



INSTITUTO  
DURANGUENSE DE  
EDUCACIÓN PARA  
ADULTOS

Plan de Recuperación en  
Caso de Desastres del IDEA

No. Control  
IDEA-STICODI-PRCD-  
DGN-01




Revisión: A

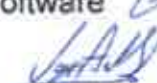
Fecha de entrada en  
vigor: 15/10/2021


Subdirección de  
TIC

### CONTROL DE FIRMAS

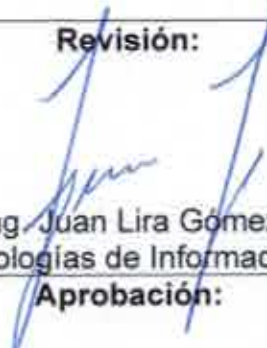
#### Elaboración:

Ing. Juan Daniel Carrillo Mercado Jefe de la Oficina de Desarrollo de Software 


Ing. Jorge Armando Solís Nájera Responsable de Aplicaciones Web 

Ing. Jesús Gerardo Domínguez Miranda Jefe de la Oficina de Mantenimiento Preventivo y Correctivo 

#### Revisión:

  
Ing. Juan Lira Gómez  
Subdirector de Tecnologías de Información y Comunicación

#### Aprobación:

  
L.A.E.T. Gabriela Guadalupe Álvarez Hernández  
Secretaría Técnica

### Control de Cambios

Revisión	Página (s) Afectadas	Descripción del Cambio	Fecha del Cambio



INSTITUTO  
DURANGUENSE DE  
EDUCACIÓN PARA  
ADULTOS

Plan de Recuperación en  
Caso de Desastres del IDEA

No. Control  
IDEA-STICODI-PRCD-  
DGN-01

Revisión: A

Fecha de entrada en  
vigor: 15/10/2021





SECRETARÍA DE  
EDUCACIÓN

Subdirección de  
TIC





INSTITUTO  
DURANGUENSE DE  
EDUCACIÓN PARA  
ADULTOS

## Plan de Recuperación en Caso de Desastres del Instituto Duranguense de Educación para Adultos

 <b>INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS</b>	<b>Plan de Recuperación en Caso de Desastres del IDEA</b>	<b>No. Control</b> <b>IDEA-STICODI-PRCD-DGN-01</b>	
		<b>Revisión: A</b>	
		<b>Fecha de entrada en vigor: 15/10/2021</b>	<b>Subdirección de TIC</b>

## Contenido

Capítulo I.....	2
Introducción.....	2
Capítulo II.....	3
Alcance.....	3
Capítulo III.....	3
Acciones Generales en Caso de Desastre .....	3
Rescatar las Operaciones en el Lugar del Desastre .....	3
Determinar el Sitio de Recuperación.....	3
Adquisición de Equipo Nuevo .....	4
Restauración de Datos a Partir de Respaldos.....	4
Restablecimiento de los Sistemas Informáticos Institucionales.....	5
Restauración de datos de Aplicación.....	5
Reubicarse en el Sitio Principal o Permanente .....	5
Capítulo IV.....	5
Riesgos de Desastre, Medidas Preventivas y Recomendaciones .....	5
Tipos de Riesgos.....	5
Capítulo V.....	11
Preparación para Desastres.....	11
Previsiones Ante un Desastre .....	11
Capítulo VI.....	12
Activación del Plan de Recuperación de Desastres. ....	12
Plan de Acción para la Activación del DRP.....	14
Capítulo VII.....	15
Respaldo de Información por el Usuario .....	15
Capítulo VIII.....	15
Clasificación del Nivel de Prioridad de la Información. ....	15
Capítulo IX.....	16
Sistema de Respaldo OneDrive Institucional.....	16

 INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS	Plan de Recuperación en Caso de Desastres del IDEA	No. Control IDEA-STICODI-PRCD-DGN-01	 SECRETARÍA DE EDUCACIÓN
		Revisión: A	
		Fecha de entrada en vigor: 15/10/2021	Subdirección de TIC

## Capítulo I

### Introducción

Este documento es la descripción y documentación del Plan de Recuperación en caso de Desastres en el Instituto Duranguense de Educación para Adultos (IDEA), también denominado DRP el cual es un acrónimo de Disaster Recovery Plan (en inglés), *Plan de Recuperación en caso de Desastres*. Este documento, es una guía en la que se establecen los procedimientos que se utilizarán antes, durante y después de una contingencia; los cuales, capacitarán al personal necesario para reducir el impacto negativo que pueda perjudicar los bienes informáticos, así como los procedimientos para restablecer la disponibilidad de los servicios de cómputo, sistemas informáticos institucionales y las comunicaciones que permiten mantener la continuidad de la operación de los servicios que brinda el IDEA, soportadas por las tecnologías de la información y comunicación.

