IEPC
DURANGO
INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA

Manual de Acción para el **Control de Riesgos** del **Programa de Resultados Electorales Preliminares**
2018

PREP
DURANGO 2018
PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES

Contenido

Glosario

AEC: Actas de Escrutinio y Cómputo.

CATD: Centro de Adquisición y Transmisión de Datos.

CV: Centro de Verificación.

PREP: Programa de Resultados Electorales Preliminares.

PREP CASIILLA: Mecanismo a través del cual, los CAE o en su caso los 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.

IEPC: Instituto Electoral y de Participación Ciudadana de Durango.

UTC: Unidad Técnica de Cómputo

Presentación

El presente documento tiene como propósito establecer una guía de acciones para controlar los riesgos identificados en el Plan de Continuidad y Seguridad para el sistema informático del Programa de Resultados Electorales Preliminares (PREP) para el Proceso Electoral Local 2017-2018 en el Estado de Durango. El presente manual deberá atenderse y estar disponible en cada uno de los Centros de Acopio y Transmisión de Datos (CATD), además del Centro de Verificación (CV).

El propósito de las acciones descritas en el presente documento es salvaguardar la integridad de la información que se suministra y se genera por el PREP, y con esto garantizar una operación continua del programa bajo cualquier circunstancia. Para cumplir este propósito se han identificado amenazas a los distintos activos críticos y se han establecido actividades que deberán llevarse a cabo de acuerdo al plan establecido para reducir o eliminar el impacto o consecuencia de la amenaza.

A continuación, se enlistan las amenazas con mayor relevancia para la operación del PREP identificadas de la A1 a la A15 y las acciones a tomar para cada caso.

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.

CATD

1. Contactar con la persona ausente para verificar si la ausencia es temporal o permanente.

    a. Si la ausencia es temporal, se debe evaluar si el horario de ausencia afecta las actividades propias del PREP, tomando en cuenta la posibilidad de cubrir la ausencia temporal con el demás personal disponible en el CATD.

        i. Si la ausencia temporal afecta las actividades del PREP, se deberá asignar personal de reserva para cubrir las actividades.

        ii. Si la ausencia temporal no afecta las actividades, se deberá acordar un horario de asistencia posterior y deberá validarse dicha asistencia.

    b. Si la ausencia es permanente, deberá evaluarse la capacidad de cubrir las actividades de dicha persona con el demás personal disponible en el CATD.

        i. Si no se cuenta con capacidad suficiente se deberá asignar personal de reserva para cubrir las actividades.

        ii. Si se determina que la capacidad del CATD es suficiente, se procederá a asumir la ausencia.

2. En el caso de no ser posible contactar con la persona, se deberá intentar con medios alternativos de contacto, como otros números de teléfono, medios de contacto electrónico como mensajería o redes sociales, contacto a través de familiares o amigos, contacto a través de visita domiciliaria.

3. En caso de no poder contactar con la persona, se deberá evaluar la capacidad de cubrir las actividades con el demás personal del CATD

        i. Si no se cuenta con capacidad suficiente se deberá asignar personal de reserva para cubrir las actividades.

        ii. Si se determina que la capacidad del CATD es suficiente, se procederá a asumir la ausencia.

RESPONSABLES: Coordinadoras de Zona, Jefes de Zona, Líder de Proyecto.

CV.

1. Contactar con la persona ausente para verificar si la ausencia es temporal o permanente.

    a. Si la ausencia es temporal, se deberán reasignar actividades del personal del CV para cubrir la ausencia.

    b. Si la ausencia es permanente, deberá evaluarse la capacidad de cubrir las actividades de dicha persona con el demás personal disponible en el CATD.

        i. Si no se cuenta con capacidad suficiente se deberá asignar personal de reserva para cubrir las actividades.

        ii. Si se determina que la capacidad del CV es suficiente, se procederá a asumir la ausencia.

2. En el caso de no ser posible contactar con la persona, se deberá intentar con medios alternativos de contacto, como otros números de teléfono, medios de contacto electrónico como mensajería o redes sociales, contacto a través de familiares o amigos, contacto a través de visita domiciliaria.

