
 sunarp Superintendencia Nacional de los Registros Públicos	Tipo de documento:	Codificación:
	DIRECTIVA	DI-001-2025-SUNARP-OTI
	Resolución de aprobación: Resolución N° 177-2025-SUNARP/GG	
	Fecha de aprobación: 3/10/2025	Páginas: 1/60

**DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL
CICLO DE VIDA DE DESARROLLO DE SOFTWARE
SEGURO**

 <p>sunarp Superintendencia Nacional de los Registros Públicos</p>	<p>DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO</p>	<p>Codificación: DI-001-2025-SUNARP- OTI</p>
--	---	---

Índice

I.	OBJETIVO	3
II.	FINALIDAD	3
III.	ALCANCE	3
IV.	BASE LEGAL	3
V.	DEFINICIÓN DE TÉRMINOS Y SIGLAS	4
VI.	RESPONSABILIDAD	5
VII.	DISPOSICIONES GENERALES	5
	7.1 Política para ciclo de vida de desarrollo de software seguro	5
	7.2 Antecedentes	7
	7.3 Sobre la implementación de la ISO/IEC 12207	7
	7.4 Sobre los procesos de la ISO/IEC 12207	8
	7.5 Sobre la Metodología de Ciclo de Vida de Desarrollo de Software Seguro (MCVDSS v1.0)	10
VIII.	DISPOSICIONES ESPECÍFICAS	12
	8.1 Estudio de Viabilidad del Sistema (EVS)	12
	8.2 Análisis del Sistema de Información (ASI)	15
	8.3 Diseño del Sistema de Información (DSI)	19
	8.4 Construcción del Sistema de Información (CSI)	23
	8.5 Implantación y Aceptación del Sistema de Información (IAS)	27
	8.6 Mantenimiento del Sistema de Información (MSI)	30
IX.	DISPOSICIONES COMPLEMENTARIAS	33
X.	ANEXOS	34

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

I. OBJETIVO

Regular y orientar los procesos de desarrollo, desarrollo seguro y mantenimiento de software de la SUNARP que permita cumplir con la regulación del Estado Peruano que, mediante Resolución Ministerial N° 041-2017-PCM aprueba el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 12207:2016 Ingeniería de Software y Sistemas. Procesos del ciclo de vida del software. 3ª Edición”.

II. FINALIDAD

Establecer un marco de trabajo estructurado y sistemático para la creación, evolución y mantenimiento de sistemas informáticos, garantizando la calidad del producto, la reducción de riesgos durante el desarrollo, y la eficiencia en la ejecución. Asimismo, asegurar la alineación del sistema con los requisitos del negocio, en cumplimiento de los estándares y normativas vigentes de la Institución.

III. ALCANCE


El ámbito de aplicación de la presente Metodología alcanza a todos los Órganos y Unidades Orgánicas de la Sunarp, así como a programas y proyectos relacionados a procesos de desarrollo y mantenimiento de software.

Es de cumplimiento obligatorio por todo el personal que labora en la SUNARP bajo cualquier modalidad de contrato, inclusive por proveedores y el personal de terceros que prestan servicio en la Institución.

IV. BASE LEGAL

- a) **Resolución Ministerial N° 041-2017-PCM**, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 12207:2016 - Ingeniería de Software y Sistemas. Procesos del ciclo de vida del software. 3ª Edición” en todas las entidades integrantes del Sistema Nacional de Informática, publicada el 2 de marzo del 2017.
- b) **Resolución N° 0176-2019-SUNARP/GG**, que aprueba el Manual N° MP-S06-00, “Manual de procedimientos Gestión de tecnologías de la información y Comunicación Sede Central”, publicada el 23/08/2019.
- c) **Resolución N° 0076-2024-SUNARP/GG**, que aprueba la Directiva N° DI-01-2024-SUNARP-OPPM, “Directiva para la aprobación de los Documentos Normativos de la Sunarp”, publicada el 02/05/2024.
- d) **Resolución N° 108-2024-SUNARP/SN**, que aprueba el Mapa de Procesos N° MP-OPPM-001, "Mapa de Procesos Nivel 0 de la Superintendencia Nacional de los Registros Públicos - Sunarp", publicada el 08/08/2024.
- e) **Marco de Referencia:**
 - **NTP ISO/IEC 12207:2016** Ingeniería de Software y Sistemas. Procesos del ciclo de vida del software. 3ª Edición.

La Norma Técnica Peruana NTP-ISO/IEC 12207:2016 es la adopción nacional del estándar internacional ISO/IEC 12207:2008, por lo que en adelante se les denominará ISO/IEC 12207, indistintamente.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--


- **Metodología Métrica 3**, de propiedad intelectual del Ministerio de Hacienda y Administraciones Públicas de España y puede ser utilizada libremente¹ con la única restricción de citar la fuente de su propiedad intelectual. Toma como modelo al Ciclo de Vida de Desarrollo propuesto en la norma ISO 12207 "Information technology – Software life cycle processes" dando lugar a una estructura en la que se distinguen procesos principales (Planificación, Desarrollo y Mantenimiento) e interfaces (Gestión de Proyectos, Aseguramiento de la Calidad, Seguridad y Gestión de Proyectos) cuyo objetivo es dar soporte al proyecto en los aspectos organizativos².

