Secretaría de Medio Ambiente y Recursos Naturales Coordinación Administrativa	MEDIO AMBIENTE SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES
Título del documento: **Procedimiento de Recuperación ante Desastres y Continuidad de Operaciones Informáticas.**	

I. Introducción.

En la actualidad, el uso intenso de tecnologías de la información representa un componente esencial para el cumplimiento de las funciones sustantivas y administrativas de la Secretaría de Medio Ambiente y Recursos Naturales de Hidalgo (SEMARNATH).
La continuidad de los servicios informáticos y la protección de los datos institucionales son elementos fundamentales para garantizar la eficiencia, transparencia y legalidad de la gestión pública.
Frente a la posibilidad de eventos disruptivos como desastres naturales, fallas técnicas, incidentes de ciberseguridad o errores humanos, es indispensable contar con mecanismos institucionales que permitan mitigar riesgos, responder con oportunidad y recuperar la operación de los sistemas informáticos de forma ordenada, segura y eficaz.
El presente procedimiento de Recuperación ante Desastres y Continuidad de Operaciones Informáticas, tiene como finalidad establecer un marco preventivo y reactivo que permita salvaguardar los recursos tecnológicos críticos, asegurar la disponibilidad de la información, proteger al personal técnico y mantener la operatividad de los servicios esenciales que presta esta Secretaría.

II. Objetivo.

Establecer las disposiciones institucionales para prevenir, responder y recuperar la operación de los sistemas informáticos de la SEMARNATH, en caso de desastres, fallas críticas o eventos que comprometan la continuidad operativa, garantizando la protección de los datos, el hardware, el software, el personal técnico y la infraestructura tecnológica.

III. Alcance.

Este procedimiento es de aplicación obligatoria para todas las áreas administrativas, unidades técnicas y operativas de la SEMARNATH que utilicen, administren o dependan de sistemas informáticos institucionales.

Asimismo, será aplicable no solo ante desastres naturales, ciberataques o eventos de fuerza mayor, sino también en casos individuales de pérdida o daño de hardware, mal uso, omisión de respaldo o cualquier situación que implique riesgo o afectación a la integridad, disponibilidad o confidencialidad de la información institucional.

IV. Fundamento legal.

1. Reglamento para el Uso y Aprovechamiento de Tecnologías de Información y Comunicaciones en el Poder Ejecutivo.
2. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público del Estado de Hidalgo.
3. Ley General de Responsabilidades Administrativas

4. Reglamento Interno de la SEMARNATH
5. Manual de Procedimientos.

V. Principios Rectores.

1. Disponibilidad: Asegurar que los sistemas críticos estén disponibles dentro del tiempo mínimo aceptable tras una interrupción.
2. Resiliencia: Diseñar la operación informática con capacidad de recuperación ante incidentes.
3. Responsabilidad compartida: Involucrar a cada unidad responsable en la gestión de sus sistemas y datos.
4. Mejora continua: Evaluar y actualizar periódicamente los planes de continuidad y recuperación.

VI. Componentes del Plan.

A. Recursos Críticos

- **Hardware:** servidores, equipos de comunicación, estaciones de trabajo esenciales.
- **Software:** sistemas institucionales, licencias, aplicaciones de respaldo.
- **Datos:** información clasificada como crítica operativa o estratégica.
- **Infraestructura:** centro de datos, cuartos de servidores, puntos de acceso remotos.

B. Personal

- Identificación de personal técnico clave.
- Asignación de responsables por sistema.
- Suplentes designados y protocolos de activación.

C. Procedimientos

- Plan de Recuperación ante desastres (DRP).
- Plan de continuidad operativa (BCP).
- Protocolos de respaldo y restauración

- Bitácoras y reportes de incidentes

Plan de Recuperación ante desastres (DRP).

Aplicación inmediata ante un evento que interrumpe los sistemas informáticos críticos.

Objetivo: Reestablecer los sistemas y servicios informáticos de forma controlada y segura tras una interrupción crítica o desastre.

