PROCESO ELECTORAL | CONCURRENTE 2020-2021 | Instituto Electoral y de Participación Ciudadana de Jalisco

Plan de Seguridad Informática

para el Programa de Resultados Electorales Preliminares (PREP) del Proceso Electoral Local 2021 del Estado de Jalisco

Abril 2021

Contenido

1. Glosario

IEPC	Instituto Electoral y de Participación Ciudadana del Estado de Jalisco
PREP 2021	Programa de Resultados Electorales Preliminares 2021
Data center	Centro del procesamiento de datos conformado por servidores informáticos.
CATD	Centro de Acopio y Transmisión de Datos.
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 2021.
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.

2. 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, 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, lineamiento 12; y Título II, Capítulo IV, lineamiento 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 Informática** 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 Informática que se utilizará para el Programa de Resultados Electorales Preliminares 2021 (PREP 2021) en el estado de Jalisco.

El Sistema PREP (SP) dará soporte al proceso electoral 2021 (PREP 2021) y consta de un conjunto de servicios, dispositivos y aplicaciones los cuales darán soporte a las tareas relativas a la digitalización, captura, verificación y publicación de información.

Para fines 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 esta.

Para ello, se tomarán como referencia:

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

3. Marco de Referencia

Debido a los múltiples acontecimientos en la actualidad de los llamados delitos informáticos es por lo que existen diversas herramientas destinadas a ayudar a cientos de compañías que existen en el mundo para proteger su activo más importante: la información. El término HACKER es muy conocido hoy día y corresponde o hace referencia a una persona que ingresa de manera indebida a los sistemas de información y sin autorización, para provocar daños en los millones de datos que estén almacenados. El ingreso ilegal, por así llamarlo, es lo que se conoce como una amenaza a la organización y/o empresa.

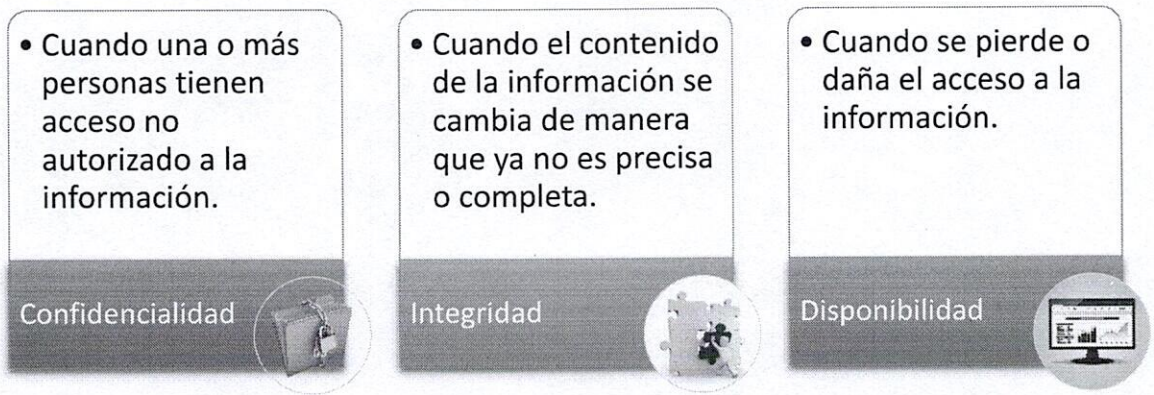
Es por esta razón, que con los avances tecnológicos se han ido creando de igual forma procedimientos y/o métodos que ayuden a descubrir con antelación esas vulnerabilidades, conocidas como debilidades, dentro de los sistemas. Estas existen tanto a nivel físico (como en el personal que administra los equipos), como a nivel lógico (en los equipos de seguridad, por ejemplo).

De esta manera, surgen las llamadas normas y metodologías de los sistemas de información, destinadas a trabajar conjuntamente con los integrantes de una empresa para determinar qué tipos de debilidades poseen, a qué tipo de amenazas están expuestos y como combatirlas o como evitarlas.

Para hablar de gestión de riesgo, se debe definir inicialmente qué es el riesgo, el cual se define como una probabilidad de que ocurra un evento. Este puede ser previsto y evitado.

Se debe tener en cuenta que el hecho de plantear una gestión para el riesgo no es solo para proteger sus activos de información, sino procurar que la empresa u organización logre cumplir su misión, por lo que al hablar de gestión se define como un ciclo reiterativo, que identifica, evalúa y ejecuta.

