IEPC
DURANGO
INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA

Plan de seguridad y continuidad del Programa de Resultados Electorales Preliminares

2018

PREP
DURANGO 2018
PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES

Contenido

Glosario

AE: Asistente Electoral contratado por el IEPC.

AEC: Actas de Escrutinio y Cómputo.

ARE: Área de Responsabilidad Electoral.

BAM: Banda Ancha Móvil.

CATD: Centro de Adquisición y Transmisión de Datos.

CRID: Centro de Recepción de Imágenes y Datos.

CV: Centro de Verificación.

DADI: Dispositivo de Adquisición Digital de Imágenes.

DIRECCIÓN MAC: Identificador de 48 bits que corresponde de forma única con un interfaz de red.

IEPC: Instituto Electoral y de Participación Ciudadana del Estado de Durango.

INE: Instituto Nacional Electoral.

PREP: Programa de Resultados Electorales Preliminares.

PREP CASIILLA: Mecanismo a través del cual, el AE obtendrá y transmitirán al CRID una imagen digital del AEC.

PROISI: Empresa ganadora de la licitación nacional pública para implementar y operar el PREP.

TOKEN: Cadena de caracteres que tienen un significado coherente en cierto lenguaje de programación.

ZORE: Zona de Responsabilidad Electoral.

Presentación

El presente documento tiene el propósito de identificar y cuantificar los riesgos que impedirían la continuidad de la operación del Programa de Resultados Electorales Preliminares (PREP) para el Proceso Electoral Local 2017-2018 en el Estado de Durango, así como especificar el impacto de la ocurrencia de los mismos. También se documentan las medidas y procedimientos de mitigación de riesgos, que serán implementados por el Instituto Electoral y de Participación Ciudadana del Estado de Durango (IEPC) ya sea por medios propios o a través de la prestación de servicios de un tercero.

De la misma forma se detallan las medidas, controles y procedimientos de seguridad creados para salvaguardar la integridad de la información que se suministra y se genera por el PREP.

De acuerdo al Reglamento de Elecciones del Instituto Nacional Electoral (INE), Capitulo IV Consideraciones de Seguridad Operativa, para la implementación de los controles de seguridad aplicables en los distintos procedimientos del PREP es conveniente contemplar los siguientes puntos: *factores de riesgo, activos críticos, áreas de amenaza, identificación de riesgos, estrategia de gestión de riesgos y plan de seguridad*. El presente documento tratará cada uno de los puntos para establecer claramente el Plan de Continuidad y Seguridad al que deberá apegarse el personal involucrado en las actividades del PREP.

1. Factores de riesgo.

Para realizar la valoración de riesgos se considera el método más utilizado en la literatura sobre Gestión de Riesgos[1] siguiendo la ecuación:

$$R = pi \qquad (1)$$

Donde:

R: es la variable que cuantifica el riesgo.
p: es la probabilidad de ocurrencia del evento.
i: es el impacto que tiene la ocurrencia del evento.

A través de la ecuación anterior se pretende identificar cuantitativamente los riesgos existentes para la continuidad de las actividades relacionadas con el Programa de Resultados Electorales Preliminares en cada uno de los sitios involucrados en el proceso, teniendo en cuenta las siguientes tablas de convenciones respecto a la probabilidad de ocurrencia y el impacto que tienen las amenazas.

Convención utilizada sobre la probabilidad de ocurrencia			
Cons.	**Ocurrencia de eventos**	**Probabilidad (p)**	**Factor de probabilidad (fp)**
1	Rara vez ocurre	0<p<0.01	0.01
2	Poco probable que ocurra	0.01<= p<0.1	0.1
3	Algunas veces ocurre	0.1<=p<0.5	0.5
4	Es probable que ocurra	0.5<=p<0.7	0.7
5	Es muy probable que ocurra	0.7<=p<1	1

Tabla 1. Convención sobre la probabilidad de ocurrencia

Convención sobre el impacto que causa la ocurrencia de amenazas			
Cons.	**Impacto**	**Nivel impacto**	**Factor de impacto (fi)**
1	Compromete el seguimiento riguroso del procedimiento establecido.	Bajo	1
2	Compromete ligeramente los tiempos para alcanzar el objetivo de la operación.	Medio Bajo	2
3	Compromete gravemente los tiempos para alcanzar el objetivo de la operación.	Medio	3
4	Impide parcialmente el objetivo de la operación	Medio Alto	4
5	Impide totalmente el objetivo de la operación.	Alto	5

Tabla 2. Convención sobre el impacto que causa la ocurrencia de amenazas.

[1] Referencia: https://en.wikipedia.org/wiki/Risk_assessment

Siguiendo la ecuación (1) y las convenciones sugeridas en las tablas 1 y 2, se puede determinar que las valoraciones para los riesgos existentes en el presente análisis oscilarán entre 0 – 5, donde el riesgo que tendrá la mayor prioridad de atención de acuerdo a su valoración dentro del Plan de Continuidad y Seguridad será aquel que se encuentre más cercano al valor de 5.

2. Activos Críticos.

Para la realización de actividades y procedimientos relacionadas con el Programa de Resultados Electorales Preliminares para el Proceso Electoral Local 2017-2018 en el Estado de Durango se pueden identificar los siguientes activos críticos:

- **Inmuebles.**

Dentro de estos activos se considera el acceso y uso de las instalaciones de las distintas sedes del IEPC en donde se tiene contemplada la realización de actividades o procedimientos propios del PREP.

- **Infraestructura Tecnológica.**

Se entiende como infraestructura tecnológica al conjunto de dispositivos utilizados para la captación, manejo, almacenamiento, transmisión y difusión de información, que permita la realización de las actividades del PREP. Dentro de este rubro se encuentran también todo el equipo relacionado con la distribución, control y almacenamiento de energía eléctrica requerida para los mismos fines dentro de las sedes del IEPC.

- **Recursos Humanos.**

En este rubro se encuentra el personal contratado para las distintas actividades relacionadas con el PREP en los sitios de operaciones del Estado.

- **Suministro de energía eléctrica.**

En este apartado se considera el conjunto de dispositivos y materiales dispuestos por la Comisión Federal de Electricidad para el abasto de energía eléctrica en las distintas sedes del IEPC, con la finalidad de permitir el funcionamiento de los equipos eléctricos y electrónicos requeridos para las actividades del PREP.

- **Comunicación de datos.**

En este activo se contemplan el conjunto de dispositivos y materiales que permiten la recepción y transmisión de datos a través de redes públicas o privadas (redes de internet, telefonía convencional, celular, satelital, etc.) para los fines propios del PREP.

- **Información**

Dentro de este campo se consideran todos los datos contenidos en las Actas de Escrutinio y Cómputo (AEC), así como la información relacionada con su traslado, registro, resguardo y almacenamiento. También se considera dentro de este activo la información del personal involucrado en cualquier proceso relacionado al PREP.

