Smart Embedded Systems

Departamento de sistemas empotrados

**Sistema de Seguridad para Hogares SSH-101**

Plan de Verificación de Software

Borrador 5

Abril de 2025

**Historial de revisiones**

|  |  |  |  |
| --- | --- | --- | --- |
| Versión # | Autor | Notas del documento | Fecha |
| Borrador 1 | G. Cubas | Estructura del documento | 2016-04-25 |
| Borrador 2 | L. Alfaro | Correcciones menores | 2020-04-13 |
| Borrador 3 | L. Alfaro | Correcciones de contenido | 2023-04-12 |
| Borrador 4 | L. Alfaro | Actualizaciones de secciones | 2025-04-01 |
| Borrador 5 | V. Sánchez  J. Ureña | Actualización de secciones 6.3 y 6.5 del Plan de Verificación | 2025-04-19 |

Tabla de contenidos

[2 Propósito 5](#_Toc479625575)

[3 Referencias 5](#_Toc479625576)

[4 Abreviaturas 5](#_Toc479625577)

[5 Definiciones 5](#_Toc479625578)

[6 Visión General 6](#_Toc479625579)

[6.1 Organización 6](#_Toc479625580)

[6.2 Cronograma 6](#_Toc479625581)

[6.3 Nivel de integridad 6](#_Toc479625582)

[6.4 Responsabilidades 6](#_Toc479625583)

[6.5 Herramientas, técnicas y métodos 6](#_Toc479625584)

[7 Procesos de verificación 6](#_Toc479625585)

[7.1 Proceso: Planeación 6](#_Toc479625586)

[7.2 Proceso: Desarrollo 6](#_Toc479625587)

[7.2.1 Actividades de verificación en la fase de requerimientos 6](#_Toc479625588)

[7.2.2 Actividades de verificación en la fase de diseño 6](#_Toc479625589)

[7.2.3 Actividades de verificación en la fase de codificación 7](#_Toc479625590)

[7.2.4 Actividades de verificación en la fase de integración 7](#_Toc479625591)

[7.2.5 Actividades de verificación en la fase de instalación y pruebas en sitio 8](#_Toc479625592)

[7.3 Proceso: Operación & Mantenimiento 8](#_Toc479625593)

[7.3.1 Actividades de verificación en la fase de operación y mantenimiento 8](#_Toc479625594)

[8 Reportes 8](#_Toc479625595)

[9 Requisitos administrativos 8](#_Toc479625596)

[9.1 Reporte y resolución de anomalías 8](#_Toc479625597)

[9.2 Política de desviación 8](#_Toc479625598)

[9.3 Estándares, prácticas y convenciones 8](#_Toc479625599)

[10 Requisitos de documentación 8](#_Toc479625600)

[Anexo 1. Ciclo de vida 9](#_Toc479625601)

[Anexo 2. Proceso de revisión técnica 10](#_Toc479625602)

[Anexo 3. Lista de verificación de requerimientos de software 11](#_Toc479625603)

[Anexo 4. Lista de verificación de diseño de software 12](#_Toc479625604)

[Anexo 5. Lista de verificación del código fuente 13](#_Toc479625605)

[Anexo 6. Plantilla de casos de prueba de software 14](#_Toc479625606)

[Anexo 7. Plantilla procedimientos prueba manuales 15](#_Toc479625607)

[Anexo 8. Lista de revisión de casos de prueba de software 16](#_Toc479625608)

# Propósito

[Definición de los objetivos del proceso de verificación y validación. Identificación del proyecto para el cual se desarrolla el presente plan.]

