DGCFT | CATHI | TRABAJO SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL |

PLAN DE CONTINGENCIA PARA LA **RECUPERACIÓN** ANTE DESASTRES

INFORMÁTICA

Instituto de Capacitación para el Trabajo del Estado de Hidalgo

Circuito Exhacienda La Concepción,
Lote 17, Edificio C, San Juan Tilcuautla,
San Agustín Tlaxiaca, Hgo. C.P. 42160
Ofic.: 771 717 4050 al 55

Introducción

El Instituto de Capacitación para el Trabajo del Estado de Hidalgo (ICATHI) es un organismo público descentralizado de la Administración Pública Estatal, sectorizado a la Secretaría del Trabajo y Previsión Social. Su misión es promover la formación integral de personas competitivas, orientadas al fortalecimiento de sus competencias laborales, con el objetivo de impulsar su desarrollo profesional y contribuir al progreso económico y social de la región.

Este propósito se concreta mediante la oferta de servicios de capacitación flexibles, pertinentes y de alta calidad, diseñados para mejorar la calidad de vida de las y los hidalguenses.

Objetivo

En este marco institucional, y con el compromiso de preservar la integridad de la información generada o recabada por cada área, plantel y unidad móvil de capacitación, así como de cumplir con las normas vigentes en materia de calidad, seguridad y continuidad operativa, se establece el presente Plan de Contingencia para la Recuperación ante Desastres. Este documento tiene como finalidad garantizar la protección, respaldo y recuperación de los activos informáticos y documentales del Instituto, ante la eventualidad de incidentes que comprometan su funcionamiento.

Alcance

Este plan contempla la continuidad de la operación de los sistemas críticos que pongan en riesgo la prestación de los servicios mediante el uso de las TICs así como del resguardo y salvaguarda de la información relevante generada y/o capturada a través de las áreas de dirección general, planteles y acciones móviles de capacitación.

Evaluación de riesgos

El Instituto de Capacitación para el Trabajo del Estado de Hidalgo (ICATHI) cuenta con infraestructura propia de telecomunicaciones (SITE), a través de la cual se administran los servicios ofertados al público y los sistemas que los gestionan. Asimismo, dispone de 15 planteles y 10 acciones móviles de capacitación, operadas por una plantilla aproximada de 300 personas. En estos espacios se genera, procesa y resguarda información sensible mediante el uso de equipos de cómputo, conexiones a internet, transferencias entre dispositivos y registros directos en los sistemas institucionales.
Derivado de estas actividades, se han identificado las siguientes amenazas que podrían comprometer la continuidad operativa, la integridad de los datos y la seguridad de los recursos tecnológicos del Instituto:

- **Ciberataques:** Incluyen la infiltración mediante software malicioso, ataques de denegación de servicio (DDoS) y secuestro de información mediante ransomware.
- **Amenazas virales:** Como troyanos, malware, adware, spyware, gusanos, puertas traseras (backdoors) y técnicas de suplantación (phishing).
- **Riesgos naturales:** Tormentas eléctricas, Sismos y siniestros como incendios.
- **Riesgos tecnológicos**: Interrupciones en el suministro eléctrico, fallas en redes o servicios de comunicación y accidentes operativos.
- **Fallas de hardware:** Por obsolescencia, desgaste natural o defectos de fabricación.
- **Amenazas internas intencionadas:** Manipulación, daño o eliminación de información por parte de personal con acceso autorizado.

La identificación de estas amenazas permite establecer un marco preventivo y reactivo para la protección de los activos institucionales, y constituye la base para el análisis de impacto y la planificación de estrategias de recuperación.

Niveles de Impacto

Cada situación de contingencia tiene un procedimiento de recuperación formalizado por las áreas responsables y dependientes de los diversos sistemas de información. Cuando exista una situación de mayor gravedad, el personal operativo de nivel 1, debe armar el grupo de emergencia y activar el plan de recuperación de desastres.

