

Análisis de Riesgos en Materia de Seguridad de la Información para el Programa de Resultados Electorales Preliminares

Proceso Electoral Local 2023-2024

Contenido

INTRODUCCIÓN 3

ANTECEDENTES 4

OBJETIVOS 6

I. FACTORES DE RIESGO 7

II. ACTIVOS CRÍTICOS 9

III. ÁREAS DE AMENAZA..... 17

IV. IDENTIFICACIÓN DE RIESGOS 19

V. ESTRATEGIA DE GESTIÓN DE RIESGOS. 29

Introducción

Hoy en día los sistemas de información son el alma de organizaciones, empresas y entidades, el grado de responsabilidad reposa en los sistemas, datos e información encaminados al logro de los objetivos internos, estos se pueden mejorar y mantener teniendo una adecuada sistematización y documentación.

El tratamiento de la información abarca aspectos que van desde el manejo de documentos en medio físico como el proceso de almacenaje y recuperación conocido también como proceso de gestión documental, hasta los sistemas de información que tenga la organización o sistemas externos a los que esté obligada a reportar información, pasando por aspectos tan importantes como la forma de almacenamiento de los datos digitales, modelos de respaldo de información y planes de contingencia o de continuidad del negocio, si existen, claro está, incluyendo además los sistemas físicos de protección y accesibilidad a sitios o áreas restringidas.

Antecedentes

En el Anexo 13 del Reglamento de Elecciones, en su Título II de la Implementación, Capítulo IV de las Consideraciones de Seguridad Operativa, en los numerales 12 y 13 se establece lo siguiente:

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

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

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

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

Objetivos

El objetivo principal del presente Plan de Seguridad es establecer las normas y procedimientos que minimicen los riesgos en los Recursos Humanos, el Equipamiento y las Telecomunicaciones que son parte de la columna vertebral del PREP. Estos procedimientos describen los mecanismos de seguridad aplicables para la prevención de los riesgos que pudiese presentarse durante la Jornada Electoral.

Así mismo, contempla restricciones a ciertos lugares, autorizaciones, perfiles de los usuarios, protocolos y todo lo necesario que permita del desarrollo del PREP, minimizando la probabilidad de posibles contingencias.

La finalidad del presente análisis es identificar los activos a proteger o evaluar, inherentes al Programa de Resultados Electorales Preliminares (PREP) que se ha de implementar para el Instituto Estatal Electoral de Hidalgo, durante la Jornada Electoral a verificarse el próximo Domingo 2 de junio del 2024, durante la cual se habrán de renovar los cargos de Diputados Locales y Ayuntamientos de la entidad.

La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis, con criterios de riesgo establecidos en este documento.

Los resultados obtenidos de este análisis van a permitir el desarrollo de un Plan de Seguridad orientado a prevenir la ocurrencia de los riesgos identificados mediante medidas específicas, esto involucra identificar el conjunto de opciones que existen para tratar los riesgos y evaluarlas.

Consecuencia de este documento, se ha generado un Plan de Continuidad encaminado a determinar las acciones que garanticen la ejecución de los procedimientos de acopio, digitalización, captura, verificación y publicación, en caso de que se suscite una situación adversa o de contingencia.

El plan deberá ser comunicado al personal involucrado en su ejecución y formar parte de los ejercicios y simulacros.

Para la realización del análisis de riesgos, se requiere evaluar los siguientes elementos:

I. Factores de Riesgo

Los criterios que se deberán tomar en cuenta para la valoración de los riesgos van de la mano con el nivel impacto que el riesgo en su ocurrencia tiene en el desarrollo y funcionamiento del PREP. En su intensidad estará el grado de magnitud en el daño potencial que represente para el PREP y estos factores los valoraremos en:

Matriz de Riesgos				
Matriz de calificación, evaluación y respuesta de riesgo				
Probabilidad	Alta	Zona de riesgo moderado Prevenir el riesgo	Zona de Riesgo Importante Prevenir el riesgo Mitigar el riesgo Transferir el riesgo	Zona de Riesgo Inaceptable Eliminar el riesgo Prevenir el riesgo Mitigar el riesgo Transferir el riesgo
	Media	Zona de Riesgo Tolerable Prevenir el riesgo	Zona de Riesgo Moderado Prevenir el Riesgo Mitigar el Riesgo Transferir el Riesgo	Zona de Riesgo Importante Eliminar el Riesgo Mitigar el Riesgo Transferir el Riesgo
	Baja	Zona de Riesgo Aceptable Aceptar el Riesgo	Zona de Riesgo Tolerable Mitigar el Riesgo Transferir el Riesgo	Zona de Riesgo Moderado Mitigar el Riesgo Transferir el Riesgo
		Bajo	Medio	Alto
Impacto				

- A. **Riesgo Bajo:** Los elementos a los que afecte no detendrán el funcionamiento del PREP; sin embargo, entorpecerán el desarrollo del mismo. Es importante al momento de determinar un Riesgo Bajo el daño que en su ocurrencia repetitiva pueda, por sí mismo, presentar el entorpecimiento del desarrollo de otras actividades lo cual en cadena representaría un Riesgo Medio o Alto.
- B. **Riesgo Medio:** Cuando el nivel de afectación puede ser mediado con la utilización de una medida emergente sin afectar el desarrollo del PREP, será considerado que el elemento presente un nivel de riesgo medio. Para los elementos definidos en este nivel será necesario que se instrumente paralelamente la medida contingente para su atención.
- C. **Riesgo Alto:** Los elementos que afecte este nivel de riesgo podrán poner en peligro la continuidad del PREP y deberán tener

la mayor prioridad en su inmediata atención. A estos elementos se les deberá poner atención permanente e implementar un plan de contingencia para solventar los daños generados por el mismo.

Para la determinación del nivel de riesgo, se deberá tomar en cuenta el tiempo que pudiese detener, en su eventual aparición, el funcionamiento del proyecto. En igual manera se medirán los tiempos para solventar la situación una vez presentada, incluyendo los recursos requeridos para su atención, ya sean humanos, financieros o materiales.

II. Activos Críticos

Los activos críticos del PREP son los elementos clave para el funcionamiento del mismo, se tipificarán de acuerdo a su naturaleza y se detallará en qué áreas de amenaza se localizan para su focalización y continuo monitoreo.