# Referencias

1. 1012-1998 IEEE Standard for Software Verification and Validation
2. 24765-2010 - Systems and software engineering -- Vocabulary.
3. 730-2014 - IEEE Standard for Software Quality Assurance Processes
4. 828-2012 - IEEE Standard for Configuration Management in Systems and Software Engineering
5. 29119-3-2013 - IEEE Software and systems engineering Software testing Part 3:Test documentation
6. 982.1-2005 - IEEE Standard Dictionary of Measures of the Software Aspects of Dependability
7. 1028-2008 - IEEE Standard for Software Reviews and Audits
8. 1044-2009 - IEEE Standard Classification for Software Anomalies
9. 829-2008 IEEE Standard for Test Documentation
10. ISO/IEC 15026-2:2011 Systems and software engineering -- Systems and software assurance -- Part 2: Assurance case

# Abreviaturas

PD: Por Definir

# Definiciones

**Caso de prueba:** Documentación que especifica las entradas, resultados esperados, y un conjunto de condiciones de ejecución para un elemento de prueba [IEEE Std 1012-1998].

**Nivel de integridad:** Una indicación de un rango de valores de una propiedad de un elemento necesario para mantener los riesgos del sistema dentro de límites aceptables. Para elementos que realizan funciones de mitigación, la propiedad es la confiabilidad con la cual el elemento debe realizar la función de mitigación. Para elementos cuya falla puede conducir a una amenaza, la propiedad es el límite en la frecuencia de esa falla [ISO/IEC 15026]

**Procedimiento de Prueba**: Documentación que especifica una secuencia de acciones para ejecutar una prueba [IEEE Std 1012-1998].

**Revisión técnica**: Evaluación sistemática de un producto de software por un equipo calificado que examina la conformidad de este con respecto a su uso programado y sus especificaciones. [IEEE Std 1012-1998].

# Visión General

## Organización

[Organigrama del proyecto indicando su relación con otras unidades de la empresa o fuera de la empresa.]

## Cronograma

[Cronograma del proyecto.]

## Nivel de integridad

Nivel de integridad de la aplicación:

* SIL-4 (máxima confiabilidad): MCDC= Multiple Condition-Decision Coverage

El nivel de integridad escogido consta de la máxima confiabilidad, donde cada una de las decisiones deben ser ejecutadas en su rama positiva y su rama negativa, y debe probarse que cada condición en cada decisión afecta la salida independientemente.

Esto asegura que todas las posibles combinaciones de condiciones que puedan afectar el flujo de ejecución del programa sean **debidamente verificadas**, reduciendo significativamente el riesgo de fallos no detectados.

## Responsabilidades

[Descripción de las responsabilidades de cada elemento organizacional sobre las tareas de verificación.]

## Herramientas, técnicas y métodos

Actividades de verificación:

* Análisis
  + Memoria. Se establece un análisis de memoria para garantizar el uso adecuado de los segmentos de memoria, entre otros.
  + Método empleado: Perfilado de memoria durante la ejecución.
  + Herramientas utilizadas: mprof.
* Pruebas
  + Desarrollo de casos de prueba para los requerimientos de alto y bajo nivel, de modo que se pueda alcanzar una cobertura máxima de las diferentes funcionalidades del sistema.
  + Técnicas aplicadas: Pruebas de caja negra en su totalidad MC/DC según lo requerido por SIL-4.
  + Herramientas utilizadas: Establecimiento de casos de prueba.

# Procesos de verificación

## Proceso: Planeación

En esta sección se describen el proceso de verificación de las actividades de planeación.

## Proceso: Desarrollo

A continuación, se describen las actividades de verificación relacionadas con los diferentes productos del ciclo de vida de software.

### Actividades de verificación en la fase de requerimientos

El propósito de las actividades verificación en la fase de requerimientos es asegurar que los requerimientos de software implementan correctamente los requerimientos de sistema. Este objetivo se lleva a cabo mediante una revisión técnica de los requerimientos de software. Esta revisión se lleva a cabo mediante el proceso descrito en el Anexo 2.

La lista de verificación para la revisión técnica del documento de requerimientos se muestra en el Anexo 3.

### Actividades de verificación en la fase de diseño

El objetivo de las actividades de verificación en la fase diseño es asegurar que la arquitectura de software y la funcionalidad de bajo nivel implementa correctamente los requerimientos de software. Para alcanzar este objetivo se lleva a cabo una revisión técnica de los documentos de diseño mediante el proceso descrito en el Anexo 2 y usando la lista de verificación mostrada en el Anexo 4.