3. Áreas de Amenaza.

A1. Ausencia temporal o permanente del personal contratado para actividades propias del PREP.

Esta amenaza se materializa cuando el personal contratado para la realización de las actividades programadas del PREP se presenta después de la hora especificada para el inicio de actividades o no se presenta en lo absoluto.

Identificación de riesgos.

A1. Ausencia temporal o permanente del personal contratado para el PREP							
Cons.	**Zona de operación**	**Impacto que causa**	**Activo crítico afectado**	**Factor de probabilidad (fp)**	**Factor de impacto (fi)**	**Valor de riesgo (R=fp*fi)**	**Consecuencia de control aplicado**
1	CATD	Medio Alto	Recursos Humanos	0.1	4	0.4	Se reduce
2	CV	Medio Alto	Recursos Humanos	0.1	4	0.4	Se reduce
3	CRID	Bajo	Recursos Humanos	0.1	1	0.1	Se transfiere
4	Casilla	Medio Alto	Recursos Humanos	0.1	4	0.4	Se reduce

Tabla 3. Identificación de riesgos A1

Estrategia de control de riesgos en CATD.

E1.A1.CATD: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir en caso de que exista la ausencia temporal o permanente del personal.

E2.A1.CATD: Se cuenta con un directorio actualizado del personal que incluye teléfonos de familiares y/o amigos que permita su localización inmediata.

E3.A1.CATD: Cada CATD contrata por lo menos a 3 personas, dos capturistas-digitalizadores y un acopiador. Todo el personal recibe una capacitación que les permite realizar las funciones de los roles involucrados en el proceso en el caso de ausencia temporal o permanente.

E4.A1.CATD: Se cuenta con una lista de reserva del personal que no se contrate en las etapas de reclutamiento y se evaluará su disponibilidad para entrar en operación en caso de ausencia temporal o permanente del personal.

Estrategia de control de riesgos en CV.

E1.A1.CV: Se cuenta con manual elaborado exprofeso que detalle las acciones a seguir en caso de que exista la ausencia temporal o permanente del personal.

E2.A1.CV: Se cuenta con un directorio actualizado del personal que incluye teléfonos de familiares y/o amigos que permita su localización inmediata.

E3.A1.CV: El CV contrata un número determinado de personas que le permite realizar los trabajos sin comprometer los tiempos de procesamiento por la ausencia de un número reducido de

personas. Todo el personal recibe una capacitación que les permite realizar las funciones de los roles involucrados en el proceso en el caso de alguno falte o tenga un imprevisto.

E4.A1.CV: Se cuenta con una lista de reserva del personal que no se contrate en las etapas de reclutamiento y se evaluará su disponibilidad para entrar en operación en caso de ausencia temporal o permanente del personal.

Estrategia de control de riesgos en CRID.

E1.A1.CRID: El Centro de Recepción de Imágenes y Datos cuenta con un esquema de máxima disponibilidad con atención 24/7 por parte de la empresa prestadora de servicios.

Estrategia de control de riesgos en Casilla.

E1.A1.CAS: Se cuenta con un directorio actualizado del personal que incluye teléfonos de familiares y/o amigos que permita su localización inmediata.

E2.A1.CAS: Se cuenta con manual elaborado exprofeso que detalle las acciones a seguir en caso de que exista la ausencia temporal o permanente del personal, dicho manual documenta los casos en que la ausencia debe ser asumida y los casos en que el personal ausente puede ser sustituido.

E3.A1.CAS: Se cuenta con una lista de reserva del personal que pudiera asistir a las casillas dentro de la ARE comprometida por ausencia del AE correspondiente. Este personal deberá estar registrado con antelación en el sistema y contar con un dispositivo móvil con la aplicación PREP Casilla instalada.

A2. Falla en la prestación del servicio de suministro eléctrico.

La amenaza se materializa cuando existe algún corte de servicio en el suministro eléctrico ya sea por desperfectos en los equipos de distribución de energía, cortes en las líneas de alimentación o demás daños generados por causas naturales o eventos fortuitos.

Identificación de riesgos.

A2. Falla en la prestación del servicio de suministro eléctrico

Cons.	Zona de operación	Impacto que causa	Activo crítico afectado	Factor de probabilidad (fp)	Factor de impacto (fi)	Valor de riesgo (R=fp*fi)	Consecuencia de control aplicado
1	CATD	Alto	Suministro de energía eléctrica	0.5	4	2	Se reduce
2	CV	Alto	Suministro de energía eléctrica	0.1	4	0.4	Se reduce
3	CRID	Alto	Suministro de energía eléctrica	0.1	4	0.4	Se evita
4	Casilla	Bajo	Suministro de energía eléctrica	0.1	1	0.1	Se acepta

Tabla 4. Identificación de riesgos A2

Estrategia de control de riesgos en CATD.

E1.A2.CATD: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir en caso de que exista el corte del servicio de suministro eléctrico. Este manual incluye información sobre como arrancar y operar los equipos de energía ininterrumpida y las plantas de energía de emergencia.

E2.A2.CATD: Se cuenta con un equipo de energía ininterrumpida (NO-BREAK) para cada equipo de cómputo involucrado en el PREP. Este equipo tiene una capacidad de independencia del suministro eléctrico hasta por 15 minutos, tiene la finalidad de mantener la operación de los equipos mientras se realiza la transferencia del suministro hacia la planta de energía de emergencia.

E3.A2.CATD: Se cuenta con una planta generadora de energía de emergencia con capacidad suficiente para soportar la operación de los equipos involucrados en el PREP hasta por una hora. Sin menoscabo de que sea posible obtener combustible que permita prolongar la operación de la planta de emergencia en caso de que el corte en el suministro de energía se mantenga.

Estrategia de control de riesgos en CV.

E1.A2.CV: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir en caso de que exista el corte del servicio de suministro eléctrico. Este manual incluye información sobre como arrancar y operar los equipos de energía ininterrumpida y las plantas de energía de emergencia.

E2.A2.CV: Se cuenta con un equipo de energía ininterrumpida (NO-BREAK) para cada equipo de cómputo involucrado en el PREP. Este equipo tiene una capacidad de independencia del suministro eléctrico hasta por 15 minutos, tiene la finalidad de mantener la operación de los equipos mientras se realiza la transferencia del suministro hacia la planta de energía de emergencia.

E3.A2.CV: Se cuenta con una planta generadora de energía de emergencia por parte del IEPC que cuenta con la capacidad de soportar los equipos involucrados en el PREP en caso del corte del suministro eléctrico.

E4.A2.CV: Se cuenta con una planta generadora de energía de emergencia con capacidad suficiente para soportar la operación de los equipos involucrados en el PREP hasta por una hora. Sin menoscabo de que sea posible obtener combustible que permita prolongar la operación de la planta de emergencia en caso de que el corte en el suministro de energía se mantenga.

Estrategia de control de riesgos en CRID.

