IHCIETI
Instituto Hondureño de Ciencia,
Tecnología y la Innovación

HONDURAS

# INSTITUTO HONDUREÑO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN (IHCIETI)

# TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES

---

# PLAN DE CONTIGENCIAS Y RECUPERACIÓN DE DESASTRES

## FECHA

## MAYO ,2025

IHCIETI
Instituto Hondureño de Ciencia, Tecnología y la Innovación

HONDURAS

## Contenido

# 1. INTRODUCCIÓN

El presente **Plan de Contingencias y Recuperación de Desastres** del Instituto Hondureño de Ciencia, Tecnología e Innovación (IHCIETI) tiene como objetivo fundamental establecer un conjunto de directrices, procedimientos y estrategias orientadas a garantizar la disponibilidad, integridad y continuidad de los servicios tecnológicos institucionales, ante la ocurrencia de eventos imprevistos que afecten la infraestructura de Tecnologías de la Información y las Comunicaciones (TIC).

La creciente dependencia institucional de sistemas tecnológicos para el desarrollo de funciones administrativas, académicas, operativas y estratégicas impone la necesidad de contar con mecanismos efectivos de respuesta ante interrupciones no planificadas. Estas interrupciones pueden derivarse de una amplia gama de amenazas, tales como fallas de hardware o software, errores humanos, ciberataques, cortes eléctricos, desastres naturales, entre otros. Cualquiera de estos eventos puede comprometer la continuidad de los servicios esenciales como la página web institucional, biblioteca virtual, cuentas de correo, plataforma administrativa, red de internet o servidores locales.

## 2. OBJETIVO GENERAL

El presente Plan tiene como objetivo general **establecer un conjunto de lineamientos estratégicos, procedimientos técnicos y acciones organizativas orientadas a prevenir, responder y recuperar de forma eficaz los servicios tecnológicos críticos del IHCIETI**, en situaciones de emergencia o interrupciones inesperadas. La finalidad es minimizar el impacto operativo, administrativo, académico y reputacional que pudiera derivarse de una eventual falla en los sistemas informáticos o tecnológicos.

Este objetivo se enmarca en el compromiso institucional con la gestión responsable de la infraestructura tecnológica, reconociendo que la continuidad operativa depende en gran medida de la disponibilidad y resiliencia de los servicios TIC. A través de este plan, se busca fortalecer la capacidad del IHCIETI para actuar con rapidez y precisión frente a situaciones adversas, reduciendo al máximo los tiempos de inactividad, protegiendo los activos digitales y asegurando la calidad del servicio a todos los usuarios.

Asimismo, el objetivo general promueve una cultura organizacional orientada a la preparación y la anticipación, donde cada miembro del equipo técnico comprenda su rol en un escenario de contingencia, y donde los procesos de recuperación no dependan de la improvisación, sino de una planificación sistemática y validada.

# 3. OBJETIVOS ESPECÍFICOS

1. **Identificar los riesgos tecnológicos que podrían causar interrupciones.** Se llevará a cabo una evaluación continua de las amenazas internas y externas que puedan comprometer la operatividad de los sistemas tecnológicos del IHCIETI. Esta identificación contempla desde fallos de hardware y software hasta ataques cibernéticos, desastres naturales, sabotajes o errores humanos. El análisis de riesgos permitirá priorizar las áreas más vulnerables y definir medidas de protección eficaces.

2. **Establecer mecanismos de prevención y mitigación de riesgos.** Se implementarán estrategias técnicas y administrativas orientadas a reducir la probabilidad de ocurrencia de incidentes y su impacto. Estas estrategias incluyen copias de seguridad periódicas, redundancia de equipos, monitoreo de sistemas, actualizaciones constantes de seguridad, protocolos de respuesta rápida, y mantenimiento preventivo de la infraestructura tecnológica.

3. **Definir responsabilidades y procedimientos en caso de contingencias.** Se documentará de manera clara el papel que desempeñan el jefe de TIC, Programador de TIC y Auxiliar de TIC, demás actores involucrados durante una emergencia tecnológica. Igualmente, se establecerán los pasos a seguir desde la detección del incidente hasta la completa recuperación de los servicios, asegurando una respuesta coordinada, eficiente y libre de improvisaciones.