### Actividades de verificación en la fase de codificación

Las actividades de verificación de esta fase pretenden minimizar errores en el código y asegurar que el código es fácil de entender y mantener. Para ello se lleva a cabo una revisión de código utilizando el proceso descrito en el Anexo 2 y la lista de verificación mostrada en el Anexo 5.

### Actividades de verificación en la fase de integración

En la fase de implementación se llevan a cabo las pruebas y análisis a fin de comprobar que el software implementa correctamente los requisitos funcionales y no funcionales. Para ello se seleccionan los casos de prueba mediante las técnicas listadas a continuación (según aplique):

* Pruebas normales
  + Variables reales y enteras deben ser probadas mediante clases de equivalencia y valores de frontera
  + Transiciones de estado válidas
  + Tablas de verdad para requerimientos con expresiones lógicas
* Pruebas de robustez
  + Valores inválidos para variables reales y enteras
  + Posibles escenarios de falla
  + Transiciones de estado inválidas

Los casos de prueba deberán utilizar la plantilla mostrada en el Anexo 6. Los casos de prueba deberán ser revisados mediante la lista de verificación mostrada en el Anexo 8.

También en la fase de integración se llevarán a cabo análisis detallados de:

* Cobertura de requerimientos por parte de las pruebas
* Cobertura estructural
* Análisis de tiempos
* Análisis de memoria
* Análisis de pila
* Otros análisis

A continuación, se describen cada uno de estos análisis.

**Cobertura de requerimientos:** Este análisis consiste en asegurar que las pruebas desarrolladas cubren todos los requerimientos de acuerdo con los criterios de selección de casos de prueba enumerados en esta sección. Para ello se hace uso de la matriz de trazabilidad de casos y procedimientos de prueba.

**Cobertura estructural:** El análisis de cobertura estructural consistirá en verificar que todas las estructuras del código han sido ejercitadas al ejecutar los casos y procedimientos de prueba. El nivel de cobertura estructural para el Proyecto SSH-101 será de Cobertura de Estatutos, correspondiente al nivel de criticidad moderado.

**Análisis de tiempos:** Este análisis consistirá en identificar los requerimientos de rendimiento, identificar el caso de peor tiempo de ejecución y ejecutar las pruebas necesarias que comprueben que el sistema cumple con los requisitos de rendimiento en estas condiciones.

**Análisis de memoria:** El análisis de memoria consiste en verificar que el programa se ajusta a las restricciones de memoria especificadas en el diseño y que la asignación de los diferentes segmentos de memoria se ajusta a la arquitectura del *hardware*. Para ello se deberá llevar a cabo un análisis minucioso del mapa de memoria (*link map*) con base en el documento de diseño.

**Análisis de uso de pila:** El análisis de pila consiste en estudiar la forma en que el programa hace uso de la pila (paso de parámetros, variables locales, almacenamiento de contexto, operaciones *push/pop*, etc) a fin de asegurar que no se presentan casos de desbordamiento (*overflow*) o agotamiento (*underflow*).

**Otros análisis:** Según sea el caso, pueden ser necesarios otros tipos de análisis: análisis de particiones, de capacidad, de algoritmos, etc.

### Actividades de verificación en la fase de instalación y pruebas en sitio

[PD]

## Proceso: Operación & Mantenimiento

### Actividades de verificación en la fase de operación y mantenimiento

[PD]

# Reportes

[Descripción de los reportes requeridos. Por ejemplo, reportes de fallas, reportes de resultados, reporte de verificación de software.]

# Requisitos administrativos

## Reporte y resolución de anomalías

[Procedimiento a seguir para reportar y resolver las anomalías detectadas.]

