

## **Capítulo II**

## Capítulo 2. Confiabilidad y Software

### 2.1 Conceptos Generales

La mayoría de nosotros estamos conscientes de las caídas que los sistemas de cómputo llegan a tener. En algunas ocasiones no podemos conocer el por qué estos sistemas se colapsan y con esto dejan de ofrecernos el servicio que les estamos solicitando; otras veces las operaciones que ejecutamos sobre estos sistemas no son siempre del todo adecuadas o cambian los datos que le estamos administrando. (Sommerville, 2002).

La caída de uno o muchos sistemas que son controlados por software llega a provocar inconveniencias y en algunas ocasiones daños que llegan a ser muy graves. Un sistema crítico es donde esa caída logra crear daños económicos o físicos importantes.

Existen diferentes tipos de sistemas críticos, es decir aquellos sistemas que si llegan a fallar pueden afectar toda la operación que se esta efectuando, este tipo de sistemas se pueden clasificar de la siguiente manera (Sommerville, 2002):

- **Sistemas de seguridad críticos:** Estos se refieren a que si existe algún fallo, se provoca una lesión, pérdida de vida o algún daño al medio ambiente.
- **Sistemas de misión críticos:** Estos sistemas se refieren a que si en algún momento fallan, provocan anomalías en las actividades que se encargan de controlar la misión de un objeto que se encuentra dirigido hacia un punto en específico.

- **Sistemas de negocios críticos:** Estos se refieren a que si fallan en algún momento se desata una caída en los negocios que utilizan dichos sistemas.

Hoy en día, la confiabilidad en un sistema es un concepto básico para que un usuario pueda realizar sus tareas. La mayoría de los sistemas sufren de fallas cuando uno está utilizándolos y no se sabe cuando éstas van a ocurrir.

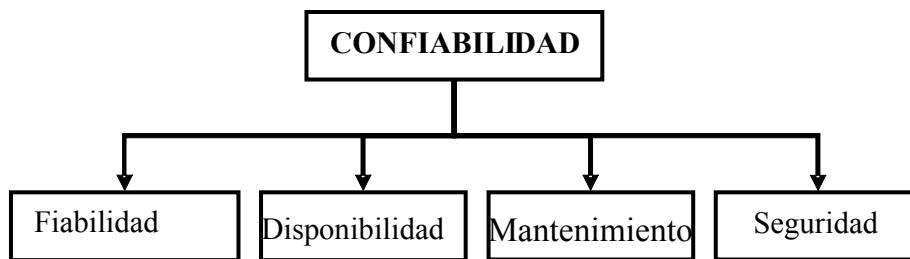
## 2.2 Definiciones

La IEEE define a la confiabilidad como “la habilidad que tiene un sistema o componente de realizar sus funciones requeridas bajo condiciones específicas en periodos de tiempo determinados”. Musa (2002) define a la confiabilidad como “la probabilidad o la capacidad de que un sistema de funciones trabajen sin falla en un periodo de tiempo y bajo condiciones o un medio ambiente también específico”.

La confiabilidad es un aspecto en el cual se involucran diferentes dimensiones. Los principales conceptos asociados a la confiabilidad del software en los setenta fueron:

- Fiabilidad.
- Disponibilidad.
- Mantenimiento.
- Seguridad.

Todos estos conceptos se lograron relacionar como medidas entre ellos mismos, pero finalmente después de muchos años se logró determinar los diferentes conceptos finales que se le atribuirían a la confiabilidad. Las dimensiones antes mencionadas se muestran posteriormente en la figura 2.1, donde la confiabilidad es el concepto que logra contener los conceptos a los que llama sus dimensiones.

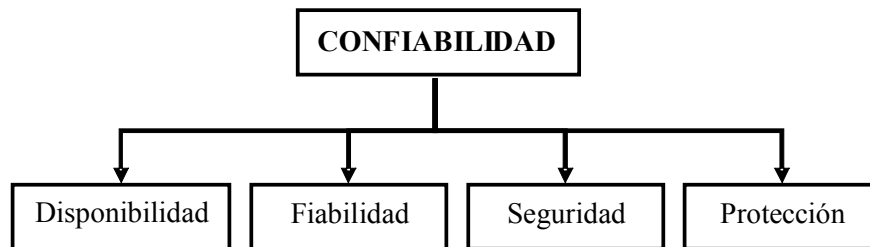


**Figura 2.1.** Dimensiones de la confiabilidad años 70 (Mohanty, 1979)

Las definiciones que se dieron para cada uno de los atributos o dimensiones de la confiabilidad se definen a continuación (Figura 2.2) (Jonsson, 1998):

- **Disponibilidad:** Se refiere a la condición de trabajo que un sistema debe de tener. Si el sistema que se esta utilizando llega a ser apagado en algún tiempo anterior al que se tenia planeado por mantenimiento, luego tendrá que ser encendido sin que afecte su rendimiento o se tenga algún problema.
- **Fiabilidad:** En la ingeniería se usa generalmente para asegurar aquella condición de trabajo que permite al usuario realizar sus tareas para que el sistema no llegue a corromperse.