Clasificaciones y definiciones de los activos por áreas de localización		
Recursos Humanos	Equipamiento	Telecomunicaciones
Centros de Acopio y Transmisión de Datos (CATD)	Centros de Acopio y Transmisión de Datos (CATD)	Centros de Acopio y Transmisión de Datos (CATD)
Centros de Captura y Verificación (CCV)	Centros de captura y verificación (CCV)	Centros de captura y verificación (CCV)
Nube de Internet	Nube de internet	Nube de internet

Acorde a lo anterior, se determinaron tres tipos de activos críticos:

- A. Recursos Humanos**
- B. Equipamiento**
- C. Telecomunicaciones**

Las Áreas en que se localizarán los Activos Críticos son:

- a) Centros de Acopio y Transmisión de Datos (CATD)**
- b) Centros de Captura y Verificación (CCV)**
- c) Nube de Internet**

Cada uno de estos activos críticos se describen en detalle a continuación:

A. Recursos Humanos: Se detalla al personal que ha de participar en los CATD, los CCV y la nube de Internet:

a) Centros de Acopio y Transmisión de Datos

Recursos Humanos por Área de Localización	
Centros de Acopio y transmisión de datos (CATD)	Coordinadores
	Acopiadores
	Digitalizadores

- 1. Coordinadores:** Estarán a cargo de la operación del CATD, incluyendo Instalación, Adecuación, Personal, Materiales y elaboración de informes. Es el enlace entre los CATD y los CCV, toma decisiones en su ámbito de operación.
- 2. Acopiadores:** Recibirán los sobres con las Actas PREP, verificará su contenido y datos de identificación, detectará inconsistencias, registra en su Bitácora para Acopio de Actas PREP la fecha y hora de recepción en las Actas PREP y las entregará a los Digitalizadores.
- 3. Digitalizadores:** Digitalizarán las actas verificando su correcta legibilidad, en caso necesario repetirá el procedimiento asegurando la calidad de la imagen generada.

b) Centros de Captura y Verificación

Recursos Humanos por Área de Localización	
Centros de captura y verificación (CVV)	Supervisor general
	Coordinadores
	Verificador/ Foliador
	Capturista/Verificador
	Verificador/Validador
	Telefonista
	Archivistas
	Organizadores
Técnicos	

1. **Supervisor General:** Estará a cargo de la operación del personal y equipos, supervisará la capacitación, estará a cargo de los CATD y los CCV.
2. **Coordinadores:** Coordinarán al personal a su cargo por áreas, dará seguimiento al funcionamiento del equipamiento y elaborará informes.
3. **Verificador/Foliador:** Verificarán la correcta identificación de las imágenes de las actas, revisará inconsistencias.
4. **Capturista/Verificador:** Revisarán los votos obtenidos para los partidos o candidatos y los captará en el sistema.
5. **Verificador/Validador:** Verificarán la información capturada de las imágenes de las actas, corregirá y procesará inconsistencias.
6. **Telefonistas:** Realizarán el pase de lista de los CATD, darán las instrucciones de arranque, verificarán el avance de sus CATD y canalizará llamadas a los técnicos y al Supervisor General.
7. **Archivistas:** Estarán a cargo de los expedientes del personal y el soporte documental generado en los ejercicios.
8. **Organizadores:** Recibirán y generarán toda la información requerida en el PREP, elaborarán la Memoria del PREP.
9. **Técnicos:** Realizarán la instalación de los CATD y los CCV, darán soporte al funcionamiento de la totalidad del Equipamiento.

c) Nube de Internet

Recursos Humanos por Área de Localización	
Nube de internet	Técnicos

1. **Técnicos:** El personal técnico estará a cargo de monitorear permanentemente las telecomunicaciones y los enlaces a la nube de Internet, asegurando la operación continua del servicio.

B. Equipamiento: Aquí detallaremos el equipamiento que ha de emplearse en los CATD, los CCV y la nube de Internet:

a) Centros de Acopio y Transmisión de Datos

Equipamiento por Área de Localización	
Centro de Acopio y Transmisión de Datos (CATD)	Modem ADSL
	Equipo Satelital
	Modem Banda Ancha Móvil
	Teléfono
	Computadora
	Scanner
	Webcam
	Ups
	Regulador
	Planta de Energía

- 1. Módem ADSL:** La red estatal estará compuesta por enlaces ADSL para la conexión con la red de Internet y la conexión se realizará mediante módems provistos con esta tecnología.
- 2. Equipo Satelital:** En donde no exista ningún tipo de servicio local de Internet, se enlazarán mediante Internet Satelital usando el equipamiento requerido para este tipo de servicio.
- 3. Módem Banda Ancha Móvil:** Como medio contingente en todas las localidades donde se cuente con cobertura Celular, se emplearán Módems de Banda Ancha Móvil 4G para la transmisión de la información.
- 4. Teléfono:** Se instalarán aparatos telefónicos en cada uno de los CATD para entablar comunicación diaria permanente con los CCV. En los CATD donde no pueda proveer el servicio de telefonía fija, se empleará telefonía celular.
- 5. Computadora:** Para operar el equipo de digitalización y transmitir las imágenes digitalizadas se emplearán equipos de cómputo en cada uno de los CATD.
- 6. Scanner:** La digitalización de las imágenes de las actas de escrutinio y cómputo se realizará mediante Scanners o Multifuncionales que permitan preparar la información para digitalizarla y transmitirlas a los CCV.

7. **Webcam:** Cada uno de los CATD estará permanentemente monitoreado con cámaras Web para vigilar el funcionamiento de los mismos.
8. **Ups:** En caso de interrupciones cortas en la energía eléctrica se asegurará el funcionamiento del equipo de cómputo y telecomunicaciones, para lo cual se deberá instalar un Ups en cada CATD.
9. **Regulador:** La corriente eléctrica deberá estar regulada para proteger el equipo de cómputo y telecomunicaciones, para lo cual se deberá instalar un regulador de voltaje en cada CATD.
10. **Planta de Energía:** En prevención de fallos en el suministro de la energía eléctrica prolongados, provista por CFE, en cada uno de los CATD se deberá instalar una Planta de Energía Portátil.

b) Centros de Captura y Verificación

Equipamiento por Área de Localización	
Centro de Captura y Verificación (CCV)	Modem ADSL
	Cable Modem
	Teléfonos
	Switches
	Computadoras
	Video Cámaras
	Cañones de Proyección
	Ups
	Reguladores
	Plantas de Energía

1. **Módems ADSL:** Para el enlace principal de salida a la nube de Internet se contratará un servicio con las características necesarias para prever la demanda de información requerida por los CCV, esto se podrá hacer vía un Enlace ADSL de alta velocidad, siempre y cuando haya facilidades para la contratación del servicio.
2. **Cable Módem:** Como enlace redundante a la nube de Internet se podrá emplear un enlace a Internet con la compañía de Cable Local, siempre y cuando existan facilidades en sitio.
3. **Teléfonos:** Se instalarán aparatos telefónicos en los CCV para entablar una comunicación diaria permanente con los CATD localizados en todo el estado.

