CAPÍTULO IV

3 CALIDAD Y SEGURIDAD

3.1 INTRODUCCIÓN

El objetivo del presente capítulo es observar el valor técnico del producto desarrollado, de esta forma evaluar la calidad del producto haciendo uso del estándar ISO 9126.

3.2 CALIDAD DE SOFTWARE

La calidad del software es una preocupación a la que se dedican muchos esfuerzos, todo proyecto tiene como objetivo producir software de calidad, que cumpla, y si puede supere las expectativas de los usuarios.

El software evoluciona a través de actualizaciones a medida que se corrigen los errores mejorando el funcionamiento del mismo, existen varias métricas de medición que permiten medir la calidad del software, uno de ellos es la norma ISO (International Standart Organization).

Para el proyecto se toma en cuenta la norma ISO 9126 que toma en cuenta los siguientes aspectos: funcionalidad, fiabilidad, usabilidad y mantenibilidad.

3.2.1 Funcionalidad

Es un conjunto de atributos que se relacionan con la existencia de un conjunto de funciones y sus propiedades específicas. Las funciones son aquellas que satisfacen las necesidades implícitas o explícitas.

La métricas del software orientadas a la función, utilizan una medida de la funcionalidad entregada por la aplicación como valor de normalización, estas serán obtenidas a partir de las entradas, consultas e interfaces externas que proporciona el sistema para la satisfacción de los requerimientos.

- Entradas de usuario: son cada una de las entradas de datos que proporciona el usuario al software.
- Salidas de usuario: son cada una de las salidas de datos que proporciona el usuario.
- Peticiones de usuario: son combinaciones únicas existente entre entrada y salida, donde una entrada genera una salida.
- Archivos: son tablas y archivos.

- Interfaces externas: son el número de interfaces, copias de seguridad y transmisión de información.

A continuación de muestran las cinco características con un factor de ponderación medio, para el calculo del punto función (Tabla 3.1).

Parámetros de medición	Cuenta	Factor de ponderación	Total
Entras de usuario	30	4	120
Salidas de usuario	30	5	200
Peticiones de usuario	10	4	40
Archivos	5	12	60
Interfaces externas	5	6	30
Cuenta Total			**450**

Tabla 3.1 *Evaluación de funcionalidad*

Fuente*: Elaboración propia*

La determinación de la complejidad es algo subjetivo, para nuestro caso utilizamos un factor de ponderación medio (Tabla 3.2).

Nro	Factor	Valor
1	Copia de seguridad y recuperación	5
2	Comunicación de datos	3
3	Proceso distribuido	3
4	Rendimiento crítico	3
5	Entorno operativo existente	5
6	Entrada de datos en línea	0
7	Transacciones de entradas en múltiples pantallas	2
8	Archivos maestro actualizados en línea	3
9	Complejidad de valores del dominio de información	2
10	Complejidad del procesamiento interno	5
11	Código rediseñado para la reutilización	3
12	Conversión – instalación en diseño	2
13	Instalaciones múltiples	5

14	Aplicación diseñada para el cambio	3
Total (N)		** **Expresión incorrecta** **

Tabla 3.2 *Determinación de complejidad*

Fuente*: Elaboración propia*

Reemplazando los datos en la ecuación:

$$PF = Cuenta\,total * (X + Min(Y) * \sum Fi)$$

$$PF = 450 * (0.65 + 0.01 * 44)$$

$$PF = 490.5$$

Entonces decimos que el sistema tiene 490.5 puntos de función, para sacar la probabilidad de la funcionalidad debemos obtener el PF máximo y lo dividimos con los puntos de función obtenida, es decir Σ = 70.

$$PF_{MAX} = 450 * (0.65 + 0.01 * 70)$$

$$PF_{MAX} = 607.5$$

De esta forma obtenemos la funcionalidad:

$$Funcionalidad = (\frac{490.5}{607.5}) * 100$$

$$Funcionalidad = 80.74$$

El porcentaje obtenido se puede interpretar de la siguiente forma: 8 de cada 10 personas consideran que el sistema responde de manera óptima a la funcionalidades necesarias para la unidad.

3.2.2 Mantenibilidad

La mantenibilidad es el esfuerzo necesario para localizar y realizar modificaciones específicas del sistema, para hallar la probabilidad de mantenibilidad utilizaremos las siguientes preguntas para obtener la mantenibilidad del sistema (Tabla 3.3).

Factor de ajuste	Valor
¿Puede ser modificado el sistema?	90
¿Deja identificar las partes que deben ser modificadas?	92
¿Permite implementar una modificación específica?	89
¿No presenta afectos inesperados con posibles errores?	80
Total	**87.75**

Tabla 3.3 *Evaluación de mantenibilidad*

***Fuente**: Elaboración propia*

Tras la evaluación al sistema el porcentaje obtenido (87.75 %) se lo puede interpretar de la siguiente forma: el esfuerzo necesario para realizar el mantenimiento al sistema es mínimo.

3.2.3 Usabilidad

Para comprobar la usabilidad del sistema se va a hacer uso de los test de usuarios que consiste en realizar una evaluación escrita después de las pruebas, en los usuarios finales esta evaluación se las hizo calificando sobre una escala del 1 al 10. El resumen de la información obtenida representa la usabilidad del sistema de acuerdo al análisis realizado (Tabla 3.4).