## Política de desviación

[Procedimiento para desviarse del plan de verificación, aprobaciones requeridas]

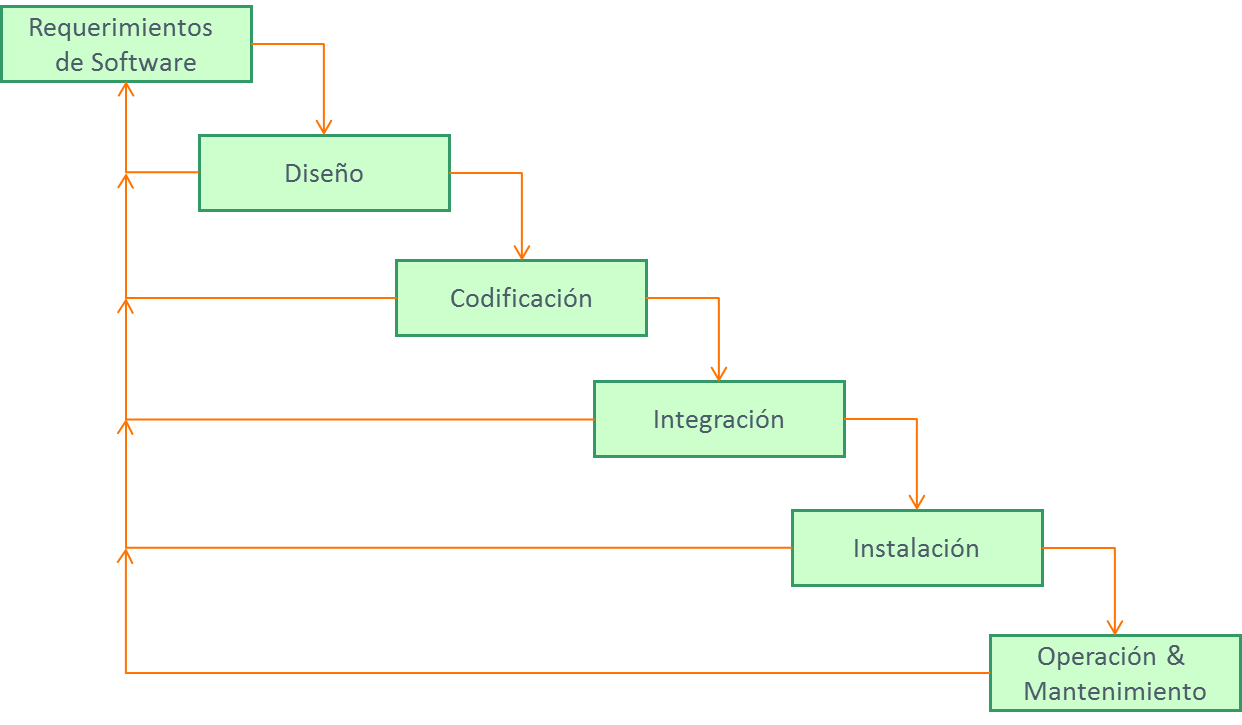
## Estándares, prácticas y convenciones

[Estándares de la industria y estándares de proyecto aplicables]