E1.A1.CRID: El Centro de Recepción de Imágenes y Datos cuenta con un esquema de máxima disponibilidad con atención 24/7 por parte de la empresa prestadora de servicios.

Estrategia de control de riesgos en Casilla.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel casilla. El valor del riesgo en este caso es mínimo.

A3. Falla en la prestación del servicio de comunicación de datos.

La amenaza se materializa cuando existe algún corte en el servicio de comunicación de datos ya sea por desperfectos en los equipos de comunicación, cortes en el cableado de la red de distribución del servicio, condiciones climáticas adversas al medio de transmisión de datos, saturación de la red por incremento en la demanda del servicio, etc.

Identificación de riesgos.

A3. Falla en la prestación del servicio de comunicación de datos							
Cons.	**Zona de operación**	**Impacto que causa**	**Activo crítico afectado**	**Factor de probabilidad (fp)**	**Factor de impacto (fi)**	**Valor de riesgo (R=fp*fi)**	**Consecuencia de control aplicado**
1	CATD	Medio Alto	Comunicación de datos	0.5	4	2	Se reduce
2	CV	Alto	Comunicación de datos	0.1	5	0.5	Se reduce
3	CRID	Alto	Comunicación de datos	0.1	5	0.5	Se reduce
4	Casilla	Bajo	Comunicación de datos	0.1	1	0.1	Se acepta

Tabla 5. Identificación de riesgos A3

Estrategia de control de riesgos en CATD.

E1.A3.CATD: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir en caso de que exista el corte del servicio de comunicación de datos.

E2.A3.CATD: El sistema informático del PREP y el personal asociado puede continuar con el proceso de captura en modo desconectado (off-line). Los datos de esta captura son almacenados en los equipos de cómputo para proceder a la transmisión de datos en bloque en el momento en que el servicio de comunicación de datos se reestablezca.

E3.A3.CATD: Se cuenta con dos proveedores del servicio de comunicación independientes. En caso de que uno de los dos proveedores deje de funcionar, el sistema PREP automáticamente contará con el servicio del otro para continuar con el proceso.

E4.A3. CATD:Se cuenta con la posibilidad de usar el equipo de comunicación de datos propio del Consejo Municipal del IEPC, mismo que es independiente a los equipos de comunicación de datos de la empresa PROISI. El procedimiento para hacer uso de este equipo de comunicaciones esta detallado en el manual de continuidad y seguridad del PREP.

E5.A3. CATD: Se cuenta con la posibilidad de enviar la información propia del PREP a través del uso de dispositivos de banda ancha móvil (BAM) y en su caso a través de conexión dial up en caso de que las demás opciones de comunicación de datos no se encuentren disponibles.

E6.A3. CATD: Cuando no exista posibilidad de restablecimiento de la comunicación de datos, el sistema PREP cuenta con la capacidad de exportar la información de captura a dispositivos de almacenamiento USB para que esta pueda ser trasladada a la unidad de transmisión más cercana. El manual de continuidad y seguridad del PREP detallará el recorrido que deberá

de realizarse en caso de contingencia, además del personal que realiza las actividades y por quien es autorizado el procedimiento.

Estrategia de control de riesgos en CV.

E1.A3.CV: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir en caso de que exista el corte del servicio de comunicación de datos.

E2.A3.CV: El sistema informático del PREP y el personal asociado puede continuar con el proceso de captura y verificación en modo desconectado (off-line). Los datos de esta captura son almacenados en los equipos de cómputo para proceder a la transmisión de datos en bloque en el momento en que el servicio de comunicación de datos se reestablezca.

E3.A3.CV: Se cuenta con tres proveedores del servicio de comunicación independientes. En caso de que uno de los dos proveedores deje de funcionar, el sistema PREP automáticamente contará con el servicio de los demás para continuar con el proceso.

E4.A3.CV: Se cuenta con la posibilidad de usar el equipo de comunicación de datos propio del de la sede principal del IEPC, mismo que es independiente a los equipos de comunicación de datos de la empresa PROISI. El procedimiento para hacer uso de este equipo de comunicaciones esta detallado en el manual de continuidad y seguridad del PREP.

E5.A3.CV: Se cuenta con la posibilidad de enviar la información propia del PREP a través del uso de dispositivos de banda ancha móvil (BAM) y en su caso a través de conexión dial up en caso de que las demás opciones de comunicación de datos no se encuentren disponibles.

E6.A3.CV: Cuando no exista posibilidad de restablecimiento de la comunicación de datos, el sistema PREP cuenta con la capacidad de exportar la información captura a dispositivos de almacenamiento USB para que esta pueda ser trasladada a la unidad de transmisión más cercana. El manual de continuidad y seguridad del PREP detallará el recorrido que deberá de realizarse en caso de contingencia, además del personal que realizará las actividades y el procedimiento de autorización requerido.

Estrategia de control de riesgos en CRID.

E1.A3.CRID: El Centro de Recepción de Imágenes y Datos cuenta con un esquema de máxima disponibilidad de comunicación de datos con atención 24/7 por parte de la empresa prestadora de servicios.

Estrategia de control de riesgos en Casilla.

E1.A3.CRID: La aplicación PREP Casilla puede funcionar en modo desconectado (off-line). Cuando se realiza la captación digital de una AEC, esta es almacenada internamente en el dispositivo móvil. En caso de que no exista una red de comunicación de datos disponible (Wifi, 3G, 4G, etc.) al realizar la fotografía, la aplicación PREP casilla monitoreará continuamente hasta que exista una red disponible para enviar la información correspondiente sin que exista mediación por parte del usuario.

E2.A3.CRID: Se cuenta con un mapa de cobertura de red de datos celulares que permita visualizar en que casillas no se podrá realizar el envío en tiempo real y hasta qué punto aproximado del trayecto del AE se podrá realizar la transmisión.

A4. Falla del equipo de cómputo utilizado para la captura de la información del PREP.

La amenaza se materializa cuando el equipo de cómputo asignado al capturista-verificador deja de funcionar por falla de hardware o software, corte del suministro eléctrico asociado a ese equipo, falla en la transmisión o recepción de datos asociada a ese equipo, desperfectos en los periféricos asociados (mouse, teclado y monitor), etc.

Identificación de riesgos.

A4. Falla en el equipo de cómputo utilizado para la captura de la información del PREP

Cons.	Zona de operación	Impacto que causa	Activo crítico afectado	Factor de probabilidad (fp)	Factor de impacto (fi)	Valor de riesgo (R=fp*fi)	Consecuencia de control aplicado
1	CATD	Alto	Infraestructura Tecnológica	0.1	5	0.5	Se evita
2	CV	Alto	Infraestructura Tecnológica	0.1	5	0.5	Se evita
3	CRID	Nulo	Infraestructura Tecnológica	0.1	0	0	Se acepta
4	Casilla	Nulo	Infraestructura Tecnológica	0.1	0	0	Se acepta

Tabla 6. Identificación de riesgos A4

Estrategia de control de riesgos en CATD.