4. **Switches:** Para establecer la red local de datos, esta será controlada mediante los switches requeridos para enlazar todos los equipos por áreas a la red local.
5. **Computadoras:** Se instalarán computadoras para todas las áreas de los CCV tanto para la captura de las actas de escrutinio y cómputo, como para el monitoreo de los sistemas.
6. **Video Cámaras:** Se instalará un sistema de video vigilancia que permita mantener la vigilancia permanente de todas las áreas que componen los CCV, tanto en interiores como en exteriores.
7. **Cañones de Proyección:** Se montarán cañones de Proyección en los CCV para monitorear el avance del proceso electoral y como medio de transparencia para los representantes de los partidos políticos acreditados ante el PREP.
8. **Ups:** Como primera medida contingente de fallo de energía, se instalarán fuentes de poder ininterrumpida (UPS) a los cuales se conectarán todos los equipos de telecomunicaciones de la red y el equipo de cómputo, asegurando su funcionamiento en caso de falla en el suministro de energía por parte de CFE.
9. **Reguladores:** Con el propósito de proporcionar un suministro de voltaje estable al equipamiento de cómputo y telecomunicaciones se instalarán reguladores de voltaje a la totalidad de estos equipos.
10. **Plantas de Energía:** Se deberá contar con plantas de energía auxiliar como segunda medida emergente para usarse en casos de fallo de la energía principal proveniente de la CFE.

c) Nube de Internet

Recursos Humanos por Área de Localización	
Nube de internet	Servidores

1. **Servidores:** Es importante que los servidores empleados para este proyecto sean monitoreados permanentemente para asegurar el funcionamiento del PREP.

C. Telecomunicaciones: Para la construcción de la red estatal del PREP se deberá realizar con las siguientes características:

a) Centros de Acopio y Transmisión de Datos

Telecomunicaciones por Área de Localización	
Centros de Acopio y Transmisión de Datos (CATD)	Línea Telefónica
	Enlace ADSL
	Enlace Satelital
	Enlace Banda Ancha Móvil

- Línea Telefónica:** Se contratarán líneas telefónicas para cada uno de los CATD donde se cuente con facilidades, los sitios donde no sea posible se instalará telefonía Celular, el principal medio de comunicación entre los CATD y los CCV será la vía telefónica.
- Enlace ADSL:** En todos los Distritos donde se cuente con facilidades técnicas, se contratarán servicios de Internet ADSL como medio primario de transmisión de la información.
- Enlace Satelital:** Cuando no se cuente con infraestructura ni facilidades con ninguna Compañía Local de Internet, se instalará el servicio de Internet Satelital en esos CATD.
- Banda Ancha Móvil:** Como medio de respaldo en caso de contingencia en todas las localidades se verificará la disponibilidad de red para Banda Ancha Móvil 4G para en caso de requerirse usarla como medio de transmisión de información emergente.

b) Centros de Captura y Verificación

Telecomunicaciones por Área de localización	
Centros de Captura y Verificación (CCV)	Líneas Telefónicas
	Enlace ADSL
	Enlace Vía Cable

- Líneas Telefónicas:** Se contratarán líneas telefónicas suficientes para establecer comunicación diaria con cada uno entre los CCV y los CATD.

2. **Enlace ADSL:** Se podrá contar con conexión a Internet mediante Enlaces ADSL de alta velocidad, los cuales proveerán el medio de transmisión requerido para los volúmenes de transmisión de información necesarios para los CCV, siempre y cuando haya facilidades para la contratación del servicio.

3. **Enlace Vía Cable:** Se instalará el servicio de Internet con la Compañía de Cable Local como medio de conexión redundante a la nube de Internet, siempre y cuando existan facilidades del servicio.

c) Nube de Internet

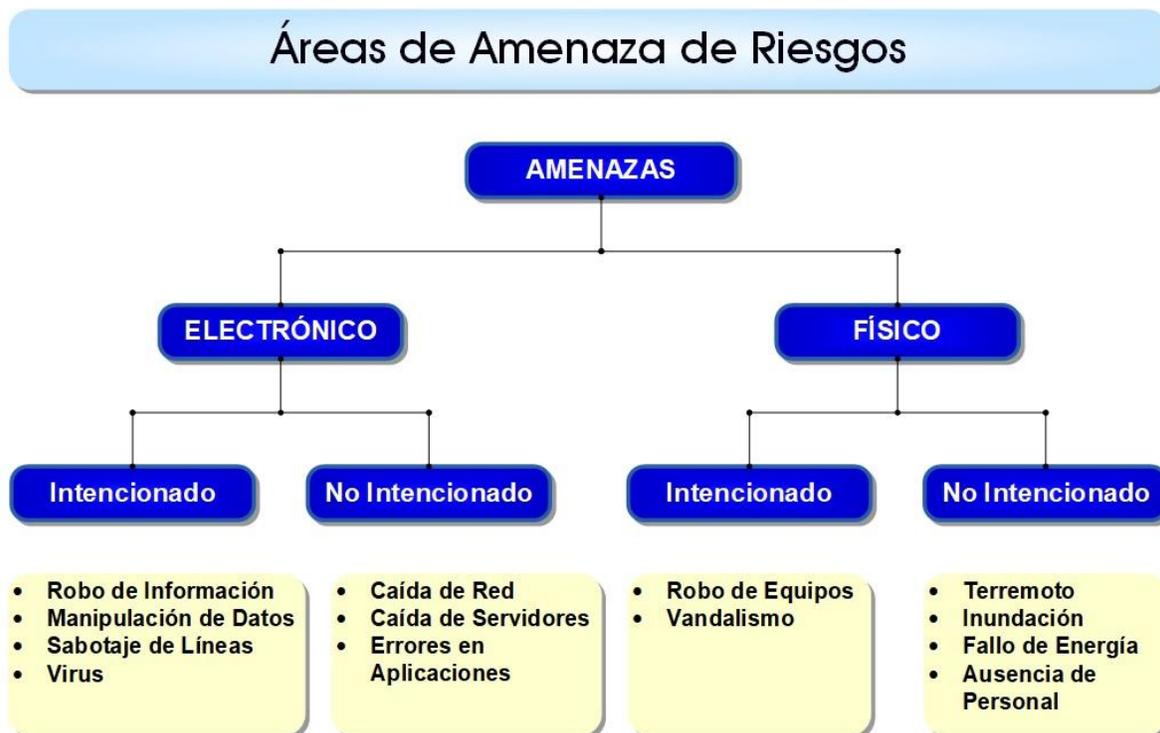
Telecomunicaciones por Área de Localización	
Nube de Internet	Enlace ADSL
	Enlace Vía Cable