Factor de ajuste	**Usuario 1**	**Usuario 2**	**Usuario 3**	**Usuario 4**	**Promedio**
¿Puede ser usado con facilidad?	8	7	8	9	** Expresión incorrecta **
¿Puede ser aprendido con facilidad?	8	7	9	8	** Expresión incorrecta **
¿El diseño es atractivo?	9	8	8	7	8
¿Las salidas son entendibles?	7	9	8	9	8.25
¿Las salidas son esperadas?	8	8	9	7	8
¿Los reportes le ayudan en su trabajo?	7	8	9	8	8
Total					**8.04**

***Tabla 3.4** Evaluación de usabilidad*

***Fuente**: Elaboración propia*

Para hallar la usabilidad convertimos la escala de 1 hasta 10 a porcentaje por cuento tenemos:

$$Usabilidad = 8.04 * 10$$
$$Usabilidad = 80.4$$

El porcentaje obtenido se lo puede interpretar de la siguiente forma: en promedio 8 de cada 10 usuarios del sistema consideran que tienen facilidad al momento de utilizar el sistema.

3.2.4 Portabilidad

El sistema puede ser transferido de una computador a otra cumpliendo los requerimientos mínimos de hardware y software, y así determinar la adaptabilidad del sistema, donde el grado de portabilidad esta dada por la siguiente formula:

$$GP = 1 - \left(\frac{CT}{CRD}\right)$$

Donde:

GP: Grado de portabilidad

CT: Costo de transporte

CRD: Costo de redesarrollo

Si GP > 0: La portabilidad es mas rentable que el redesarrollo

Si GP = 1: La portabilidad es perfecta

Si GP < El redesarrollo es mas rentable que la portabilidad

Realizando los cálculos:

$$GP = 1 - \left(\frac{20}{9600}\right)$$
$$GP = 0.9979$$

Por lo tanto podemos concluir que el sistema desarrollado tiene un grado de portabilidad de 99.79 %, lo que permite afirmar que el sistema puede adaptarse y transportarse a nuevas plataformas sea cual sea el sistema operativo.

3.2.5 Escala de medición de aceptabilidad

Interpretando los datos obtenidos hasta ahora y tomando como referencia la siguiente escala de medición:

- Insatisfactorio (0 – 40) %
- Aceptabilidad marginal (40 – 60) %
- Satisfactorio (60 – 100) %

Obtenemos la Tabla 3.5:

Características	
Funcionalidad	80.74
Mantenibilidad	87.75
Usabilidad	80.4
Portabilidad	99.79
Calidad global del sistema	**87.17**

Tabla 3.5 *Resumen de datos obtenidos*

Fuente*: Elaboración propia*

Podemos concluir que las escalas de aceptabilidad es del 87.17 % con lo que se considera al sistema satisfactorio.

3.3 SEGURIDAD DE SOFTWARE

Todos los esquemas de firma digital comparten los siguientes requisitos previos básicos, independientemente de la teoría o criptográfico disposición legal:

- Algoritmos de Calidad: Algunos algoritmos de clave pública son conocidos por ser ataques inseguros, prácticas contra ellos de haber sido descubiertos.
- Implementaciones de calidad: Una implementación de un buen algoritmo (o protocolo) con error (s) no funcionará.
- La clave privada debe permanecer privada: Si la clave privada se conoce a ningún otro partido, ese partido puede producir firmas digitales perfectas de cualquier cosa.
- El propietario de la clave pública debe ser verificable: Una clave pública asociada a Bob en realidad procedían de Bob. Esto se hace habitualmente utilizando una infraestructura de clave pública (PKI) y la asociación key↔user pública es atestiguado por el operador de la PKI (llamado una autoridad de certificación). Para PKI "abiertos" en el que cualquier persona puede solicitar un certificado tales (universalmente encarnado en un certificado de identidad protegida criptográficamente), la posibilidad de certificación equivocada es no trivial. Operadores PKI comerciales han sufrido varios problemas conocidos públicamente. Tales errores pueden conducir a falsos firmó, y así erróneamente atribuida, documentos. Sistemas PKI 'Cerrado' son más caros, pero con menos facilidad subvertidas de esta manera.
- Usuarios (y su software) deben llevar a cabo el protocolo de firma correctamente:

> Sólo si todas estas condiciones se cumplen será una firma digital en realidad ser cualquier evidencia de quien envió el mensaje, y por lo tanto de su asentimiento a su contenido. Promulgación legal no puede cambiar esta realidad de las posibilidades de ingeniería existentes, aunque algunos como no han reflejado esta realidad.

Las legislaturas, siendo importunaban por las empresas que esperan sacar provecho de operación de una PKI, o por la vanguardia tecnológica abogar nuevas soluciones a viejos problemas, han promulgado leyes y / o regulaciones en muchas jurisdicciones que autorizan, Apoyar, fomentar o permitir la firma digital y la prestación para (o limitar) su efecto legal. El primero parece haber sido en Utah en los Estados Unidos, seguido de cerca por los estados de Massachusetts y California. Otros países también han aprobado leyes o emitido reglamentos en esta área, así y la ONU ha tenido un proyecto de ley modelo activo durante algún tiempo. Estas representaciones (o decretos propuestos) variar de un lugar a otro, se han incorporado típicamente expectativas en la varianza (optimista o pesimista) con el estado de la ingeniería criptográfico subyacente, y han tenido el efecto neto de los usuarios potenciales de confusión y especificadores, casi todos los cuales no son criptográficamente bien informado. La adopción de normas técnicas para las firmas digitales se han quedado atrás la mayor parte de la legislación, lo que retrasa una posición de ingeniería más o menos unificada en la interoperabilidad, la elección de algoritmos, longitudes de clave, y así en lo que la ingeniería está tratando de proporcionar.