Niveles de impacto	
Alerta	Definición
Bajo	Generado por eventos o acciones que afectan a equipos de cómputo y su atención no afecte otros servicios o sistemas ni procesos.
Medio	Provocad por incidentes que afectan el acceso a los sistemas de información de del instituto, interrumpiendo la operación normal de la entidad por un periodo mayor a 4 horas continuas y hasta 1 día.
Alto	Interrupción total al máximo tolerable afectando los procesos, sistemas y actividades del instituto por más de 24 horas.

Escenarios del Plan de Recuperación de Desastres

Los escenarios de activación del presente Plan de recuperación de Desastres son aquellos eventos y circunstancias reconocidas en la operación de TI, los cuales, impactan de forma no deseada la prestación de los servicios ofertados por el Instituto.
Para poner en marcha el plan de recuperación de desastres, se debe seguir los siguientes pasos:

1. Análisis del caso.
2. Localización del evento y su procedimiento respectivo
3. Puesta de marcha del Plan (DRP).
4. Monitoreo.

Evaluación de Impacto

A continuación, se analizan los servicios, procesos y equipos críticos de TI y el impacto al Instituto:

Procesos Críticos (Servicios)	Impacto (Bajo, Medio, Alto)	Identificación del recurso o sistema de TI	Tiempo de Recuperación objetivo
SITE	ALTO	Control de Operaciones de Servidores	1 dia
	MEDIO	Aire Acondicionado	1 día
	MEDIO	Sistema Eléctrico	0.5 días
Intranet	ALTO	Switches	1 día
	ALTO	Routers	1 día
	ALTO	Firewall	1 día
	MEDIO	PBX - Conmutador	1 día
Sistemas	ALTO	SCE	1 día
	ALTO	SACG	1 día
	ALTO	SMARPA	1 día
	ALTO	ASPEL	1 día
Página Web	ALTO	Sub dominios	2 días
	ALTO	Archivos de servidor	1 día
Servicios	MEDIO	Correo electrónico	ANS – Alta disponibilidad de servicio con el proveedor
	ALTO	Hosting	
	ALTO	Comunicaciones	3 días
Equipo	MEDIO	PC	1 día
	ALTO	Servidores	2 días

Algunos de estos riesgos están documentados y registrados en la matriz de riesgos del ICATHI con el código ICAT-PRE-CLC-03.01 por el área interna de evaluación y control de los mismos con el código clave ICAT-PRE-CLC-03.03 Mantenimiento de equipo e infraestructura (Informática), donde se documenta el proceso de acciones operativas a implementar.

Limitaciones

El presente Plan de Contingencia reconoce que, ante ciertos escenarios de desastre, existen limitaciones técnicas, logísticas y presupuestales que pueden afectar la capacidad de respuesta y recuperación del ICATHI.
En particular, cuando se presentan daños severos en uno o varios equipos críticos, tales como: switches, routers, firewalls o servidores, derivados de accidentes como incendios, cortocircuitos, sobrecargas eléctricas u otros eventos que los dejen inoperables e irreparables.
El restablecimiento de los servicios dependerá de los siguientes factores:

- **Disponibilidad presupuestal:** La adquisición de equipos de reemplazo está sujeta a la suficiencia financiera del Instituto y a los tiempos de autorización conforme a la normatividad vigente.
- **Tiempos de adquisición y entrega:** La reposición de componentes tecnológicos puede verse afectada por la disponibilidad en el mercado, los procesos de licitación o compra directa, y los tiempos de envío por parte de los proveedores.
- **Dependencia de terceros:** En algunos casos, la recuperación de servicios puede requerir la intervención de proveedores externos, fabricantes o instancias gubernamentales, lo cual podría extender los plazos de reactivación.

Estas limitaciones no representan una omisión en la planificación, sino una consideración realista que permite priorizar acciones, gestionar expectativas y fortalecer la resiliencia institucional ante escenarios adversos.

Estrategia de Recuperación

La estrategia de recuperación comienza desde el procedimiento de manejo de incidencias, el cual detecta, escala los requerimientos y define si es necesario iniciar el plan de recuperación.

Procedimiento de manejo de Incidencias

Este procedimiento tiene como objetivo garantizar una atención oportuna, eficiente y escalable ante cualquier falla que afecte el funcionamiento de los sistemas institucionales, plataformas digitales o equipos de cómputo utilizados por el personal administrativo y capacitandos.