1. **Enlace ADSL:** Se podrá contar con conexión a Internet mediante Enlaces ADSL de alta velocidad, los cuales proveerán el medio de transmisión requerido para los volúmenes de transmisión de información necesarios para los CCV, siempre y cuando haya facilidades para la contratación del servicio.

2. **Enlace Vía Cable:** Se instalará el servicio de Internet con la Compañía de Cable Local como medio de conexión redundante a la nube de Internet, siempre y cuando existan facilidades del servicio.

III. Áreas de Amenaza

De acuerdo al análisis del PREP, se detectaron tres áreas de amenaza que deberán ser consideradas durante todo el presente análisis:



Las Áreas en que se localizarán las Amenazas son:

A. Centros de Acopio y Transmisión de Datos

En cada uno de los Consejos Distritales Electorales definidos por el Instituto Estatal Electoral de Hidalgo, se instalará un CATD, el cual Acopiará y Digitalizará las Actas de Escrutinio y Cómputo para las elecciones de Diputados y Ayuntamientos, estos a su vez transmitirán la información de manera electrónica a los CCV del PREP para su proceso y publicación en la nube de Internet.

B. Centros de Captura y Verificación

En la Capital del Estado se instalarán los CCV, los cuales serán el ente neural del PREP y sus funciones serán las de recibir las imágenes de las actas procedentes de los CATD, capturar la información contenida en las mismas y publicar el resultado en la nube de Internet, incluyendo tanto las imágenes de las actas de escrutinio y cómputo como los datos capturados de estas.

C. Nube de Internet

Tanto la transmisión de los resultados desde los CATD a los CCV, como la publicación de los resultados del PREP será a través del uso de Servidores en la Nube de Internet. Es por ello que los mecanismos de transmisión desde los CATD a la Nube de Internet, como de la publicación de los datos procesados desde los CCV en la Nube de Internet, deberá incluir mecanismos de cifrado de la información tipo AES-256, los cuales garantizarán la confiabilidad de los datos recibidos y transmitidos de un punto a otro. Así mismo se contarán con mecanismos de Firewall internos que garanticen la no intromisión de intrusos en la red local y la red estatal del PREP.

Para simplificar el desglose de estas Áreas de Amenaza, en cada una de las Áreas en que se localizarán, las referiremos como:

- 1. Amenazas Electrónicas Intencionadas (AEI).**
- 2. Amenazas Electrónicas No Intencionadas (AEN).**
- 3. Amenazas Físicas Intencionadas (AFI).**
- 4. Amenazas Físicas No Intencionadas (AFN).**

IV. Identificación de Riesgos

Para la identificación de los riesgos potenciales del proyecto, tomaremos en cuenta los activos críticos previamente identificados de acuerdo a su área de amenaza y los elementos que le componen. Así mismo detallaremos su nivel de riesgo en cuanto al grado de afectación en el desarrollo del PREP.



Matriz de Identificación de Riesgos			
Activo Crítico	Área de Localización	Área de Amenaza	Afectación
Recursos Humanos	CATD	AEI	Aplica
		AEN	No Aplica
		AFI	Aplica
		AFN	Aplica
	CCV	AEI	Aplica
		AEN	No Aplica
		AFI	Aplica
		AFN	Aplica
	Nube de Internet	AEI	Aplica
		AEN	No Aplica
		AFI	No Aplica
		AFN	No Aplica
Equipamiento	CATD	AEI	Aplica
		AEN	Aplica
		AFI	Aplica
		AFN	Aplica
	CCV	AEI	Aplica
		AEN	Aplica
		AFI	Aplica
		AFN	Aplica
	Nube de Internet	AEI	Aplica
		AEN	Aplica
		AFI	No Aplica
		AFN	Aplica
Telecomunicaciones	CATD	AEI	Aplica
		AEN	Aplica
		AFI	Aplica
		AFN	Aplica
	CCV	AEI	Aplica
		AEN	Aplica
		AFI	Aplica
		AFN	Aplica
	Nube de Internet	AEI	Aplica
		AEN	Aplica
		AFI	Aplica
		AFN	Aplica

A. Recursos Humanos: Aquí detallaremos al personal que ha de participar en los CATD, los CCV y en la Nube de Internet:

Clasificación del activo	Área de localización	Área de amenaza	Afectación	Activo crítico	Nivel de riesgo
Recursos humanos	CATD	AEI	Aplica	1. Coordinadores	Bajo
		AEN	No Aplica		2. Acopiadores
		AFI	Aplica	3. Digitalizadores	Bajo
		AFN	Aplica		Medio
	CCV	AEI	Aplica	1. Supervisión general	Bajo
				2. Coordinadores	
		AEN	No Aplica	3. Verificador	Bajo
		AFI	Aplica	4. Capturista	Bajo
		AFN	Aplica	5. Verificador/ validador	
	6. Telefonista				
			7. Archivistas	Bajo	
			8. Organizadores		
			9. Técnicos		
	Nube de Internet	AEI	Aplica	1. Técnico	Bajo
		AEN	No Aplica		Bajo
		AFI	No Aplica		Bajo
AFN		No Aplica	Medio		
				Medio	

a) Centros de Acopio y Transmisión de Datos

- 1. Coordinadores:** Representan un nivel Bajo de Riesgo dado que en su ausencia el Acopiador podrán suplir sus funciones.
- 2. Acopiadores:** Se tipificó un Riesgo de nivel Bajo puesto que, en caso de ausentarse, sus funciones podrán ser realizadas por su compañero el Digitalizador o el Coordinador.
- 3. Digitalizadores:** En caso de que no se presentara, la ausencia del Digitalizador representa un nivel de Riesgo Bajo, ya que sus funciones podrán ser realizadas por su compañero el Acopiador o el Coordinador.

b) Centros de Captura y Verificación

- 1. Supervisor General:** Este puesto conlleva un nivel de Riesgo Medio, ya que esta persona tiene a su cargo el

funcionamiento de los CCV. En caso de su ausencia, los Coordinadores podrán realizar sus funciones.