- **Seguridad:** Este concepto no solo describe el comportamiento del sistema, también nos define la habilidad que tiene éste para poder resistir los ataques externos.
- **Protección:** Este concepto se refiere a la capacidad del sistema de permitir las fallas de manera inmediata, en caso de que el sistema llegara a fallar existirá alguna manera de proteger la información o las acciones que el sistema realice.



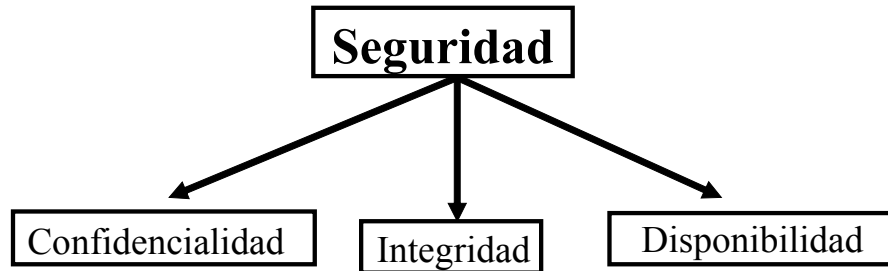
**Figura 2.2** Dimensiones de la confiabilidad (Jonsson, 1998)

De la misma manera que la confiabilidad tiene sus dimensiones, algunos atributos de la confiabilidad tienen dentro de sí mismos otros campos que los componen como son:

**Seguridad** tiene diferentes campos (Figura 2.3), los cuales se dividen en:

- **Confidencialidad:** Es la prevención de la divulgación no autorizada de la información.
- **Integridad:** Se refiere a prever cualquier modificación de la información de manera que no sea autorizada.

- **Disponibilidad:** Se refiere a la prevención de la retención no autorizada de la información.



**Figura 2.3.** Campos de la seguridad (Jonsson, 1998)

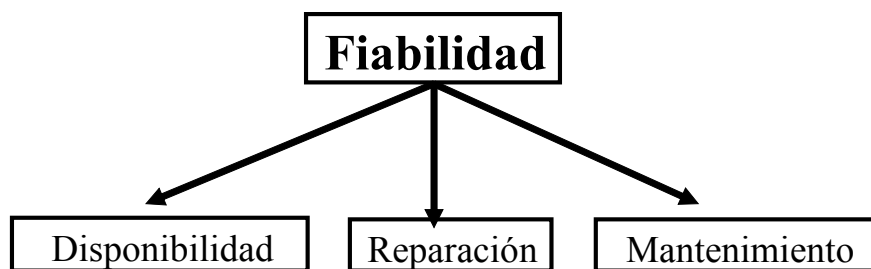
Según Wilikens, además de los conceptos anteriores, la seguridad consta de otras dos llaves extras, las cuales son (Wilikens, 2000):

- **Autenticación:** Se refiere a que todas las personas, programas y sistemas utilizados tienen que ser previamente identificados.
- Sin desconocimiento: Se refiere a las comunicaciones recibidas desde personas, programas o sistemas para asegurarse que han sido enviados por sus emisores aparentes

Según Zacks, los conceptos que afectan a la fiabilidad como dimensión de la confiabilidad de la ingeniería del software son: la disponibilidad, mantenimiento y reparación de los sistemas, los cuales se describen a continuación (Zacks, 1992) (Figura 2.4):

- **Disponibilidad:** Se refiere a la condición de trabajo que un sistema debe de tener, cuando el sistema es apagado en un tiempo anterior al ya establecido para mantenimiento y después volver a encenderlo.

- **Mantenimiento:** Este concepto está estrechamente relacionado con lo que se refiere a reparación, y puede definirse en términos de distribución del tiempo de apagado de la máquina, como la probabilidad de que cuando el mantenimiento se realizó bajo condiciones específicas, el sistema volverá a su condición de trabajo dentro de un período específico.
- **Reparación:** Es la probabilidad de falla que tiene un sistema y que puede ser reparada bajo condiciones y periodos específicos de tiempo.