# Requisitos de documentación

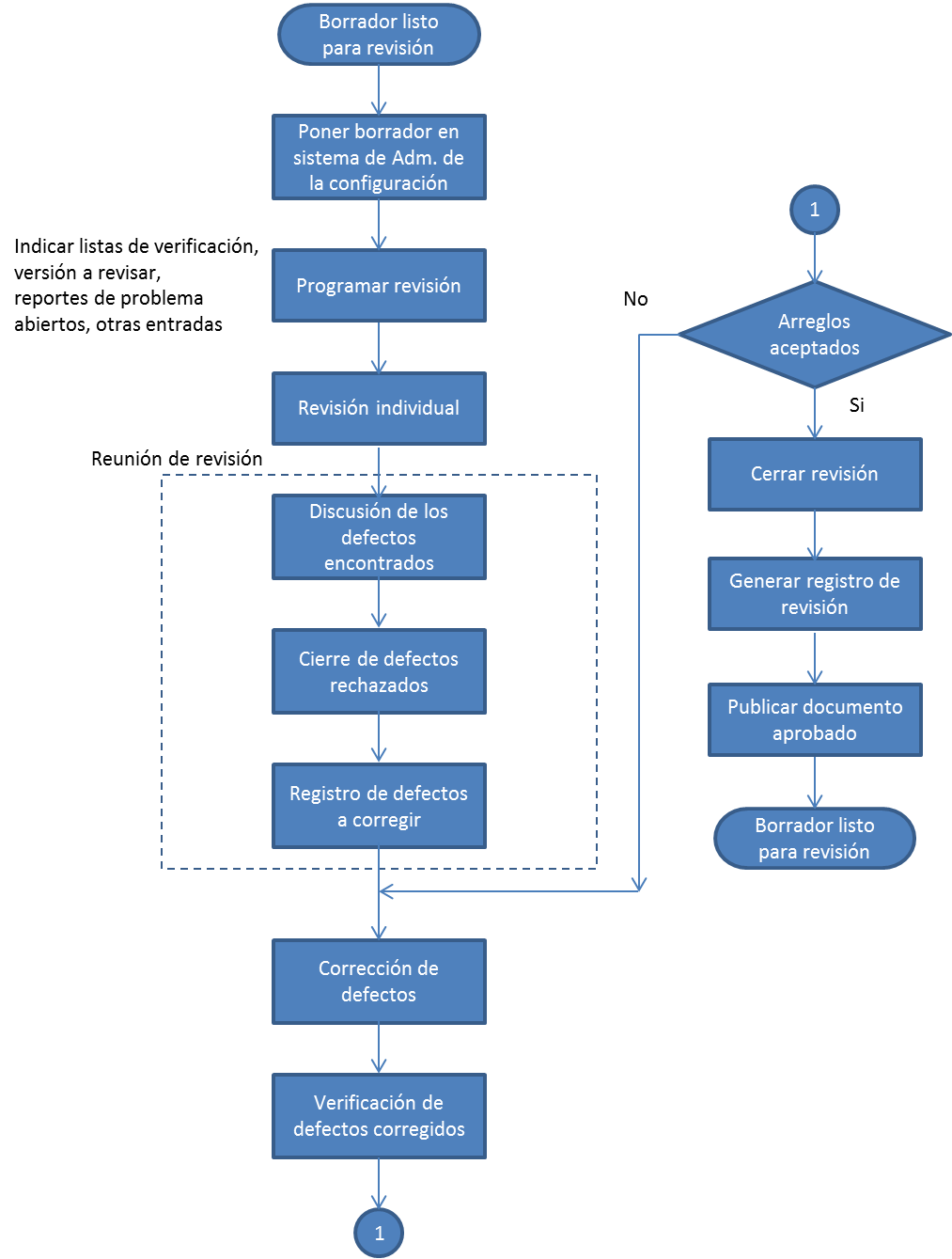
[En esta sección se indican los requerimientos para la documentación de verificación tal como, el plan de verificación, plan de pruebas, casos de prueba, procedimientos de prueba, resultados de verificación etc.]

# Ciclo de vida



|  |  |  |
| --- | --- | --- |
| Fase | Productos | Actividades de Verificación |
| Requerimientos | Documento de requerimientos de software (SRD) | Revisión de SRD |
| Diseño | Documento de diseño de software (SDD): Requerimientos de bajo nivel + Arquitectura de software  Documento de especificación de interfaces | Revisión de documentos de diseño |
| Codificación | Código fuente | Revisión de código |
| Integración | Código ejecutable | Pruebas  Análisis de tiempos  Análisis de memoria  Análisis de pila  Otros análisis |
| Implantación | Sistema operacional | Pruebas de aceptación |
| Mantenimiento | Parches, actualizaciones | Pruebas de regresión |