2. **Coordinadores:** Se deberán contar con un grupo de Coordinadores para cada 8 a 12 personas por área de trabajo, dada su función de Coordinación y la toma de decisiones que se le encomendarán el nivel de Riesgo se tomará como Bajo, ya que, en caso de ausencia, otro Coordinador realizará sus funciones.
3. **Verificador/Foliador:** Ya que esta función en primera instancia es quien recibe e identifica las actas su nivel de riesgo es Bajo, puesto que, en caso de ausencia, cualquier otro compañero realizará sus funciones.
4. **Capturista/Verificador:** La confiabilidad de la información depende del personal de Captura, de ahí que el nivel de Riesgo para los mismos es Bajo y deberán implementarse mecanismos para asegurar el buen proceso de la información alimentada por ellos. En caso de ausencia cualquier otro Capturista puede suplir sus funciones.
5. **Verificador/Validador:** Este es el filtro final antes de la publicación de la información, por lo que su nivel de riesgo es Bajo, puesto que caso de su ausencia, cualquier otro compañero puede suplir sus funciones.
6. **Telefonistas:** Puesto que la función informativa que desempeñan no es en ninguna situación crítica para el proyecto, se les da un nivel de Riesgo Bajo, puesto que caso de su ausencia, cualquier otro compañero puede suplir sus funciones.
7. **Archivistas:** La actividad administrativa que desarrollan los Archivistas, es de bajo impacto en el desempeño que requiere el proyecto, por ello su nivel de Riesgo es Bajo. En caso de su ausencia, cualquier otro compañero u Organizador puede suplir sus funciones.
8. **Organizadores:** Dadas sus funciones netamente administrativas la falta de alguno no tendría repercusiones serias en el proyecto, por ello su nivel de Riesgo es Bajo. En caso de su ausencia, cualquier otro compañero o Archivista puede suplir sus funciones.

9. Técnicos: Para el caso de los Técnicos el nivel de Riesgo se tipificó como Medio, ya que en caso de ausencia de los mismos serían suplidos por un compañero de reserva.

c) Nube de Internet

1. Técnicos: Este personal, dada su función será Importante para el desarrollo del proyecto y por ende el nivel de Riesgo que representa es Medio. En caso de su ausencia, un compañero de reserva del área técnica puede suplir sus funciones.

- B. Equipamiento:** Aquí detallaremos los niveles de Riesgo para el equipamiento que ha de emplearse en los CATD, el CCV y en la nube de Internet:

Elementos de Riesgo							
Clasificación del Archivo	Área de localización	Área de Amenaza	Afectación	Activo Critico	Nivel de Riesgo		
Equipamiento	CATD	AEI	Aplica	1. <i>Modem ADSL</i>	Medio		
				2. <i>Equipo Satelital</i>	Medio		
		AEN	Aplica	3. <i>Modem Banda Ancha móvil</i>	Bajo		
				4. <i>teléfonos</i>	Bajo		
				5. <i>Computadoras</i>	Bajo		
				6. <i>Scanner</i>	Bajo		
		AFI	Aplica	7. <i>Web cam</i>	Bajo		
				8. <i>Ups</i>	Bajo		
		AFN	Aplica	9. <i>Regulador</i>	Bajo		
				10. <i>Planta de energía</i>	Medio		
	AEI			Aplica	1. <i>Modem ADSL</i>	Medio	
					2. <i>Cable Modem</i>	Medio	
		3. <i>teléfonos</i>	Bajo				
	AEN	Aplica	4. <i>Switches</i>	Bajo			
			5. <i>Computadoras</i>	Bajo			
			6. <i>Video cámaras</i>	Bajo			
			7. <i>Cañones de proyección</i>	Bajo			
	AFI	Aplica	8. <i>Ups</i>	Bajo			
			9. <i>Regulador</i>	Bajo			
	AFN	Aplica	10. <i>Planta de energía</i>	Medio			
AEI			Aplica	1. <i>Servidores</i>	Medio		
						AEN	Aplica
						AFI	No Aplica
	AFN	Aplica					

a) Centros de Acopio y Transmisión de Datos

- Módems ADSL:** En aquellos Consejos donde la conexión a la red de Internet sea mediante Telmex, el módem ADSL será el medio primario de envío de información, de ahí que su función es de Riesgo Medio.
- Equipo Satelital:** En donde no exista ningún tipo de servicio local de Internet, se enlazarán mediante Internet Satelital usando el equipamiento requerido para este tipo de servicio. Tanto los Módems Satelitales como el equipo requerido para la operación Satelital comparten el nivel de Riesgo Medio.

3. **Módems Banda Ancha Móvil:** Al ser un medio secundario y redundante su nivel de Riesgo es Bajo en cuanto al desempeño de la Red.
4. **Teléfonos:** Ya que existe cobertura de telefonía Celular en todas las cabeceras Distritales el nivel de Riesgo se tipifica en Bajo.
5. **Computadora:** La transmisión de la información digitalizada del contenido de las actas de escrutinio y cómputo a la nube de Internet estará controlada por un equipo de cómputo en cada CATD y se justifica como de Bajo Riesgo ya que habrá equipo de soporte.
6. **Scanner:** Conjuntamente al equipo de cómputo, el Scanner representa un elemento crucial en la digitalización de la información, por ello su riesgo es Bajo puesto que habrá equipo de soporte.
7. **Webcam:** El monitoreo por cámara en cada Distrito es requerido más no indispensable de ahí que su nivel de riesgo es Bajo.
8. **Up's:** El uso de las fuentes de poder ininterrumpido no es vital para evitar cortes de alimentación en el voltaje, ya que se contará con plante de energía auxiliar, por ello su nivel de Riesgo es Bajo.
9. **Regulador:** La buena alimentación de Voltaje eléctrico es indispensable para el funcionamiento de los CATD y los reguladores representan un activo crítico con Bajo Riesgo puesto que se deberán tener suficientes de respaldo.
10. **Planta de Energía:** Dada la frecuencia de recortes en el suministro de energía en el interior del estado, las plantas de energía tienen una prioridad de Riesgo Medio.

b) Centros de Captura y Verificación

1. **Módem ADSL:** La primera opción de enlace será mediante el uso de diversos enlaces ADSL de alta velocidad, por ello su nivel de Riesgo es Medio, siempre y cuando existan facilidades de servicio.
2. **Cable Módem:** El Módem para Internet por Cable es el equipo para establecer el enlace secundario redundante a la

red de Internet y por ello su nivel de Riesgo es Medio, siempre y cuando existan facilidades de servicio.