V. DEFINICIÓN DE TÉRMINOS Y SIGLAS

- a) **Elemento del sistema:** Miembro de un conjunto de elementos que constituyen un sistema. Un elemento del sistema es una parte separada de un sistema que se puede implementar para satisfacer requisitos específicos. Un elemento del sistema puede ser hardware, software, datos, personas, procesos (por ejemplo, procesos para proveer el servicio a los usuarios), procedimientos (por ejemplo, instrucciones del operador), instalaciones, materiales y entidades de origen natural (por ejemplo, el agua, organismos, minerales) o cualquier combinación.
- b) **Ciclo de vida del software:** Evolución de un sistema, producto, servicio, proyecto u otra entidad elaborada por el hombre desde la concepción hasta su retiro.
- c) **Clase:** Una clase describe las características de un tipo de objetos, de los que se pueden crear múltiples instancias. Las clases se pueden definir en función de objetos u otras clases definidas previamente, bien por especialización, extensión, agregación, asociación, etc. lo que reduce considerablemente la complejidad de la definición del gran número de instancias que requiere una aplicación.
- d) **Cliente:** Organización (interna/externa) o persona que recibe un producto o un servicio. Un cliente puede ser interno o externo a la organización. Otros términos que se usan comúnmente para cliente son: usuario, adquirente, comprador y consumidor.
- e) **Cobertura de la prueba:** Grado hasta el cual los casos de prueba demuestran el cumplimiento de los requisitos para el sistema o el producto de software.
- f) **Desarrollo Seguro:** Como *Interfaz de Seguridad* de la Metodología Métrica 3, tiene como objetivo integrar controles y mecanismos de seguridad complementarios que permitan prevenir vulnerabilidades, mitigar riesgos y proteger la información y el sistema. No es un proceso aislado, sino una responsabilidad transversal a lo largo de todo del ciclo de vida del proyecto.
- g) **Parte interesada:** Individuo u organización que tenga un derecho, acción, reclamo o interés en un sistema o en las que posee características que cumplen sus necesidades y expectativas.
- h) **Producto software:** Conjunto de programas de computador, procedimientos y posiblemente documentación y datos asociados.

¹ https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Metrica_v3.html#.Wbv7f5DRa70

² Fuente: "APORTACIONES DE MÉTRICA VERSIÓN 3" del documento INTRODUCCIÓN a la metodología MÉTRICA Versión 3.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

- i) **Sistema:** Combinación de elementos organizados que interactúan para lograr uno o más propósitos establecidos. Un sistema puede ser considerado como un producto o como los servicios que presta.
- j) **Software Release Management:** en castellano, **gestión de entregas de software**, es el proceso de entregas de software nuevo o de actualizaciones del software. El proceso es mucho más que crear una nueva versión o actualizar un programa. Cuando se necesita una nueva entrega hay que seguir varios pasos. Reunir las nuevas exigencias y conocer las dependencias con los componentes existentes es el primer paso. Después se puede producir la nueva versión, se le somete a prueba y se prepara la nueva entrega. La entrega que es llevada finalmente al entorno de operaciones consiste en un programa listo para ser instalado, con los manuales de uso, de diseño y pruebas.
- k) **Usuario:** Individuo o grupo que se beneficia de un sistema durante su utilización. Los roles del usuario y del operador pueden estar asignados, simultáneamente o en secuencia en el mismo individuo u organización.
- l) **Validación:** Confirmación, mediante la aportación de evidencia objetiva de que se han cumplido los requisitos para una utilización o aplicación específica prevista. La validación en un ciclo de vida es el conjunto de actividades para asegurar y obtener confianza en que un sistema es capaz de cumplir su uso previsto, las metas y los objetivos (es decir, cumplir los requisitos de las partes interesadas) en el entorno operativo.
- m) **Verificación:** Confirmación mediante la aportación de evidencia objetiva de que se han cumplido los requisitos especificados. La validación en un ciclo de vida es un conjunto de actividades que compara un sistema o elemento del sistema frente a sus requisitos. Esto puede incluir, pero no se limita, a los requisitos especificados, descripción del diseño y del propio sistema.
- n) **Versión:** Instancia identificada de un elemento. La modificación de una versión de un producto de software, que resulte en una versión nueva, requiere la gestión de la configuración.

VI. RESPONSABILIDAD

La Oficina de Tecnologías de la Información es la responsable de velar por el cumplimiento de la presente Directiva, de gestionar las plantillas o formatos de los artefactos que viabilizan su aplicación (elaboración, actualización, mejora, conservación, eliminación y accesibilidad), así como brindar asistencia técnica en la ejecución de las etapas del ciclo de vida de desarrollo de software.

VII. DISPOSICIONES GENERALES

7.1 Política para ciclo de vida de desarrollo de software seguro

[Referencia: ISO/IEC 27002:2022 capacidad operativa #Seguridad de aplicaciones]

- a. La Sunarp, en lo posible, se compromete a garantizar que todo software desarrollado, o mantenido cumpla con principios de **seguridad por diseño, seguridad por defecto y mejora continua**, asegurando que los requisitos de **confidencialidad, integridad, disponibilidad, trazabilidad y conformidad normativa** se encuentren integrados en todas las fases del Ciclo de Vida de Desarrollo de Software (CVDS).

b. **Procedimientos operativos documentados**

[ISO/IEC 27001:2022 control 5.37]

Todos los procesos relacionados con el desarrollo, despliegue, mantenimiento y cambios de software deberán estar **documentados, actualizados y disponibles** para el personal autorizado, garantizando la continuidad operativa y la trazabilidad de la seguridad.