# Proceso de revisión técnica



# Lista de verificación de requerimientos de software

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lista de verificación de requerimientos de software** | | | | | | |
| Nombre del proyecto: |  | Versión: |  | | | |
| No. de documento: |  | Revisor: |  | | | |
| Autor: |  | Fecha de revisión: |  | | | |
| **S=Satisface; NS=No Satisface; N/A=No Applica.** | | | | | | |
| **Criterio** | | | | **S** | **NS** | **N/A** |
| 1. ¿El documento se ajusta a la plantilla aprobada? | | | |  |  |  |
| 1. ¿La historia de revisiones del documento es correcta? | | | |  |  |  |
| 1. ¿La ortografía y redacción son correctas? | | | |  |  |  |
| 1. ¿Los documentos referidos están disponibles? | | | |  |  |  |
| 1. ¿Se especifican los requerimientos de rendimiento? | | | |  |  |  |
| 1. ¿Se indican las restricciones de recursos? | | | |  |  |  |
| 1. ¿Se indican los interfaces del sistema? | | | |  |  |  |
| 1. ¿Se incluyen mecanismos de detección de fallas? | | | |  |  |  |
| 1. ¿Se implementan todos los requerimientos de sistema? | | | |  |  |  |
| 1. ¿Los requerimientos son claros y concisos? | | | |  |  |  |
| 1. ¿Los requerimientos son consistentes y no presentan contradicciones? | | | |  |  |  |
| 1. ¿Los requerimientos están completos y libres de omisiones? | | | |  |  |  |
| 1. ¿Los requerimientos son verificables? ¿Es posible identificar acciones que verifiquen que el software implementa los requerimientos correctamente? | | | |  |  |  |
| **Comentarios adicionales:** | | | | | | |
|  | | | | | | |
| Firma: | | Fecha: | | | | |
|  | |  | | | | |

# Lista de verificación de diseño de software

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lista de verificación del diseño de software** | | | | | | |
| Nombre del proyecto: |  | Versión: |  | | | |
| No. de documento: |  | Revisor: |  | | | |
| Autor: |  | Fecha de revisión: |  | | | |
| **S=Satisface; NS=Not Satisface; N/A=No Applica.** | | | | | | |
| **Criterio** | | | | **S** | **NS** | **N/A** |
| 1. ¿Se describen los algoritmos con precisión? | | | |  |  |  |
| 1. ¿El SDD contiene una descripción de la arquitectura del software? | | | |  |  |  |
| 1. ¿Se ofrece una descripción de los interfaces del sistema? | | | |  |  |  |
| 1. ¿Se identifican las restricciones de recursos? | | | |  |  |  |
| 1. ¿Se ofrecen descripciones de cada módulo o función? | | | |  |  |  |
| 1. ¿Todos los requerimientos de bajo nivel y arquitectura de software son trazables a requerimiento de software en el SRD? | | | |  |  |  |
| 1. ¿Los requerimientos de bajo nivel son verificables? | | | |  |  |  |
| 1. ¿Los requerimientos de bajo nivel son claros, consistentes y verificables? | | | |  |  |  |
| 1. ¿La arquitectura de software es compatible con la arquitectura de HW? | | | |  |  |  |
| 1. ¿El diseño es claro y permite escribir el código a partir de él? | | | |  |  |  |
| **Comentarios adicionales:** | | | | | | |
|  | | | | | | |
| Firma: | | Fecha: | | | | |
|  | |  | | | | |

# Lista de verificación del código fuente

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lista de verificación del diseño de software** | | | | | | |
| Nombre del proyecto: |  | Versión: |  | | | |
| No. de documento: |  | Revisor: |  | | | |
| Autor: |  | Fecha de revisión: |  | | | |
| **S=Satisface; NS=No Satisface; N/A=No Applica.** | | | | | | |
| **Criterio** | | | | **S** | **NS** | **N/A** |
| 1. ¿El código fuente cuenta con comentarios que describan la implementación? | | | |  |  |  |
| 1. No se utilizan números mágicos, sino constantes | | | |  |  |  |
| 1. Las expresiones booleanas no contienen más de 4 condiciones | | | |  |  |  |
| 1. No se redefinen identificadores de variables o funciones | | | |  |  |  |
| 1. Las funciones no tienen más de 100 líneas de código ejecutable | | | |  |  |  |
| 1. Las funciones solo tienen un camino de salida | | | |  |  |  |
| 1. Los estatus switch definen una opción por omisión (*default*) | | | |  |  |  |
| 1. Todas las variables y punteros son inicializadas antes de usarse | | | |  |  |  |
| 1. No se modifican los índices dentro de los ciclos for | | | |  |  |  |
| 1. Se utilizan paréntesis para hacer el orden de evaluación más evidente | | | |  |  |  |
| 1. El código fuente se ajusta a la descripción de la arquitectura de software definida en el documento de diseño | | | |  |  |  |
| 1. En los casos en que se puede presentar una división por cero, se cuenta con una rutina de manejo de error | | | |  |  |  |
| 1. Se utiliza *indentación* para asegurar la legibilidad del código | | | |  |  |  |
| 1. Los nombres de las variables o funciones son descriptivos | | | |  |  |  |
| **Comentarios adicionales:** | | | | | | |
|  | | | | | | |
| Firma: | | Fecha: | | | | |
|  | |  | | | | |