4. **Coordinar acciones para la recuperación ordenada de los servicios TIC.** Este objetivo busca garantizar que, una vez superada la fase crítica del incidente, se ejecuten acciones que permitan restaurar la funcionalidad de los sistemas de manera progresiva, segura y validada. La recuperación ordenada contempla tanto la restauración técnica como la verificación funcional y la comunicación efectiva a los usuarios sobre la normalización de los servicios.

## 4. ALCANCE DEL PLAN

Este plan aplica a todos los sistemas tecnológicos del IHCIETI, incluyendo:

- Página web institucional
- Biblioteca virtual
- Cuenta de correos institucional
- Servidor local en físico
- Red de internet
- Plataforma administrativa interna
- Plataforma Moodle

## 5. IDENTIFICACIÓN DE RIESGOS POTENCIALES

- Fallas eléctricas o en UPS
- Fallos en servidores físicos o virtuales
- Ataques cibernéticos (ransomware, phishing, DDoS)
- Eliminación o corrupción de datos
- Incendios, inundaciones o desastres naturales
- Errores humanos críticos
- Caídas en la red de internet

## 6. CLASIFICACIÓN DE SISTEMAS CRÍTICOS

| SISTEMA/SERVICIO | NIVEL DE CRITICIDAD |
|---|---|
| Página web institucional | Medio |
| Biblioteca virtual | Medio |
| Servidor de correos institucional | Alto |
| Servidor local físico | Crítico |
| Red de internet | Crítico |
| Plataforma Moodle | Medio |
| Plataforma Administrativa Externa | Medio |

# 7. ESTRATEGIAS DE PREVENCIÓN Y CONTENCIÓN

## 7.1. Políticas de respaldo

- Copias de seguridad diarias en unidades externas y nubes privadas.
- Verificación y prueba de respaldo mensual.

## 7.2. Redundancia

- Conexión a red secundaria ante fallos en el proveedor principal.
- Doble suministro de energía con UPS y planta eléctrica.

## 7.3. Seguridad informática

- Antivirus Kaspersky actualizado.
- Firewall activo y monitoreo continuo.

## 7.4. Capacitación del personal

- Simulacros anuales de recuperación.
- Respuesta rápida para todo el equipo TIC.

# 8. ACTIVACIÓN DEL PLAN

## 8.1. Detección y evaluación

Se identifica la naturaleza del evento, su impacto y se clasifica según su gravedad.

## 8.2. Clasificación

- Nivel 1: Impacto leve, no requiere activación total.
- Nivel 2: Impacto medio, activación parcial del plan.
- Nivel 3: Impacto crítico, activación completa del PCRD.

## 8.3. Notificación

Se notifica a la Dirección Ejecutiva.

# 9. PROCEDIMIENTO DE RECUPERACIÓN

1. Activación del sitio alterno o respaldo local.
2. Restauración de servicios desde copias de seguridad.
3. Validación de integridad y funcionalidad de sistemas.
4. Comunicación con los usuarios sobre la reactivación.
5. Documentación del evento y acciones tomadas.

# 10. ROLES Y RESPONSABILIDADES

| ROL | Función |
|---|---|
| Jefe de TIC | Lidera y coordina la ejecución del PCRD, comunica con la Dirección. Administra servidores y redes, ejecuta procedimientos de restauración. |
| Programador de TIC | Recupera plataformas digitales, da soporte web y soluciona errores. |
| Auxiliar de TIC | Asiste en tareas operativas, soporte básico y documentación técnica. |
| Proveedores Externos | Brindan soporte técnico y garantía de continuidad de servicios. |

# 11. COMUNICACIÓN DURANTE LA CONTINGENCIA

Se utilizarán medios alternos como:

- Llamadas directas a celulares del equipo TIC.
- Aplicaciones de mensajería instantánea (ej. WhatsApp).
- Correos personales si el correo institucional no está disponible.

El Jefe de TIC será el vocero oficial ante la Dirección Ejecutiva y la comunidad institucional.

# 12. EVALUACIÓN POST-INCIDENTE

Tras superar el incidente:

- Se convoca una reunión de análisis con todos los involucrados.
- Se documentan causas, consecuencias y acciones tomadas.
- Se generan recomendaciones para mejorar procesos y sistemas.

# 13. MANTENIMIENTO Y ACTUALIZACIÓN DEL PLAN

- Este plan será revisado anualmente o luego de un incidente.
- Las actualizaciones serán responsabilidad del Jefe de TIC.
- Se realizarán simulacros cada 12 meses y auditorías técnicas cada 6 meses.