c. **Acceso al código fuente**

[ISO/IEC 27001:2022 control 8.4]

El **acceso a los repositorios de código fuente y configuración** estará restringido, gestionado mediante autenticación fuerte y segregación de roles, con registro y monitoreo de toda actividad, para preservar la integridad del software.

d. **Control de utilidades privilegiadas**

[ISO/IEC 27001:2022 control 8.18]

Las **utilidades y herramientas privilegiadas** que puedan anular controles de seguridad deberían estar identificadas, restringidas a cuentas autorizadas y sujetas a monitoreo continuo para evitar uso indebido.

e. **Instalación de software en sistemas operativos**

[ISO/IEC 27001:2022 control 8.19]

La **instalación, actualización y mantenimiento de software** en entornos operativos se realizará únicamente mediante procedimientos autorizados, bajo un esquema de listas blancas y control de integridad.

f. **Reglas para el ciclo de vida de desarrollo seguro**

[ISO/IEC 27001:2022 control 8.25]

Todo desarrollo procurará seguir reglas de **CVDS seguro**, asegurando la integración de controles de seguridad desde las fases de análisis y diseño hasta pruebas, implantación y mantenimiento.

g. **Requisitos de seguridad de la aplicación**

[ISO/IEC 27001:2022 control 8.26]

Los **requisitos de seguridad funcionales y no funcionales** deberán ser identificados, documentados y validados antes del inicio del diseño, manteniendo trazabilidad hacia pruebas y aceptación.

h. **Principios de ingeniería y arquitectura segura**


[ISO/IEC 27001:2022 control 8.27]

Se podrán establecer y aplicar **principios de ingeniería y arquitectura segura** que orienten la construcción de software confiable, resiliente y alineado con buenas prácticas internacionales.

i. **Codificación segura**

[ISO/IEC 27001:2022 control 8.28]

Se adoptarán **estándares y guías de codificación segura** para cada lenguaje, y, en lo posible, aplicar revisiones de código, análisis estático/dinámico y gestión segura de dependencias.

 <p>sunarp Superintendencia Nacional de las Regiones Públicas</p>	<p>DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO</p>	<p>Codificación: DI-001-2025-SUNARP-OTI</p>
---	---	--

j. Pruebas de seguridad en desarrollo y aceptación

[ISO/IEC 27001:2022 control 8.29]

Todas las aplicaciones podrán estar sujetas a **pruebas de seguridad planificadas**, incluyendo análisis de vulnerabilidades, pruebas de penetración y validación de controles antes de su liberación.

k. Desarrollo tercerizado

[ISO/IEC 27001:2022 control 8.30]

Los contratos con proveedores de software deberán incluir **cláusulas de seguridad**, evidencias de prácticas seguras, revisiones de código, y garantías contra la inclusión de código malicioso o funcionalidades no autorizadas.

l. Separación de entornos de desarrollo, prueba y producción

[ISO/IEC 27001:2022 control 8.31]

Los **entornos de desarrollo, prueba y producción** estarán segregados física y/o lógicamente, con controles de acceso diferenciados y protección de datos sensibles.

m. Gestión de cambios

[ISO/IEC 27001:2022 control 8.32]

Todos los cambios en el software y sus componentes estarán sujetos a un **proceso de gestión de cambios**, que incluirá planificación, autorización, pruebas de aceptación, documentación y posibilidad de retorno atrás (*rollback*).

7.2 Antecedentes

El Estado Peruano, mediante Resolución Ministerial N° 041-2017-PCM, de fecha 27/02/2017, aprobó el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 12207:2016- Ingeniería de Software y Sistemas. Procesos del ciclo de vida del Software. 3ª Edición”, en todas las entidades del Sistema Nacional de Informática.

7.3 Sobre la implementación de la ISO/IEC 12207


Respecto a la implementación o utilización, la norma ISO/IEC 12207 menciona textualmente lo siguiente (los subrayados son adicionados):

“INTRODUCCIÓN

(...)

Esta Norma se puede utilizar en uno o más de los siguientes modos:

- **Por una organización** - para ayudar a establecer un entorno de procesos deseados. *Estos procesos pueden ser soportados por una infraestructura de métodos, procedimientos, técnicas, herramientas y personal capacitado. La organización puede emplear este medio para realizar y gestionar sus proyectos y el progreso de sus sistemas a través de las fases de su ciclo de vida. En este modo, esta Norma se utiliza para evaluar la conformidad de un conjunto declarado y establecido de procesos del ciclo de vida para su disposición.*
- **Por un proyecto** - para ayudar a seleccionar, estructurar y emplear los elementos de un conjunto establecido de procesos del ciclo de vida para proporcionar productos y servicios. *En este modo, Esta Norma se utiliza en la evaluación de la conformidad del proyecto para el entorno declarado y establecido.*
- **Por un adquirente y un proveedor** - para ayudar a elaborar un acuerdo relacionado a procesos y actividades. *A través del acuerdo; los procesos y actividades en esta norma se seleccionan, negocian, acuerdan y ejecutan. En este modo, esta norma se utiliza para la orientación en el desarrollo del acuerdo.*

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

- **Por organizaciones y evaluadores** - para realizar evaluaciones que se pueden utilizar para apoyar la mejora del proceso organizacional.”

(...)