3. En caso de no poder contactar con la persona, se deberá evaluar la capacidad de cubrir las actividades con el demás personal del CATD

        i. Si no se cuenta con capacidad suficiente se deberá asignar personal de reserva para cubrir las actividades.

        ii. Si se determina que la capacidad del CV es suficiente, se procederá a asumir la ausencia.

Casilla.

1. Contactar con la persona ausente para verificar si la ausencia es temporal o permanente.

    a. Si la ausencia es temporal, se deberá monitorear su asistencia en el nuevo horario acordado.

    b. Si la ausencia es permanente, se asumirá el riesgo al no tomar acciones y esperar a que la información llegue a través del CATD.

2. En el caso de no ser posible contactar con la persona, se deberá intentar con medios alternativos de contacto, como otros números de teléfono, medios de contacto electrónico como mensajería o redes sociales, contacto a través de familiares o amigos, contacto a través de visita domiciliaria.

3. En caso de no poder contactar con la persona, se asumirá el riesgo al no tomar acciones y esperar a que la información llegue a través del CATD, o en su defecto quedar en la espera de que se comunique la persona al CV.

RESPONSABLES: Coordinadora de Zona, Líder de Proyecto.

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.

CATD

1. En el caso de estar llevando alguna actividad de registro de información se deberá terminar dicho proceso.

2. Esperar de 2 a 3 minutos, en caso de que no se restablezca el suministro eléctrico, se debe reportar al CV.

3. De acuerdo al origen de la falla y el caso particular que se presente se tomarán acciones, tomando como guía lo siguiente:

    a. Si la falla se presenta únicamente en un equipo, indica desperfecto o falla en el equipo o en las conexiones del equipo incluyendo multicontactos, cableado, reguladores, no-break, entre otros, en esta situación se debe proceder a probar cada uno de los equipos para identificar el que presenta la falla y que pueda ser reemplazado.

    b. En caso de que el fallo se presente en todo el edificio, se trata de corte en la línea eléctrica o en los equipos de distribución como transformadores, si no se restablece el suministro en 10 minutos se debe hacer uso de planta de emergencia.

    c. En el caso de que las condiciones climatológicas presenten lluvias fuertes, vientos, o cualquier tipo de estado del clima que pueda afectar las líneas o equipos de distribución de energía, se tomará como origen de la falla causas naturales, si no se restablece el suministro en 10 minutos se debe hacer uso de planta de emergencia.

    d. En el caso de presentarse algún accidente o situación que haya ocasionado daños en equipos o líneas de distribución de energía, se considerará como evento fortuito, por lo general en este tipo de situaciones no hay restablecimiento del suministro de manera inmediata por lo que se deberá hacer uso de planta de emergencia.

CV

1. En caso de haber falla en el suministro de energía eléctrica se escuchará la alerta sonora de los equipos de suministro de energía ininterrumpida no-break.

2. Se debe proceder a verificar que la planta de emergencia de luz haya entrado en funcionamiento.

3. Si la planta de emergencia se encuentra operando correctamente o se ha restablecido el suministro eléctrico se deberá continuar trabajando normalmente.

4. En el caso de que la planta de emergencia de luz no haya iniciado correctamente, se debe proceder a terminar las actividades en proceso.

5. Solicitar apoyo al personal del IEPC para verificar el estado de la planta de emergencia, en caso de obtener respuesta de su funcionamiento dentro de los primeros 15 minutos después de haber sucedido el fallo, las actividades se pondrán en estado de espera hasta que se cuente con suministro eléctrico.

6. En caso de no haber respaldo por la planta de emergencia de las instalaciones del IEPC se deberá proceder a utilizar plantas de emergencia portátiles para poner en funcionamiento el equipo básico para no interrumpir las actividades del PREP.