El mantenimiento y la actualización del presente **Plan de Contingencias y Recuperación de Desastres (PCRD)** son elementos fundamentales para asegurar su efectividad, vigencia y alineación con las condiciones reales del entorno tecnológico y operativo del IHCIETI. Un plan desactualizado o desatendido puede generar una falsa sensación de preparación y poner en riesgo la capacidad de respuesta de la institución ante situaciones críticas.

De igual forma, se realizarán **auditorías técnicas internas cada seis (6) meses**, en las que se revisarán elementos clave como:

- La existencia y calidad de los respaldos de información.
- El estado de los sistemas de alimentación eléctrica (UPS, generadores).
- La configuración y seguridad de los servidores físicos y virtuales.
- El cumplimiento de los procedimientos de monitoreo y prevención.
- La disponibilidad y vigencia de la documentación de soporte.

# 14. CONCLUSIÓN

El presente **Plan de Contingencias y Recuperación de Desastres (PCRD)** representa un instrumento estratégico esencial para la preservación de la continuidad operativa del IHCIETI ante eventos que puedan comprometer la disponibilidad, integridad o confidencialidad de los sistemas tecnológicos institucionales.

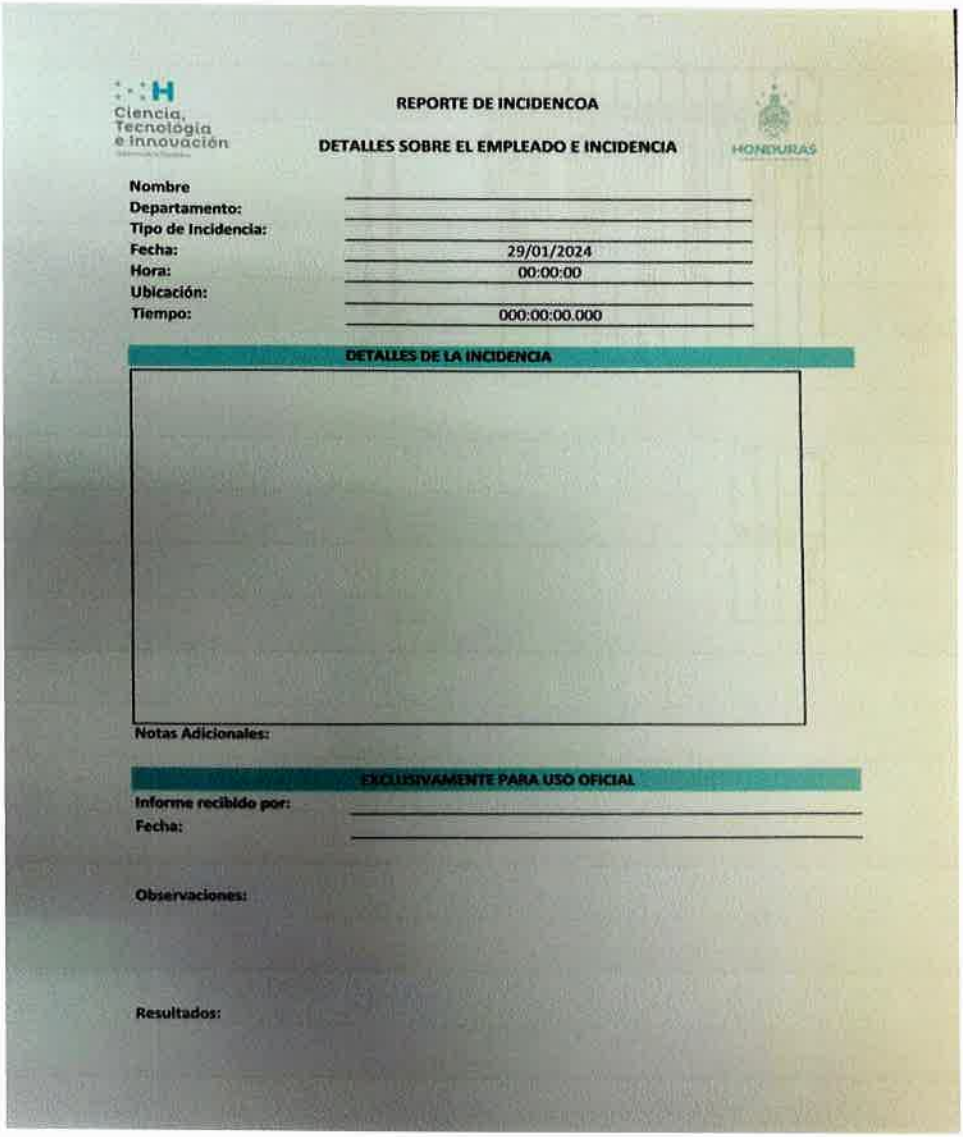
Dado que las plataformas digitales y los servicios TIC —como la página web institucional, la biblioteca virtual, el servidor local, la red de internet, las cuentas de correo institucional y los sistemas administrativos— constituyen pilares fundamentales en el desarrollo de las funciones académicas, administrativas y técnicas, se hace indispensable contar con una respuesta estructurada y eficaz ante situaciones de emergencia.