2 CONFORMIDAD

2.1 Propósito de uso

(...) Esta norma establece los requisitos para una serie de procesos adecuados para su utilización durante el ciclo de vida de un producto o un servicio software. Se reconoce que proyectos u organizaciones en particular pueden no necesitar utilizar todos los procesos proporcionados por esta norma. Por lo tanto, la implementación de esta Norma usualmente consiste en seleccionar un conjunto de procesos adecuados para la organización o proyecto. Hay dos maneras en que una implementación puede ser declarada conforme a los requisitos de esta Norma.

Cualquier declaración de conformidad está descrita en una de las dos siguientes formas.

2.2 Conformidad completa

Una declaración de conformidad completa indica el conjunto de procesos para el cual la conformidad es concedida. La conformidad completa se logra mediante la demostración de que todos los requisitos del conjunto de procesos declarados han sido cumplidos usando los resultados como evidencia.

2.3 Conformidad a medida

Cuando esta Norma se utiliza como base para el establecimiento de un conjunto de procesos que no reúnen los requisitos para la conformidad completa, los capítulos de esta norma se seleccionan o modifican de acuerdo con el proceso de adaptación prescrito en el Anexo A. El texto adaptado, por el cual se declara la conformidad a medida, se anuncia. La conformidad a medida se logra demostrando que los requisitos para los procesos a medida, se han cumplido usando los resultados como evidencia.

(...)”

En la presente Directiva, la Sunarp implementa la ISO/IEC 12207 en **Conformidad a medida**, estableciendo el conjunto de procesos seleccionados, así como los procedimientos y sus respectivos artefactos (herramientas).

Los artefactos de los procesos seleccionados serán establecidos para cada proyecto de desarrollo o mantenimiento en el Acta de Aplicabilidad, en caso de que el informe del estudio de viabilidad tenga conclusión favorable.

7.4 Sobre los procesos de la ISO/IEC 12207

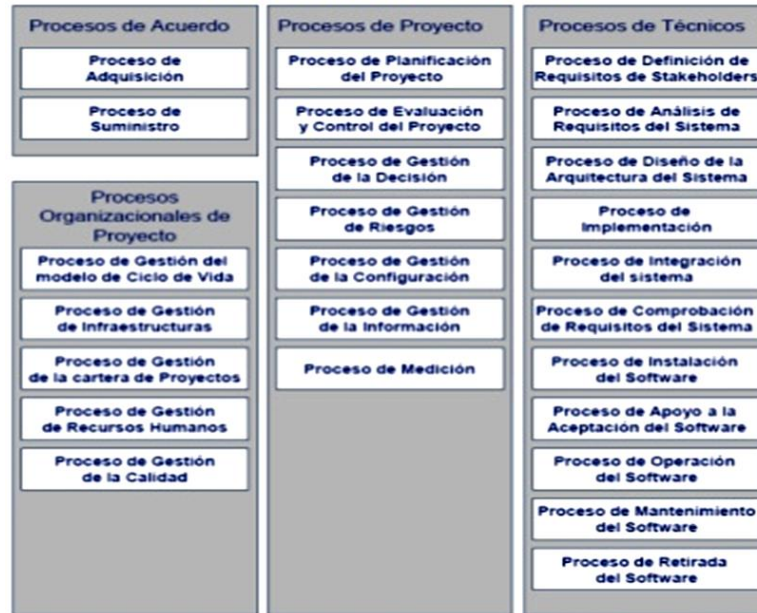
La Norma Técnica Peruana (NTP) ISO/IEC 12207 es un estándar internacional adoptado por el Estado Peruano, que establece un marco de trabajo común para los procesos del ciclo de vida del software y contiene procesos, actividades y tareas que son aplicables durante la adquisición de un producto o servicio de software y durante el suministro, desarrollo, operación, mantenimiento y disposición de los productos software ya sea que se ejecute interna o externamente a una organización.

Incluye aspectos de la definición del sistema, necesarios para proporcionar el contexto para los productos y servicios software. Asimismo, proporciona un proceso que se puede emplear para definir, controlar y mejorar los procesos del ciclo de vida del software.

Esta norma comprende 43 procesos que se agrupan en las siguientes categorías:

- Procesos del Ciclo de Vida del Sistema,
- Procesos del Ciclo de Vida del Software.

Procesos del Contexto del Sistema




Procesos Específicos del Software



Sin embargo, tiene las siguientes limitaciones³:

- Esta Norma no detalla los procesos del ciclo de vida en términos de métodos o procedimientos que se requieren para cumplir los requisitos y resultados de un proceso.
- Esta Norma no detalla la documentación en términos de nombre, formato, contenido explícito ni medios de registro. La Norma puede requerir el desarrollo de documentos de similar clase o tipo; varios planes son un ejemplo. Sin embargo, esta Norma no implica que tales documentos se desarrollen o

³ Extraído literalmente de la cláusula 1.3 *Limitaciones* de la NTP ISO/IEC 12207:2016.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

empaqueten por separado o combinados de alguna manera. Estas decisiones se dejan al usuario de esta Norma.