Pasos para poner en funcionamiento planta de emergencia:

1. Termine cualquier actividad que este en proceso.
2. Apague los equipos.
3. Coloque planta de emergencia en un lugar ventilado.
4. Poner en marcha la planta de forma manual
5. Conectar la extensión eléctrica de ser necesario si la ubicación del equipo está lejos de la planta, en caso contrario conectar la pila a la planta de emergencia para continuar trabajando
6. Revisar periódicamente el nivel del combustible, si la falla eléctrica continúa se procede a solicitar más combustible.
7. Si la falla eléctrica no se corrigió después de 2 hrs. considerar el traslado de la información y de las actas a un CATD donde pueda continuar enviando las actas pendientes

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.

CATD

1. Cuando se presenta falla en la conexión a internet se deberá informar al CV para recibir instrucciones.

2. En el caso en que se cuente con una opción alternativa propia del PREP para conexión a internet, se hará uso de ella.

3. En el caso de que no se cuente con alguna alternativa de conexión a internet propia se procederá a solicitar el uso de la conexión del Consejo sede del CATD.

4. En caso de no lograr transmitir datos a través de las opciones anteriores, se procederá a la captura fuera de línea y se enviará la información en bloques mediante el uso de una Banda Ancha Móvil para la transmisión de datos. Se tendrá disponible una BAM en cada uno de los CATD, como alternativa de conexión a internet.

5. En el caso de que sea imposible establecer la conexión a internet, se procederá a trabajar fuera de línea, guardando los datos localmente, posteriormente se extraerán los datos en una memoria USB, la cual será colocada en un sobre para ser sellado y rubricado por representantes de partidos y el presidente del Consejo, para su posterior traslado al CATD más cercano, con el apoyo de un Jefe de Zona, se deberá ratificar el sobre con la información por parte de los representantes de partidos y presidente del CATD receptor.

CV

1. Se deberá monitorear constantemente la conexión a internet de los tres proveedores, y en el caso de identificar falla en alguno de ellos se deberá mantener en revisión hasta su restablecimiento.

2. En caso de que no se restablezca la conexión de algún proveedor se levantará reporte con el proveedor para su re conexión inmediata.

3. En caso de ser necesario, ya que el CV se localiza dentro de las instalaciones del Instituto, se podrá disponer de la conexión propia del IEPC como alternativa en caso de falla.

4. Si por algún motivo falla la conexión a internet de los tres proveedores se deberá hacer uso de conexión a internet vía Banda Ancha Móvil o señal 4G.

5. En caso de ser imposible tener conexión a internet en las instalaciones del CV, se procederá a trasladar la operación del CV a la unidad de transmisión de datos más cercana, éste procedimiento deberá ser autorizado por el IEPC.

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.

CATD.

1. En caso de detectar que el equipo para captura de información PREP no funcione correctamente se procede a continuar la captura con los equipos restantes.

2. El capturista deberá notificar al CV o al personal de soporte técnico asignado al CATD, con la finalidad de recibir instrucciones detalladas.

3. Mediante instrucciones del personal de soporte o del jefe de zona, se hará una evaluación rápida de la falla para determinar si hay fallas en las conexiones de los periféricos, de suministro eléctrico, conexiones de red o cualquier otro fallo que pueda solucionase re-conectando el equipo.

4. Se contará con un equipo de cómputo como respaldo en cada uno de los CATD en caso de que no se haya podido habilitar el dañado.

5. Se deberá revisar el equipo dañado para poder habilitarlo en caso de que se requiera reemplazar algún otro equipo.

CV.

1. Se procede a continuar el trabajo de verificación con los equipos restantes.

2. Se hará una evaluación rápida de la falla para determinar si hay fallas en las conexiones de los periféricos, de suministro eléctrico, conexiones de red o cualquier otro fallo que pueda solucionase re-conectando el equipo.

3. En caso de no resolver el problema en corto tiempo, el personal de soporte del CV deberá reemplazar el equipo para seguir operando en el menor tiempo posible.

4. Se deberá revisar el equipo dañado con la finalidad de habilitarlo en caso de que se requiera reemplazar algún otro equipo.

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.

CATD.