# Plantilla de casos de prueba de software

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Trazabilidad** | **Descripción** | **Variables de prueba** | | | | | | | **Comentario** |
| **Condiciones iniciales** | | **Entradas** | | | **Salidas** | |
| # | Req. ID |  | E1 | En | V1 | V2 | Vn | A1 | An |  |

Donde:

ID: Identificador del caso de prueba

Trazabilidad: Trazabilidad al requisito que se desea probar

Condiciones iniciales: Estado de las variables de estado al inicio de la prueba

Entradas: Mensajes recibidos, valores de las variables o eventos que generan una respuesta del sistema

Salidas: Acciones que debe ejecutar el software. Son los resultados esperados que se deben verificar.

Comentarios: Comentarios indicando el propósito de la prueba o la justificación del caso de prueba. Puede indicarse si la prueba es normal o de robustez, o el criterio para la selección del caso de prueba.

# Plantilla procedimientos prueba manuales

<Encabezado>

[Nombre-Empresa]

[Nombre-Proyecto]

Identificador Procedimiento de Prueba: [Identificador del Procedimiento de prueba]

Autor: [Nombre autor]

Trazabilidad a versión de requerimientos de software: [ID y versión de doc. de requerimientos]

Historial de cambios:

[Borrador: fecha de desarrollo del procedimiento]

[Revisión: Fecha de cierre de la revisión del procedimiento]

[Aprobación y publicación: fecha de aprobación y publicación]

Datos de la ejecución del procedimiento

Fecha de ejecución: [fecha]

Nombre: [nombre de la persona que ejecuta el procedimiento]

Trazabilidad a versión de código: [versión de software sobre la que se ejecutó el procedimiento]

Procedimiento:

<Inicialización del ambiente de prueba: >

Paso 1: [instrucciones de inicialización]

Paso 2: [instrucciones de inicialización]

Paso 3: [instrucciones de inicialización]

.

.

.

Paso n: Verifique que [resultados esperados] [Traza hacia el identificador del caso de prueba]

Valor esperado:

Valor obtenido:

Resultado: 🞏 Pasó 🞏 Falló

.

.

Paso z: [Instrucciones de apagado o Re inicialización del ambiente de prueba]

# Lista de revisión de casos de prueba de software

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lista de verificación de los casos de prueba de software** | | | | | | |
| Nombre del proyecto: |  | Versión: |  | | | |
| No. de documento: |  | Revisor: |  | | | |
| Autor: |  | Fecha de revisión: |  | | | |
| **S=Satisface; NS=Not Satisface; N/A=No Applica.** | | | | | | |
| **Criterio** | | | | **S** | **NS** | **N/A** |
| 1. Se ofrece una breve descripción del caso de prueba | | | |  |  |  |
| 1. Los casos de prueba verifican todos los requerimientos | | | |  |  |  |
| 1. Se prueban las variables reales y enteras mediante clases de equivalencia y valores de frontera | | | |  |  |  |
| 1. Se prueban los requerimientos con expresiones booleanas mediante tablas de verdad | | | |  |  |  |
| 1. Se indican claramente los resultados esperados | | | |  |  |  |
| 1. Se prueban todas las transiciones válidas de las máquinas de estados finitos | | | |  |  |  |
| 1. Se incluyen pruebas de robustez | | | |  |  |  |
| 1. Se prueban los requerimientos de tiempo | | | |  |  |  |
| **Comentarios adicionales:** | | | | | | |
|  | | | | | | |
| Firma: | | Fecha: | | | | |
|  | |  | | | | |