No	Actividad	Responsable	Tiempo Estimado	Evidencia
1	Detectar y reportar el incidente (falla, intrusión, desastre natural etc.)	Usuario o primer respondiente.	Inmediato	Registro de incidente.
2	Comunicar a la Subdirección Adjunta de Sistemas y Tecnologías de la Información	Director de Área.	10 min.	Notificación interna.
3	Aislar sistemas afectados para evitar propagación de daños.	Departamento de Soporte Tecnológico y Operativo.	15 min.	Bitácora de incidencias.
4	Evaluar daño y definir plan de recuperación (infraestructura, conectividad).	Subdirección Adjunta de Sistemas y Tecnologías de la Información	1 hr.	Informe técnico.
5	Ejecutar Plan de Acción.	Subdirección Adjunta de Sistemas y Tecnologías de la Información	2-6 hrs.	Bitácora de incidencias
6	Validar funcionamiento del sistema.	Subdirección Adjunta de Sistemas y Tecnologías de la Información	30 min.	Bitácora de incidencias
7	Notificar reanudación de operaciones.	Subdirección Adjunta de Sistemas y Tecnologías de la Información	10 min.	Comunicado interno.
8	Documentar acciones correctivas.	Subdirección Adjunta de Sistemas y Tecnologías de la Información.	2 días hábiles	Informe post-incidente.

Plan de continuidad operativa (BCP).

Aplicable cuando se requiere mantener los servicios en marcha durante una interrupción prolongada.

Objetivo: Asegurar la prestación de servicios informáticos esenciales mediante mecanismos alternativos ante una interrupción operativa prolongada.

No	Actividad	Responsable	Tiempo Estimado	Evidencia
1	Identificar sistemas afectados.	Subdirección Adjunta de Sistemas y Tecnologías de la Información	30 min.	Registro de incidente
2	Notificar a usuarios y activar plan de continuidad.	Subdirección Adjunta de Sistemas y Tecnologías de la Información	15 min.	Comunicado
3	Ejecutar Plan de Acción con medios alternativos (uso de equipos locales, respaldos en nube o dispositivos extraíbles).	Subdirección Adjunta de Sistemas y Tecnologías de la Información	1-4 hrs.	Bitácora de incidencias
4	Establecer rutas alternas de atención a usuarios (correo, drive, forms).	Coordinación Administrativa/Enlaces de Unidades Administrativas.	Según área.	Bitácora de incidencias
6	Evaluar condiciones para reanudación total.	Coordinación Administrativa/ Subdirección Adjunta de Sistemas y Tecnologías de la Información.	Diario.	Acta o minuta de trabajo
7	Reincorporar servicios a operación normal.	Subdirección Adjunta de Sistemas y Tecnologías de la Información.	Según evaluación.	Informe de cierre

Protocolos de respaldo y restauración.

Objetivo: Garantizar la protección y disponibilidad de la información crítica mediante procedimientos estructurados para realizar respaldos periódicos y restaurar datos en caso de pérdida, daño, corrupción o eventos de desastre.

Aplica a todos los sistemas informáticos institucionales que resguarden información operativa, administrativa, financiera, técnica o legal que sea esencial para el funcionamiento de la SEMARNATH.

Protocolo de respaldo

No	Actividad	Responsable	Tiempo Estimado	Evidencia
1	Identificar sistemas y bases de datos críticos a respaldar.	Subdirección Adjunta de Sistemas y Tecnologías de la Información. / Enlaces de Unidades Administrativas.	Quincenal	Lista de sistemas críticos.
3	Verificar integridad del respaldo (pruebas)	Jefe de Departamento de Soporte Tecnológico y Operativo.	Semanal	Bitácora de respaldos.
4	Almacenar respaldos en sitio seguro (servidor local) y fuera de sitio (nube u otra sede) y dispositivos extraíbles (Disco duro externo y USB)	Jefe de Departamento de Soporte Tecnológico y Operativo.	Semanal	Bitácora de respaldos.
5	Registrar cada respaldo con servidor, fecha, hora, usuario y observaciones.	Jefe de Departamento de Soporte Tecnológico y Operativo.	Semanal	Bitácora de respaldos.

Medidas de Seguridad:

- Solo personal autorizado podrá acceder a los repositorios.
- Los dispositivos físicos deben estar protegidos contra incendios, humedad y robos.