1. En caso de detectar que el equipo de adquisición de imágenes de las actas PREP no funcione correctamente se procede a continuar la digitalización con los equipos restantes.

2. El capturista deberá notificar al CV o al personal de soporte técnico asignado al CATD, con la finalidad de recibir instrucciones detalladas.

3. Mediante instrucciones del personal de soporte o del jefe de zona, se hará una evaluación rápida de la falla para determinar si hay fallas en las conexiones de los periféricos, de suministro eléctrico, conexiones de red o cualquier otro fallo que pueda solucionase re-conectando el equipo.

4. Se contará con un equipo de digitalización como respaldo en cada uno de los CATD.

5. El jefe de zona deberá revisar el equipo dañado para poder habilitarlo en caso de que se requiera reemplazar algún otro equipo.

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.

Casilla

1. En caso de falla en el dispositivo móvil para el mecanismo de PREP Casilla, el usuario del dispositivo móvil deberá reportar la falla al CV.
2. Personal de soporte proporcionará instrucciones para restablecer el funcionamiento del dispositivo móvil.
3. En caso de ser falla por conexión de datos en la zona de la Casilla se deberá proceder a realizar la captura en modo fuera de línea, para posteriormente trasladarse a una zona con acceso a internet, ya sea mediante datos de la red celular o mediante internet inalámbrico.
4. En el caso de no ser posible restablecer el funcionamiento del dispositivo o la aplicación, se podrá solicitar autorización por parte del Consejo para hacer uso de algún otro dispositivo o línea como reemplazo del equipo con fallos.
5. En caso de no ser posible el uso de equipo o línea alternativos, se aceptará el riesgo y se quedará en espera de recibir la información de la casilla en el CATD.

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.

CATD

1. El personal deberá portar de manera permanente su identificación laboral y se permitirá únicamente el acceso al área designada como CATD al personal autorizado y plenamente identificado, esto permitirá identificar de manera inmediata personal ajeno a la operación del PREP en el CATD.

2. En caso de identificar personal ajeno a las actividades del PREP se deberá notificar al consejo para solicitar apoyo de las autoridades correspondientes, personal del consejo, protección civil o seguridad pública.
3. Notificar al CV de la situación.
4. Resguardar las AEC.
5. De ser posible realizar un respaldo de las actas mientras se resuelve la situación.
6. Proceder a cerrar sesión en los sistemas, incluyendo el sistema operativo.
7. De no ser posible continuar con la captura se procederá a trasladar las actas respaldadas físicamente al CATD más cercano, esto con apoyo del Jefe de Zona.

CV.

1. En caso de identificar personal ajeno a las actividades del PREP se deberá notificar al Instituto y solicitar apoyo a las autoridades correspondientes, personal del IEPC, protección civil o seguridad pública.

2. Se deberá proceder a bloquear los equipos para evitar comprometer la información.

3. De no ser posible continuar con la captura se podrá implementar un plan de contingencia que permita trasladar las actividades del CV a otras instalaciones en condiciones de operar.

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.

CATD

1. En caso de detectar acceso no autorizado al sistema de captura PREP o a los equipos de digitalización de imágenes se deberá notificar al CV informando sobre el área en que se presenta el problema y registrar la hora del percance.

2. El equipo de soporte de sistemas deberá proceder a bloquear los accesos al sistema de los usuarios asignados en la zona para prevenir la introducción de información falsa o incompleta.

3. El equipo de soporte de sistemas deberá revisar la bitácora de registro de los usuarios afectados a partir de la hora informada, para poder identificar cualquier registro con sospecha de ser información falsa o incompleta, esto con la finalidad de hacer una revisión de los registros con apoyo de personal del Instituto.

CV.

1. El equipo de soporte de sistemas deberá proceder a bloquear los accesos al sistema de los usuarios afectados en la zona la introducción de información falsa o incompleta.

2. El equipo de soporte de sistemas deberá revisar la bitácora de registro de los usuarios afectados a partir de la hora informada, para poder identificar cualquier registro con sospecha de ser información falsa o incompleta, esto con la finalidad de hacer una revisión de los registros con apoyo de personal del Instituto.

