UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERIA

ANALISÍS Y DISEÑO DE SISTEMAS 2

**Documento Atributos de Calidad**

|  |  |
| --- | --- |
| Grupo 4 | |
| Andrés Javier Cardona Galindo | 201021211 |
| José Alfredo Avalos Pérez | 201020983 |
| Angél Estuardo Cajas Ochoa | 201020757 |

Fecha: 04/01/2014

Historial de Revisiones

|  |  |  |
| --- | --- | --- |
| **Fecha** | **Descripción** | **Autores** |
| 23/12/2013 | Creación del Documento, listado de atributos de Calidad. | Angel Cajas |
| 23/12/2013 | Agregados Descripción de Tácticas a implementar | Andrés Cardona |
| 02/01/2014 | Agregados diagramas de tácticas | Ángel Cajas |
| 03/01/2014 | Se le dio formato al archivo | José Avalos |

Tabla de Contenidos

[1. Atributos de Calidad 4](#_Toc376562495)

[2. Tácticas 4](#_Toc376562496)

[2.1 Tácticas de Disponibilidad 4](#_Toc376562497)

[2.2 Tácticas de Modificabilidad 5](#_Toc376562498)

[2.3 Tácticas de Rendimiento 6](#_Toc376562499)

[2.4 Tácticas de Seguridad 6](#_Toc376562500)

[2.5 Tácticas de Pruebas 7](#_Toc376562501)

[2.6 Tácticas de Integridad 7](#_Toc376562502)

[2.7 Tácticas de Usabilidad 8](#_Toc376562503)

Atributos de Calidad

# Atributos de Calidad

* 1. **Disponibilidad:** La medida del tiempo en que el sistema está operativo y ejecutando correctamente.
  2. **Modificabilidad**: La facilidad con la cual el software puede adecuarse a los cambios.
  3. **Rendimiento:** Grado en el cual un sistema o componente cumple sus funciones dentro de restricciones dadas tales como velocidad, exactitud, o uso de memoria.
  4. **Seguridad:** Habilidad del sistema para resistir intentos no autorizados a usar servicios del sistema, mientras permanece proveyendo servicios a usuarios legítimos.
  5. **Pruebas:** La facilidad con la cual se puede demostrar que el software falla.
  6. **Integrabilidad:** la habilidad de hacer el desarrollo de componentes en forma separada y que el sistema trabaje correctamente al juntarlas.
  7. **Usabilidad**: la facilidad de uso y de entrenamiento de los usuarios finales del sistema.

# Tácticas

## Tácticas de Disponibilidad

**Detección de Fallas:** Monitoreo de actividad y reporte de fallas.

* **Ping:** Enviar un ‘ping’ y espera recibir una respuesta.
* **Heartbeat:** se emite un mensaje ‘heartbeat’ periódicamente a otro componente que tiene que estar escuchando, si falla se asume que el componente origen falló, se notifica a una componente de corrección de errores.
* **Excepciones:** disparadas cuando ocurre un error/falla.

**Recuperación de Fallas**

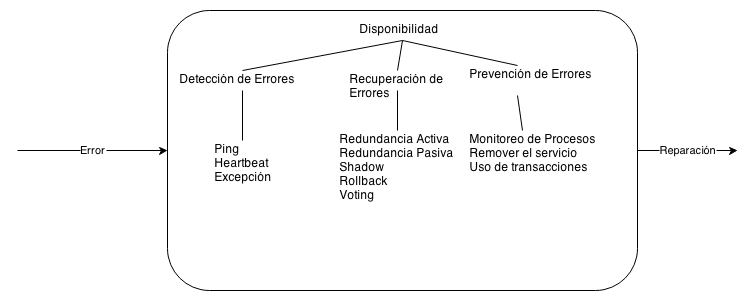
* **Redundancia de componentes críticas activas: Todos** los componentes responden a los eventos. Solo es considerada una respuesta.
* **Redundancia de componentes críticas pasivas:** El componente primario responde, actualiza los secundarios.
* **Sincronización:** responsabilidad de la componente primaria

**Prevención de Fallas**

** Remoción desde el servicio:** reiniciar las componentes periódicamente.

** Transacciones:** Bloques de varios pasos secuenciales. Se deshacen en bloque. Control de integridad de datos.

** Monitor de Procesos**: Detecta fallas en los procesos, y reinicia nuevas instancias.



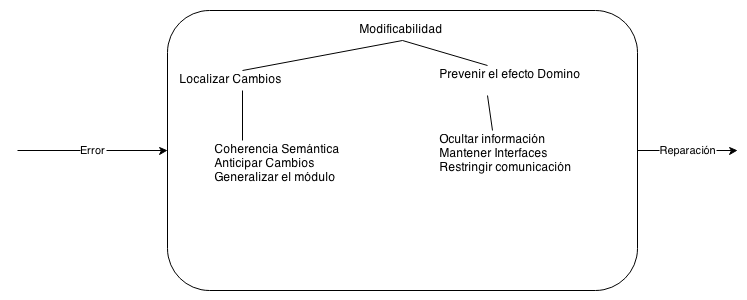
## Tácticas de Modificabilidad

**Localizar Cambios**

* **Coherencia Semántica**
* **Anticipar Cambios**
* **Generalizar el módulo:** Pequeño número de patrones de diseño