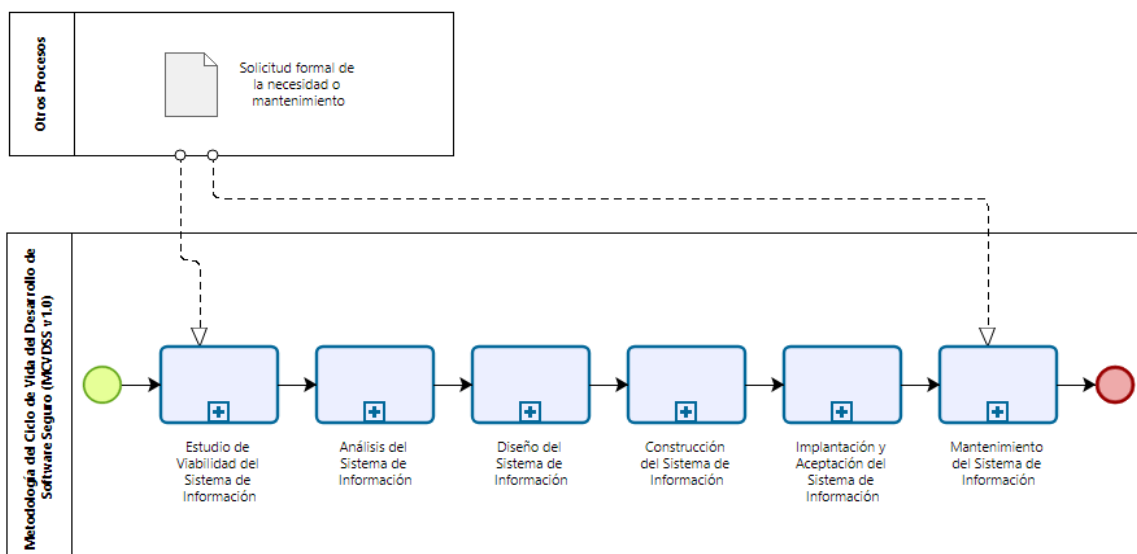
- Esta Norma no establece de manera específica un modelo de ciclo de vida, metodología de desarrollo, método, modelo o técnica de sistema o software. Las partes interesadas de la Norma son responsables de seleccionar un modelo de ciclo de vida para el proyecto software y de mapear los procesos, actividades y las tareas de esta Norma, para dicho modelo.

7.5 Sobre la Metodología de Ciclo de Vida de Desarrollo de Software Seguro (MCVDSS v1.0)

Con el fin de viabilizar la aplicación metodológica de la ISO/IEC 12207 y sus procesos, se adopta como modelo operativo la metodología Métrica Versión 3, la cual proporciona una herramienta eficaz para sistematizar las actividades que dan soporte al ciclo de vida del software. Esta se complementa con el enfoque de Desarrollo Seguro, que incorpora medidas y controles orientados a garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información y del sistema. Esta integración permite alcanzar los siguientes objetivos:


- Productos software que satisfagan las necesidades de los usuarios dando una mayor importancia al análisis de requisitos.
- Mejorar la productividad del área de Sistemas y Tecnologías de la Información, permitiendo una mayor capacidad de adaptación a los cambios y teniendo en cuenta la reutilización en la medida de lo posible.
- Facilitar la comunicación y entendimiento entre los distintos participantes en la producción de software a lo largo del ciclo de vida del proyecto, teniendo en cuenta su papel y responsabilidad, así como las necesidades de todos y cada uno de ellos.
- Facilitar la operación, mantenimiento y uso de los productos software obtenido.
- Integrar prácticas de seguridad en cada fase del ciclo de vida para prevenir vulnerabilidades y mitigar riesgos de seguridad.
- Incorporar durante la fase de desarrollo las funciones y mecanismos que refuerzan la seguridad del nuevo sistema y del propio proceso de desarrollo, asegurando su consistencia y seguridad.

En ese sentido, el proceso de la presente Metodología de Ciclo de Vida de Desarrollo de Software Seguro (MCVDSS v1.0) es el siguiente:



El alineamiento a la normativa vigente, materia de cumplimiento legal, será el siguiente:

Procesos de la OGTI (Resoluciones N° 0108-2024-SUNARP/SN y N° 176-2019-SUNARP/GG)		Procesos de la MCVDS v1.0 de la Sunarp	Procesos de Metodología Métrica 3	Procesos de la ISO/IEC 12207 (Resolución Ministerial N° 041-2017-PCM)	
NIVEL 0: S06 Gestión de Tecnologías de la Información y Comunicación	NIVEL 1: S06.02 Administración de TICs	NIVEL 2: S06.02.01 Ingeniería de software y Gestión del cambio de TICs	8.1. Estudio de Viabilidad del Sistema (EVS)	3. Proceso de Estudio de Viabilidad del Sistema	7.1.1. Proceso de Implementación del Software
			8.2. Análisis del Sistema de Información (ASI)	4. Proceso de Análisis del Sistema de Información	7.1.2. Proceso de Análisis de Requisitos del Software
			8.3. Diseño del Sistema de Información (DSI)	5. Proceso de Diseño del Sistema de Información	7.1.3. Proceso de Diseño Arquitectural del Software
			8.4. Construcción del Sistema de Información (CSI)	6. Construcción del Sistema de Información	7.1.4. Proceso de Diseño Detallado del Software
					7.1.5. Proceso de Construcción del Software
					7.1.6. Proceso de Integración del Software
8.5. Implantación y Aceptación del Sistema (IAS)	7. Implantación y Aceptación del Sistema	7.1.7. Proceso de Pruebas de Calificación del Software	6.4.7. Proceso de Instalación del Software		

 <p>sunarp Superintendencia Nacional de los Registros Públicos</p>	<p align="center">DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO</p>	<p>Codificación: DI-001-2025-SUNARP-OTI</p>
--	--	--

