**INVESTIGACION:**

**METRICA**: Una métrica es una medida efectuada sobre los programas, documentación, su desarrollo y mantenimiento, o sobre algún aspecto del sistema en desarrollo.

No es un objetivo en si mismo sino un medio para controlar el desarrollo de un sistema de software.

Procesos principales:   
*Planificación de Sistemas de Información*.   
*Desarrollo de Sistemas de Información*.   
*Mantenimiento de Sistemas de Información*.

**DOCUMENTACION – SOPORTE DE LAS PRUEBAS DEL SOFTWARE:**

Son los procesos que permiten verificar y revelar la calidad de un producto software. Son utilizadas para identificar posibles fallos de implementación, calidad, o [usabilidad](http://es.wikipedia.org/wiki/Usabilidad) de un programa de ordenador o [videojuego](http://es.wikipedia.org/wiki/Videojuego). Básicamente es una fase en el desarrollo de [software](http://es.wikipedia.org/wiki/Software) consistente en probar las aplicaciones construidas.

La prueba de software involucra las operaciones del sistema bajo condiciones Controladas y evaluando los resultados. Las condiciones controladas pueden ser normales o anormales. La prueba puede intencionalmente esforzar al programa y producir errores en las respuestas para determinar si los sucesos ocurren cuando no tendrían que ocurrir o cuando los hechos no suceden cuando deberían suceder. La prueba de software esta detectada a la detección. La mayoría de las grandes organizaciones asumen la responsabilidad del control de calidad y prueba de software a tal medida que en la producción se incluyen desarrolladores de sistemas (analistas , programadores) y un grupo dedicado a la prueba de software para que estos grupos antes mencionados trabajen en conjunto cumpliendo el control de calidad (prevención) y la prueba de software (detección) logrando una tarea exitosa*.*

**Pasos para el desarrollo de pruebas:**

* Obtener los requerimientos en forma clara.
* Obtener planificación de diseño.
* Determinar funcionalidad.
* Identificar aplicaciones de alto riesgo o con prioridad de prueba.
* Determinar métodos de prueba.
* Determinar contexto de la prueba.
* Obtener datos de prueba.
* Estimar tiempo de prueba.
* Clasificar errores del programa.
* Documentar errores del programa.
* Redactar los casos de prueba que encontraron fallas.
* Aprobar una revisión en la prueba.
* Evaluar resultados en reportes.
* Volver a probar si es necesario.
* Actualizar el plan de prueba.

**PLAN DE CONTIGENCIA EN PRUEBAS DEL SOFTWARE**:

Se entiende por PLAN DE CONTINGENCIA los procedimientos alternativos al orden normal de una empresa, cuyo fin es permitir el normal funcionamiento de esta, aún cuando alguna de sus funciones se viese dañada por un accidente interno o externo.  
  
Que una organización prepare sus planes de contingencia, no significa que reconozca la ineficacia de su empresa, sino que supone un avance a la hora de superar cualquier eventualidad que puedan acarrear perdidas o importantes pérdidas y llegado el caso no solo materiales sino personales.

Los Planes de Contingencia se deben hacer de cara a futuros acontecimientos para los que hace falta estar preparado.  
La orientación principal de un plan de contingencia es la **continuidad de las operaciones** de la empresa, no sólo de sus sistemas de información.

Su elaboración la podemos dividir en cuatro etapas:

1. Evaluación.  
   2. Planificación.  
   3. Pruebas de viabilidad.  
   4. Ejecución.  
   5. Recuperación.

En esta área el plan de contingencia forma parte de un documento más amplio donde se tiene en cuenta los planes de mantenimiento, políticas de backups, inventarios, planes de formación, etc.

**Inventario de sistemas**  
Disponer de forma actualizada la situación de la infraestructura de equipos y sistemas, así como aplicaciones instaladas. Es importante para conocer cual era la situación de cada equipo.

**Plan de Mantenimiento**  
Tanto Preventivo como Correctivo. Se trata por un lado de garantizar el correcto funcionamiento de los sistemas, estableciendo un calendario periódico de actuación y por otro lado, el correctivo, en el que se dispone de una guía con los fallos y las acciones a realizar para la pronta disposición del sistema.

**Política de Backups**La política de backups forma parte de la necesidad del dato. Los sistemas podrán ser renovados comprando nuevo material o realizando nuevas instalaciones de software base pero el dato no es recuperable. El conocimiento no es recuperable si se destruye. Por ello una buena política de copias de seguridad garantiza la tranquilidad de la organización.