La seguridad, integridad y salud del personal son de interés primario. Los procedimientos considerados solo deberán ser ejecutados si pueden ser realizados sin ningún riesgo.

Para efecto de este documento se entiende por:

**DRP:** Plan de recuperación en caso de desastres.

**Estado:** El Estado libre y soberano de Durango.

**Hardware:** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.



**IDEA:** Instituto Duranguense de Educación para Adultos.

**Instituto:** Instituto Duranguense de Educación para Adultos.

**Microsoft Office 365:** Herramienta creada por la compañía Microsoft que permite crear, acceder y compartir documentos por medio de internet entre distintos usuarios.

**Nube:** Servicio de almacenamiento de datos en servidores a través de internet.

**OneDrive:** Servicio de Microsoft que permite el almacenamiento y protección de archivos en la nube.

 <p>INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS</p>	<p>Plan de Recuperación en Caso de Desastres del IDEA</p>	<p>No. Control IDEA-STICODI-PRCD-DGN-01</p>	
		<p>Revisión: A</p>	
		<p>Fecha de entrada en vigor: 15/10/2021</p>	<p>Subdirección de TIC</p>

**Site:** Cuarto de telecomunicaciones de un edificio, es un área utilizada para el uso exclusivo de equipo asociado con el sistema de telecomunicaciones.

**STIC:** Subdirección de Tecnologías de Información y Comunicación del IDEA.

**Software:** Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

**Terabyte:** Termino dado a 1000 gigabytes.

**Usuario:** Persona que trabaja en el IDEA.

## Capítulo II

### Alcance

1. Es importante tener presente que uno de los objetivos de un DRP es identificar aquellas áreas que tienen prioridad, tanto por su naturaleza jerárquica en la organización y por la relevancia de la información que manejan, si estas unidades suspenden su operación se puede ver afectado o comprometido el trabajo y la operación de algunas áreas administrativas o de todo el Instituto.
2. Este plan se enfoca en las actividades y servicios que se brindan por medio de los equipos de cómputo como elementos fundamentales en los cuales se concentra la información de cada área administrativa, los sistemas informáticos que operan en las mismas, así como los responsables de dar respuesta y recuperación de la operación normal de los servicios informáticos y de comunicación institucionales.

## Capítulo III



### Acciones Generales en Caso de Desastre

#### Rescatar las Operaciones en el Lugar del Desastre

3. Se consideran los esfuerzos inmediatos a la ocurrencia del desastre para proteger y preservar el equipo de cómputo, en particular cualquier medio magnético y óptico de almacenamiento de datos deberá ser identificado y protegido o movido a un lugar seguro lejos del lugar del desastre.

#### Determinar el Sitio de Recuperación

4. Al mismo tiempo, una exploración de la escena del desastre deberá ser realizada por personal de la STIC y el titular de cada área administrativa afectada para estimar el tiempo requerido en reestablecer

 INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS	Plan de Recuperación en Caso de Desastres del IDEA	No. Control IDEA-STICODI-PRCD-DGN-01	 SECRETARÍA DE EDUCACIÓN
		Revisión: A	
		Fecha de entrada en vigor: 15/10/2021	Subdirección de TIC

el orden de trabajo de los sistemas afectados. Se deberá valorar y evaluar la magnitud del desastre con el objetivo de tomar la decisión de utilizar un sitio alternativo, que deberá ser un sitio lejano a la escena del desastre donde pueden reestablecerse temporalmente las capacidades computacionales y de redes de comunicación hasta que el sitio primario esté listo.



El trabajo deberá realizarse de manera inmediata, en cuanto lo permitan las condiciones del área afectada, para evaluar los costos y la reparación o reconstrucción del sitio primario, estimando el tiempo en que se podrán reestablecer los sistemas y la operación misma.

#### **Adquisición de Equipo Nuevo**

5. El proceso de recuperación se apoya fuertemente en la disponibilidad de recursos tecnológicos y económicos del IDEA, por lo que de esto dependerá la capacidad de respuesta para la adquisición de bienes y materiales necesarios que resulten dañados o que no pudieran ser rescatados del desastre.
6. El IDEA se apoyará en los procedimientos gubernamentales de emergencia que deban aplicarse para la inmediata generación y autorización de órdenes de compra para la adquisición de los bienes y materiales dañados.
7. Recuperación y reensamblaje de equipo tecnológico en el sitio de recuperación. - Los componentes rescatados y nuevos son reensamblados en el sitio de recuperación de acuerdo a instrucciones contenidas en este plan. Si los proveedores no pueden proveer un cierto componente en los tiempos requeridos, puede ser necesario efectuar sustituciones de último minuto. Después de que la fase de reensamblaje se ha completado, el trabajo siguiente será llevar a cabo los procedimientos de recuperación de datos.