3. **Teléfonos:** Ya que existe cobertura de telefonía Celular en todas las cabeceras Distritales el nivel de Riesgo se tipifica en Bajo.
4. **Switches:** Se requieren diversos tipos de Switches para conformar la Red Local, y se podrán sustituir por equipo de soporte, por ello su prioridad de Riesgo es Bajo.
5. **Computadoras:** Los equipos de Cómputo son el medio principal de alimentación de información al sistema y su Riesgo es Bajo dado que habrá suficientes equipos de respaldo.
6. **Video Cámaras:** Las cámaras de video representan un nivel de Riesgo Bajo ya que no son indispensables para funcionamiento continuo del PREP.
7. **Cañones de Proyección:** El uso de los cañones para la exhibición interna de los resultados es de Riesgo Bajo, ya que la misma información estará visible en cualquier equipo conectado a Internet.
8. **Up's:** El uso de las fuentes de poder ininterrumpido no es vital para evitar cortes de alimentación en el voltaje, ya que se contará con plante de energía auxiliar, por ello su nivel de Riesgo es Bajo.
9. **Reguladores:** Al igual que los Up's los reguladores son de nivel de Riesgo Bajo para el buen funcionamiento de la red eléctrica, ya que deberá haber suficiente equipo de respaldo.
10. **Plantas de Energía:** Es de suma importancia asegurar el suministro continuo de la energía eléctrica de ahí que las Plantas de Energía son de nivel de Riesgo Medio.

c) **Nube de Internet**

1. **Servidores:** Todos los servidores empleados para el proceso son intrínsecamente indispensables para el funcionamiento del PREP por eso su nivel de Riesgo es Medio dado que existirán servidores de respaldo.

C. Telecomunicaciones: En cuanto a las telecomunicaciones se identificaron los siguientes elementos:

Elementos de riesgo						
Clasificación del archivo	Área de localización	Área de amenaza	Afectación	Activo critico	Nivel de riesgo	
Telecomunicaciones	CATD	AEI	Aplica	1.Línea telefónica	Medio	
		AEN	Aplica	2. Enlace ADSL	Medio	
		AFI	Aplica	3. Enlace satelital	Medio	
		AFN	Aplica	3. enlace de banda Ancha móvil	Bajo	
	CCV	AEI	Aplica	1.linea telefónica	Medio	
		AEN	Aplica	2.Enlace ADSL	Medio	
		AFI	Aplica	3.Enlace Vía Cable	Medio	
		AFN	Aplica		Medio	
	Nube de Internet	AEI	Aplica	1.Enlace ADSL	Medio	
		AEN	Aplica		Medio	
		AFI	Aplica	2.Enlace Vía Cable	Medio	
		AFN	Aplica		Medio	

a) Centros de Acopio y Transmisión de Datos

- 1. Línea Telefónica:** Las líneas telefónicas serán los principales medios de que se emplearán para establecer la comunicación entre los CATD con los CCV, más aún en los sitios donde se emplearán enlaces ADSL el buen funcionamiento de la línea es crítico para portar esta señal ADSL, es por ello que el nivel de Riesgo para las mismas es Medio ya que se puede usar comunicación celular.
- 2. Enlace ADSL:** Donde existan facilidades de Telmex, el principal medio de transmisión de información será la señal ADSL, de ahí que se dará prioridad al buen funcionamiento de la misma elevando con ello el Riesgo a Medio, salvo de no existir cobertura 3G se pudiera considerar Alto.
- 3. Enlace Satelital:** Si en algún Consejo no existe ningún tipo de servicio local de Internet, se empleará señal de Internet Vía Satelital como medio primario de transmisión de información siendo un nivel de Riesgo Medio.

4. **Enlace Banda Ancha Móvil:** En todos los Distritos donde se tenga cobertura celular, se tendrá una conexión vía Banda Ancha Móvil como medio alternativo redundante para transmisión de información más al ser redundante no resulta crítico y su nivel de Riesgo será Bajo.

b) Centros de Captura y Verificación

1. **Línea Telefónica:** Desde los CCV se llevará el monitoreo de todos los Centros de Acopio y Transmisión de Datos, esto realizará tanto por vía telefónica como por un sistema dedicado de monitoreo, es por ello que las líneas telefónicas son vitales para este propósito siendo de Medio Riesgo su disponibilidad ya que se cuenta con comunicación vía celular.
2. **Enlace ADSL:** La conexión principal con la Nube de Internet será primariamente Enlace ADSL, los cuales deberán funcionar permanentemente desde su instalación hasta el día posterior a la Jornada Electoral, su prioridad de riesgo es por lo mismo Medio dado que existen enlaces redundantes.
3. **Enlace vía Cable:** El enlace redundante secundario para la transmisión y recepción de información será mediante un enlace vía la Compañía de Cable Local, el cual deberá funcionar permanentemente desde su instalación hasta el día posterior a la Jornada Electoral, su prioridad de riesgo es Medio.