El orden en el cual se realiza el escalamiento de las incidencias se puede ver en la siguiente tabla.

Nivel de Operación	Encargado	Rol	Contacto
1	Director(a) de área de Planeación	Coordinador	7717174050 ext 500
2	Jefe de Informática	Líder y Gerente de recuperación	7717174050 ext 507
3	Auxiliar 1 Informática	Integrante Auxiliar	7717174050 ext 513
4	Auxiliar 2 Informática	Integrante Auxiliar	7717174050 ext 513
5	Auxiliar 2 Informática	Integrante Auxiliar	7717174050 ext 513

El procedimiento se activa cuando se detecta una anomalía, error o interrupción que impida el uso adecuado de los servicios tecnológicos. Una vez identificada la incidencia, esta deberá ser reportada al área de Informática, conforme a los niveles de operación establecidos (2, 3, 4 o 5), según el grado de afectación.

El proceso contempla las siguientes etapas:

1. **Registro y clasificación**: Las incidencias se reportan en la plataforma SICODI institucional, con fecha, hora, descripción del problema, área afectada y nivel de prioridad. Se clasifica como menor, moderada o crítica, según su impacto en la operación institucional.
2. **Diagnóstico técnico**: El personal especializado evalúa el tipo de daño, error o afectación, determinando si es posible corregirlo mediante acciones inmediatas (reparación, reinicio, reconfiguración, restauración de respaldo, entre otras).
3. **Resolución o escalamiento**:
    - Si la incidencia es menor y puede ser resuelta internamente por los niveles de operación 3, 4 y 5, se procede con la solución técnica correspondiente.
    - Si la afectación excede la capacidad operativa del área de Informática en los niveles 3, 4 y 5 o compromete la integridad de los sistemas, se escala al nivel de operación 2, reportándolo de manera telefónica o por correo electrónico.
4. **Activación del Plan de Recuperación ante Desastres**: El plan se activa únicamente cuando la incidencia se convierte en un evento crítico que compromete la continuidad operativa del Instituto, como en los siguientes casos:
    - Pérdida total o parcial de información sensible sin posibilidad de recuperación inmediata.
    - Fallas irreparables en infraestructura tecnológica clave (servidores, firewalls, sistemas centrales)
    - Ataques cibernéticos que afecten la confidencialidad, disponibilidad o integridad de los datos.
    - Eventos naturales o tecnológicos que imposibiliten el funcionamiento de los planteles o unidades móviles.
5. **Seguimiento y cierre**: Una vez resuelta la incidencia, se documenta la solución aplicada, el tiempo de respuesta y las medidas preventivas recomendadas. Se genera un informe técnico para retroalimentación y mejora continua.

Este procedimiento permite al ICATHI mantener un enfoque proactivo, ordenado y resiliente ante cualquier situación que afecte sus activos tecnológicos, fortaleciendo la seguridad operativa y la confianza institucional.

Proceso de operaciones de respaldo

Con el propósito de garantizar la seguridad de la información digital y dar cumplimiento a las normas vigentes en materia de calidad y protección de datos, se establece el siguiente procedimiento institucional para el resguardo de archivos generados en cada área, plantel y acción móvil del Instituto. Para ello, cada área descrita cuenta con dispositivos de almacenamiento tipo disco duro externo de 2 tb, destinados exclusivamente a conservar documentos de valor técnico, operativo o administrativo, tales como archivos en formato Excel, Word, PowerPoint, PDF, entre otros.

Lineamientos Generales para el personal administrativo

1. **Identificación de respaldos:** Cada respaldo deberá almacenarse en una carpeta nombrada con el puesto del generador de información y la fecha del resguardo. Ejemplo: AUXFINANZAS1-24-09-2025. Cada persona será responsable directa del resguardo de la información que genere.