#### **Restauración de Datos a Partir de Respaldos**

8. La recuperación de datos recae enteramente en el uso de respaldos guardados en ubicaciones fuera de sitio, principalmente con el servicio en la nube mediante el OneDrive, para este proceso de respaldo, todo el personal del IDEA tiene asignada una cuenta de correo institucional de Microsoft Office 365, la cual incluye la aplicación de OneDrive con una capacidad de almacenamiento de 1 terabyte, misma que deberá ser utilizada como medio de almacenamiento y respaldo de la información institucional.

 <p>INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS</p>	<p>Plan de Recuperación en Caso de Desastres del IDEA</p>	<p>No. Control IDEA-STICODI-PRCD- DGN-01</p>	 <p>SECRETARÍA DE EDUCACIÓN</p>
		<p>Revisión: A</p>	
		<p>Fecha de entrada en vigor: 15/10/2021</p>	<p>Subdirección de TIC</p>

9. Las unidades administrativas que manejen información relevante deberán realizar respaldos en medios magnéticos, ópticos, u otro medio de almacenamiento, siendo los mandos medios o superiores los responsables de llevar una bitácora de verificación del respaldo de la información que se genera en su área de adscripción por cada uno de sus colaboradores.

#### **Restablecimiento de los Sistemas Informáticos Institucionales**

10. En el proceso para restablecer los sistemas informáticos de las áreas afectadas, la STIC realizará la instalación inmediata de los sistemas operativos de cada sistema de cómputo, seguido de la recuperación de las aplicaciones y datos de usuario a partir de los respaldos; los usuarios que poseen aplicaciones especiales deberán involucrarse en la recuperación de sus aplicaciones con el objetivo de que éstas se reestablezcan con la configuración y funcionalidad correspondiente.

#### **Restauración de datos de Aplicación**

11. En este punto, el personal técnico de la STIC y los usuarios que resultaron afectados deberán colaborar de manera conjunta en la recuperación completa del servicio partiendo de la información resguardada en el último respaldo fuera del sitio con respecto a la fecha del desastre. Los usuarios deberán tener medios para recuperar los datos de bases de datos hasta el punto del desastre, y deberán ser capaces de introducir los datos generados en el sitio alterno para actualizar los sistemas institucionales a la fecha en que haya sucedido el desastre.

#### **Reubicarse en el Sitio Principal o Permanente**

12. Al término del proceso de restauración de los servicios en el sitio principal, se desmantela el equipo instalado en el sitio alterno y se llevan al sitio permanente.

## **Capítulo IV**

### **Riesgos de Desastre, Medidas Preventivas y Recomendaciones**

#### **Tipos de Riesgos**

13. Los riesgos considerados como amenazas que causen un posible desastre se encuentran los de tipo natural, o los ocasionadas por el ser humano, en base en estas causales se considera la siguiente clasificación:



- a. Por fuego.
- b. Por inundación.
- c. Por accidentes, derrumbes o daños por vientos fuertes.
- d. Por crimen cibernético.
- e. Por artefactos explosivos o de sabotaje.
- f. Por incidente que afecte el acceso a las instalaciones.

### Riesgo de Desastre por Fuego

14. Una amenaza de fuego en las instalaciones del IDEA es algo real y posee un índice de riesgo probable ya que el edificio central cuenta con un gran número de equipos de cómputo y dispositivos eléctricos, que combinado con el material de Tablaroca de algunas oficinas resulta un elemento propicio para que pueda suceder fuego por un sobrecalentamiento de las líneas eléctricas o un corto circuito.



Las medidas preventivas para actuar ante este riesgo se consideran:

- a. Alarma de incendio. – El IDEA deberá contar en sus instalaciones con sistemas de alarma contra incendio, con actuadores manuales, sirenas y señalamiento visual instalado en puntos estratégicos.
- b. Extinguidores. – Disponibles en lugares visibles y estratégicos en cada área administrativa.
- c. Entrenamiento y documentación. – Contar con instrucciones detalladas de las acciones a realizar cuando suceda un incendio, proporcionadas por la comisión de seguridad e higiene, así como la operación de los extinguidores y procedimientos de simulacro de incendio.

Recomendaciones:

- a. Revisión regular de los procedimientos. – Realizar una revisión periódica para asegurar que se encuentren al día, así como realizar ejercicios de simulacros contra incendios que puedan realizarse con el apoyo de personal de la dirección municipal de protección ciudadana con el objetivo de evaluar las acciones y procedimientos de reacción y a su vez contar con un informe escrito de los acierto y áreas de oportunidad ante la actuación del personal sobre la amenaza.