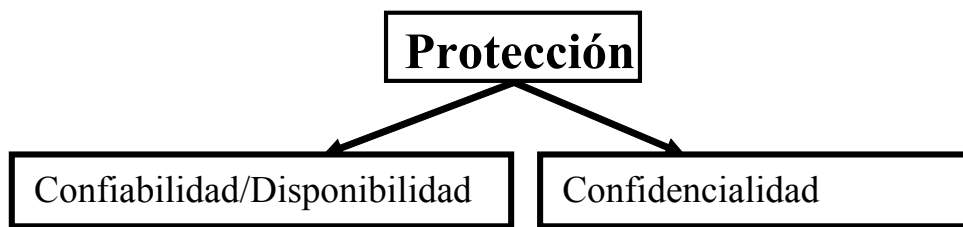
**Figura 2.4.** Campos de la fiabilidad (Zacks, 1992)

Por último tenemos a la protección, la cual nos habla de como el sistema no debe fallar de manera inmediata. Dentro de protección tenemos diferentes aspectos que pueden ser interpretados como comportamientos y términos de prevención, dentro de las dimensiones de protección tenemos a (Figura 2.5):

- **Disponibilidad:** Se define como la habilidad del sistema a entregar este servicio solamente a usuarios que estén autorizados. Los usuarios autorizados son aquellos que son previstos en las especificaciones del sistema. Disponibilidad

como atributo de protección tiene el mismo significado que disponibilidad como atributo de confiabilidad.

- **Confidencialidad:** Está relacionado con la habilidad del sistema de negar el servicio a los que no son usuarios autorizados. Este es así un concepto de comportamiento, pero en diferencia a otros atributos, este comportamiento de sistema es definido con respecto a los que no son usuarios.



**Figura 2.5.** Campos de la Protección (Jonsson, 1998)

El saber y poder especificar las condiciones en las cuales se encuentra un proyecto es de suma importancia, ya que la caída de un componente puede expandirse y lograr afectar toda la operación y dañar también a otros componentes del sistema (Musa, Iannino, Okumoto, 1987).

Existen diferentes tipos de especificaciones, una especificación es aquella que valida los requisitos, la calidad y provee la descripción formal del modelo que se va a efectuar. Las especificaciones varían dependiendo del tipo y el impacto que tienen dentro de los proyectos, a continuación se dará una pequeña descripción de estas (Bittanti, 1988):



**Especificación de la fiabilidad del Software.** Existen tres dimensiones dentro de esta especificación que se deben considerar para su buen funcionamiento, las cuales son:

- **Fiabilidad del hardware:** Cuánta y cuál es la probabilidad de que el hardware falle y cuanto tiempo y dinero cuesta repararlo.
- **Fiabilidad del software:** Que tan fácil es que un sistema a la hora de utilizarlo nos devuelva una salida incorrecta, ya sea por el mal manejo del software o por un error que éste tenga.
- **Operador:** Cuánta facilidad existe en el sistema para que quien lo está ocupando cometa un error.

En lo que se refiere a la **especificación de la seguridad** se debe considerar ésta durante el proceso de ingeniería de los requerimientos, las contingencias potenciales que puedan llegar a surgir. En pocas palabras la característica requerida es la operación segura. Por último tenemos a la **especificación de la protección** la cual va ligada con los requerimientos de seguridad.

### 2.3 Significados de confiabilidad en el software

La confiabilidad es aquella cuyo uso y medición nos ayuda a desarrollar programas de una manera confiable, rápida y a menor costo. La confiabilidad se puede definir como la probabilidad de que se tengan operaciones libres de caídas en un tiempo definido y en un medio adecuado para propósitos específicos (Littlewood, Strigini, 2000). Algunos puntos básicos son (Figura 2.6):

- Ayuda a probar la fiabilidad en un mínimo de tiempo y costo
- Incrementa la productividad de las pruebas y reduce el tiempo de venta de un producto.
- Mejora la satisfacción del cliente.

<i>Valor del Cliente Añadido Correspondencia de Necesidades</i>
<i>Valor del Cliente Añadido Concentración</i>
<i>Valor Original del Cliente</i>

**Tabla 2.1.** Tabla de Valores con respecto al cliente (Musa, 2002)

El ciclo de vida del software está compuesto por diferentes fases como son: análisis del problema, diseño y desarrollo de la aplicación, pruebas e integración. Hoy en día se tienen diferentes métodos para el diseño de la evaluación de cada una de estas fases, para el aseguramiento de la calidad y la evaluación estadística de la confiabilidad del software (Beane, Giddinga, Silverman, 1984).

