# Procedimientos y políticas en caso de desastre

Es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que El Independiente de Hidalgo pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

A continuación se presenta la propuesta de procedimientos y políticas y procedimientos para en caso de desastres para aplicar en El Independiente de Hidalgo

## OBJETIVOS GENERALES Y ESPECÍFICOS

### Generales:

Garantizar la continuidad de las actividades del EL INDEPENDIENTE DE HIDALGO, ante eventos que podrían alterar el normal funcionamiento de la Tecnología de la Información y Comunicaciones - TICs, a fin de minimizar el riesgo no previsible, críticos o de emergencia, y responder de forma inmediata hacia la recuperación de las actividades normales.

Específicos:

* Contar con documentación práctica y actualizada que garantice al EL INDEPENDIENTE DE HIDALGO la continuidad de las operaciones de los sistemas informáticos sin sufrir paralizaciones o pérdidas relevantes.
* Identificar y analizar riesgos posibles que pueden afectar las operaciones y procesos informáticos de la institución.
* Establecer las estrategias adecuadas para asegurar la continuidad de los servicios informáticos en caso de interrupción y que ésta no exceda las 24 horas.
* Contar con personal debidamente capacitada y organizada para afrontar adecuadamente las contingencias que puedan presentarse en las actividades del EL INDEPENDIENTE DE HIDALGO.

## ALCANCE

La Implementación del Plan de Contingencia informático, incluye los elementos referidos a los sistemas de información, equipos, infraestructura, personal, servicios y otros, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la institución.

### Acciones a ser consideradas:

* **Antes**, como un plan de respaldo o de prevención para mitigar los incidentes.
* **Durante**, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
* **Después**, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

El Plan de Contingencia permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna.

El término “incidente” en este contexto será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático en el EL INDEPENDIENTE DE HIDALGO.

## Plan de Prevención

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en los factores identificados en el presente plan.

El plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

## Plan de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente de contingencia y que activa un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible.

Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

Plan de Recuperación Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

Todo Plan de Contingencia informático debe tener un carácter recursivo que permita retroalimentar y mejorar continuamente los planes en cada una de las etapas descritas, logrando así tener un documento dinámico.

## Plan de Pruebas

El Plan de Pruebas, será presentado a la Dirección Ejecutiva del EL INDEPENDIENTE DE HIDALGO para su aprobación previa a su implementación. El resultado de las pruebas efectuadas será presentado igualmente para su conformidad.

Las pruebas relacionadas a este plan, se ejecutaría semestralmente, mes de Junio y Diciembre con el fin de evaluar la preparación de la organización ante la ocurrencia de un siniestro y realizar los ajustes necesarios.

## METODOLOGÍA

La presente metodología es el resultado de la experiencia práctica de EL INDEPENDIENTE DE HIDALGO en la implementación de planes de contingencia, mitigación de riesgos y seguridad, también en base a experiencias en otras instituciones, lo cual garantiza que el documento final sea necesariamente objetivo y práctico, a fin de contar con una herramienta efectiva en caso de una contingencia real.

Para elaborar el Plan de Contingencia se seguirá una metodología que tiene las siguientes fases:

* Fase 1: Organización
* Fase 2: Identificación y priorización de riesgos
* Fase 3: Definición de eventos susceptibles de contingencia
* Fase 4: Elaboración del Plan de Contingencia 6
* Fase 5: Definición y Ejecución del Plan de Pruebas
* Fase 6: Implementación del Plan de Contingencia

Fases de la metodología propuesta:

## Organización del Plan de Contingencia

Uno de los aspectos que evidencia un carácter formal y serio en toda organización es que ésta se encuentre siempre preparada para afrontar cualquier evento de contingencia o dificultades en general y que le permitan poder superarlos por lo menos de manera transitoria mientras dure dicho evento.

Es necesario entonces que la definición de un Plan de Contingencia informático deba hacerse de manera formal y responsable de tal forma que involucre en mayor o menor medida a toda la organización en el Plan de Prevención, Ejecución y Recuperación, pero definiendo un grupo responsable para su elaboración, validación y mantenimiento.

## Identificación y Priorización de Riesgos

Denominamos INCIDENCIA al hecho que se pueda presentar en cualquier momento, bajo una probabilidad de ocurrencia.