 <p>INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS</p>	<p>Plan de Recuperación en Caso de Desastres del IDEA</p>	<p>No. Control IDEA-STICODI-PRCD-DGN-01</p>	 <p>SECRETARÍA DE EDUCACIÓN</p>
		<p>Revisión: A</p>	
		<p>Fecha de entrada en vigor: 15/10/2021</p>	<p>Subdirección de TIC</p>

- d. Inspección regular del equipo de prevención de incendio. - Realizar una bitácora y calendario de inspección del funcionamiento y vigencia del material activo de extinguidores y demás equipo y herramienta contra incendio.

### Riesgo de Desastre por Inundación

15. Algunas instalaciones del IDEA se encuentran en pisos a desnivel o en sótanos, ese factor acopiado a la posibilidad de que una tormenta deposite grandes cantidades de lluvia representa una amenaza de inundación. Esta posibilidad también existe en el Site del Instituto puesto que está en la planta más alta y se podría filtrar el agua por el techo del mismo. La misma situación pudiera suceder en alguna otra instalación del Instituto al interior del Estado.

#### Medidas preventivas:

- a. Se llevó a cabo la construcción y modificaciones de los drenajes principales de las instalaciones, tanto en la planta baja como en la superficie del edificio, con esto se reduce dramáticamente el riesgo de inundación severa.



#### Recomendaciones:

- b. Inspección periódica a los sistemas de drenaje verificando que estén libres de obstrucciones, verificar fugas de agua especialmente el drenaje de aguas de lluvia proveniente del techo del edificio que pasa por el cuarto del Site principalmente en temporada de lluvia.
- c. Colocar sensores de agua en lugares estratégicos para detectar niveles de inundación principalmente donde se encuentre equipo de cómputo y telecomunicaciones.
- d. Realizar entrenamiento y capacitación de procedimientos de apagado regularmente, así como entrenamiento al personal para la atención a víctimas por electrocución.

### Riesgo de Desastre por Accidentes, Derrumbes o Daños por Vientos Fuertes

16. Debido a la zona geográfica donde están ubicados los edificios del IDEA no existen grandes posibilidades de vientos de intensidad suficiente como para provocar desastres mayores, sin embargo, se deben tomar medidas de precaución por si pudiera existir la eventualidad de que una ráfaga de viento produzca un daño mayor a las instalaciones.

#### Medidas preventivas:

 INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS	Plan de Recuperación en Caso de Desastres del IDEA	No. Control IDEA-STICODI-PRCD-DGN-01	
		Revisión: A	
		Fecha de entrada en vigor: 15/10/2021	Subdirección de TIC

- a. Inspección constante a los domos, ventanas y puertas, puesto que si resultan dañados se puede provocar la entrada de grandes cantidades de polvo o lluvia.
- b. En lo que respecta al cuarto del Site no existen estos elementos que puedan producir daños a los equipos, pero se tiene revisión constante de la puerta de entrada al mismo.

**Recomendaciones:**



- a. El personal del IDEA debe de conocer los riesgos de desprendimiento de ventanas o fractura de puertas o muros por algún accidente o por la presencia de vientos fuertes y conocer los lugares adecuados para protegerse en caso de desastre.
- b. El personal en general deberá estar preparado para contar con materiales y equipo que pudiera necesitar para cubrir o resguardar el equipo electrónico.

**Riesgo de Desastre por Crimen Cibernético**

17. El crimen cibernético se ha vuelto más común y más peligroso a medida que los sistemas se vuelven más complejos y el acceso se encuentra más ampliamente distribuido, con las nuevas tecnologías de red, se presentan fugas de acceso potenciales. El crimen cibernético usualmente no afecta los dispositivos de hardware en una forma destructiva. Tal vez sea más insidioso, y puede seguido venir del interior. Alguna persona mal intencionada puede infiltrar virus o bombas de tiempo en aplicaciones y código de sistemas.

**Medidas preventivas:**

- a. Asegurarse de que todos los sistemas y equipos cuentan con elementos de seguridad que protegen contra accesos no autorizados.
- b. Que los sistemas estén protegidos por contraseñas, especialmente aquellos que permiten actualizaciones a los datos.
- c. A todos los usuarios se les pide cambiar su contraseña de manera periódica.
- d. Implementar en los sistemas mecanismos de seguridad que registren los intentos inválidos de acceder a datos y los administradores de seguridad revisen estos registros diariamente.
- e. Realizar los respaldos de seguridad correspondientes, respaldando estos en un lugar diferente al de los datos originales.

 <p>INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS</p>	<p>Plan de Recuperación en Caso de Desastres del IDEA</p>	<p>No. Control IDEA-STICODI-PRCD-DGN-01</p>	
		<p>Revisión: A</p>	
		<p>Fecha de entrada en vigor: 15/10/2021</p>	<p>Subdirección de TIC</p>

f. La seguridad física del área de respaldos y almacenamiento de datos se implementa correctamente.