Control de Acceso.

- Para controlar el acceso a los Sistemas para la operación del PREP, se abordarán distintas actividades orientadas a mantener la seguridad de la información.
- Los equipos contarán con usuario y contraseña para acceder al sistema operativo, las credenciales de acceso serán definidas antes de la instalación de los equipos en los CATD y CV, y serán controladas por el CV.
- El acceso al sistema operativo será controlado de manera local en el equipo, por lo que se podrán abordar las actividades de asignación y distribución de accesos, en caso de pérdida de datos de acceso, a través de la coordinación en el CV se podrá notificar nuevamente los accesos.
- Los sistemas informáticos para la operación del PREP contarán con usuario y contraseña, los cuales serán administrados por el personal de sistemas, para su distribución se abordarán las actividades necesarias por parte de la coordinación de cada zona desde el CV. En caso de pérdida de los accesos, se deberá notificar al CV y a través del equipo de sistemas se podrá re-asignar un nuevo acceso al sistema.
- Para fortalecer la seguridad de los accesos, los usuarios y contraseñas de los sistemas podrán ser renovados de un simulacro a otro, a consideración del líder de proyecto, y de manera obligatoria se deberán renovar todos los accesos para el día de la Jornada Electoral.
- La distribución de los usuarios del sistema operativo se hará de manera presencial en cada uno de los CATD y en el CV.
- La distribución de los usuarios para los sistemas informáticos del PREP se hará vía telefónica, a través de las líneas telefónicas propias y bajo plena identificación del personal.

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.

CATD

1. La red de datos del CATD deberá controlarse, deshabilitando la conexión inalámbrica y restringiendo el acceso al área donde se encuentra el modem y el equipo de red, el jefe de zona se encargará de instalar y configurar la red del CATD. Como prestación de seguridad, la comunicación con los servidores siempre se hará bajo protocolo HTTPS con cifradas bajo certificados SSL.
2. En caso de detectar acceso no autorizado a la red de datos del PREP, debido a que la conexión inalámbrica no estará habilitada, se deberá notificar al CV para recibir instrucciones.
3. Es probable que sea necesario deshabilitar la red temporalmente para evitar acciones mal intencionadas.
4. El jefe de zona o personal de soporte deberá dar instrucciones para monitorear los nodos de conexión a la red y lograr identificar el nodo de conexión afectado.
5. Se deberá bloquear el acceso no autorizado.
6. Se procederá a restablecer la red.
7. Se continuará con las actividades.

CV

1. En caso de detectar acceso no autorizado a la red de datos del PREP, debido a que la conexión inalámbrica no estará habilitada, se deberá deshabilitar la red temporalmente para evitar acciones mal intencionadas.
2. El personal de soporte deberá monitorear los nodos de conexión a la red y lograr identificar el nodo de conexión afectado.
3. Se deberá bloquear el acceso no autorizado.
4. Se procederá a restablecer la red.
5. Se continuará con las actividades.

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.

Con el objetivo de minimizar errores en la captura de datos del AEC, se tomará como referencia el catálogo de inconsistencias proporcionado por el IEPC, a través de la UTC, para la toma de decisiones referente al registro de datos del AEC.

CATD

1. En caso de detectar haber cometido algún error en la captura del AEC, se deberá notificar al CV.

2. El Coordinador(a) de zona o jefe de zona deberá determinar la causa del error mediante la evaluación de los datos capturados y la justificación presentada por el CATD, en caso de identificar intención deliberada se deberá notificar al líder de proyecto para tomar acciones.

3. Durante la primera validación del AEC y los datos capturados se deberá rechazar la captura, por lo tanto, pasará a una segunda validación.

4. Durante la segunda validación, de ser posible se deberá corregir la captura, de lo contrario se deberá reiniciar la captura de dicha acta para que sean ingresados los datos nuevamente desde el CATD.

5. Mediante comunicación permanente con el CV, el CATD deberá llevar a cabo nuevamente la captura para que pase al proceso de primera validación.