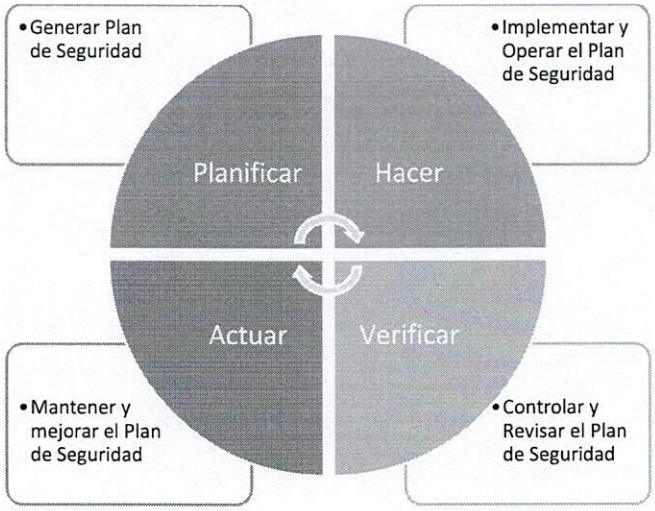
Los tipos de riesgos que la información sensible y de valor sufre se agrupan en 3 categorías:



Estos tipos de riesgo de seguridad de la información se conocen como "CID".

Los riesgos en la seguridad de la información generalmente surgen debido a la presencia de amenazas para los activos que procesan, almacenan, mantienen, protegen o controlan el acceso a la información, lo que da lugar a incidentes. Los activos en este contexto suelen ser personas, equipos, sistemas o infraestructura.

La ISO 27001 se basa en el ciclo PHVA o ciclo de Deming, el cual se puede resumir de la siguiente manera:



4. Objetivo

El objetivo de este documento es fortalecer la confidencialidad, integridad y disponibilidad de los activos de información para garantizar la correcta operación del Programa de Resultados Electorales Preliminares del proceso electoral 2021, desde su preparación, operación y actos posteriores a la Jornada Electoral.

4.1. 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 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.

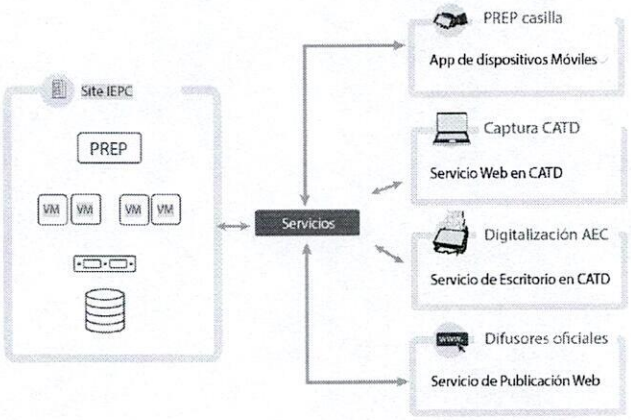
5. Alcance

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 2021, considerando al menos:

a. 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.
b. La implementación de los controles de seguridad en los distintos procesos y procedimientos electrónicos, a fin de mitigar los riesgos.
c. La confiabilidad y alta disponibilidad del sistema PREP.
d. Verificación de los resultados de la jornada electoral publicados.

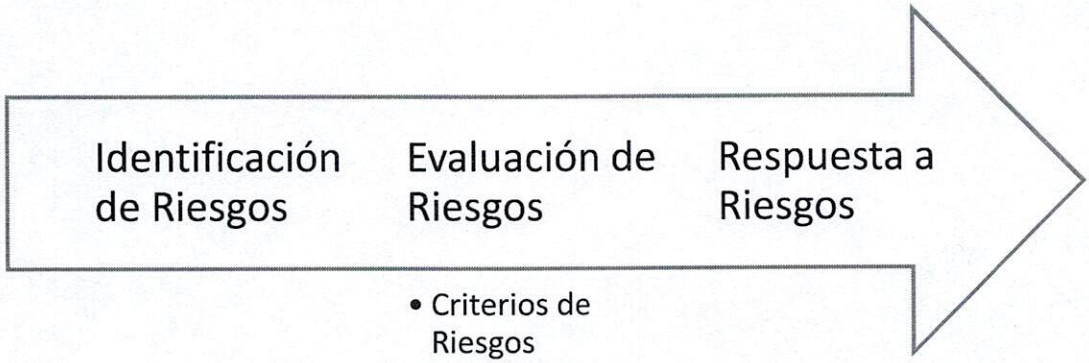
6. Sistema Informático PREP

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.