**Recomendaciones:**

- a. Mejora continua a las funciones de seguridad de cada plataforma.
- b. Políticas coercitivas y procedimientos especiales cada vez que se detecten violaciones a la seguridad.
- c. Regularmente dar a conocer a los usuarios la importancia de mantener sus contraseñas en secreto.
- d. Informar a los usuarios criterios de como establecer una contraseña segura y difícil de adivinar.
- e. Mejorar la seguridad de red.

**Desastre por Artefactos Explosivos o Sabotaje**



18. Los sistemas de telecomunicaciones son siempre blancos potenciales para amenazas y de sabotaje tales como algún artefacto explosivo y eliminación de información, en este rubro, la seguridad del Site resulta de relevante importancia.

**Medidas preventivas:**

- a. Dada la libertad que se goza en el Estado, y las instalaciones de IDEA, casi nadie aceptara una planeación de seguridad a gran escala, las restricciones y costos que serían necesarios para la protección del edificio en si ante un atentado. De cualquier modo, pueden aplicarse algunos principios de sentido común.
- b. Realizar inspección física de objetos que ingresa el personal y visitantes a las instalaciones.
- c. Contar con equipo de videovigilancia.

**Recomendaciones:**

- a. Las instalaciones del Site debe ser estructuralmente confiable.
- b. Las entradas al cuarto del Site deberán estar cerradas en todo momento.
- c. Solamente las personas autorizadas deberán de permitírseles la entrada.
- d. Las personas sospechosas deberán ser inspeccionadas y reportadas a los elementos de seguridad.

 <p>INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS</p>	<p>Plan de Recuperación en Caso de Desastres del IDEA</p>	<p>No. Control IDEA-STICODI-PRCD- DGN-01</p>	
		<p>Revisión: A</p>	
		<p>Fecha de entrada en vigor: 15/10/2021</p>	<p>Subdirección de TIC</p>

- e. Estar siempre pendientes de quien ingresa a las instalaciones.
- f. Las puertas del cuarto del Site deberán mantenerse cerradas en todo momento, todos los visitantes al cuarto del Site deberán recibir autorización con anticipación, así como registro de entrada y salida.

### **Desastre por Incidente que Impide el Acceso a las Instalaciones**



19. En esta clasificación se considera una pérdida total o parcial del acceso a las instalaciones del Instituto, dentro de las posibles causas se consideran a las manifestaciones del personal con un motivo de huelga, conflictos colectivos de trabajo, por recomendaciones de autoridades de salud, por seguimiento a un posible delito cometido, secuestro de las instalaciones por un acto delictivo, entre otras.

#### **Medidas preventivas:**

- a. Estar atentos a procesos administrativos que impliquen afectaciones al personal.
- b. Realizar evaluaciones de clima organizacional para conocer el sentir de los colaboradores.
- c. Mantenerse informados de los comunicados de las autoridades de salud.
- d. Ser conocedores de posibles grupos de interés que pudieran ser una amenaza dentro y fuera del Instituto.

#### **Recomendaciones:**

- a. Todo el personal deberá de tener su información respaldada en el OneDrive.
- b. Atender al personal inconforme con el resultado de algún proceso administrativo.
- c. Estar siempre atentos a los llamados de las autoridades de salud y de seguridad ciudadana, con el objetivo de prever los planes de acción inmediatos si es necesario trabajar fuera de las instalaciones del Instituto.

 <p>INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS</p>	<p>Plan de Recuperación en Caso de Desastres del IDEA</p>	<p>No. Control IDEA-STICODI-PRCD-DGN-01</p>	
		<p>Revisión: A</p>	
		<p>Fecha de entrada en vigor: 15/10/2021</p>	<p>Subdirección de TIC</p>

## Capítulo V

### Preparación para Desastres

#### Previsiones Ante un Desastre

20. Para facilitar la recuperación a partir de un desastre que destruye todo o parte de las instalaciones del IDEA, ciertas previsiones debieron realizarse con antelación. A continuación, se describe los aspectos que se deberán considerar para establecer un camino rápido y ordenado en la restauración de los servicios que operan en el Instituto:



- a. Planeación y recuperación ante el desastre.
- b. Definición del espacio temporal para la recuperación.
- c. Equipo de reemplazo.
- d. Respaldos de seguridad.

#### Planeación y Recuperación ante el Desastre

21. Un aspecto fundamental es contar con un DRP, mismo que servirá a los tomadores de decisiones para responder ante un desastre. Las condiciones bajo las que este plan puede ser efectivo dependen en gran parte de las previsiones y planes de contingencias con que cuente el Instituto, por lo que resulta relevante coordinar las actividades que se tengan consideradas en los diferentes planes de contingencia y equipos de trabajo para la atención de un desastre. El personal de cada área administrativa deberá contar con planes de acción de cómo realizar sus actividades en caso de desastre, tanto en su lugar de trabajo como en un sitio distinto.