2. **Acceso y consulta:** En caso de requerir la consulta o incorporación de nueva información al dispositivo de almacenamiento, se deberá notificar previamente al director del plantel o área correspondiente, quien autorizará la operación y supervisará la generación de un nuevo respaldo. En caso de requerir el acceso a algún respaldo ya vaciado en el servidor designado para este fin, se realizará por medio de oficio dirigido a la dirección de planeación, justificando el motivo por el cual requieren una copia del respaldo.

3. **Frecuencia de respaldo:** La generación de respaldos deberá realizarse al finalizar cada mes. No obstante, si alguna persona requiere realizar el respaldo antes de dicho periodo, podrá hacerlo previa notificación.

4. **Permanencia de la información:** Todos los respaldos serán conservados de manera indefinida en el dispositivo de almacenamiento. Quedará estrictamente prohibido eliminar cualquier contenido previamente resguardado.

5. **Consolidación anual:** Al finalizar el año, se procederá a compactar todos los respaldos en un archivo comprimido (.zip), el cual será igualmente resguardado en el dispositivo de almacenamiento correspondiente hasta el vaciado de los resguardos por área, plantel o acción móvil que será realizado por el departamento de informática en el servidor de almacenamiento destinado para este fin.

6. **Supervisión técnica:** El Departamento de Informática del Instituto en cualquiera de sus niveles de operación, será responsable de revisar y validar, conforme a la agenda anual de mantenimiento institucional, que se esté cumpliendo con el manejo y resguardo adecuado de la información. En caso de detectar alguna irregularidad, se notificará de inmediato al área correspondiente para su atención oportuna.

7. **Resguardo de respaldos:** Para el vaciado anual de los respaldos de cada área generadora, el departamento de informática a solicitud de cada área, realizara el vaciado y control de respaldos en el servidor designado para esta función, así como el formateo de cada dispositivo de almacenamiento externo para su uso y gestión del nuevo ciclo a respaldar.

Lineamientos Generales del área de informática

Con el objetivo de garantizar la integridad, disponibilidad y recuperación de la información generada y capturada de los sistemas, datos y configuraciones de los diferentes softwares y/o sistemas, el área de Informática deberá implementar un proceso sistemático de respaldos que contemple los siguientes lineamientos:

1. **Modalidades de respaldo:** Los respaldos de sistemas, datos y configuraciones deberán realizarse en tres niveles complementarios:
    - **Respaldo local:** Copia dentro del mismo servidor que aloja el sistema o base de datos.
    - **Respaldo externo:** Copia en dispositivos de almacenamiento físico (discos duros externos) debidamente etiquetados y resguardados.
    - **Respaldo centralizado:** Copia en el servidor institucional designado exclusivamente para la función de resguardo de respaldos y archivos.

2. **Identificación y organización:** Cada respaldo deberá almacenarse en una carpeta debidamente nombrada con la clave del servidor y la fecha de generación, siguiendo el formato: NOMBREDELServidor-DD-MM-AAAA. Ejemplo: SERVERZEUS-24-09-2025.
   La persona asignada con nivel de operación 2 será responsable directo del manejo, organización y resguardo de dicha información.

3. **Frecuencia de respaldo:** La periodicidad de los respaldos será determinada conforme al tipo de sistema, volumen de datos y criticidad operativa, considerando las siguientes opciones:
    - Mensual
    - Quincenal
    - Semanal

   Adicionalmente, podrán generarse respaldos extraordinarios a solicitud de los usuarios o cuando los procesos institucionales lo requieran, especialmente en casos de actualizaciones, migraciones o eventos relevantes.

4. **Supervisión técnica:** La persona con nivel de operación 1 será responsable de verificar que los respaldos se realicen conforme a los lineamientos establecidos, validando su integridad, ubicación y accesibilidad. En caso de detectar alguna irregularidad, deberá notificar de inmediato al área y nivel de operación correspondiente para su atención o corrección.

5. **Resguardo y ciclo anual:** Al finalizar cada ciclo anual, el área de Informática, en cualquiera de sus niveles de operación, deberá realizar el vaciado, consolidación y resguardo de los respaldos en el servidor institucional designado. Asimismo, se procederá al formateo seguro de los dispositivos de almacenamiento externo, garantizando su disponibilidad para el nuevo ciclo operativo.
   Este proceso podrá ser solicitado por las áreas administrativas que gestionan directamente los sistemas, y deberá documentarse mediante bitácoras o informes técnicos que respalden la trazabilidad de la información.