## **2.4 Características de la confiabilidad en el software**

Existe un programa relacionado a las diferentes características medibles que son relativas a la prueba de programas, basadas en la noción que un programa puede ser representado directamente como una etiqueta gráfica que ha sido creada. Otras

características del software son aquellas que pueden ser modulares, modificables y portables (Mohanty, 1979).

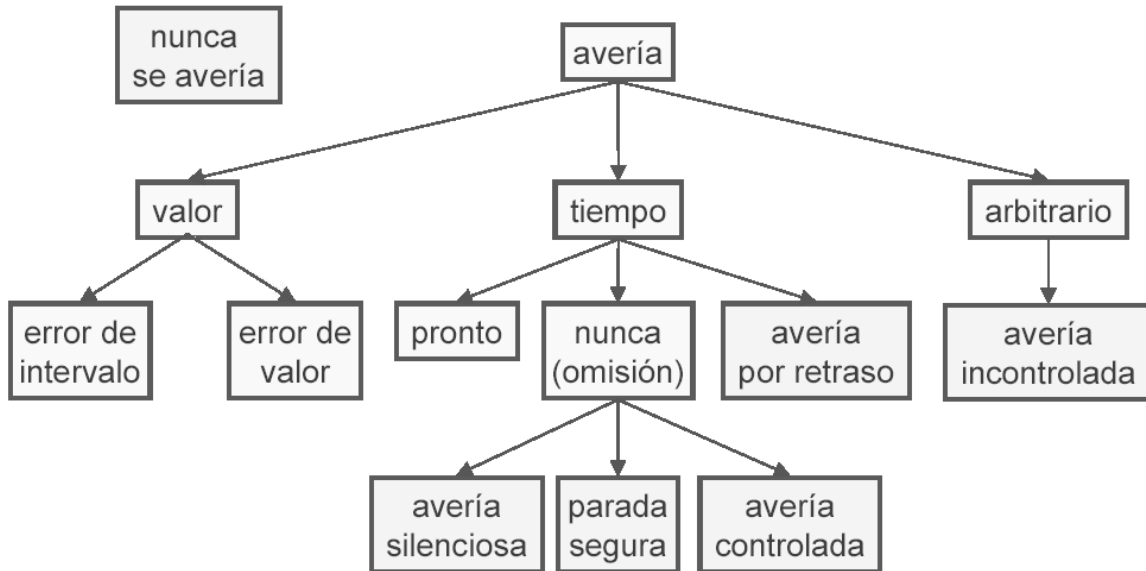
La estimación de la confiabilidad de un programa de computadora no es algo sencillo de hacer, pero su cuantificación es muy importante para el buen funcionamiento de sus atributos en orden de como estos nos pueden ayudar a realizar la compensación entre las decisiones de confiabilidad, el funcionamiento del programa, costo y calendario del sistema de software. Las dos maneras en la que la confiabilidad se divide son (Mohanty, 1979):

1. **Predicción de la confiabilidad** está definida como un lineamiento del programa basado en la evaluación segura y fácilmente medible de las propiedades del código. Los modelos de predicción de confiabilidad están basados en acercamientos relativos los cuales en el momento, probablemente no son 100% claros pero en un futuro se comprobara su eficiencia, y son análogos a los modelos de predicción de confiabilidad del hardware.
2. **Estimación de la confiabilidad** pronostica cambios confiables como una función en el calendario de tiempo, en el tiempo de uso del CPU, u horas de persona que son acumuladas. Los modelos de estimación de confiabilidad son consecutivos a la evaluación de los valores de los parámetros de la confiabilidad. Estos modelos son basados en la estimación de la tarifa de detección de error, la cual se asume es proporcional al número de errores que pueden llegar a faltar.

La fiabilidad de un sistema está altamente vinculada con la cantidad de averías y fallos que éste llega a tener. Se define a una avería como una desviación del comportamiento de un sistema con respecto de su especificación. Las averías se manifiestan en el comportamiento externo del sistema, pero son el resultado de errores internos. Las causas mecánicas o algorítmicas de los errores se denominan fallos (Buns y Wellings, 1990).