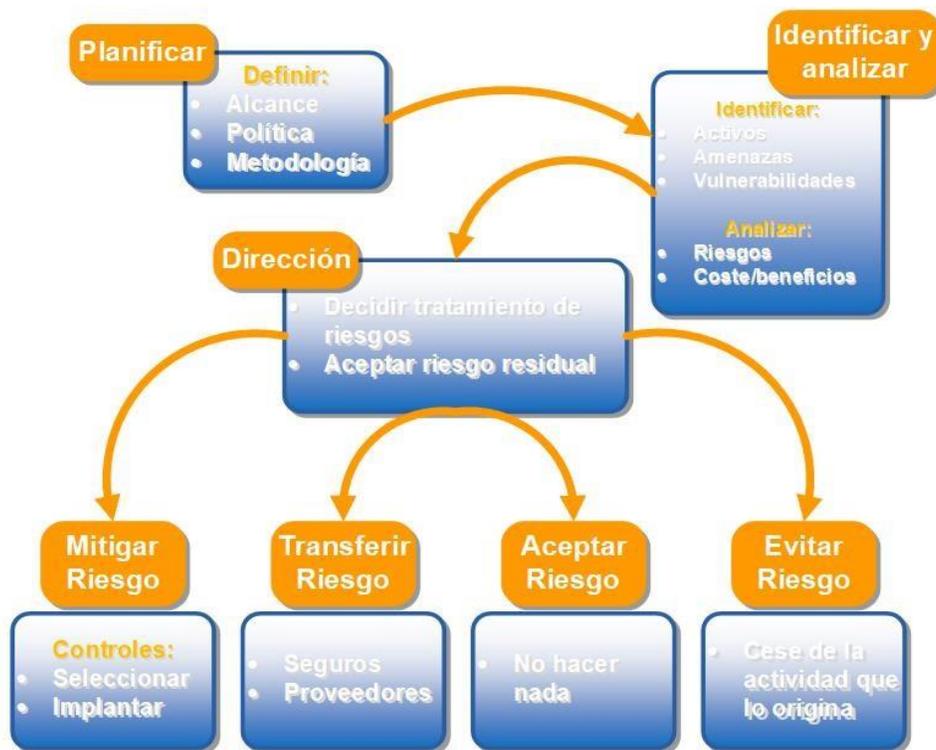
c) Nube de Internet

1. **Enlace ADSL:** La conexión principal con la Nube de Internet será primariamente Enlace ADSL, los cuales deberán funcionar permanentemente desde su instalación hasta el día posterior a la Jornada Electoral, su prioridad de riesgo es por lo mismo Medio, puesto que existen enlaces redundantes.
2. **Enlace Vía Cable:** El enlace redundante secundario para la transmisión y recepción de información será mediante un enlace vía la Compañía de Cable Local, el cual deberá funcionar permanentemente desde su instalación hasta el día posterior a la Jornada Electoral, su prioridad de riesgo es Medio. Nota se evaluará cuál de los dos medios proporciona el mejor servicio para seleccionar cual será el principal y cuál será el redundante, ya sea ADSL o Cable, siempre y cuando existan facilidades de servicio.

V. Estrategia de Gestión de Riesgos.

Con el propósito de dictar medidas tendientes a la Gestión de los Niveles de Riesgos identificados, se elaborará tanto un Plan de Seguridad tendiente a la prevención de los mismos, como un Plan de Continuidad que será implementado en caso de ocurrir cualquier contingencia.

Estrategia de Gestión de riesgos



- **Mitigar:** Aplicar las estrategias de gestión mediante la aplicación del plan de continuidad.
- **Transferir:** Transferir el riesgo a terceros o proveedores de servicios.
- **Aceptar:** Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos.
- **Eliminar:** Eliminar el riesgo, mediante el cese de las actividades que lo originan.

De acuerdo con la Identificación de Riesgos, seleccionaremos la estrategia para afrontar cada uno de ellos:

A. Recursos Humanos: Aquí detallaremos al personal que ha de participar en los CATD, los CCV y en la nube de Internet:

Estrategia de Gestión de Riesgos							
Clasificación del activo	Área de Localización	Área de Amenaza	Afectación	Activo Critico	Nivel de Riesgo	Estrategia	
Recursos Humanos	CATD	AEI	Aplica	1.Coordinadores	Bajo	Mitigar	
		AEN	No Aplica	2.Acopiadores	Bajo	Mitigar	
		AFI	Aplica				
		AFN	Aplica	3.Digitalizadores	Bajo	Mitigar	
	CCV		AEI	Aplica	1.Supervisor General	Medio	Mitigar
					2.Coordinadores	Bajo	Mitigar
			AEN	No Aplica	3.Verificador/Foliador	Bajo	Mitigar
					4-Capturista	Bajo	Mitigar
					5.Verificador/Validador	Bajo	Mitigar
			AFI	Aplica	6.Telefonista	Bajo	Mitigar
					7.Archivista	Bajo	Mitigar
					8.Organizadores	Bajo	Mitigar
					9.Tecnicos	Bajo	Mitigar
	Nube de Internet		AEI	No Aplica	1.Tecnicos	Medio	Mitigar
			AEN	No Aplica			
			AFI	No Aplica			
AFN			No Aplica				

a) Centros de Acopio y Transmisión de Datos

- 1. Coordinadores:** La contingencia es mitigable ya que, en caso de no presentarse, el Acopiador o el Digitalizador podrá suplir su ausencia.
- 2. Acopiadores:** De no presentarse durante la Jornada, el Digitalizador o el Coordinador podrá mitigar su ausencia asumiendo sus responsabilidades.
- 3. Digitalizadores:** En caso de que no se presentara, se podrá mitigar su ausencia, ya que sus funciones podrán ser realizadas por su compañero el Acopiador o el Coordinador.

b) Centros de Captura y Verificación

1. **Supervisor General:** Para poder mitigar su ausencia, se deberá prever dicha contingencia con la capacitación de los Coordinadores para asumir sus funciones.
2. **Coordinadores:** Se deberán contar con suficientes Coordinadores para que la ausencia de uno pueda ser mitigada con la ayuda de un similar.
3. **Verificador/Foliador:** Se mitigará la ausencia de alguno capacitando adecuadamente a Capturistas/Verificadores en esta función.
4. **Capturista/Verificador:** Previendo la contingencia de ausencia de Capturistas/Verificadores se deberá contar con personal adicional al requerido que mitigará como comodines a los Verificadores y Capturistas/Verificadores.
5. **Verificador/Validador:** Se mitigará la ausencia de alguno capacitando adecuadamente a Capturistas/Verificadores en esta función.
6. **Telefonistas:** En caso de ocurrir la inasistencia de alguna, se mitigará con el auxilio de su Coordinador.
7. **Archivistas:** En caso de no contar con algún archivero, dicha inasistencia podrá ser mitigable con la asistencia de los Organizadores.
8. **Organizadores:** Si no se contara con alguno de los Organizadores, se mitigará su falta con el auxilio de un Archivero.
9. **Técnicos:** Dado lo importante de sus funciones, los técnicos serán todos capacitados en las mismas funciones para que cualquiera de ellos pueda realizar las funciones de los demás mitigando esta posible contingencia de ausencia en alguno.

c) Nube de Internet

1. **Técnicos:** Previendo la ausencia de alguno de estos técnicos, se mitigará con la presencia de técnicos de reserva, contando con el nivel de experiencia requerido.