E1.A4.CATD: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir en caso de que se presente una falla en el equipo de cómputo utilizado para la captura de la información PREP.

E2.A4.CATD: Cada CATD cuenta con un equipo de cómputo adicional disponible en las instalaciones, con el software y hardware necesario para su funcionamiento. Este equipo y sus periféricos (monitor, ratón, teclado, cables, etc.) están a disponibilidad del personal del PREP para su uso en caso de falla del equipo principal.

E3.A4.CATD: Se cuenta con plan de respuesta a problemas de infraestructura en donde existirá personal de soporte para atender contingencias, mismos que también contará con equipos de cómputo para sustituir en caso de que sea necesario.

Estrategia de control de riesgos en CV.

E1.A4.CV: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir en caso de que se presente una falla en el equipo de cómputo utilizado para la captura de la información PREP.

E2.A4.CV: El CV cuenta con un equipo de cómputo adicional disponible en las instalaciones, con el software y hardware necesario para su funcionamiento. Este equipo y sus periféricos (monitor, ratón, teclado, cables, etc.) están a disponibilidad del personal del PREP para su uso en caso de falla del equipo principal.

E3.A4.CV: Se cuenta con plan de respuesta a problemas de infraestructura en donde existirá personal de soporte para atender contingencias, mismos que también contará con equipos de cómputo para sustituir en caso de que sea necesario.

Estrategia de control de riesgos en CRID.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel CRID, ya que aquí no se realizan procedimientos de captura. El valor del riesgo en este caso es nulo.

Estrategia de control de riesgos en Casilla.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel Casilla, ya que aquí no se realizan procedimientos de captura. El valor del riesgo en este caso es nulo.

A5. Falla del equipo de adquisición de imágenes de las Actas PREP.

La amenaza se materializa cuando un dispositivo de adquisición de imágenes de las actas PREP deja de funcionar, por corte en el suministro eléctrico asociado a ese equipo, falla en el dispositivo alimentador de papel, reducción en la calidad de las imágenes generadas, etc.

Identificación de riesgos.

A5. Falla del equipo de adquisición de imágenes de las Actas PREP							
Cons.	**Zona de operación**	**Impacto que causa**	**Activo crítico afectado**	**Factor de probabilidad (fp)**	**Factor de impacto (fi)**	**Valor de riesgo (R=fp*fi)**	**Consecuencia de control aplicado**
1	CATD	Alto	Infraestructura Tecnológica	0.1	4	0.4	Se evita
2	CV	Alto	Infraestructura Tecnológica	0.1	4	0.4	Se evita
3	CRID	Nulo	Infraestructura Tecnológica	0.1	0	0	Se acepta
4	Casilla	Nulo	Infraestructura Tecnológica	0.1	0	0	Se acepta

Tabla 7. Identificación de riesgos A5

Estrategia de control de riesgos en CATD.

E1.A5.CATD: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir en caso de que se presente una falla en el equipo de adquisición de imágenes de las actas PREP.

E2.A5.CATD: Cada CATD cuenta con un equipo DADI adicional disponible en las instalaciones, el software para el equipo adicional está instalado y ha sido probado el funcionamiento correcto del equipo sustituto.

E3.A5.CATD:Se cuenta con plan de respuesta a problemas de infraestructura en donde existirá personal de soporte para atender contingencias, mismos que también contarán con equipos de adquisición de imágenes para sustituir en caso de que sea necesario.

Estrategia de control de riesgos en CV.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel CV, ya que aquí no se realizan procedimientos de adquisición de imágenes de actas PREP. El valor del riesgo en este caso es nulo.

Estrategia de control de riesgos en CRID.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel CRID, ya que aquí no se realizan procedimientos de adquisición de imágenes de actas PREP. El valor del riesgo en este caso es nulo.

Estrategia de control de riesgos en Casilla.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel Casilla, ya que aquí no se realizan procedimientos de adquisición de imágenes de actas PREP (a través de DADI). El valor del riesgo en este caso es nulo. El caso particular en el que falla el dispositivo móvil con el que se toma la fotografía en el mecanismo PREP Casilla, está contemplado en otra amenaza por separado.

A6. Falla o ausencia del dispositivo móvil para el mecanismo PREP Casilla.

La amenaza se materializa cuando el dispositivo móvil para realizar la fotografía contemplada en el mecanismo PREP casilla deja de funcionar, por falta de carga eléctrica, por falla en la aplicación predestinada para esa tarea. Se contempla dentro de la misma amenaza el caso en que el dispositivo móvil no cuente con conexión a la red de datos de forma permanente por falta de infraestructura de telecomunicaciones o por falta de los servicios de red celular de datos (plan de datos, recarga, prepago, etc.). Se considera también dentro de este apartado la ausencia del dispositivo móvil, por olvido, extravío o indisponibilidad presupuestal.

Identificación de riesgos.

A6. Falla o ausencia del dispositivo móvil para el mecanismo PREP Casilla

Cons.	Zona de operación	Impacto que causa	Activo crítico afectado	Factor de probabilidad (fp)	Factor de impacto (fi)	Valor de riesgo (R=fp*fi)	Consecuencia de control aplicado
1	CATD	Nulo	Infraestructura Tecnológica	0.1	0	0	Se acepta
2	CV	Nulo	Infraestructura Tecnológica	0.1	0	0	Se acepta
3	CRID	Nulo	Infraestructura Tecnológica	0.1	0	0	Se acepta
4	Casilla	Alto	Infraestructura Tecnológica	0.5	4	2	Se acepta

Tabla 8. Identificación de riesgos A6

Estrategia de control de riesgos en CATD.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel CATD ya que aquí no se utiliza el mecanismo PREP Casilla. El valor del riesgo en este caso es nulo.

Estrategia de control de riesgos en CV.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel CV ya que aquí no se utiliza el mecanismo PREP Casilla. El valor del riesgo en este caso es nulo.

Estrategia de control de riesgos en CRID.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel CRID ya que aquí no se utiliza el mecanismo PREP Casilla. El valor del riesgo en este caso es nulo.

Estrategia de control de riesgos en Casilla.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel Casilla. Se tiene planeado utilizar los dispositivos móviles personales de aquellos AE que acepten el uso de la aplicación.

A7. Falla o pérdida de datos del Centro de Datos Primario.

La amenaza se materializa cuando uno o varios servidores de cómputo para el procesamiento, almacenamiento y transmisión de datos dejan de funcionar de manera que resulta imposible la continuidad del flujo de información debido a que se impiden las actividades propias del PREP: captura de los datos de las actas, transmisión de imágenes de las mismas, cálculo de operaciones, validación de registros, verificación contra errores, publicación de datos, etc. Esta amenaza también contempla la pérdida de datos parcial o total contenida en los servidores involucrados en el proceso.

Identificación de riesgos.