7. Proceso de Administración de Riesgos

El proceso de Administración de Riesgos contempla tres fases (identificación, evaluación y respuesta a los riesgos) divididas en seis actividades principales como se muestra a continuación:



- Criterios de Riesgos
- Evaluación de Riesgos
- Interacción de Riesgos
- Priorizar Riesgos

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

7.1. 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.

Eventos/Factores de Riesgo	Riesgo	Efecto
FACTORES INTERNOS		
Falla en la operación del sistema PREP	• No acceso al sistema. • No envío y/o recepción de datos.	• No procesamiento de datos. • No publicación de resultados en tiempo y forma.
Falla o alteración maliciosa en los equipos y/o celulares.	• 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 en tiempo y forma requeridos.	• 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.
Problemas de acceso al sistema por restricciones en la red.	• No tener acceso al sistema.	• No se podría capturar los resultados de las actas. • No 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. • 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 en el tiempo necesario.	• Posibilidad de pérdida de datos. • Imposibilidad de regresar a un punto específico en el tiempo.

Eventos/Factores de Riesgo	Riesgo	Efecto
Extravío de dispositivos de los equipos de cómputo o celulares asignados a los CAE (cables, accesorios, cargadores, etc.)	• No poder utilizar los equipos o celulares durante el PREP.	• Insuficiencia de equipos.
	FACTORES EXTERNO	
Corte de energía eléctrica en data center principal	• Suspensión de servicios en forma abrupta de todos los servicios tecnológicos. • Daño en la operación de los servidores. • Daño en las bases de datos. • Suspensión en envió de información y replicación hacia el data center secundario.	• Interrupción de recepción, almacenamiento, procesamiento y publicación de la información. • No acceso al sistema PREP y su información. • No acceso a la información, 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 2021.
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 de proceso electoral general y 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 2021.
Robo de celulares de los CAE	• No poder enviar la imagen de las actas.	• No poder verificar los resultados de las casillas.

Eventos/Factores de Riesgo	Riesgo	Efecto
Fallas en el servicio de internet (en las Sedes del IEPC, CATD y/o casillas)	• Incapacidad de envió de datos al data center principal para su procesamiento.	• Inconsistencia en el procesamiento automatizado de resultados.

7.2. Evaluación de Riesgos

7.2.1. 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 no mayor al 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 la actualización de los resultados.	Existe un retraso no mayor a 30 minutos en la actualización de resultados	Caída en los sistemas de publicación de los Resultados, que no permite hacer la consulta de los mismos
	Afectación de la credibilidad e imagen del PREP	La información relacionada con incidente de seguridad se conoce dentro del área de TI	La información relacionada con incidente de seguridad se conoce dentro del IEPC	La información relacionada con incidente de seguridad se conoce públicamente
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 el Presidente del IEEC.	El incidente de seguridad afecta gravemente al PREP y es conocido por la mayoría de los Consejeros Electorales

CRITERIO DE EVALUACIÓN DEL RIESGO	ÁREA DE IMPACTO	Nivel de Impacto		
		BAJO	MEDIO	ALTO
	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.
Seguridad/Salud	Riesgo en la Vida de las personas que participarán en el PREP.	No hay pérdida de vidas humanas o amenazas significativas de las personas que participan en el PREP. No es necesario establecer ningún procedimiento legal.	Existe un riesgo de pérdida de la vida de alguna persona, pero se recobra con tratamiento médico. Es posible que haya algún procedimiento legal ante el riesgo presentado.	Se pierde la vida de alguna persona, lo que desencadena procedimientos judiciales, así como altos costos económicos.
	Salud de las personas que participarán en el PREP.	Se afecta la salud de forma mínima de alguna persona que participa en el PREP. La salud es recobrada totalmente a los pocos días	Se afecta la salud de forma temporal alguna persona que participa en el PREP. La recuperación de la salud puede tomar varios días o incluso semanas. Existen gastos relacionados con el tratamiento médico	Se afecta gravemente la salud de alguna persona que participa en el PREP, al punto de ser permanente o que pueda tomar varias semanas o meses en recuperar. Existen altos costos de tratamiento médico, y se pueden presentar demandas legales.