B. Equipamiento: Aquí detallaremos los niveles de Riesgo para el equipamiento que ha de emplearse en los CATD, el CCV y en la nube de Internet:

Estrategia de gestión de riesgo								
Clasificación del archivo	Área de localización	Área de amenaza	Afectación	Activo critico	Nivel de riesgo	Estrategia		
Equipamiento	CATD	AEI	Aplica	1.Modem ADSL	Medio	Transferir		
						Transferir		
						Mitigar		
					2.Equipo Satelital		Mitigar	
					3.Modem De Banda Ancha Móvil		Mitigar	
			AEN	Aplica	4.Telefonos	Medio	Mitigar	
					5.Computadoras			
					6.Escaner			
			AFI	Aplica	7.Web Cam	Medio	Mitigar	
		8. Ups			Mitigar			
		9.Regulador			Mitigar			
		10.Planta De Energía			Mitigar			
		AFN	Aplica		Bajo	Mitigar		
		CCV	AEI	Aplica	1.Modem ADSL	Medio	Transferir	
							Transferir	
							Mitigar	
					3.Modem De Banda Ancha Móvil		Mitigar	
							Mitigar	
			AEN	Aplica	4.Telefonos	Medio	Mitigar	
					5.Computadoras		Mitigar	
			AFI	Aplica	6.Escaner	Medio	Mitigar	
					7.Web Cam			
	AFN	Aplica	8. Ups	Medio	Mitigar			
			9.Regulador		Mitigar			
			10.Planta De Energía		Mitigar			
	Nube de Internet	AEI	Aplica	1.Servidores	Medio	Transferir		
		AEN	Aplica		Medio			
		AFI	No Aplica		Medio			
		AFN	Aplica		Medio			

a) Centros de Acopio y Transmisión de Datos

1. **Módems ADSL:** Previendo la falla en alguno de estos equipos, se transferirá al proveedor la posible falla de alguno, solicitando con anticipación equipos de respaldo y mitigarlo de forma inmediata.
2. **Equipo Satelital:** En caso de falla en alguno de estos equipos, se transferirá al proveedor la posible falla de alguno, contando con equipo suficiente de respaldo para esta contingencia y mitigarlo de forma inmediata.
3. **Módem Banda Ancha Móvil:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
4. **Teléfonos:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia. Adicionalmente se contará con equipos celulares de respaldo.
5. **Computadoras:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
6. **Scanner:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
7. **Webcam:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
8. **Ups:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
9. **Regulador:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
10. **Planta de Energía:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.

b) Centros de Captura y Verificación

1. **Módem ADSL:** Previendo la falla en alguno de estos equipos, se transferirá al proveedor la posible falla de alguno, solicitando con anticipación equipos de respaldo y mitigarlo de forma inmediata.
2. **Cable Módem:** Previendo la falla en alguno de estos equipos, se transferirá al proveedor la posible falla de alguno, solicitando su reposición inmediata, contando con equipo suficiente de respaldo para esta contingencia y mitigarlo de forma inmediata.
3. **Teléfonos:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia. Adicionalmente se contará con equipos celulares de respaldo.
4. **Switches:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
5. **Computadoras:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
6. **Video Cámaras:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
7. **Cañones de Proyección:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
8. **Ups:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.
9. **Reguladores:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.

10. Plantas de Energía: En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.

c) Nube de Internet

1. Servidores: Dado que los servidores se hallan en la nube de Internet se transferirá al proveedor la contingencia de falla en alguno, pero se contará adicionalmente con servidores redundantes para esta contingencia.

C. Telecomunicaciones: En cuanto a las telecomunicaciones se identificaron los siguientes elementos:

Elementos de riesgo						
Clasificación del archivo	Área de localización	Área de amenaza	Afectación	Activo crítico	Nivel de riesgo	Estrategia
Telecomunicaciones	CATD	AEI	Aplica	1.Línea telefónica	Medio	Transferir
		AEN	Aplica	2. Enlace ADSL	Medio	Transferir
		AFI	Aplica	3. Enlace satelital	Medio	Transferir
		AFN	Aplica	3. enlace de banda Ancha móvil	Bajo	Mitigar
	CCV	AEI	Aplica	1.linea telefónica	Medio	Transferir
		AEN	Aplica	2.Enlace ADSL	Medio	Transferir
		AFI	Aplica	3.Enlace Vía Cable	Medio	Transferir
		AFN	Aplica		Medio	Transferir
	Nube de Internet	AEI	Aplica	1.Enlace ADSL	Medio	Transferir
		AEN	Aplica		Medio	Transferir
		AFI	Aplica	2.Enlace Vía Cable	Medio	Transferir
		AFN	Aplica		Medio	Transferir

a) Centros de Acopio y Transmisión de Datos

- 1. Línea Telefónica:** De presentarse fallas en las líneas se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usarán líneas celulares.
- 2. Enlace ADSL:** De presentarse fallas en los servicios se transferirá al proveedor el reporte para su reparación

inmediata. Como contingencia se usarán conexiones de Banda Ancha Móvil.

3. **Enlace Satelital:** De presentarse fallas en los servicios se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usarán conexiones Banda Ancha Móvil.
4. **Conexión Banda Ancha Móvil:** En caso de falla en alguno de estos equipos, se mitigará contando con equipo suficiente de respaldo para esta contingencia.

b) Centros de Captura y Verificación

1. **Línea Telefónica:** De presentarse fallas en las líneas se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usarán líneas celulares.
2. **Enlace ADSL:** De presentarse fallas en el servicio se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se emplearán otro enlace redundante o el enlace Vía Cable.
3. **Enlace Vía Cable:** De presentarse fallas en el servicio se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usará el Enlace ADSL.

c) Nube de Internet

1. **Enlace ADSL:** De presentarse fallas en el servicio se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se emplearán El enlace Vía Cable.
2. **Enlace Vía Cable:** De presentarse fallas en el servicio se transferirá al proveedor el reporte para su reparación inmediata. Como contingencia se usará la el Enlace ADSL.