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.

CATD

1. Los equipos de cómputo utilizados para la operación del PREP son de uso exclusivo para tales fines, por lo que queda prohibido el uso del equipo para otro tipo de actividades. Adicional a esto no se hará uso de ningún dispositivo USB que no esté considerado como parte de la operación. Como medida de seguridad los equipos cuentan con software Antivirus previamente instalado, el cual cuenta con actualizaciones automáticas activadas para asegurarse de tener siempre la última versión de las definiciones de virus, spyware y malware.
2. En caso de detectar virus o malware en el equipo de cómputo se deberá reportar al CV para recibir instrucciones.
3. El equipo deberá ser desconectado de la red para evitar problemas en otros equipos.
4. Mediante el uso de antivirus previamente instalado (Windows Essentials) en el equipo se procederá a analizar el equipo en busca de problemas.
5. El antivirus detectará y solucionará el problema.
6. Conectar el equipo nuevamente a la red y realizar una captura a manera de prueba para verificar la

corrección del problema.

7. En caso de no ser corregido el problema el equipo deberá ser reportado como dañado y ser desconectado.
8. El jefe de zona deberá proporcionar un equipo de reemplazo o autorizar el uso del equipo de cómputo de respaldo.

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.

CATD

1. En caso de presentarse una situación de toma de instalaciones o cualquier otra que incapacite el uso del área designada para el PREP, se deberán abandonar las instalaciones de forma inmediata y en lo posible llevar a cabo las siguientes actividades hasta el punto que sea posible.
    a. Resguardar AEC.
    b. Desconectar equipo de cómputo.
    c. Resguardar equipo de cómputo (CPU principalmente)
2. Notificar al CV de la situación.
3. El jefe de zona deberá dar soporte para el traslado del personal y las AEC al CATD más cercano para continuar con la operación del PREP, esto en coordinación con el Consejo.

*EN NINGÚN CASO SE DEBERÁ PONER EN RIESGO LA INTEGRIDAD FÍSICA DEL PERSONAL POR LLEVAR A CABO ALGUNA DE LAS ACTIVIDADES PROPIAS DEL PREP.

CV

1. En caso de presentarse una situación de toma de instalaciones o cualquier otra que incapacite el uso del área designada para el PREP, se deberán abandonar las instalaciones de forma inmediata y en lo posible llevar a cabo las siguientes actividades hasta el punto que sea posible.
    a. Desconectar equipo de cómputo.
    b. Resguardar equipo de cómputo.
2. Notificar al IEPC y a las autoridades correspondientes de la situación, protección civil o seguridad pública.
3. En coordinación con el IEPC se podrá poner en operación el CV en instalaciones alternativas disponibles.

*EN NINGÚN CASO SE DEBERÁ PONER EN RIESGO LA INTEGRIDAD FÍSICA DEL PERSONAL POR LLEVAR A CABO ALGUNA DE LAS ACTIVIDADES PROPIAS DEL PREP.

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.

CATD

1. En caso de presentarse algún desastre natural que incapacite el uso del área designada para el PREP, se deberán evacuar las instalaciones de forma inmediata en caso de que el riesgo sea en el interior de las instalaciones o permanecer dentro de ellas en el caso de que el riesgo sea en el exterior como el caso de un huracán, y en lo posible llevar a cabo las siguientes actividades hasta el punto que sea posible.
    a. Resguardar AEC.
    b. Resguardar equipo de cómputo (CPU principalmente)
2. Notificar al CV de la situación.
3. El jefe de zona deberá dar soporte para el traslado del personal y las AEC al CATD más cercano para continuar con la operación del PREP, esto en coordinación con el Consejo.

*EN NINGÚN CASO SE DEBERÁ PONER EN RIESGO LA INTEGRIDAD FÍSICA DEL PERSONAL POR LLEVAR A CABO ALGUNA DE LAS ACTIVIDADES PROPIAS DEL PREP.

CV.