**Plan de Recuperación ante Desastres o de Contingencia**Aunque el nombre puede variar en función de la severidad en definitiva se trata de recoger las acciones para que en caso de gravedad máxima sea posible la recuperación del funcionamiento.

En cualquier caso y dado que la realización de un plan puede ser tan amplio como la propia organización, es necesario simplificar y focalizar en los puntos más importantes tales como:

**Inventario de Sistemas**Análisis de los riesgos y su clasificación según criticidad  
Elaboración del Sistema de Contingencia,  
Asignación de responsabilidades  
Calendario de implantaciones y puesta en marcha  
Plan de pruebas y simulaciones

**Inventario de Sistemas**

Recoger todo el equipamiento hardware, comunicaciones, arquitectura, software, etc. y su clasificación según áreas o funcionalidad realizada. Muy importante también será la relación existente entre los diferentes equipos, cuales son las dependencias entre ellos y otros sistemas.

Un ejemplo, es el acceso a Internet. Por mucho que exista un hardware de reemplazo, la conexión a Internet no funcionará si no disponemos de una alternativa a las comunicaciones.

**Análisis de Riesgos y clasificación**

En este apartado se identificarán los riesgos y además se realizará la clasificación de las mismas. Es importante destacar que será necesario elegir un criterio de selección ya sea por salvaguarda de la confidencialidad o integridad o disponibilidad.

Después se determinará la frecuencia con que puede ocurrir. Cada cuanto se da el problema.

Toda esta información se analizará decidiendo la clasificación de los riesgos según su trascendencia en la organización.

**Elaboración del Plan de Contingencia**

En este apartado se realizará el citado plan recogiendo las posibles alternativas para solucionar el problema.

Se podría contemplar alternativas tan validas como replicación de centros de proceso de datos en otros edificios, alquiler de CPD, Housing, etc. Se tendrán en cuenta el costo y complejidad técnica como elementos decidores.

También se recogerán las políticas de backups y mantenimientos como parte del informe y determinados según la alternativa seleccionada.

El plan también debe recoger las actuaciones necesarias para la puesta en marcha del sistema alternativo, estableciendo el procedimiento de actuación a seguir para cada tipo de incidencia y cada sistema.

Muy importante indicar la secuencia y responsable de actuación de cada secuencia. Todo el mundo debe conocer perfectamente cual es la acción que debe realizar.

**Asignación de Responsabilidades**

En definitiva delimitar y conocer las personas implicadas y sus responsabilidades en el plan de actuación. Así como suministradores de equipamiento y servicios que puedan aunar conjuntamente esfuerzos. En este caso, disponer de contratos de mantenimiento adecuados con terceras empresas especializadas en Seguridad podría significar una gran diferencia del éxito de la contingencia.  
También se determina como fundamental el Equipo de Crísis con capacidad de decisión y responsabilidad que pueda ser capaz de asumir y redirigir los problemas que se puedan dar durante la crisis.

Calendario de Implantación

Conocer cual es el programa en el tiempo y poder valorar adecuadamente el momento en que se encuentre la puesta en marcha del plan

**Plan de pruebas y simulaciones**

Por último, indicar que un buen plan de contingencia conlleva la realización periódica de pruebas y simulaciones de crisis. Sólo conociendo de antemano que problemas podrían aparecer ante un desastre, el plan de contingencia podrá ser perfeccionado o sustituido y así asegurar el éxito del mismo.

**DOCUMENTACION**

Esta etapa, también de gran valor, consiste en elaborar los manuales de usuario y la ayuda en línea de aplicación. Su finalidad es garantizar el buen usu y fácil manejo del producto por parte de los diferentes usuarios y así poder obtener el mayor rendimiento de la aplicación.  
La documentación incluye los requerimientos de hardware y software de la aplicación para asegurar su buen funcionamiento.

<http://www.abartiateam.com/noticias-tecnologicas/200806_como-elaborar-un-plan-de-contingencia>

SUEGERENCIA DE LECTURA <http://todoenprogramacionelinformatico.blogspot.com/2010/09/prueba-del-plan-de-contingencias.htm>

[www.pol.una.py/archivos/IngeInfo/.../Ingenieria\_**software**\_III.pdf](http://www.pol.una.py/archivos/IngeInfo/.../Ingenieria_software_III.pdf)