CRITERIO DE EVALUACIÓN DEL RIESGO	ÁREA DE IMPACTO	Nivel de Impacto		
		BAJO	MEDIO	ALTO
	Seguridad Física y Ambiental	La seguridad física del Recinto Central o de los CATDs se ve comprometida en forma mínima. No se requiere presentar demandas legales, y las afectaciones económicas son de bajo costo (menores a $10,000.00).	La seguridad física del Recinto Central o de los CATDs se ve afectada. Es posible que se requiere presentar demandas legales, y las afectaciones económicas son inferiores a los $100,000.00 pesos.	Se presenta una violación grave a la seguridad física del Recinto Central o de los CATDs. Es obligado que se presente demandas legales así como investigaciones por las autoridades competentes. Se generan gastos superiores a los $100,000.
Implicaciones Legales	Multas	El incidente de seguridad generan multas menores a $1,000.00	El incidente de seguridad generan multas menores a $10,000.00	El incidente de seguridad generan multas superiores a $10,000.00
	Demandas	Existe el riesgo de una demanda, generada por algún incidente de seguridad.	Se presenta una demanda generada por el incidente de seguridad, y además genera gastos económicos inferiores a los $10,000.00. Existe el riesgo de la inhabilitación de un funcionario relacionado con el PREP.	Se presenta un incidente grave de seguridad, que genera una demanda, que pudiera generarse acciones penales. Además de generaron gastos económicos superiores a los $10,000.00. Existe la inhabilitación de algún funcionario relacionado con el PREP.
	Acciones Penales	Se genera un riesgo de alguna acción penal, sin que la gravedad amerite la privación de la libertad.	Se genera un incidente de seguridad que desencadena en una acción penal.	Se genera un incidente grave de seguridad, que provoca la aprehensión de alguna persona relacionada con el PREP.

7.2.2. 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 2021, 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 celulares, y su cargador, para envío de imágenes de actas. • Escáner para digitalización de actas. • Planta de energía eléctrica en data center principal y secundario. • UPS 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
Salud	• Medidas de sanitización y prevención de COVID 19

Servicios Críticos de Terceros para el PREP 2021:

- Servicio de internet en las sedes del IEPC para la publicación de resultados
- Servicio de internet (Infinitum) en los CATD.
- Servicio de Electricidad (CFE)
- Servicio de Telefonía Celular
- Sitios web de difusores.

7.2.2.1. Áreas de Amenaza

Se identifican las siguientes áreas de amenaza para el proceso PREP 2021:

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

7.2.3. 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	Muy Alto
Vital	Alto
Importante	Medio
Débil	Bajo
Marginal	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 Alto	Muy Alto	10
Crítico	Alto	Muy Alto	9
Vital	Muy Alto	Muy Alto	9
Crítico	Medio	Muy Alto	8
Vital	Alto	Muy Alto	8
Importante	Muy Alto	Muy Alto	8
Crítico	Bajo	Alto	7
Vital	Medio	Alto	7
Importante	Alto	Alto	7
Débil	Muy Alto	Alto	7
Crítico	Muy Bajo	Medio	6
Vital	Bajo	Medio	6
Importante	Medio	Medio	6
Débil	Alto	Medio	6
Marginal	Muy Alto	Medio	6
Vital	Muy Bajo	Medio	5
Importante	Bajo	Medio	5
Débil	Medio	Medio	5
Marginal	Alto	Medio	5
Importante	Muy Bajo	Baja	4
Débil	Bajo	Baja	4
Marginal	Medio	Baja	4
Débil	Muy Bajo	Baja	3
Marginal	Bajo	Baja	3
Marginal	Muy Bajo	Muy Baja	2

La exposición al riesgo de los eventos y/o factores de riesgo identificados para el PREP 2021 son los siguientes:

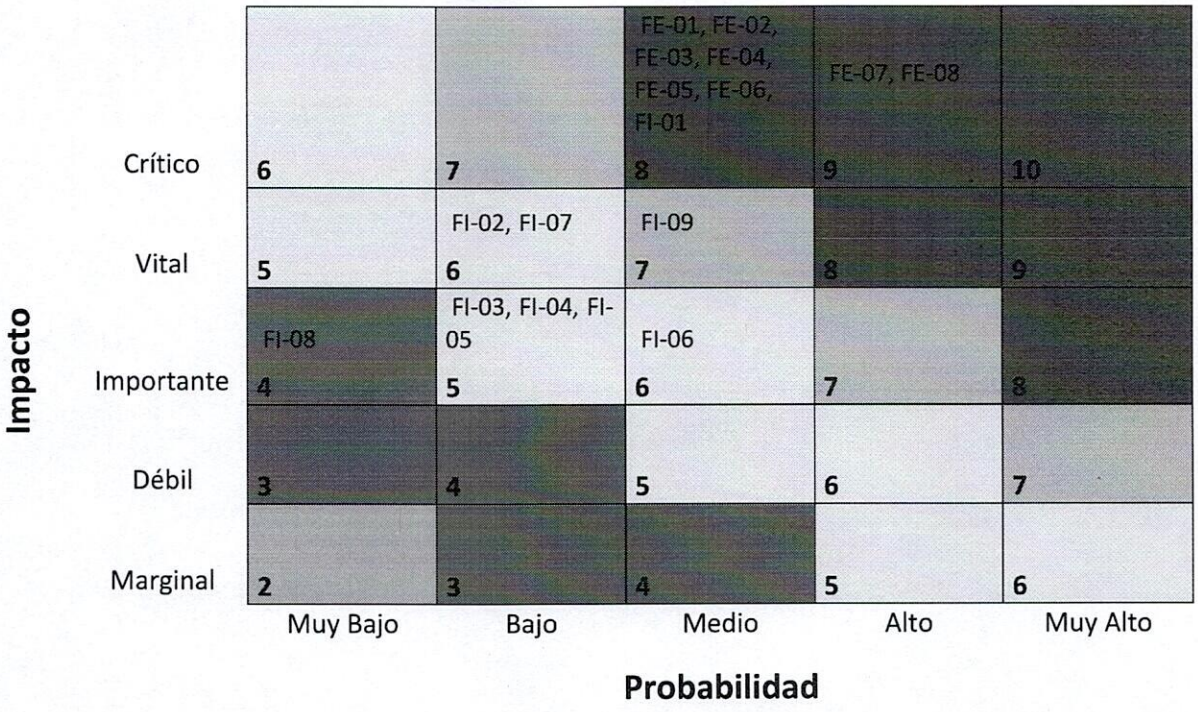
ID	Tipo de Factor	Eventos/Factores de Riesgo	IMPACTO	PROBABILIDAD	Exposición al Riesgo	
FE-01	Externo	**Corte de energía eléctrica en data center principal**	Crítico	Medio	Muy Alto	8
FE-02	Externo	**Corte de energía eléctrica en data center secundario**	Crítico	Medio	Muy Alto	8
FE-03	Externo	**Corte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

Los eventos ordenados por la Exposición al Riesgo quedan de la siguiente manera:

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

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

Dando como resultado el siguiente **Mapa de Riesgo**:



7.2.4. Priorización de Riesgos

La priorización de riesgos es el proceso donde se determinan las prioridades 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 Alto	Requiere de un plan de mitigación o control inmediato.
Alto	Se requiere asegurar estar preparado al riesgo.
Medio	Dar seguimiento al impacto acumulado de los riesgos.
Bajo	Requiere poco monitoreo.
Muy Bajo	Operación normal.

7.3. Respuesta a Riesgos

Los riesgos identificados y evaluados en los puntos anteriores serán mitigados mediante la implementación del Plan de Seguridad Informática y Políticas de Seguridad Informática.

7.3.1. Plan de Seguridad Informática

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

7.3.1.1. Plan de Concientización

Se implementará una campaña interna de concientización para el personal involucrado en la operación del PREP. Dicho plan contará con las siguientes características:

- Objetivo

  Dar a conocer los riesgos y amenazas que enfrenta el PREP y la forma de minimizarlos.

- Alcance

  Este plan será aplicable para todo el personal involucrado en la operación del PREP 2021.

- Reporte de Situación Actual

  Se llevará a cabo una encuesta, la cual nos permitirá conocer el nivel de concientización actual en el personal.

- Capacitación.