1. En caso de presentarse algún desastre natural que incapacite el uso del área designada para el PREP, se deberán seguir las instrucciones de acuerdo al tipo de desastre, lo que podría implicar abandonar las instalaciones de forma inmediata o permanecer dentro de ellas hasta nuevo aviso, y en lo posible llevar a cabo las siguientes actividades hasta el punto que sea posible.
    a. Resguardar equipo de cómputo (CPU principalmente)
2. Notificar al IEPC de la situación y a las autoridades competentes, protección civil.
3. En coordinación con el IEPC, dependiendo el tipo de desastre, se podrá poner en operación el CV en instalaciones alternativas disponibles o reanudar la operación del CV.

*EN NINGÚN CASO SE DEBERÁ PONER EN RIESGO LA INTEGRIDAD FÍSICA DEL PERSONAL POR LLEVAR A CABO ALGUNA DE LAS ACTIVIDADES PROPIAS DEL PREP.

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.

CATD

1. En caso de presentarse un incendio, se contará con un extintor en cada uno de los CATD, por lo que como primera opción se intentará hacer uso del mismo para apagar el fuego. (Seguir instrucciones de uso de extintores).
2. En caso de presentarse un incendio que no se pueda controlar se deberán abandonar las instalaciones, y en lo posible llevar a cabo las siguientes actividades hasta el punto que sea posible.
    a. Resguardar AEC.
    b. Resguardar equipo de cómputo (CPU principalmente)
3. Notificar al CV de la situación.
4. El jefe de zona deberá dar soporte para el traslado del personal y las AEC al CATD más cercano para continuar con la operación del PREP, esto en coordinación con el Consejo.

*EN NINGÚN CASO SE DEBERÁ PONER EN RIESGO LA INTEGRIDAD FÍSICA DEL PERSONAL POR LLEVAR A CABO ALGUNA DE LAS ACTIVIDADES PROPIAS DEL PREP.

CV

1. En caso de presentarse un incendio, se contará con un extintor en el CV, por lo que como primera opción se intentará hacer uso del mismo para apagar el fuego. (Seguir instrucciones de uso de extintores).
2. En caso de presentarse un incendio se deberán abandonar las instalaciones, y en lo posible llevar a cabo las siguientes actividades hasta el punto que sea posible.
    a. Resguardar equipo de cómputo.
3. Notificar al IEPC y a las autoridades correspondientes de la situación, protección civil o seguridad pública.
4. En coordinación con el IEPC se podrá poner en operación el CV en instalaciones alternativas disponibles.

*EN NINGÚN CASO SE DEBERÁ PONER EN RIESGO LA INTEGRIDAD FÍSICA DEL PERSONAL POR LLEVAR A CABO ALGUNA DE LAS ACTIVIDADES PROPIAS DEL PREP.

INSTRUCCIONES PARA USO DE EXTINTORES

- Mantener la calma e indagar qué es lo que se quema.
- Avisar a otras personas para que estén alertas (si se puede).
- Tomar el extintor adecuado.
- Sujetar firmemente del asa del acarreo y boquilla.
- Desprender la espoleta de seguridad.
- Pruebe el extintor accionando brevemente a través de la palanca de operación.
- Si está operable diríjase al sitio donde se está sucediendo el conato de incendio.
- Tome en cuenta la dirección del viento y ubíquese a favor de él.
- Sitúese a más o menos 1,50 metros del foco del fuego.
- Dirija la boquilla de la manguera hacia la base del fuego.
- Accione la palanca de operación y proceda a hacer el combate del fuego haciendo un movimiento de izquierda a derecha con la boquilla de la manguera y el cuerpo si es necesario.
- Ya extinguido el fuego o terminado el contenido del extintor, retírese del sitio sin dar la espalda.
- Reporte la descarga del extintor y colóquelo en un sitio donde nadie lo use equivocadamente.

Importante.

La amenaza contemplada con el identificador A7. Falla del Centro de Datos Primario no se tiene contemplada dentro del presente documento dado que el Centro de Datos presta servicio en la nube sin radicación física en algún CATD o en el CV.