Procesos de la OGTI (Resoluciones N° 0108-2024-SUNARP/SN y N° 176-2019-SUNARP/GG)	Procesos de la MCV DSS v1.0 de la Sunarp	Procesos de Metodología Métrica 3	Procesos de la ISO/IEC 12207 (Resolución Ministerial N° 041-2017-PCM)
			6.4.8. Proceso de Soporte de la Aceptación del Software
	NIVEL 2: S06.03 Soporte de TICs	8.6. Mantenimiento de Sistemas de Información (MSI)	6..10. Proceso de Mantenimiento del Software

VIII. DISPOSICIONES ESPECÍFICAS

La descripción de los subprocesos del presente procedimiento o Metodología de Ciclo de Vida de Desarrollo de Software Seguro (MCVDSS v1.0) es el siguiente:

8.1 Estudio de Viabilidad del Sistema (EVS)

8.1.1 Propósito


El propósito del proceso del Estudio de Viabilidad del Sistema (EVS), es analizar un conjunto concreto de necesidades para proponer una solución a corto plazo, que tenga en cuenta restricciones técnicas y operativas. La solución obtenida como resultado del estudio puede ser la definición de uno o varios proyectos que afecten a uno o varios sistemas de información ya existentes o nuevos. Para ello, se identifican los requisitos que se deben satisfacer y se evalúa si su atención procede en la situación actual.

La solución obtenida puede implicar desarrollos a medida, soluciones basadas en la adquisición de productos software del mercado o soluciones mixtas, y desarrollos ejecutados por un tercero.

El propósito de la Interfaz de Seguridad en el proceso del Estudio de Viabilidad del Sistema (EVS), tiene como objetivo incorporar mecanismos complementarios de protección a los definidos en la metodología base, garantizando que el desarrollo de cualquier tipo de sistema se realice con un enfoque preventivo y alineado a los principios fundamentales de la seguridad de la información: autenticación, confidencialidad, integridad y disponibilidad (ACID). Esta interfaz permite que la seguridad sea considerada desde las fases iniciales del proyecto, integrando directrices y recomendaciones específicas que orienten el diseño, desarrollo e implantación de sistemas seguros por defecto.

8.1.2 Resultados

Nº	Descripción del Resultado
1.	Se define y establece el alcance de la solicitud de desarrollo o mantenimiento.
2.	Se definen y establecen los requisitos asignados a los elementos del software del sistema y sus interfaces, con el cliente.

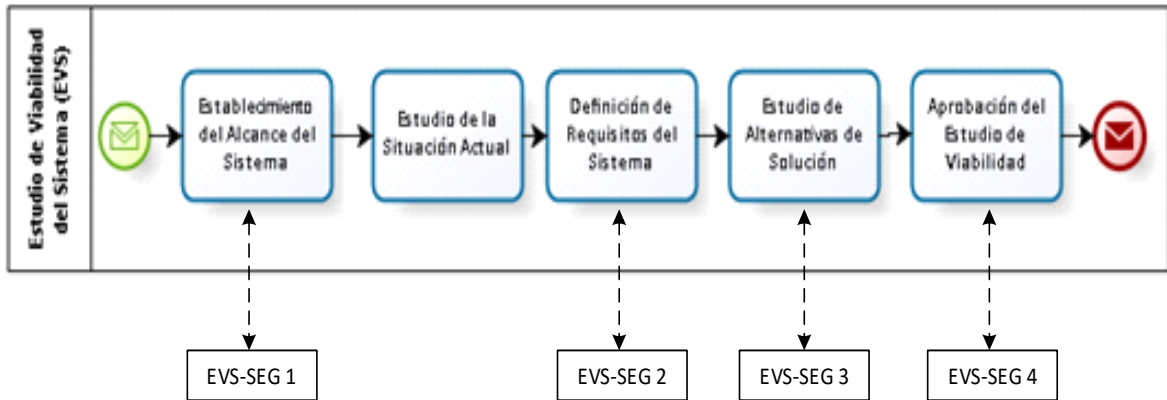
	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Nº	Descripción del Resultado
3.	Se evalúan la viabilidad económica, técnica, legal y operativa.
4.	Se estudia la priorización de los requisitos del software y la alternativa de solución.
5.	Se aprueba los requisitos de desarrollo y/o mantenimiento de software y la alternativa de solución propuesta.
6.	Se analizan las amenazas y vulnerabilidades de cada solución propuesta.
7.	Se recomiendan mecanismos de salvaguarda (preventivos, detectivos, correctivos).
8.	Se conforma el equipo de seguridad que participará en las siguientes fases del proyecto.
9.	Se definen recomendaciones de seguridad para el sistema, basadas en el umbral de riesgo aceptado y en el estudio de amenazas y vulnerabilidades
10.	Se establece el control de la seguridad tanto a nivel de ejecución de actividades como de los productos obtenidos (niveles de autenticación, confidencialidad, integridad y disponibilidad)
11.	Se detalla el estudio de riesgos, la especificación de funciones de seguridad y los mecanismos de seguridad
12.	Se establece la catalogación y archivo de los productos en función de su nivel de seguridad, considerando el soporte de almacenamiento y el sistema de gestión de configuración de la organización
13.	Se clasifica la sensibilización de los documentos y modelos generados.