Acciones de Recuperación

Para facilitar la rápida restauración de los sistemas, servicios y/o equipos después de un desastre, se establecen los siguientes procedimientos:

1. Procedimiento de recuperación ante fallas en el sistema operativo de equipos de computo administrativos y/o de capacitación

En caso de que algún equipo quede inoperable por daño en el sistema de archivos del sistema operativo se debe:

1. Verificar que sea un fallo errático o fijo.
2. Reportar la incidencia mediante el sistema SICODI, anotando fecha, observaciones, marca, modelo y numero de inventario del o los equipos.
3. La persona resguardante del equipo o encargada de servicios y mantenimiento de cada plantel o Acción móvil de capacitación deberá llevar el equipo al área de informática para su valoración y reparación.
4. El personal operativo en los niveles 2, 3, 4 o 5 revisara el equipo para determinar si será reparado o formateado según sea el daño.

5. En caso de ser necesario el formateo se notificará al área o persona resguardante del equipo, para la recuperación de la información, así como del ultimo respaldo que se tenga para su reparación y reincorporación.
6. El personal operativo en los niveles 2, 3, 4 o 5 realizara las pruebas necesarias para garantizar la funcionalidad del equipo reparado y recuperado.
7. Se realizará la entrega del equipo mediante el vale de entrega **ICAT-PRS-PLN-01.06** a la persona resguardante del equipo o encargada de servicios y mantenimiento de cada plantel o Acción móvil de capacitación para su reincorporación al área de trabajo.
8. El personal operativo anotara las observaciones y recomendaciones necesarias en el sistema SICODI institucional, así como en el vale de entrega **ICAT-PRS-PLN-01.06,** dando por terminado este proceso.

2. Procedimiento de recuperación ante fallas en el sistema operativo de equipos de servidores

En caso de que algún servidor quede inoperable por daño en el sistema de archivos del sistema operativo se debe:

1. Verificar que sea un fallo errático o fijo.
2. El personal con el nivel de operación 2 o el nivel que con el conocimiento necesario se encuentre en el área afectada para determinar y valorar el daño, origen y acciones a realizar.
3. Se notificará al personal operativo de nivel 1 en todo momento para su conocimiento y acciones necesarias a realizar para su posible reemplazo o adquisiciones requeridas para su reparación.
4. Se realizarán las acciones necesarias para la recuperación y aseguramiento de la información necesaria, así como del último respaldo disponible de ser necesario.
5. En caso de daño en algún componente de hardware se notificará al personal operativo de nivel 1, solicitando la autorización de solicitud de compra de la o las piezas y/o refacciones necesarias.
6. El personal de informática en cualquier nivel procederá a la reparación del sistema o reinstalación del mismo según sea el caso.
7. Se realizará la instalación del sistema, software y configuraciones necesarias para su restablecimiento.

8. El personal operativo de nivel 2 realizara las pruebas necesarias para determinar el funcionamiento adecuado del servidor.
9. Se notificará al personal operativo de nivel 1 de la reparación y restauración del servidor, así como al área dependiente de este servicio.
10. Se realizará el reporte informando de las afectaciones, origen y acciones realizadas, dando por terminado este proceso.

3. Procedimiento de recuperación ante fallas o indisponibilidad de o los sistemas

En caso de que algún servicio o sistema no esté recibiendo peticiones o genere intermitencia, se debe:

1. El personal operativo o usuario de algún sistema o servicio que detecte alguna falla en estos, deberá notificarlo oportunamente mediante correo electrónico o número de contacto al personal operativo de nivel 2 y en caso de ser necesario con oficio de atención al área de Planeación del Instituto, anexando los datos de la falla, fecha, hora y de ser necesario capturas de pantalla visibles y legibles donde se muestre el error o fallo.
2. El personal operativo de cualquier nivel que cuente con los conocimientos necesarios y autorización deberá:
    - **2.1.** Ingresar al servidor donde se encuentre el sistema.
    - **2.2.** Revisar alertas y alarmas configuradas.
    - **2.3.** Identificar componentes y/o servicios sin funcionamiento. Si el componente caído es el servicio de base de datos, se debe ir al **procedimiento de recuperación ante caída de la base de datos.**
    - **2.4.** Revisar los valores asignados a cada componente o servicio.
    - **2.5.** Realizar copia de seguridad del componente o servicio caído.
    - **2.6.** Intentar reiniciar el servicio caído.
    - **2.7.** Si no hay componentes caídos, pasar a **procedimiento de recuperación ante la falla de software**.
    - **2.8.** En caso de que el componente no pueda ser reiniciado, se debe restaurar desde su última copia de respaldo.
    - **2.9.** Si la copia de respaldo no soluciona el problema, se debe restaurar desde la última imagen estable de la solución.
    - **2.10.** Realizar pasos 2.2 a 2.6 hasta solucionar el problema.

3. El personal operativo de nivel 2 notificara al o las áreas dependientes de la restauración del servicio.
4. Se realizará el reporte informando de las afectaciones, origen y acciones realizadas, dando por terminado este proceso.

4. Procedimiento de recuperación ante fallas de software o sistemas informáticos.

Este procedimiento solo se puede ejecutar si el Procedimiento de recuperación ante fallas o indisponibilidad de o los sistemas identifica que no existe componente o servicio caído. Todo componente o servicio en el servidor debe estar activo:

1. El personal operativo en cualquier nivel encargado de los desarrollos de software o sistemas se encargará de darle seguimiento.
2. Se realizará el respaldo extraordinario de la base de datos.
3. Se realizará una copia de seguridad del proyecto de desarrollo y sistema compilado o generado.
4. Revisar logs del sistema para identificar problemas.
5. Si problema está relacionado a alguna actualización reciente, se debe restaurar software a la versión previa en el ambiente de desarrollo.
    a. Si se corrige problema en ambiente de desarrollo. entonces se debe corregir el software en dicho ambiente, realizando hotfix (parche rápido).
    b. Se ejecutan las pruebas unitarias de la solución.
    c. Si todas las pruebas están correctas y la solución, en ambiente QA, está operativa, entonces se realiza un paso a producción.
    d. Se realizan nuevas pruebas unitarias que eviten que el error se repita en el futuro.
6. Si el problema está relacionado a alguna configuración del sistema,
    a. Replicar las copias de seguridad del ambiente productivo en un ambiente de desarrollo.
    b. Realizar pruebas de configuración para identificar problemas.
    c. Corregir problema en ambiente de desarrollo.
    d. Realizar pruebas unitarias de la solución.
    e. Realizar pruebas de usuario.
    f. Si no hay errores, se debe realizar paso a producción. En caso contrario, iterar punto 7.

g. Realizar configuraciones en ambiente productivo.
h. Documentar error.

7. El personal operativo de nivel 2 notificara al o las áreas dependientes de la restauración del servicio.
8. Se realizará el reporte informando de las afectaciones, origen y acciones realizadas, dando por terminado este proceso.

5. Procedimiento de recuperación ante fallas o caída de base de datos.

En caso de que algún servicio o sistema no esté recibiendo ni administrando peticiones de información o genere intermitencia, se debe:

contactar al personal operativo de nivel 2 o encargado de desarrollo de sistemas y bases de datos.

1. El personal operativo o usuario de algún sistema o servicio que detecte alguna falla en estos, deberá notificarlo oportunamente mediante correo electrónico o número de contacto al personal operativo de nivel 2 y en caso de ser necesario con oficio de atención al área de Planeación del Instituto, anexando los datos de la falla, fecha, hora y de ser necesario capturas de pantalla visibles y legibles donde se muestre el error o fallo.
2. El personal operativo de cualquier nivel que cuente con los conocimientos necesarios y autorización deberá:
    2.1 Realizar respaldo extraordinario de la base de datos.
    2.2 Realizar copia de seguridad de los servidores de base de datos.
    2.3 Restaurar en un ambiente de desarrollo la base de datos. En dicho ambiente revisar que la base de datos tenga espacio disponible en disco.
    2.4. Corregir espacio si falta.
    2.5. Revisar logs de la base de datos.
    2.6. Revisar alertas de ambiente de datos.
    2.7. Identificar y corregir problemas en base de datos.
    2.8. Realizar pruebas en ambiente de desarrollo. Si fallan las pruebas, volver al punto 2.5.
    2.9. Realizar paso a producción de modificaciones y correcciones.