## Elaboración de los Planes de Contingencia

Una de las fases importantes del Plan de Contingencia es la documentación y revisión de la información que se plasmará en una guía práctica y de claro entendimiento por el personal del EL INDEPENDIENTE DE HIDALGO.

Es por ello, que una fase importante de la metodología considera un formato estándar de registro de todos los eventos definidos que forman parte del plan, así se tendrá finalmente un entregable acorde con los requerimientos y políticas definidas para tal fin.

## Definición y ejecución del plan de pruebas

Conscientes que una situación de contingencia extrema puede presentarse en cualquier momento, y por ende convertirse en un problema prioritario de atender si éste se produjera en el horario de oficina que pueda resultar impactante durante las actividades del EL INDEPENDIENTE DE HIDALGO; es que se hace necesario definir de manera específica todas las acciones necesarias para asegurar que, en caso real de contingencia y tener un conjunto de prestaciones y funcionalidades mínimas que permitan posteriormente ejecutar el plan de recuperación de manera rápida y segura

## Implementación del Plan de Contingencia

La implementación del presente plan se realizará en el segundo mes de su aprobación.

## DESARROLLO DE LAS FASES, ACTIVIDADES, ESTRATÉGIAS, PROGRAMAS Y POLÍTICAS

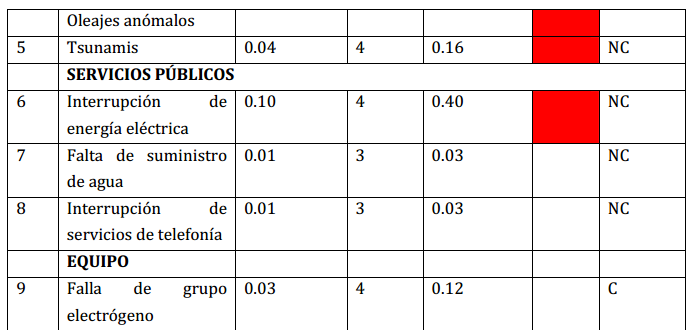
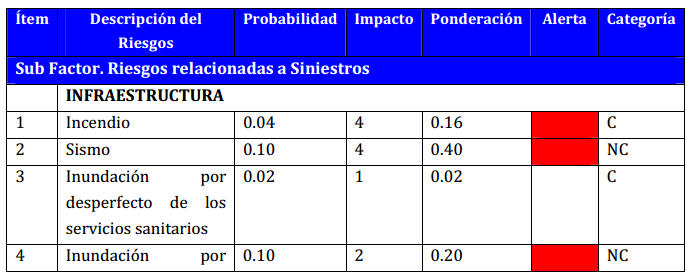
Como parte del presente capítulo, la Unidad de Informática, plantea el desarrollo de los tópicos, utilizando la metodología expuesta anteriormente. Este desarrollo incluirá las siguientes fases de la metodología

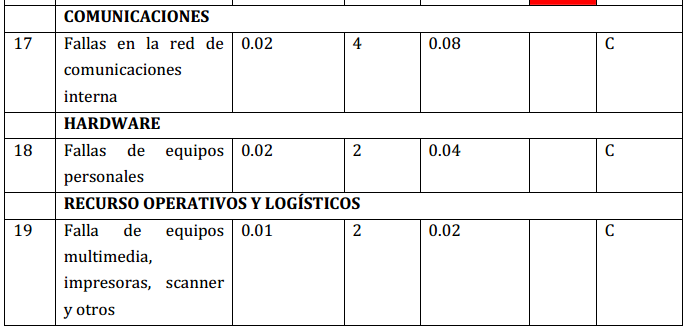
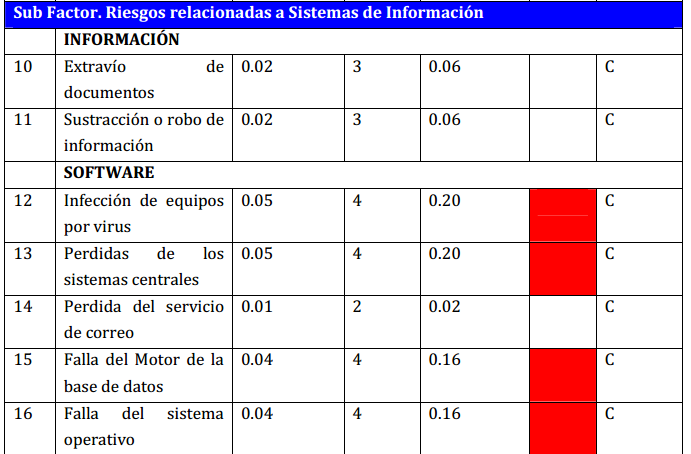
* Identificación y Priorización de riesgos
* Definición de Eventos susceptibles de Contingencia.
* Elaboración del Plan de Contingencia.