8.1.3 Roles


Abrev. Rol	Descripción del Rol
AF	Analista Funcional
DOC	Documentador
J-TI	Jefe de la OTI
UL	Usuario Líder (Jefe del usuario o su representante)
UE	Usuario(s) Experto(s)
AAI	Analista de Aseguramiento de la Información
AS	Analista(s) de Sistemas
RS	Responsable de Seguridad
ES	Especialista de Seguridad

8.1.4 Diagrama del Subproceso



8.1.5 Lista de Actividades y Tareas

Nº	Actividad	Tareas	Responsable	Participantes
A1.	Recibir la solicitud formal de necesidad	Asignar el responsable del estudio de viabilidad (AF)	AS	---
A2.	Establecimiento del Alcance del Sistema (EVS1)	Estudio de la Solicitud	AF	DOC, UL, UE
		Identificación del alcance del Sistema		
		Catalogar los usuarios participantes (forma parte del Catálogo de Requisitos).		
		Estudio de la Seguridad requerida en el proceso	RS	ES
		Selección del equipo de Seguridad		
A3.	Estudio de la Situación Actual (EVS2)	Estudio de la situación actual de los procesos y sistemas del negocio.	AF	AS
A4.	Definición de Requisitos del Sistema (EVS3)	Identificación de normativa del negocio y estándares técnicos, aplicables.	AF	DOC, UL, UE
		Identificación y catalogación de requisitos (Catálogo de Requisitos).		
		Elaboración de recomendaciones adicionales de Seguridad	RS	ES
A5.	Estudio de Alternativas de Solución (EVS4, EVS5 y EVS6)	Descripción, evaluación y selección de la alternativa de solución.	AS	AF, UL, UE
		Validación y Evaluación de la Seguridad de las alternativas de solución	RS	ES
A6.		Presentación y aprobación del Informe de Viabilidad	AS	J-TI, AF, UL

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Nº	Actividad	Tareas	Responsable	Participantes
	Aprobación del Estudio de Viabilidad	Descripción detallada de la Seguridad de la solución propuesta Clasificación y catalogación de los productos de Seguridad	RS	ES
A7.	<i>En caso de que el informe del estudio de viabilidad tenga conclusión favorable:</i> Acta de Aplicabilidad de la MCVDS	Elaboración y firma del Acta de Aplicabilidad de la MCVDS	AS	DOC, AAI

8.1.6 Artefactos

De entrada		De salida	
Código Formato	Descripción	Código Formato	Descripción
MCVDSS-0001	Solicitud formal	MCVDSS-EVS-0101	Informe de Viabilidad Técnica
		MCVDSS-00002	Acta(s) de Reunión(es)
		MCVDSS-EVS-0102	Catálogo de Requisitos
		MCVDSS-EVS-0103	Acta de Aplicabilidad de la MCVDS

8.2 Análisis del Sistema de Información (ASI)

8.2.1 Propósito

El propósito del proceso de Análisis del Sistema de Información (ASI) es la obtención de una especificación detallada del sistema de información que satisfaga las necesidades de información de los usuarios y sirva de base para el posterior diseño del sistema.


El propósito de la Interfaz de Seguridad en el proceso de Análisis del Sistema de Información (ASI) tiene como objetivo incorporar desde esta fase las funciones y mecanismos de seguridad necesarios para garantizar la protección del sistema de información frente a riesgos lógicos (como ataques externos, fallos o virus). Esto implica identificar, analizar y definir los requisitos de seguridad que deben implementarse, asegurando que el sistema cumpla con los estándares de seguridad y la política de la organización, facilitando la construcción de un sistema seguro y confiable.

8.2.2 Resultados

Nº	Descripción del Resultado
1.	Descripción inicial del sistema de información. Se delimita el alcance del sistema, se genera un catálogo de requisitos generales y se describe el sistema mediante unos modelos iniciales de alto nivel. Se elabora el plan de trabajo a seguir.
2.	Se define los requisitos del nuevo sistema y se actualiza el catálogo de requisitos detallado, que permita describir con precisión el sistema de información.
3.	Se identifica Subsistemas de Análisis.
4.	Se analiza los Casos de Uso.
5.	Se analiza las Clases.
6.	Se elabora el Modelo de Datos.
7.	Se define las Interfaces de Usuario.
8.	Se establece el control de la seguridad tanto a nivel de ejecución de actividades como de los productos obtenidos
9.	Se analiza si la modelación de procesos implica tratamiento de información sensible.
10.	Se identifican requisitos de seguridad derivados de los requisitos funcionales
11.	Se analiza la protección de la integridad y confidencialidad de los datos modelados.
12.	Se definen medidas de control de acceso, cifrado, trazabilidad, validación y sesiones en las interfaces.
13.	Se define la inclusión de pruebas específicas para validar mecanismos de seguridad implementados
14.	Se clasifican los productos (diagramas, documentos, especificaciones) por nivel de seguridad (ACID) y establecen controles de archivo
15.	Se identifican atributos sensibles y definir necesidades de protección (integridad, confidencialidad).