**Prevenir Efecto Domino**

* **Ocultar Información:** Uso de capas e información pública y privada
* **Mantener Interfaces:** nombre y firma
* **Restringir Comunicación**



## Tácticas de Rendimiento

**Demanda de Recursos**

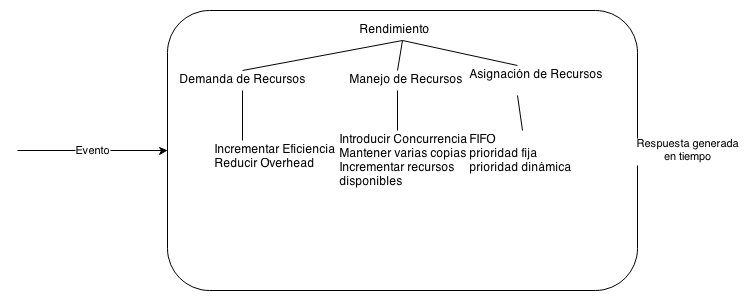
* **Incrementar Eficiencia**
* **Reducir Overhead**

**Manejo de Recursos**

* **Concurrencia**
* **Incrementar recursos disponibles**
* **Mantener copias**

**Asignación de Recursos**

* **FIFO**
* **Prioridad Fija**
* **Prioridad Dinámica**



## Tácticas de Seguridad

**Resistencia a ataques**

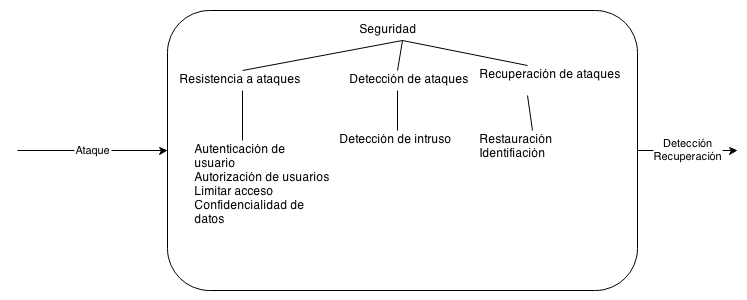
* **Autenticación de usuarios**
* **Autorización de usuarios**
* **Confidencialidad de los datos:** Encriptacion y desencriptacion, VPN (Virtual Private Network) o SSL (Secure Sockets Layer).
* **Limitar acceso:** Firewalls, DMZ (Demilitarized Zone).

**Detección de Ataques**

* **Detección de intruso**

**Recuperación de Ataques**

* **Restauración e Identificación de ataque**



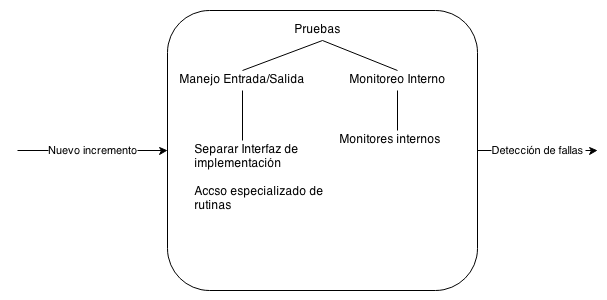
## Tácticas de Pruebas

**Manejo Entradas/Salidas**

* **Separar Interfaz de Implementación**
* **Acceso especializado de rutinas**

**Monitoreo Interno**

* **Monitores internos**

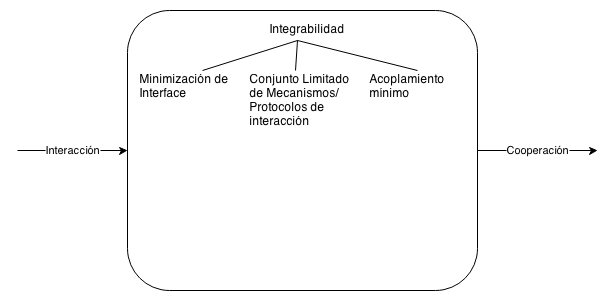


## Tácticas de Integridad

**Minimización de Interface**

**Conjunto Limitado de Mecanismos de Interacción**

**Acoplamiento Mínimo**



## Tácticas de Usabilidad

**Separar Interfaz de usuario**

**Soportar Iniciativa de Usuario**

* **Cancelar**
* **Deshacer**
* **Agregar**

**Soportar Iniciativa del Sistema**

* **Modelo del Usuario**
* **Modelo del Sistema**
* **Modelo de Tarea**