A7. Falla del Centro de Datos Primario							
Cons.	**Zona de operación**	**Impacto que causa**	**Activo crítico afectado**	**Factor de probabilidad (fp)**	**Factor de impacto (fi)**	**Valor de riesgo (R=fp*fi)**	**Consecuencia de control aplicado**
1	CATD	Nulo	Infraestructura Tecnológica	0.1	0	0	Se acepta
2	CV	Nulo	Infraestructura Tecnológica	0.1	0	0	Se acepta
3	CRID	Alto	Infraestructura Tecnológica	0.1	5	0.5	Se reduce
4	Casilla	Nulo	Infraestructura Tecnológica	0.1	0	0	Se acepta

Tabla 9. Identificación de riesgos A7

Estrategia de control de riesgos en CATD.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel CATD ya que aquí no se cuenta con Centro de Datos Primario. El valor del riesgo en este caso es nulo.

Estrategia de control de riesgos en CV.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel CV ya que aquí no se cuenta con Centro de Datos Primario. El valor del riesgo en este caso es nulo.

Estrategia de control de riesgos en CRID.

E1.A7.CRID: Las bases de datos de información capturada, servidores de aplicación, servidores de publicación, generadores de contenidos, servidores de imágenes, etc. utilizados en el funcionamiento del sistema informático PREP tiene redundancia a través de creación de réplicas, clones y respaldos, mismos que entrarán en funcionamiento de manera automática en caso de falla. El arreglo de servicios de servidores contempla el funcionamiento permanente de dos centros de datos que mantienen la misma información para evitar la pérdida de poder de procesamiento o información al intercambiar hacia el uso de la instancia redundante de manera automática.

Estrategia de control de riesgos en Casilla.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel Casilla ya que aquí no se cuenta con Centro de Datos Primario. El valor del riesgo en este caso es nulo.

A8. Acceso de personal no autorizado al área de trabajo del PREP.

La amenaza se materializa cuando existe la presencia de personal no autorizado en las instalaciones destinadas para los CATD y CV que pudieran impedir, obstaculizar o retardar las actividades del PREP, asimismo causar el cese de actividades o el daño de los dispositivos eléctricos y electrónicos relacionados a la operación del programa.

Identificación de riesgos.

A8. Acceso de personal no autorizado al área de trabajo del PREP							
Cons.	**Zona de operación**	**Impacto que causa**	**Activo crítico afectado**	**Factor de probabilidad (fp)**	**Factor de impacto (fi)**	**Valor de riesgo (R=fp*fi)**	**Consecuencia de control aplicado**
1	CATD	Bajo	Inmueble	0.1	1	0.1	Se reduce
2	CV	Bajo	Inmueble	0.1	1	0.1	Se reduce
3	CRID	Nulo	Inmueble	0.1	0	0	Se acepta
4	Casilla	Nulo	Inmueble	0.1	0	0	Se acepta

Tabla 10. Identificación de riesgos A8

Estrategia de control de riesgos en CATD.

E1.A8.CATD: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir en caso de que personal no autorizado se introduzca al área de trabajo del PREP.

E2.A8.CATD: El personal autorizado para realizar funciones para el PREP cuenta en todo momento con el uniforme correspondiente y una identificación visible que lo acredita para laborar dentro del área de trabajo del programa. La identificación es validada por la Unidad Técnica de Cómputo y autorizada por la Secretaría Ejecutiva del IEPC Durango.

Estrategia de control de riesgos en CV.

E1.A8.CV: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir en caso de que personal no autorizado se introduzca al área de trabajo del PREP.

E2.A8.CV: El personal autorizado para realizar funciones para el PREP cuenta en todo momento con el uniforme correspondiente y una identificación visible que lo acredita para laborar dentro del área de trabajo del programa. La identificación es validada por la Unidad Técnica de Cómputo y autorizada por la Secretaría Ejecutiva del IEPC Durango.

Estrategia de control de riesgos en CRID.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel CRID ya que aquí no se cuenta con la presencia de personal para la realización de actividades del PREP. El valor del riesgo en este caso es nulo.

Estrategia de control de riesgos en Casilla.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel Casilla ya que aquí no se cuenta con la presencia de personal para la realización de actividades del PREP. El valor del riesgo en este caso es nulo. Se considera que la presencia de los AE para las funciones correspondientes al mecanismo PREP Casilla no forma parte del personal autorizado del PREP.

A9. Acceso no autorizado al sistema de captura de datos o al equipo de digitalización de imágenes del PREP.

La amenaza se materializa cuando personal no autorizado o ajeno al programa accede al sistema de captura del PREP o tiene disposición de los equipos para la digitalización de imágenes, provocando la introducción de información errónea, incompleta o falsa en los registros de las bases de datos del sistema, o en su caso generando imágenes sin relación a los objetivos del PREP.

Identificación de riesgos.

A9. Acceso no autorizado al sistema de captura de datos o al equipo de digitalización de imágenes del PREP							
Cons.	**Zona de operación**	**Impacto que causa**	**Activo crítico afectado**	**Factor de probabilidad (fp)**	**Factor de impacto (fi)**	**Valor de riesgo (R=fp*fi)**	**Consecuencia de control aplicado**
1	CATD	Medio Alto	Información	0.1	4	0.4	Se reduce
2	CV	Medio Alto	Información	0.1	4	0.4	Se reduce
3	CRID	Medio Alto	Información	0.1	4	0.4	Se reduce
4	Casilla	Medio Alto	Información	0.1	4	0.4	Se reduce

Tabla 11. Identificación de riesgos A9

Estrategia de control de riesgos en CATD.

E1.A9.CATD: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir para acceder a los sistemas de captura de datos y digitalización de imágenes.

E2.A9.CATD: El personal autorizado debe pasar por doble autenticación para acceder a los sistemas de captura de datos y digitalización de imágenes.

E3.A9.CATD: Se cuenta con una bitácora digital de acceso y desarrollo de actividades dentro de los sistemas de captura de datos y digitalización de imágenes.

E4.A9.CATD: Se cuenta con configuración de bloqueo automático de pantalla por inactividad del usuario.

Estrategia de control de riesgos en CV.

E1.A9.CV: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir para acceder a los sistemas de captura de datos y digitalización de imágenes.

E2.A9.CV: El personal autorizado debe pasar por doble autenticación para acceder a los sistemas de captura de datos y digitalización de imágenes.

E3.A9.CV: Se cuenta con una bitácora digital de acceso y desarrollo de actividades dentro de los sistemas de captura de datos y digitalización de imágenes.

E4.A9.CV: Se cuenta con configuración de bloqueo automático de pantalla por inactividad del usuario.

Estrategia de control de riesgos en CRID.

E1.A9.CRID: Solo se permite acceso a los sistemas de captura de datos y digitalización de imágenes a través de las instalaciones de los CATD.

Estrategia de control de riesgos en Casilla.