Existen diferentes tipos de fallos los cuales provocan inestabilidad dentro de la fiabilidad de los productos de software. A continuación se describen algunos tipos fallos existentes, a este tipo de fallos debe impedírseles que logren causar alguna avería (Figura 2.6):

- Fallos transitorios: desaparecen solos al cabo de un tiempo
- Fallos permanentes: permanecen hasta que se reparan
- Fallos intermitentes: fallos transitorios que ocurren de vez en cuando



**Figura 2.6.** Tipos de avería (Buns y Wellings, 2001)

Existen diferentes maneras para poder aumentar la fiabilidad dentro de un sistema las cuales se pueden agrupar en dos sectores:

- **Prevención de fallos** se trata de evitar la introducción de fallos en el sistema antes de que empiece su funcionamiento, se divide en:
  - **Evitar fallos:** Consiste en evitar la introducción de fallos antes de la construcción del sistema.
  - **Eliminación de fallos:** Consiste en encontrar y eliminar los fallos que se producen en el sistema una vez construido.
- **Tolerancia de fallos** lo que significa lograr que el sistema continúe funcionando a pesar de que se introduzcan fallos.

Existen hoy en día diferentes técnicas para poder evitar este tipo de fallos, en la cuestión del software se pueden definir diferentes aspectos como:

- Proporcionar una especificación de requisitos rigurosa o formal.
- Aplicar métodos de diseño comprobados.

- Lenguajes con abstracción de datos y modularidad.
- Utilización de entornos de desarrollo con computador adecuados para gestionar los componentes}.

En lo referente a comprobaciones:

- Revisiones frecuentes del diseño.
- Verificar el buen funcionamiento de los programas.
- Realizar una inspección rigurosa del código.

Al realizar las pruebas, se llegan a tener diferentes problemas, pero aún así es necesario llevarlas a cabo, a continuación se enlistan algunos de los problemas que se pueden llegar a tener:

- Las pruebas nunca pueden llegar a ser exhaustivas.
- Solo sirven para demostrar que el programa tiene errores, no que no los tienen.
- Es casi imposible el reproducir las condiciones reales.
- Los errores de especificación no se detectan.

Todas estas técnicas anteriormente descritas se utilizan como prevención pero no significa que sean infalibles, ya que muchas veces el hardware llega a fallar a pesar de las técnicas de prevención; la alternativa ante esto es el utilizar técnicas de tolerancia de fallos. Existen diferentes grados en la tolerancia de fallas, el grado de tolerancia dependerá principalmente de las alternativas que se tomen y de la aplicación que se este corriendo en ese momento, los diferentes grados son:

- Tolerancia completa: El sistema continuará funcionando por un tiempo, sin necesidad de que pierda funcionalidad o algunas de sus prestaciones o herramientas.
- Degradación aceptable: El sistema continúa funcionando durante un tiempo con una pérdida de funcionalidad o de sus prestaciones hasta el momento de la reparación.
- Parada segura: El sistema es detenido en un estado que asegura la integridad del entorno hasta que es reparado el problema.

Todos estos conceptos de tolerancia están basados en un concepto llamado **redundancia**, en el cual se utilizan algunos componentes adicionales para lograr detectar las fallas y lograr recuperar el comportamiento que es correcto. Al utilizar este tipo de métodos la complejidad del sistema aumenta y puede introducir otro tipo de errores dentro del programa. Existen diferentes tipos de redundancia en lo que al software se refiere y se utilizan principalmente para corregir y detectar los errores que existen en el diseño, y estos son (Mejía, 2001):

- **Redundancia estática:** Es el tipo de programación que se utiliza cuando se realiza programación con N número de versiones.
- **Redundancia dinámica:** Es la alternativa que permite al programador manejar fallos dinámicamente en un tipo de programación con N número de versiones.

Las fases que se identifican son:

- Se divide en dos etapas; detección y recuperación de fallos.

- Bloques de recuperación los cuales proporcionan información hacia atrás.
- Excepciones los cuales proporcionan información hacia delante.

La confiabilidad de un sistema es una medida de conformidad dependiendo de la especificación que se encuentra autorizada a su comportamiento, a su vez esta es usada para la prevención o tolerancia de fallos de un sistema y con se la confiabilidad en la ingeniería es usada generalmente para asegurar cierto grado de funcionamiento con éxito de un dispositivo o sistema en un ambiente determinado, durante un periodo específico de tiempo. Se puede distinguir entre la confiabilidad de la misión de un dispositivo, el cual es construido para llevar a cabo el funcionamiento de una misión, así como también la operación de confiabilidad de un sistema el cual puede ser o no ejecutado interminablemente para el funcionamiento de un cierto tipo de misiones.