Este plan no solo define un marco de actuación claro para mitigar riesgos y garantizar la recuperación oportuna de los servicios críticos, sino que también promueve una cultura de prevención, responsabilidad y mejora continua dentro del equipo TIC. La participación del **Jefe de TIC**, el **Programador**, el **Auxiliar** y demás personal asignado será clave para su aplicación exitosa, así como para la protección de los activos informáticos y el cumplimiento de los objetivos institucionales.

Finalmente, es importante resaltar que este documento es dinámico y deberá ser revisado, probado y actualizado de manera regular, incorporando aprendizajes derivados de simulacros y experiencias reales. Solo a través de una gestión proactiva y comprometida será posible fortalecer la resiliencia tecnológica del IHCIETI y garantizar la confianza de sus usuarios y aliados estratégicos frente a cualquier adversidad.

# 15. ANEXOS

1.0 Formato de incidencia



Ciencia, Tecnología e Innovación

**REPORTE DE INCIDENCOA**

**DETALLES SOBRE EL EMPLEADO E INCIDENCIA**

HONDURAS

**Nombre**
**Departamento:**
**Tipo de Incidencia:**
**Fecha:** 29/01/2024
**Hora:** 00:00:00
**Ubicación:**
**Tiempo:** 000:00:00.000

**DETALLES DE LA INCIDENCIA**

**Notas Adicionales:**

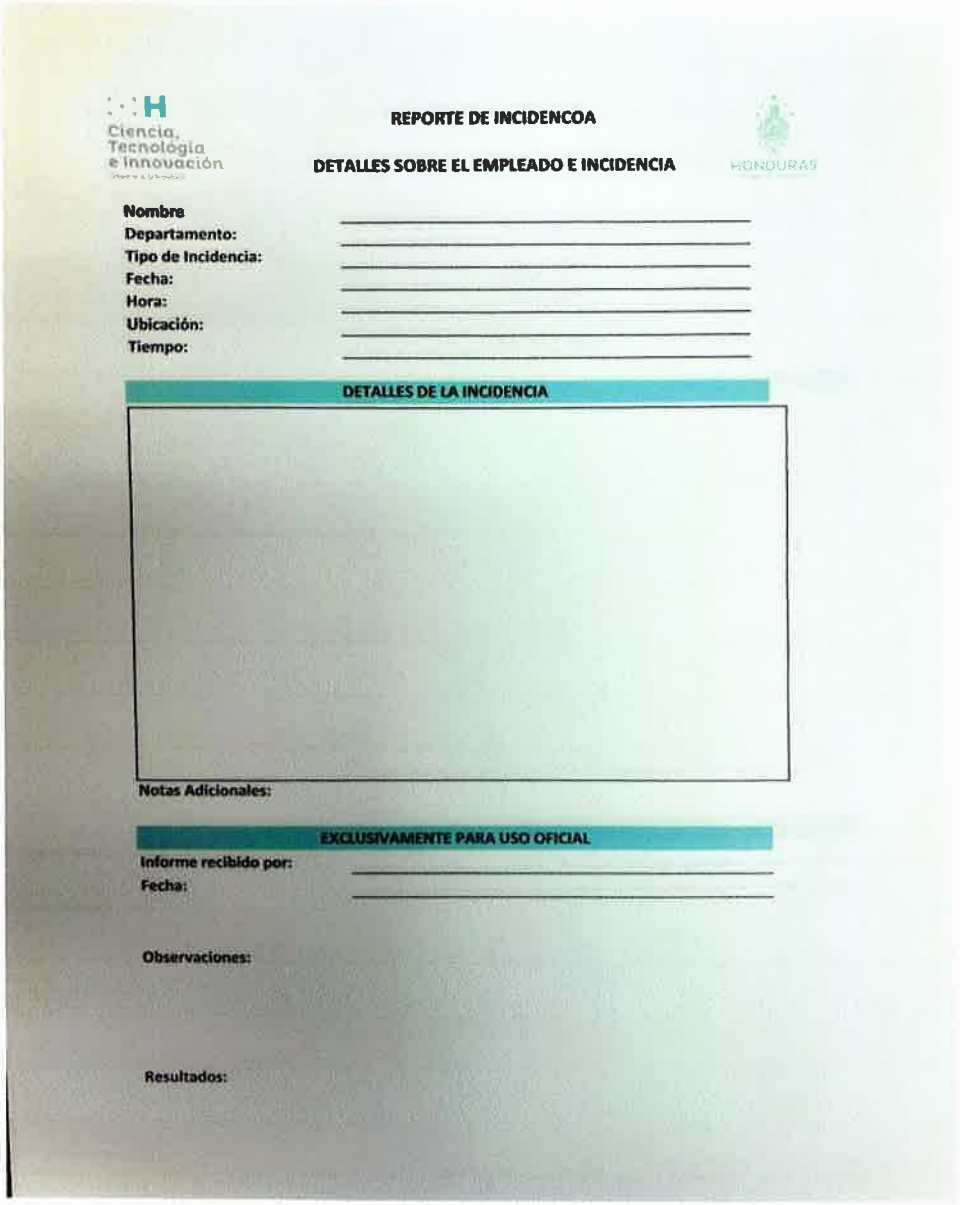
**EXCLUSIVAMENTE PARA USO OFICIAL**

**Informe recibido por:**
**Fecha:**

**Observaciones:**

**Resultados:**

1.1 Formato de incidencia



Ciencia, Tecnología e Innovación