E1.A9.CAS: Solo se permite acceso a los sistemas de captura de datos y digitalización de imágenes a través de las instalaciones de los CATD.

A10. Acceso no autorizado a la red de datos del PREP.

La amenaza se materializa cuando sujetos o entes externos al PREP logran acceder a la red datos propia del sistema con la intención de modificar registros, obtener información o provocar fallas en el funcionamiento de los equipos participantes de la red.

Identificación de riesgos.

A10. Acceso no autorizado a la red de datos del PREP							
Cons.	**Zona de operación**	**Impacto que causa**	**Activo crítico afectado**	**Factor de probabilidad (fp)**	**Factor de impacto (fi)**	**Valor de riesgo (R=fp*fi)**	**Consecuencia de control aplicado**
1	CATD	Medio Alto	Información	0.1	4	0.4	Se reduce
2	CV	Medio Alto	Información	0.1	4	0.4	Se reduce
3	CRID	Medio Alto	Información	0.1	4	0.4	Se reduce
4	Casilla	Medio Alto	Información	0.1	4	0.4	Se reduce

Tabla 12. Identificación de riesgos A10

Estrategia de control de riesgos en CATD.

E1.A10.CATD: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir para la configuración de los equipos de red y de cómputo participantes en el PREP.

E2.A10.CATD: El sistema informático PREP dentro del CATD funciona manteniendo sus recursos y servicios a través de una red privada virtual segura. La comunicación de datos se realiza sobre canales cifrados con el uso de tokens y claves de usuario.

E3.A10.CATD: Validación de los equipos usados en los CATD a nivel dirección MAC.

Estrategia de control de riesgos en CV.

E1.A10.CV: Se cuenta con manual elaborado exprofeso que detalla las acciones a seguir para la configuración de los equipos de red y de cómputo participantes en el PREP.

E2.A10.CV: El sistema informático PREP dentro del CATD funciona manteniendo sus recursos y servicios a través de una red privada virtual segura. La comunicación de datos se realiza sobre canales cifrados con el uso de tokens y claves de usuario.

E3.A10.CV: Validación de los equipos usados en los CATD a nivel dirección MAC.

Estrategia de control de riesgos en CRID.

E1.A10.CRID: Uso de dispositivos de detección de intrusos a nivel red (Network IDS) y de servidores (host IDS).

E2.A10.CRID: Control de acceso mediante rangos de IP permitidas para validar que las fuentes de información sean las autorizadas.

E3.A10.CRID: Uso de dispositivos de filtrado de paquetes de red (firewalls) en el perímetro del CRID.

E3.A10.CRID: El sistema informático PREP en el CRID funciona manteniendo sus recursos y servicios a través de una red privada virtual segura. La comunicación de datos se realiza sobre canales cifrados con el uso de tokens y claves de usuario.

Estrategia de control de riesgos en Casilla.

E1.A10.CAS: La comunicación de datos se realiza sobre canales cifrados con el uso de tokens y claves de usuario.

E2.A10.CAS: El uso de la aplicación móvil PREP Casilla solo se permite mediante código de confirmación enviado a los usuarios que hayan sido previamente registrados y autorizados.

A11. Error de captura de datos del AEC.

La amenaza se materializa cuando se captura información diferente a la contenida en el AEC por error humano, desconocimiento del procedimiento, o con intención deliberada de alterar los resultados a registrar.

Identificación de riesgos.

A11. Error de captura de datos del AEC

Cons.	Zona de operación	Impacto que causa	Activo crítico afectado	Factor de probabilidad (fp)	Factor de impacto (fi)	Valor de riesgo (R=fp*fi)	Consecuencia de control aplicado
1	CATD	Medio Alto	Información	0.5	4	2	Se reduce
2	CV	Medio Alto	Información	0.5	4	2	Se reduce
3	CRID	Nulo	Información	0.1	0	0	Se acepta
4	Casilla	Nulo	Información	0.1	0	0	Se acepta

Tabla 13. Identificación de riesgos A11

Estrategia de control de riesgos en CATD.

E1.A11.CATD: Se cuenta con manual elaborado exprofeso que detalla los pormenores del procedimiento de captura de actas y enlista los casos más probables de error y la forma de proceder al respecto.

E2.A11.CATD: El sistema informático PREP utiliza auxilio visual a través de nomenclatura, colores, íconos y mensajes que facilitan la identificación de los campos de captura y el tipo de información que corresponde a cada campo.

E3.A11.CATD: El programa verifica que el número total de votos de la AEC incluyendo los votos nulos, no exceda la cantidad de boletas emitidas para la casilla correspondiente. En caso de excederse, se rechaza el ingreso de datos al sistema.

E4.A11.CATD: Se cuenta con un proceso de captura doble que reduce el riesgo de "error de dedo". El sistema solicitará que se capture de nueva cuenta el AEC hasta en tanto las dos capturas previstas no coincidan.

E5.A11.CATD: Se cuenta con un proceso de validación de la información capturada. Este es realizado por personal distinto al que realiza la captura y la digitalización, quien valida que la imagen contenga la misma información que fue capturada en el proceso de doble captura. Si se detecta error o inconsistencia entre la imagen y captura, se realiza la corrección pertinente antes de publicar la información correspondiente.

E6.A11.CATD: Se publican las imágenes digitalizadas de las AEC obtenidas a través de mecanismo PREP Casilla y el procedimiento convencional de acopio de actas.

E7.A11.CATD: Se implementa un método para garantizar la autenticidad y el origen de las imágenes de las actas a través de la generación de un identificador único asociado a cada imagen de acta PREP (SHA 256).

Estrategia de control de riesgos en CV.

E1.A11.CV: Se cuenta con manual elaborado exprofeso que detalla los pormenores del procedimiento de captura de actas y enlista los casos más probables de error y la forma de proceder al respecto.

E2.A11.CV: El sistema informático PREP utiliza auxilio visual a través de nomenclatura, colores, íconos y mensajes que facilitan la identificación de los campos de captura y el tipo de información que corresponde a cada campo.

E3.A11.CV: El programa verifica que el número total de votos de la AEC incluyendo los votos nulos, no exceda la cantidad de boletas emitidas para la casilla correspondiente. En caso de excederse, se rechaza el ingreso de datos al sistema.

E6.A11.CV: Se publican las imágenes digitalizadas de las AEC obtenidas a través de mecanismo PREP Casilla y el procedimiento convencional de acopio de actas.

E7.A11.CV: Se implementa un método para garantizar la autenticidad y el origen de las imágenes de las actas a través de la generación de un identificador único asociado a cada imagen de acta PREP (SHA 256).

Estrategia de control de riesgos en CRID.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel CRID ya que aquí no se realiza la captura de los datos del acta PREP. El valor del riesgo en este caso es nulo.

Estrategia de control de riesgos en Casilla.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel Casilla ya que aquí no se realiza la captura de los datos del acta PREP. El valor del riesgo en este caso es nulo.