  Se impartirá un curso sobre este tema al personal involucrado. Parea ello, se llevará a cabo el diseño de formatos y material de apoyo, así como su contenido.

- Plan de Trabajo

  Se definirá un plan de trabajo para el desarrollo de esta campaña interna.

- Reporte de Situación Final

  Una vez impartida la capacitación al personal involucrado se aplicará una encuesta, la cual nos permita conocer el nivel de concientización del personal.

7.3.1.2. 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 2021, se optará por la contratación de servicios en la nube (servidores virtuales) para fines de asegurar la alta disponibilidad de los servicios durante el proceso electoral.
	Equipo de cómputo	Se solicitará el apoyo a la Secretaría de Administración para el préstamo en comodato de equipos de cómputo nuevos para el proceso.
	Teléfonos celulares	Se llevará a cabo la contratación de servicios de telefonía celular 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 fines de dar atención con prioridad alta en caso de una falla en el servicio de energía eléctrica.
Software	Sistema PREP	De acuerdo al análisis previo realizado por la Dirección de Informática del IEPC Jalisco, se decidió que el sistema informático que dará soporte al PREP 2021 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 (sistemas operativos, aplicaciones, etc.) vigentes, los cuales cuenten con soporte técnico por parte de los fabricantes.

Categoría	Subcategoría	Acciones
Telecomunicaciones	Enlaces de telecomunicaciones	*Redundancia en enlaces, ampliación de ancho de banda durante el PREP, etc.*
	Servicio de internet	Se ampliará el ancho de banda temporalmente para fines de contar con la capacidad requerida durante el PREP 2021, en el site de Bodega.
Seguridad Informática	Esquema de seguridad y telecomunicaciones.	Se revisará, actualizará y fortalecerá el esquema de seguridad en sus diferentes capas.

7.3.1.3. 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 cerrar 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 verificar y 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, por medio de 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.

7.3.1.4. 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:

- Contar con un enlace de telecomunicaciones, adicional al actual durante el proceso electoral.
- Se contará con servidores de alto desempeño con una configuración en paralelo con el Data center secundario, de tal forma de que en caso de una falla se active 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, 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. 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 2021. 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 en el Plan de Continuidad.
- 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. 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 contará con un sistema de enfriamiento (aire acondicionado) adecuado al tamaño, cantidad y características del equipo que se encuentre dentro. También se establecerá un plan alterno para en caso de que este sistema falle, el cual deberá contempla la utilización de un equipo de aire acondicionado de respaldo.
- Se reforzarán las medidas de seguridad mediante el apego a las políticas respectivas.

7.3.1.5. Seguridad en la Transmisión

Para reforzar la seguridad e 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 2021 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 y 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 enfocado 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 deben de seguir este principio.

Categoría	Acciones
	• 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).

7.3.1.6. 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 restringiera 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

Categoría	Acciones
	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 (Storage Area Network) 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.

7.3.1.7. 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.

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.

La conexión a los medios se propone que se realice a través de enlaces de comunicación dedicados, mediante los cuales se depositarán archivos en un equipo dedicado del difusor.

Además, deberán apegarse a las Políticas de Seguridad mencionadas en este plan.

7.3.1.8. 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, 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: o Tener una bitácora para el registro de quienes ingresan y salen del edificio. o Los empleados del IEPC, especialmente quienes participarán en el PREP, deberán portar el gafete oficial de la institución, siempre a la vista. o 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. o Aplicar las medidas sanitarias pertinentes antes de ingresar a las instalaciones: sanitización de las personas, uso de cubre bocas en todo momento, aplicación de gel anti bacterial, etc. • Monitoreo permanente mediante equipo de CCTV (Circuito Cerrado de Televisión) en las instalaciones del IEPC y en los Data center. De ser posible, se sugiere lo mismo para los CATD. • Controles Ambientales • 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 2021. • 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 2021. • 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. • Contar con sensores de incendio • Revisar las condiciones de las instalaciones de alimentación eléctrica. • Establecer un plan de evacuación en caso de incendio, sismo o algún evento meteorológico.

7.3.1.9. Creación del Plan de Contingencia

La Dirección de Informática y sus Coordinaciones definirán los planes de contingencia para el PREP 2021, 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 2021 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 2021
- 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.

7.3.1.10. 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.