3. Si la base de datos no puede ser corregida, se debe restaurar la última versión respaldada, notificando al área dependiente y al personal operativo de nivel 1 de este suceso.
4. El personal operativo de nivel 2 notificara al o las áreas dependientes de la restauración del servicio.
5. Se realizará el reporte informando de las afectaciones, origen y acciones realizadas, dando por terminado este proceso.

Guía de Activación

La presente guía establece los pasos secuenciales para la activación del Plan de Recuperación ante Desastres (DRP) del ICATHI, en caso de presentarse una contingencia que afecte la operación institucional. Su propósito es garantizar una respuesta ordenada, eficaz y coordinada ante eventos críticos.

1. **Evaluación inicial del alcance e inventario de eventos críticos:** Se realiza un diagnóstico inmediato para identificar el tipo de incidente, las áreas afectadas, los sistemas comprometidos y el nivel de impacto operativo.

2. **Determinación del nivel de contingencia:** Se clasifica el evento conforme al nivel de alerta establecido en el plan:
    - *Baja*: afectación limitada, sin interrupción significativa.
    - *Media*: afectación relevante, con interrupción parcial de servicios.
    - *Alta*: afectación crítica, con interrupción total o pérdida de activos clave.

3. **Comunicación institucional permanente:** Se informa de manera continua y oficial a los equipos internos y externos involucrados, incluyendo responsables técnicos, administrativos y autoridades superiores.

4. **Activación de alertas concertadas:** Se ponen en marcha los protocolos de alerta definidos en el plan, según el nivel de contingencia, asegurando que cada área reciba instrucciones claras y oportunas.

5. **Inicio del DRP y ejecución de procedimientos técnicos:** Se activa formalmente el Plan de Recuperación ante Desastres, iniciando los procedimientos específicos de recuperación en cada área afectada, conforme a los manuales técnicos y operativos.

6. **Supervisión y seguimiento continuo:** Se establece un sistema de monitoreo permanente para evaluar la evolución del evento, validar las acciones ejecutadas y ajustar las estrategias conforme a la situación.

7. **Transición hacia la normalidad operativa:** Una vez controlado el evento, se inicia el proceso de retorno a la operación normal, activando el plan de retorno de contingencia definido para cada plataforma tecnológica.

8. **Comunicado de cierre de emergencia:** Se emite un comunicado institucional que declara el fin del evento crítico, informando a todas las áreas sobre la reanudación de actividades y medidas preventivas posteriores.

9. **Revisión y ajuste del DRP:** Se realiza una evaluación técnica del desempeño del plan, identificando áreas de mejora, actualizando metodologías de prueba y fortaleciendo los protocolos existentes.

10. **Documentación de lecciones aprendidas y cierre formal del incidente:** Se elabora un informe final que documenta los eventos ocurridos, las acciones ejecutadas, los aprendizajes institucionales y se formaliza el cierre del incidente conforme a los procedimientos establecidos.

Término de la crisis

El personal operativo de nivel 1 debe definir el retorno a la normalidad, definiendo los siguientes aspectos: día, fecha y hora de la activación de los sistemas de información, valoración explicando si hubo daños y afectaciones de los equipos físicos y/o virtuales, sincronización de sistemas de telecomunicaciones, actualización de la matriz de riesgos y gestión de incidentes.

Control de Cambios

Fecha	Versión	Cambios Introducidos	Simplificación o mejora
23/09/2025	1.0	Creación del documento	Mejora

Créditos

Elaboro	Revisión y Aprobación
José Ramón Nájera Vargas **Encargado del departamento de Informática**	Maribel Azpeitia Camargo **Directora de Planeación**