personal se le pedirá que se retire a sus casas y se mantenga en comunicación constante con su área.

## **Contingencia en el Centro de Datos Secundario**

Si el sitio en contingencia es el Centro de Datos Secundario:

1. El director de Informática notificará al Consejo General sobre la contingencia.
2. El director de Informática girará instrucciones para la realización de respaldos de emergencia en el Centro de Datos Principal, iniciando con un respaldo completo y continuando con respaldos diferenciales o incrementales en forma periódica.

## **Contingencia en CATD**

Si la contingencia se presenta en un CATD:

1. Cualquier CATD, en caso necesario, tendrá la posibilidad de mover los trabajos propios del PREP a otro domicilio, haciendo uso del equipo con el que se cuenta, previa notificación y autorización del área central.
2. En el supuesto que no se pueda realizar el traslado de los equipos para continuar con la operación del PREP, se notificará al área central, para que las tareas se realicen en otro CATD.

# Fin de la Contingencia

Una vez concluida la contingencia, el área responsable, quien notificó inicialmente de la misma, notificará a las áreas correspondientes de la rehabilitación de los servicios y el regreso a la operación normal.

# Conclusiones

El presente Plan de Seguridad y Continuidad se ha desarrollado tomando como referencia las mejores prácticas de la norma ISO 27001:2013, la Metodología de Administración de Riesgos del INE y la metodología OCTAVE Allegro, aplicando estas en forma personalizada para el PREP 2024.

El objetivo de este es fortalecer la confidencialidad, integridad y disponibilidad de la información y los servicios tecnológicos que intervienen en el PREP 2024.

Se ha tomado como base los resultados obtenidos del proceso de administración de riesgos, en el cual se identificaron, evaluaron y definieron respuestas a los mismos.

De acuerdo con los criterios de evaluación de riesgo identificados, los activos críticos detectados con mayor exposición al riesgo para el PREP 2024 son:

* Sistema PREP (software)
* Servidores (de aplicaciones y bases de datos)
* Equipos de cómputo
* Celulares
* Planta de energía eléctrica
* UPS y su banco de baterías
* No Break
* Elementos del esquema de seguridad (antivirus, sistema de respaldos, *firewalls, switches*, etc.)
* Enlaces de telecomunicaciones.
* Servicio de Internet
* Data center principal y secundario
* Recursos humanos:
  + Personal técnico que desarrollará e implementará el sistema PREP.
  + Personal que operará el sistema PREP.
  + Personal técnico que dará soporte al sistema.
  + Auditores externos

Los servicios críticos brindados por terceros son:

* Servicio de Internet en las sedes del IEPC Jalisco para la publicación de resultados
* Servicio de Internet en los CATD.
* Servicio de electricidad (CFE)
* Servicio de telefonía móvil
* Sitios web de difusores

Los eventos o factores de riesgo con mayor exposición a los riesgos detectados son:

* Robo o alteración de equipos o dispositivos en los CATD
* Robo de celulares de los CAE
* Corte de energía eléctrica en data center principal
* Corte de energía eléctrica en data center secundario
* Corte de energía eléctrica en ubicaciones con urna electrónica, equipos de cómputo y/o escáneres
* Ataque malicioso al sistema PREP
* Ataque a los servidores físicos y/o en la nube
* Fallas en el servicio de Internet (en las sedes del IEPC Jalisco, CATD y/o casillas)
* Falla en la operación del sistema PREP
* Falla en el escáner

Con base en los puntos anteriores, se elaboró el **plan de seguridad informática**, dividido en los siguientes puntos:

* Fortalecimiento de la infraestructura tecnológica
* Seguridad en la captura de datos
* Seguridad en el data center principal y secundario
* Seguridad en la transmisión de datos
* Seguridad en el procesamiento de datos
* Seguridad en la publicación de resultados
* Robustecimiento de los controles de seguridad física y ambiental
* Creación del plan de contingencia

Además, se reforzaron las **políticas de seguridad**, las cuales se dividen en los siguientes temas:

* Políticas de seguridad sobre usuarios
* Políticas de control de accesos
* Políticas de seguridad en hardware
* Políticas de seguridad en sistemas institucionales y software de terceros
* Políticas de seguridad en telecomunicaciones
* Políticas de seguridad en Internet y redes sociales
* Políticas de acceso a los centros de datos (data centers)
* Resguardo de la información
* Participación del ente auditor del PREP

Finalmente, se cuenta con un **Plan de Continuidad** del PREP, el cual fue elaborado tomando en consideración los análisis de riesgos detallados con anterioridad, y enfocado en garantizar de la manera más eficiente, eficaz y oportuna la operación del Programa de Resultados Electorales Preliminares ante la concurrencia de diversos escenarios adversos.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Historial de versiones | | | | | **Número** | **Modificado** | **Autoría** | **Comentario** | | 1 | 01/Marzo/2024 | HGRS | Anteproyecto | | 1.1  1.2 | 02/Marzo/2024  02/Marzo/2024 | VMLT  HGA | Edición del anteproyecto  Edición del anteproyecto |   1.3 16/Marzo/2024 VMLT Edición del anteproyecto |