7.3.2. Políticas de Seguridad Informática

7.3.2.1. Políticas generales

- Se llevarán a cabo campañas internas de seguridad, por lo menos una vez cada año.
- Se llevarán a cabo revisiones simultáneas en las diferentes áreas, por parte de la Dirección de Informática y/o sus Coordinaciones, esto con el fin de verificar que los usuarios apliquen las políticas de seguridad informática en el desempeño de sus labores.
- Se contará con un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación de Desastres (DRP), los cuales serán actualizados por lo menos una vez cada año.
- El Plan de Seguridad Informática deberá ser revisado y actualizado por lo menos una vez cada año.
- Todas las políticas de Seguridad Informática serán actualizadas por lo menos una vez cada año.

7.3.2.2. 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 quienes requieran acceso a los servicios y sistemas institucionales deberán:
  - Pertenecer oficialmente al IEPC, 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 a sistemas y aplicaciones institucionales a través del correo electrónico.
- 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.
    - 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.

7.3.2.3. 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 en Software	• Sistemas institucionales • Servicios web
Coordinación en 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 en forma personalizada cada usuario y contraseña (un correo para cada usuario o 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.

7.3.2.4. 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.
- Control de acceso a equipos mediante uso de usuario y contraseña.
- Los usuarios y contraseñas son administrados en forma centralizada por el área de hardware del IEPC Jalisco.
- Cerrar accesos de navegación (que no puedan navegar en internet)
- Se cuenta con un inventario de todos los equipos y dispositivos tecnológicos del IEPC, el cual es actualizado una vez al año.
- Toda información generada como producto de las funciones de un servidor público (usuario) del IEPC 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 sistemas, por lo cual el usuario deberá apegarse al punto anterior.
- Queda prohibido el uso del equipo de cómputo asignado por el IEPC para fines personales.

7.3.2.5. Políticas de Seguridad en Sistemas Institucionales y Software de Terceros

- El desarrollo de software para el IEPC 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 Android y IOS.
  - 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 a 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.

7.3.2.6. 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

7.3.2.7. 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 Área de Comunicación Social.
- Toda publicación requerida por las diferentes áreas deberá ser validada por dicha área.
- La administración del sitio web principal del IEPC (https://iepc.jalisco.org.mx) es responsabilidad de la Dirección de Informática. La administración del sitio, más no sus contenidos.
- Los contenidos publicados serán responsabilidad del área quien lo publica.

7.3.2.8. 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 a los centros de datos con líquidos y alimentos.

- Diariamente se lleva a cabo un check-list, 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.

7.3.2.9. 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.

8. Conclusiones y Recomendaciones

8.1. Conclusiones

El presente Plan de Seguridad Informática 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 2021.

El objetivo del mismo es fortalecer la confidencialidad, integridad y disponibilidad de la información y los servicios tecnológicos que intervienen en el PREP 2021.

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 a los criterios de evaluación de riesgo identificados, los activos críticos detectados con mayor exposición al riesgo para el PREP 2021 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
- Medidas de sanitización y prevención de COVID 19

Los servicios críticos, brindados por terceros son:

- Servicio de internet en las sedes del IEPC para la publicación de resultados
- Servicio de internet (Infinitum) en los CATD.
- Servicio de Electricidad (CFE)
- Servicio de Telefonía Celular
- 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, 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 Planes de Contingencia

Además, se reforzaron las Políticas de Seguridad, las cuales se dividen en los siguientes temas:

- Políticas generales
- 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

8.2. Recomendaciones

Las sugerencias o recomendaciones sobre el Plan de Seguridad son las siguientes:

- El IEPC Jalisco debería asegurarse, en forma anticipada, de contar con la infraestructura tecnológica adecuada para cada jornada electoral. Esto es, contar con:
    - Servidores de alto rendimiento con las capacidades de procesamiento y almacenamiento adecuadas para cada ejercicio electoral.
    - Se requiere incrementar la capacidad de almacenamiento de información.
    - Equipos de cómputo no obsoleto en el cual se puedan realizar pruebas anticipadas.
    - Solicitar a la Secretaría de Administración se provea, aún en préstamo o comodato anticipado, la asignación de equipos de cómputo al IEPC con las características de aquellos que serán brindados para la jornada electoral.
    - El IEPC deberá contar con las versiones vigentes (actuales) y el licenciamiento del software requerido durante la jornada electoral. No más software obsoleto o carencia de licencias.