#### Ubicación Temporal de Recuperación

22. Si el lugar donde haya ocurrido el desastre es destruido o se encuentra comprometido o inaccesible, será necesario restaurar los sistemas institucionales, servicios de conectividad y la operación administrativa en general en un lugar alternativo, por lo que la dirección general del IDEA en conjunto con los mandos medios necesarios deberá considerar y valorar el mejor sitio para la instalación provisional de los sistemas y servicios institucionales.

 INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS	Plan de Recuperación en Caso de Desastres del IDEA	No. Control IDEA-STICODI-PRCD-DGN-01	 SECRETARÍA DE EDUCACIÓN
		Revisión: A	
		Fecha de entrada en vigor: 15/10/2021	Subdirección de TIC

### Equipo de Reemplazo

23. El personal de la STIC deberá realizar un inventario de los equipos de cómputo, sistemas institucionales y enlaces de comunicación comprometidos en el desastre para determinar el equipo necesario para el reemplazo; también deberá evaluar la capacidad de respuesta que tenga el Instituto con el equipo y refacciones disponibles en su inventario. Para un inmediato restablecimiento de los sistemas y servicios institucionales la STIC deberá realizar un diagnóstico que considere los siguientes aspectos:
- Viabilidad de reubicar equipo de cómputo de áreas administrativas no comprometidas.
  - Equipo de cómputo que se pueda ser ensamblado con las refacciones en su inventario.
  - Equipo de cómputo que se pueda considerar por adquisición o arrendamiento con algún proveedor del IDEA.
  - Equipo de cómputo propiedad del personal institucional que sea viable para la operación de los sistemas institucionales.

### Respaldos

24. Este proceso se realizará con la última versión completa de la copia de seguridad que haya realizado el usuario del equipo de cómputo involucrado en el desastre, por esta razón, todo el personal del IDEA que procese información deberá asegurarse de tener copias de seguridad en la nube en las carpetas del OneDrive Institucional. Para los sistemas institucionales o bases de información que por alguna razón no se puedan respaldar en el OneDrive institucional, el responsable de cada área administrativa deberá asegurarse de realizar respaldos de seguridad en medios de almacenamiento externos que pueda resguardar fuera de su lugar de trabajo.

## Capítulo VI

### Activación del Plan de Recuperación de Desastres.

25. El director general del IDEA, en colaboración con los mandos medios de las subdirecciones y mandos medios de las áreas administrativas involucradas en el desastre, decidirán la activación del DRP después de haber valorado y evaluado los daños del desastre para lo cual deberán tener en cuenta lo siguiente:



INSTITUTO  
DURANGUENSE DE  
EDUCACIÓN PARA  
ADULTOS

## Plan de Recuperación en Caso de Desastres del IDEA

No. Control  
IDEA-STICODI-PRCD-  
DGN-01

Revisión: A

Fecha de entrada en  
vigor: 15/10/2021



SECRETARÍA DE  
EDUCACIÓN

Subdirección de  
TIC

- a. Si el evento no es considerado como desastre, se aplican los procedimientos de soluciones de problemas de día a día.
  - b. Si el evento se declara como desastre el director general toma la decisión final respecto de donde se habrá de realizar el proceso de recuperación.
  - c. Evaluación preliminar de los daños para establecer la extensión del daño al equipo de cómputo, sistemas institucionales, enlaces de comunicación afectados y demás mobiliario y equipo.
  - d. El daño estructural del inmueble.
  - e. Afectación en la red eléctrica.
  - f. Sistemas de ventilación.
  - g. Infraestructura de comunicaciones.
  - h. Servicios de agua y drenaje.
  - i. Subestación y transformadores eléctricos.
  - e. Días estimados para la recuperación del sitio en desastre.
26. Activado el DRP es de extrema importancia que todo equipo de cómputo, discos magnéticos u ópticos, documentación importante y otros elementos en el sitio dañado, en la medida de lo posible, sean resguardados en espacios seguros para evitar robo o daños mayores.
27. En el momento que sea posible, todo equipo de cómputo, de comunicación, consumibles y material de comunicación rescatable deberán ser trasladado a una ubicación segura. Si se encuentran sin daños deberán trasladarse al sitio de recuperación o a alguna área protegida mientras el sitio de recuperación esté listo.
28. Si el equipo ha sido dañado, pero puede ser reparado o reconstruido, deberá trasladarse a almacén para su resguardo o algún espacio seguro si el almacén está comprometido. Personal de la STIC o el personal de informática en las coordinaciones de zona realizarán inventario del equipo de cómputo rescatable y una estimación del tiempo que tardará en estar listo para volverse a usar.