**REPORTE DE INCIDENCOA**

**DETALLES SOBRE EL EMPLEADO E INCIDENCIA**

HONDURAS

**Nombre** _____
**Departamento:** _____
**Tipo de Incidencia:** _____
**Fecha:** _____
**Hora:** _____
**Ubicación:** _____
**Tiempo:** _____

**DETALLES DE LA INCIDENCIA**

**Notas Adicionales:**

**EXCLUSIVAMENTE PARA USO OFICIAL**

**Informe recibido por:** _____
**Fecha:** _____

**Observaciones:**

**Resultados:**

1.3 Departamentos IHCIETI

| # | Departamentos |
|---|---|
| 1 | Dirección |
| 2 | Sub-Dirección |
| 3 | RRHH |
| 4 | INFOTEC |
| 5 | FORMACIÓN ACADÉMICA |
| 6 | ICDT |
| 7 | COOPORACIÓN INTERNACIONAL |
| 8 | PLANIFICACIÓN |
| 9 | BIENES NACIONALES |
| 10 | SERVICIOS GENERALES |
| 11 | LEGAL |
| 12 | COMUNICACIÓN |
| 13 | TALLERES Y LABORATORIOS |
| 14 | OTROS (AGG) |

| # | Tiempo |
|---|---|
| 1 | H |
| 2 | m |
| 3 | s |

Elaborado por: Marcial Casildo

19/5/2025

Aprobado por: Luther Castillo

20/5/2025

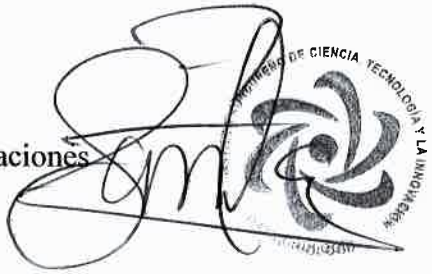
Ciencia,
Tecnología
e Innovación

# MEMORANDO

**IT-045--2025**

Para: **Lic. Regis Hernández**
Coordinador de Planificación Estratégicas

De: **Ing. Santos Marcial Casildo**
Jefe de Tecnología de la Información y las Comunicaciones




FECHA: 20 de mayo del 2025

Asunto: **Remisión de Plan de Contingencias**

Por medio de la presente, me permito remitir el plan de contingencias y recuperación de desastres en cumplimiento al plan anual de marco rector institucional.

**Nota:** Se adjunta el documento en físico

Tegucigalpa, Honduras
Teléfono 2235-9193