A12. Falla ocasionada por virus o malware informático.

La amenaza se materializa cuando existe y acciona un virus o malware en el equipo de cómputo que impide la realización de las actividades propias del PREP, oculta o inhabilita los archivos que contienen información relacionada al programa.

Identificación de riesgos.

A12. Falla ocasionada por virus o malware informático

Cons.	Zona de operación	Impacto que causa	Activo crítico afectado	Factor de probabilidad (fp)	Factor de impacto (fi)	Valor de riesgo (R=fp*fi)	Consecuencia de control aplicado
1	CATD	Medio Alto	Información	0.1	4	0.4	Se reduce
2	CV	Medio Alto	Información	0.1	4	0.4	Se reduce
3	CRID	Medio Alto	Información	0.1	4	0.4	Se transfiere

A12. Falla ocasionada por virus o malware informático							
Cons.	**Zona de operación**	**Impacto que causa**	**Activo crítico afectado**	**Factor de probabilidad (fp)**	**Factor de impacto (fi)**	**Valor de riesgo (R=fp*fi)**	**Consecuencia de control aplicado**
4	Casilla	Medio Alto	Información	0.1	4	0.4	Se acepta

Tabla 14. Identificación de riesgos A12

Estrategia de control de riesgos en CATD.

E1.A12.CATD: Los equipos utilizados dentro del sistema informático del PREP utilizan software instalado con el propósito específico de la realización de las actividades y existe control de administrador para la instalación de cualquier software adicional. Para la utilización de los equipos se han instalado todos los controladores y programas requeridos desde la realización del primer simulacro, con lo cual los capturistas y verificadores se han familiarizado a los mismos y se han podido detectar requerimientos adicionales en caso de existir.

E2.A12.CATD: El sistema operativo de los equipos utilizados en el CATD cuentan con control de acceso a través de contraseña.

E3.A12.CATD: El sistema operativo de los equipos utilizados en el CATD cuentan con las actualizaciones de seguridad recomendadas por el fabricante.

E4.A12.CATD: Los equipos utilizados en los CATD cuentan con software antivirus con las actualizaciones más recientes recomendadas por el fabricante.

E5.A12.CATD: Se cuenta con manual de usuario que detalla el método de acceso al sistema operativo y el uso del software antivirus.

E6.A12.CATD: Las políticas de uso del equipo de los CATD restringen el uso de dispositivos de almacenamiento USB a aquellas acciones que se emprendan en la estrategia E6.A3.CATD.

Estrategia de control de riesgos en CV.

E1.A12.CV: Los equipos utilizados dentro del sistema informático del PREP utilizan software instalado con el propósito específico de la realización de las actividades y existe control de administrador para la instalación de cualquier software adicional. Para la utilización de los equipos se han instalado todos los controladores y programas requeridos desde la realización del primer simulacro, con lo cual los capturistas y verificadores se han familiarizado a los mismos y se han podido detectar requerimientos adicionales en caso de existir.

E2.A12.CV: El sistema operativo de los equipos utilizados en el CV cuentan con control de acceso a través de contraseña.

E3.A12.CV: Los equipos utilizados en el CV cuentan con software antivirus con las actualizaciones más recientes recomendadas por el fabricante.

E6.A12.CV: Se cuenta con manual de usuario que detalla el método de acceso al sistema operativo y el uso del software antivirus.

E7.A12.CV: Las políticas de uso del equipo de los CATD restringen el uso de dispositivos de almacenamiento USB a aquellas acciones que se emprendan en la estrategia E6.A3.CV.

Estrategia de control de riesgos en CRID.

Los servidores de procesamiento en el CRID se proveen con servicios en la nube donde se mantienen ajenos a la posibilidad de infección de virus o malware.

Estrategia de control de riesgos en Casilla.

Se elabora una lista de recomendaciones para los usuarios del mecanismo PREP Casilla con la finalidad de mantener el dispositivo móvil ajeno a software potencialmente dañino para la operación y con espacio en disco suficiente para el almacenamiento de las fotografías.

A13. Toma de instalaciones de las sedes del IEPC o incapacidad para usar las áreas designadas para el PREP.

La amenaza se materializa cuando existe la limitación total o parcial para el uso de las instalaciones de las distintas sedes del IEPC por la presencia de grupos sociales, manifestantes, delincuencia organizada, o demás entes ajenos al IEPC que pongan en riesgo la integridad física de los participantes en actividades del PREP.

Identificación de riesgos.

A13. Toma de instalaciones de las sedes del IEPC o incapacidad para usar las áreas designadas para el PREP

Cons.	Zona de operación	Impacto que causa	Activo crítico afectado	Factor de probabilidad (fp)	Factor de impacto (fi)	Valor de riesgo (R=fp*fi)	Consecuencia de control aplicado
1	CATD	Alto	Inmuebles	0.1	5	0.5	Se reduce
2	CV	Alto	Inmuebles	0.1	5	0.5	Se reduce
3	CRID	Nulo	Inmuebles	0.1	0	0	Se acepta
4	Casilla	Nulo	Inmuebles	0.1	0	0	Se acepta

Tabla 15. Identificación de riesgos A13

Estrategia de control de riesgos en CATD.

E1.A13.CATD: En caso de que la sede se encuentre comprometida se redireccionarán las actividades hacia otra sede de CATD, siempre que exista la posibilidad de contar con las AEC para darle continuidad a la captura de la información y el envío de datos.

E2.A13.CATD: Se cuenta con manual de usuario que detalla las acciones a seguir en caso de la toma de instalaciones privilegiando la seguridad e integridad de las personas en primera instancia, en segunda instancia las AEC y en última instancia la infraestructura tecnológica. El documento define también el procedimiento a seguir en caso de las actividades se puedan trasladar a la sede del CATD más cercano.

E3.A13.CATD: Se cuenta con directorio de autoridades de seguridad y protección civil en caso de que sea requerido el auxilio de la fuerza pública.

Estrategia de control de riesgos en CV.

E1.A13.CV: En caso de que la sede se encuentre comprometida se redireccionarán las actividades hacia otra sede de CATD para darle continuidad a verificación y captura de la información, así como el envío de datos.

E2.A13.CV: Se cuenta con manual de usuario que detalla las acciones a seguir en caso de la toma de instalaciones privilegiando la seguridad e integridad de las personas en primera instancia, en segunda instancia las AEC y en última instancia la infraestructura tecnológica. El documento define también el procedimiento a seguir en caso de las actividades se puedan trasladar a la sede del CATD más cercano.

E3.A13.CV: Se cuenta con directorio de autoridades de seguridad y protección civil en caso de que sea requerido el auxilio de la fuerza pública.

Estrategia de control de riesgos en CRID.

Los servidores de procesamiento en el CRID se proveen con servicios en la nube donde se mantienen ajenos a la posibilidad de que dejen de funcionar por la toma de instalaciones. La empresa garantiza el funcionamiento de los servicios proveyendo de la seguridad para la continuidad de sus operaciones. No se cuenta con estrategias propias de control de riesgos para esta amenaza a nivel CRID. El valor del riesgo en este caso es mínimo.