INSTITUTO  
DURANGUENSE DE  
EDUCACIÓN PARA  
ADULTOS

## Plan de Recuperación en Caso de Desastres del IDEA

No. Control  
IDEA-STICODI-PRCD-  
DGN-01

Revisión: A

Fecha de entrada en  
vigor: 15/10/2021

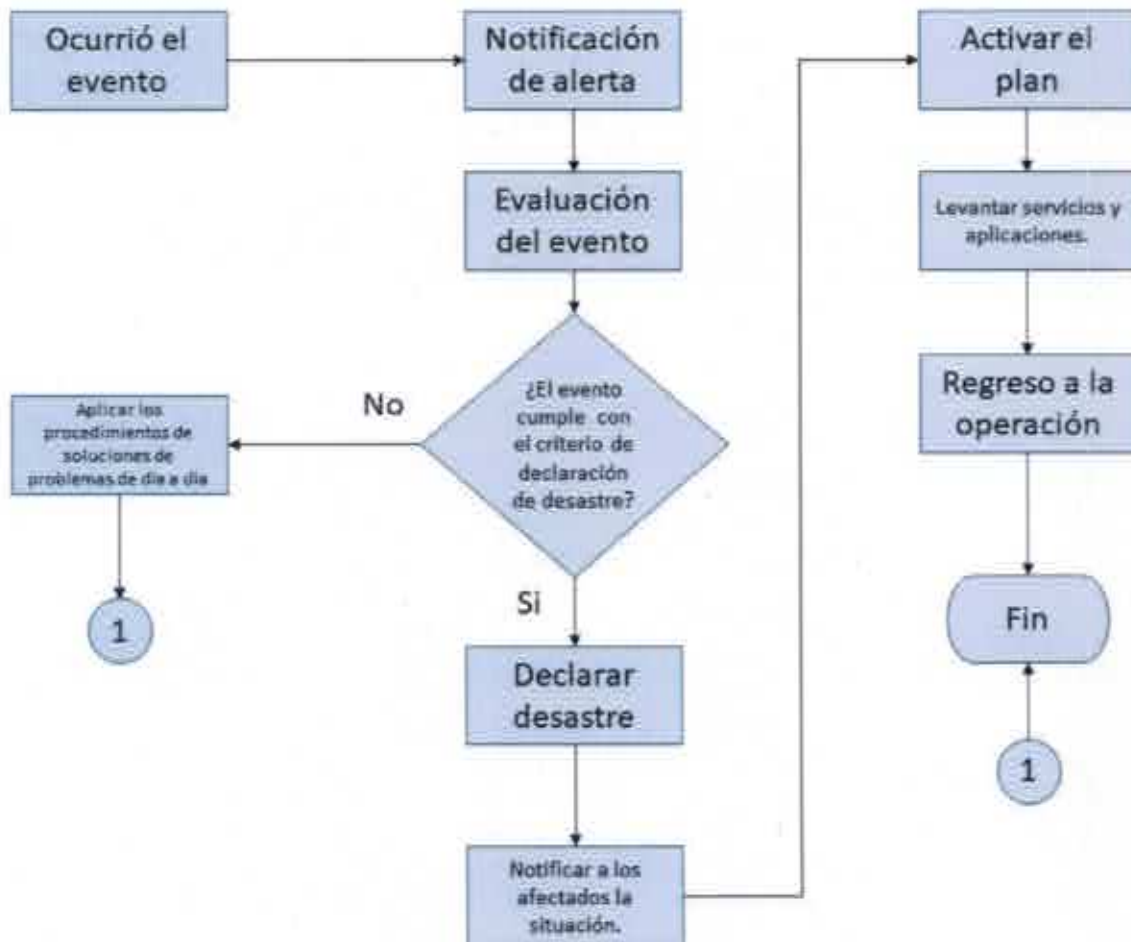


SECRETARÍA DE  
EDUCACIÓN



Subdirección de  
TIC

29. Con base en los inventarios de los daños en el equipo de cómputo y materiales de comunicación, el titular de Subdirección de Administración y Finanzas del IDEA deberá iniciar los procesos de cotización y adquisición de suministros y refacciones.