Protocolo de restauración

No	Actividad	Responsable	Tiempo Estimado	Evidencia
1	Detectar incidente de pérdida de datos.	Usuario/ Departamento de Soporte Tecnológico y Operativo.	Inmediato	Reporte de incidente
2	Notificar al área de Sistemas y Tecnologías de la Información para activación de protocolo.	Director de Área.	10 min.	Ticket.
3	Verificar el tipo de información afectada.	Departamento de Soporte Tecnológico y Operativo.	30 min.	Informe técnico.
4	Ejecutar restauración desde respaldo seguro.	Departamento de Soporte Tecnológico y Operativo.	1-4 hrs.	Log de restauración.
5	Validar funcionalidad e integridad post-restauración.	Subdirector Adjunto de Sistemas y Tecnologías de la Información/ Usuario final.	1 hr.	Lista de verificación
6	Documentar el incidente, acciones correctivas.	Departamento de Soporte Tecnológico y Operativo.	24-48 hrs.	Informe post-evento.

VII. Responsabilidades.

Subdirección Adjunta de Sistemas y Tecnologías de la Información:

- Coordinar y ejecutar los planes de recuperación y continuidad.
- Mantener actualizados los inventarios y respaldos.
- Capacitar al personal clave.

Usuarios/as de los equipos

- Realizar respaldos periódicos de la información institucional contenida en sus equipos, conforme a los establecido en el Manual de las Tecnologías de la Información.
- Guardar los respaldos en los medios autorizados y en ubicaciones seguras.
- En caso de no haber efectuado respaldo previo y presentarse una falla física o lógica del equipo (por ejemplo, daño en disco duro), se entenderá que la **recuperación de información no podrá ser garantizada**, dicha situación **no será atribuible al área técnica.**
- Notificar oportunamente a la Subdirección Adjunta de Sistemas y Tecnologías de la Información de cualquier incidente relacionado con pérdida o riesgo de pérdida de la información.

Titulares de áreas:

- Identificar procesos críticos
- Facilitar información técnica para los planes.
- Aplicar la política en su área.

VIII. Fundamento legal y atribuciones para la validación.

Con fundamento en lo dispuesto por los artículos 1, 2 y 4 de la **Ley Orgánica de la Administración Pública del Estado de Hidalgo**, que facultan a las dependencias del Poder Ejecutivo para ejercer sus funciones conforme a su Reglamento Interior; así como en el **Reglamento Interior de la Secretaría de Medio Ambiente y Recursos Naturales de Hidalgo**, en su Capítulo VI, Sección I, artículo 18, fracciones X, XI y XV, que otorgan atribuciones al Área Administrativa para coordinar y supervisar la gestión institucional, y a la Dirección de Administración y Finanzas para la administración de los recursos humanos y materiales de la dependencia.

Asimismo, de conformidad con lo establecido en el **Acuerdo por el que se emiten las Disposiciones y el Manual Administrativo de Aplicación Estatal en Materia de Control Interno del Estado de Hidalgo**, específicamente en su Título II, Capítulo I, numeral 9, **TERCERA. ACTIVIDADES DE CONTROL**, Principio 12.02 la Administración debe documentar mediante políticas para cada unidad su responsabilidad sobre el cumplimiento de los objetivos de los

procesos, de sus riesgos asociados, del diseño de actividades de control, de la implementación de los controles y de su eficacia operativa y Principio 12.03 el personal de las unidades que ocupa puestos clave puede definir con mayor amplitud las políticas a través de los procedimientos del día a día, dependiendo de la frecuencia del cambio en el entorno operativo y la complejidad del proceso operativo.

Así como, lo previsto en los artículos 1, 3, 4, 5, 7, 11, 12 y 27 del **Código de Ética de la Administración Pública del Estado de Hidalgo**, y el Capítulo II del **Código de Conducta de la Secretaría de Medio Ambiente y Recursos Naturales de Hidalgo**, que obligan a los servidores públicos a actuar conforme a principios de integridad, responsabilidad, legalidad y eficiencia en el ejercicio de sus funciones.

Por lo anterior, las personas que suscriben este documento cuentan con las atribuciones legales y administrativas para su elaboración, revisión y autorización en el marco del **Procedimiento de Recuperación ante Desastres y Continuidad de Operaciones Informáticas.**

Fecha de validación: 28 de mayo de 2025.

Tabla de Actualizaciones

No	Fecha	Observación
1	28 de mayo de 2025	Validación inicial.

Autorizó

L.C. Claudia González Pérez
Coordinadora Administrativa

Revisó

LSC. David Ibarra Vite
Subdirector Adjunto de Sistemas y Tecnologías de la

Información.

Elaboró

Lic. Omar Romero Monroy
Jefe de Departamento de Soporte Tecnológico y Operativo.