Estrategia de control de riesgos en Casilla.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel casilla. El valor del riesgo en este caso es nulo.

A14. Inundación, Huracán, Sismo o demás desastres naturales.

La amenaza se materializa cuando algún fenómeno natural causa la imposibilidad del uso de las instalaciones de las sedes del IEPC, la inoperancia de los equipos y materiales destinados para el programa o pone en riesgo la integridad física del personal participante en las labores.

Identificación de riesgos.

A14. Inundación, huracán, sismo o demás desastres naturales							
Cons.	**Zona de operación**	**Impacto que causa**	**Activo crítico afectado**	**Factor de probabilidad (fp)**	**Factor de impacto (fi)**	**Valor de riesgo (R=fp*fi)**	**Consecuencia de control aplicado**
1	CATD	Alto	Inmuebles	0.1	5	0.5	Se acepta
2	CV	Alto	Inmuebles	0.1	5	0.5	Se acepta
3	CRID	Alto	Inmuebles	0.1	5	0.5	Se acepta
4	Casilla	Alto	Inmuebles	0.1	5	0.5	Se acepta

Tabla 15. Identificación de riesgos A14

Estrategia de control de riesgos en CATD.

E1.A14.CATD: En caso de que la sede se encuentre comprometida por desastre natural o evento fortuito, se redireccionarán las actividades hacia otra sede de CATD, siempre que exista la posibilidad de contar con las AEC para darle continuidad a la captura de la información y el envío de datos.

E2.A14.CATD: Se cuenta con manual de usuario que detalla las acciones a seguir en caso de desastre natural o evento fortuito privilegiando la seguridad e integridad de las personas en primera instancia, en segunda instancia las AEC y en última instancia la infraestructura tecnológica. El documento define también el procedimiento a seguir en caso de las actividades se puedan trasladar a la sede del CATD más cercano.

E3.A14.CATD: Se cuenta con directorio de autoridades de seguridad y protección civil en caso de que sea requerido el auxilio de la fuerza pública o cuerpos de emergencia.

Estrategia de control de riesgos en CV.

E1.A14.CV: En caso de que la sede se encuentre comprometida por desastre natural o evento fortuito, se redireccionarán las actividades hacia otra sede de CATD para darle continuidad a verificación y captura de la información, así como el envío de datos.

E2.A14.CV: Se cuenta con manual de usuario que detalla las acciones a seguir en caso de desastre natural o evento fortuito privilegiando la seguridad e integridad de las personas en primera instancia, en segunda instancia las AEC y en última instancia la infraestructura tecnológica. El documento define también el procedimiento a seguir en caso de las actividades se puedan trasladar a la sede del CATD más cercano.

E3.A14.CV: Se cuenta con directorio de autoridades de seguridad y protección civil en caso de que sea requerido el auxilio de la fuerza pública o cuerpos de emergencia.

Estrategia de control de riesgos en CRID.

Los servidores de procesamiento en el CRID se proveen con servicios en la nube donde se mantienen con una probabilidad de que dejen de funcionar por desastres naturales. La empresa garantiza el funcionamiento de los servicios proveyendo de la seguridad para la continuidad de sus operaciones. No se cuenta con estrategias propias de control de riesgos para esta amenaza a nivel CRID. El valor del riesgo en este caso es mínimo.

Estrategia de control de riesgos en Casilla.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel casilla. El valor del riesgo en este caso es mínimo.

A15. Incendio.

La amenaza se materializa cuando existe la presencia de fuego dentro de las instalaciones que pone en riesgo la integridad física del personal participante en las labores del PREP, así como produce la inoperancia de los equipos y materiales destinados para el programa.

Identificación de riesgos.

A15. Incendio							
Cons.	**Zona de operación**	**Impacto que causa**	**Activo crítico afectado**	**Factor de probabilidad (fp)**	**Factor de impacto (fi)**	**Valor de riesgo (R=fp*fi)**	**Consecuencia de control aplicado**
1	CATD	Alto	Inmuebles	0.1	5	0.5	Se acepta
2	CV	Alto	Inmuebles	0.1	5	0.5	Se acepta
3	CRID	Alto	Inmuebles	0.1	5	0.5	Se acepta
4	Casilla	Alto	Inmuebles	0.1	5	0.5	Se acepta

Tabla 15. Identificación de riesgos A15

Estrategia de control de riesgos en CATD.

E1.A14.CATD: En caso de que la sede se encuentre comprometida por incendio, se redireccionarán las actividades hacia otra sede de CATD, siempre que exista la posibilidad de contar con las AEC para darle continuidad a la captura de la información y el envío de datos.

E2.A14.CATD: Se cuenta con manual de usuario que detalla las acciones a seguir en caso de incendio privilegiando la seguridad e integridad de las personas en primera instancia, en segunda

instancia las AEC y en última instancia la infraestructura tecnológica. El documento define también el procedimiento a seguir en caso de las actividades se puedan trasladar a la sede del CATD más cercano.

E3.A14.CATD: Se cuenta con directorio de autoridades de seguridad y protección civil en caso de que sea requerido el auxilio de la fuerza pública o cuerpos de emergencia.

E4.A14.CATD: Se cuenta con extintor de incendios dentro de las instalaciones del CATD.

Estrategia de control de riesgos en CV.

E1.A14.CV: En caso de que la sede se encuentre comprometida por incendio, se redireccionarán las actividades hacia otra sede de CATD, siempre que exista la posibilidad de contar con las AEC para darle continuidad a la captura de la información y el envío de datos.

E2.A14.CV: Se cuenta con manual de usuario que detalla las acciones a seguir en caso de incendio privilegiando la seguridad e integridad de las personas en primera instancia, en segunda instancia las AEC y en última instancia la infraestructura tecnológica. El documento define también el procedimiento a seguir en caso de las actividades se puedan trasladar a la sede del CATD más cercano.

E3.A14.CV: Se cuenta con directorio de autoridades de seguridad y protección civil en caso de que sea requerido el auxilio de la fuerza pública o cuerpos de emergencia.

E4.A14.CV: Se cuenta con extintor de incendios dentro de las instalaciones del CATD.

Estrategia de control de riesgos en CRID.

Los servidores de procesamiento en el CRID se proveen con servicios en la nube donde se mantienen con una probabilidad de que dejen de funcionar por causa de incendio. La empresa garantiza el funcionamiento de los servicios proveyendo de la seguridad para la continuidad de sus operaciones. No se cuenta con estrategias propias de control de riesgos para esta amenaza a nivel CRID. El valor del riesgo en este caso es mínimo.

Estrategia de control de riesgos en Casilla.

No se cuenta con estrategias de control de riesgos para esta amenaza a nivel casilla. El valor del riesgo en este caso es mínimo.