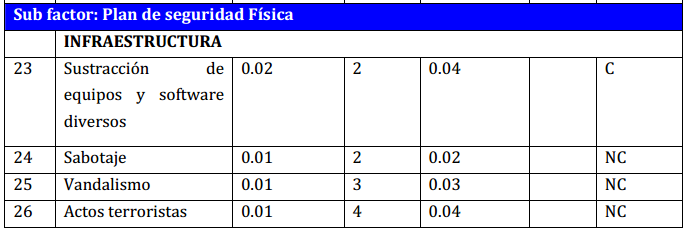
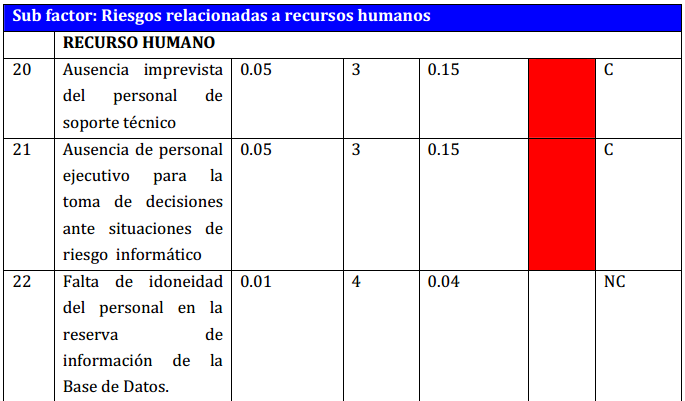
### Identificación y Priorización de Riesgos

El cuadro N °4 muestra la matriz de Riesgo de Contingencia, ponderado de acuerdo a los valores de riesgo e impacto en el servicio (operatividad), usando el conocimiento y la experiencia práctica de Informática en Gestión de Sistemas de Información:

Cuadro N °4: Matriz de Riesgo de Contingencia





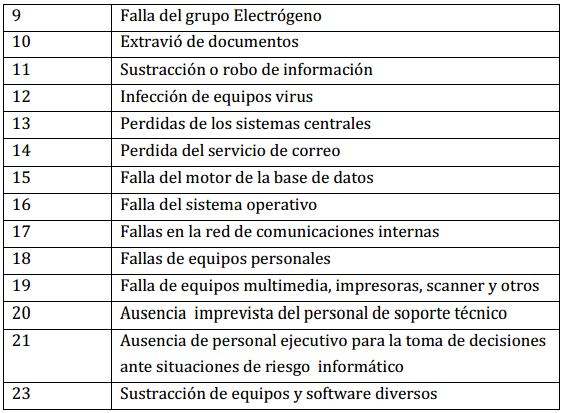
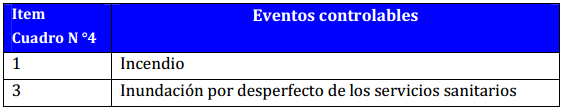


Nota: El color rojo de la alerta representa que el evento es altamente impactante en el servicio por lo tanto debe ser obligatoriamente controlado.

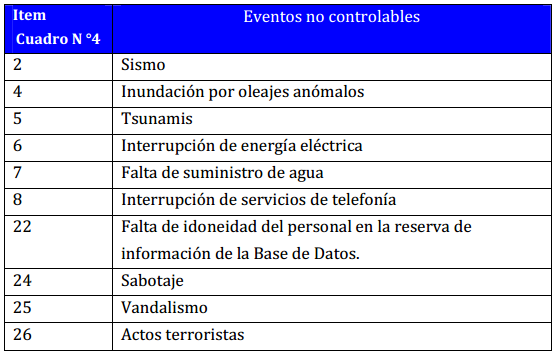
En la columna CATEGORÍA por cada evento, se considera la identificación de aquellos eventos Controlables (C), y No Controlables (NC).

En los cuadros N° 5 y N° 6 se resumen los eventos según la categorización de eventos controlables y no controlables:

Cuadro N °5: Eventos Controlables



Cuadro N °6: Eventos no Controlables



Hackeo