### Plan de Acción para la Activación del DRP





 INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS	Plan de Recuperación en Caso de Desastres del IDEA	No. Control IDEA-STICODI-PRCD-DGN-01	
		Revisión: A	
		Fecha de entrada en vigor: 15/10/2021	Subdirección de TIC

## Capítulo VII



### Respaldo de Información por el Usuario

30. La pérdida de información en forma parcial o total es un riesgo que se corre en cualquier organización, esto puede ser debido a errores involuntarios de los usuarios, fallas de hardware, fallas de software, virus informáticos, y los desastres mencionados anteriormente. La información que se almacena en los equipos de cómputo posee un valor cuantitativo y cualitativo para el IDEA por lo que es importante tomar medidas para reducir la afectación en la operación del Instituto, en el caso de pérdida de información se considera como medida preventiva los respaldos de información realizadas por el usuario.
31. Entiéndase por respaldo de información la copia de los archivos electrónicos que utilizan y generan los usuarios para realizar sus actividades almacenados en un dispositivo primario o varios dispositivos secundarios, para efectos de este DRP, en el servicio de almacenamiento en la nube del OneDrive Institucional.
32. Los usuarios de los equipos de cómputo serán los responsables de la información contenida en el equipo de cómputo asignado y de que esta sea debidamente archivada y respaldada.
33. En los equipos que funcionan como servidores de datos se hacen respaldos completos mensualmente almacenando la información en unidades de almacenamiento externas. Como estos son los que tienen un nivel de prioridad mayor se programa una tarea en la cual se especifica el día y la hora de respaldo de la información, por ejemplo, todas las semanas el día lunes a las 8:00 horas se realice una copia de la información de los mismos.

## Capítulo VIII

### Clasificación del Nivel de Prioridad de la Información.

34. Para efectos de identificar los diferentes tipos de información en relación a su importancia o por su sensibilidad para la operación del IDEA, se clasificará ésta en base a la siguiente tabla de prioridades:



 INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS	Plan de Recuperación en Caso de Desastres del IDEA	No. Control IDEA-STICODI-PRCD-DGN-01	
		Revisión: A	
		Fecha de entrada en vigor: 15/10/2021	Subdirección de TIC

Nivel de Prioridad	Descripción de Datos	Disponibilidad
0	Archivos personales del trabajador	No aplica / No relevante
1	Carpetas específicas con archivos de formatearía, documentos de comunicación interna.	Poco relevante para el funcionamiento de sistemas institucionales o servicios.
2	Bases de datos de diferentes sistemas y aplicaciones desarrollados, como el respaldo de estos mismos, página web y sistemas de comunicación	Debe estar disponible todo el tiempo

## Capítulo IX

### Sistema de Respaldo OneDrive Institucional

35. Para efectos de este DRP se utilizarán los respaldos en la nube ya que este tipo de sistemas en línea resultan ser una excelente estrategia de seguridad, sencilla, económica y permite realizar un respaldo de información de manera manual o programada.
36. La plataforma autorizada para las copias de seguridad de la información del Instituto será el OneDrive en la nube de Microsoft con usuarios de acceso institucional, esta herramienta también será el medio de almacenamiento de la información que el usuario genere diariamente.
37. El personal técnico de la STIC apoyará y orientará con la instalación y configuración de la herramienta OneDrive de cada usuario con el perfil institucional correspondiente.
38. La información clasificada con nivel de prioridad 2 deberá ser respaldada diariamente, mientras que la información con nivel 1 o 0 podrá ser respaldada de manera semanal.
39. Para los casos en que algún usuario necesite respaldar grandes cantidades de información como respaldos de seguridad, bases de datos, sistemas institucionales u otro tipo de información en los que el servicio en la nube no sea suficiente, el usuario deberá solicitar los medios de almacenamiento externo como disco de estado sólido u óptico con la capacidad de almacenamiento necesaria.

 INSTITUTO DURANGUENSE DE EDUCACIÓN PARA ADULTOS	<b>Plan de Recuperación en          Caso de Desastres del IDEA</b>	No. Control IDEA-STICODI-PRCD- DGN-01	
		Revisión: A	
		Fecha de entrada en vigor: 15/10/2021	Subdirección de TIC

40. Es responsabilidad de cada usuario tener respaldada la información de nivel 1 y 2 en el OneDrive institucional para que, en el caso de alguna eventualidad considerada en este plan, se pueda recuperar de manera inmediata y evitar contratiempos en la operación.
41. El titular de cada área administrativa deberá de llevar una bitácora de verificación del respaldo de la información de cada uno de sus colaboradores. En dicha bitácora se deberá especificar nombre del archivo, nivel de prioridad de la Información, fecha en que se realizó el último respaldo, fecha de verificación del respaldo, usuario responsable del respaldo, firma del usuario que realizó el respaldo y firma del titular que realizó la verificación del respaldo; esto como mecanismo de aseguramiento de que la información estará disponible y para deslindar una posible responsabilidad administrativa.
42. A excepción de una situación de contingencia o desastre, queda prohibido el uso de herramientas de almacenamiento personales, sean estos dispositivos electrónicos o sistemas de almacenamiento en la nube de perfiles de acceso no institucionales.