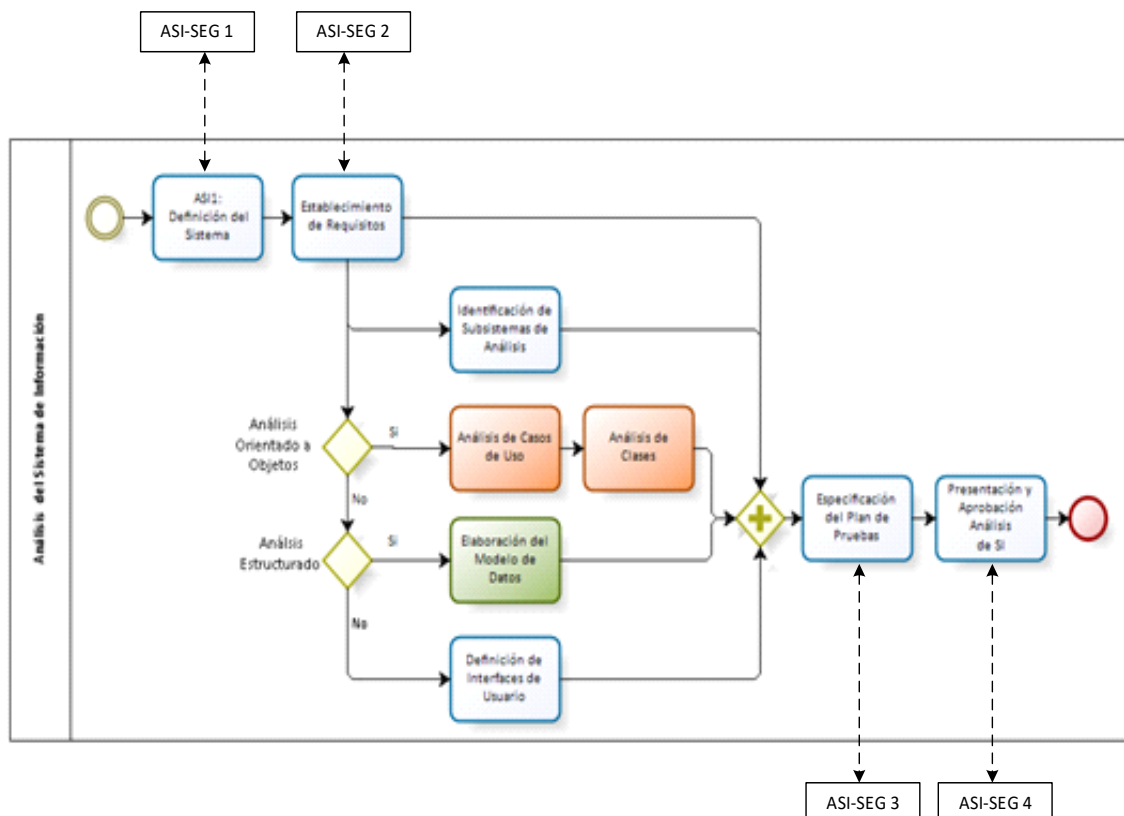
8.2.3 Roles

Abrev. Rol	Descripción del Rol
AF	Analista Funcional
AS	Analista(s) de Sistemas
ADS	Administrador de Servidores
ABD	Administrador de Base de Datos
DOC	Documentador
J-TI	Jefe de la OGTI
J-P	Jefe de Proyecto
UL	Usuario Líder (Jefe del usuario o su representante)
UE	Usuario(s) Experto(s)

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación:
		DI-001-2025-SUNARP-OTI

RS	Responsable de Seguridad
ES	Especialista de Seguridad

8.2.4 Diagrama del Subproceso



8.2.5 Lista de Actividades y Tareas

Nº	Actividad	Tareas	Responsable	Participantes
A1	Definición del Sistema (ASI1)	Determinación del Alcance del Sistema	AF	AS, UL
		Identificación del Entorno Tecnológico		AS, ADS, ABD
		Actualizar el Catálogo de Usuarios Participantes finales (CUP)		AS, UL
		Estudio de la Seguridad requerida en el análisis	RS	ES
A2	Establecimiento de Requisitos (ASI2)	Obtención de Requisitos (detallado)	AF	AS, UE
		Especificación de Casos de Uso		
		Validación de Requisitos		
		Descripción de las funciones y mecanismos de Seguridad	RS	ES

Nº	Actividad	Tareas	Responsable	Participantes
A3	Identificación de Subsistemas de Análisis (ASI3)	<p>Determinación de Subsistemas de Análisis:</p> <p>a) Identificar y definir las dependencias entre subsistemas.</p> <p>b) Especificar la interfaz de los subsistemas de análisis.</p> <p>c) Definir el comportamiento del sistema.</p> <p>d) Asignar Requisitos y Casos de Uso a cada uno de los Subsistemas identificados actualizando el catálogo de requisitos.</p> <p>Integración de Subsistemas de Análisis: Asegurar la ausencia de duplicidad de elementos y la precisión en la utilización de los términos del glosario para tener una visión global y unificada de los distintos modelos</p>	J-P	AF, AS
A4	<i>En el caso de Análisis Orientado a Objetos:</i> Análisis de Casos de Uso (ASI4)	<p>Identificar las Clases asociadas a los Casos de Uso</p> <p>Análisis de la Realización de los Casos de Uso</p>	J-P	AS
A5	<i>En el caso de Análisis Orientado a Objetos:</i> Análisis de Clases (ASI5)	<p>Identificación de Responsabilidades y Atributos</p> <p>Identificación de Asociaciones y Agregaciones</p> <p>Identificación de Generalizaciones</p>	J-P	AS
A6	<i>En el caso de Análisis Estructurado:</i> Elaboración del Modelo de Datos (ASI6)	<p>Elaboración del Modelo Conceptual de Datos</p> <p>Elaboración del Modelo Lógico de Datos</p> <p>Normalización del Modelo Lógico de Datos</p> <p>Especificación de Necesidades de Migración de Datos y Carga Inicial</p>	J-P	AS, UE
A7	Definición de Interfaces de Usuario (ASI8)	<p>Especificación de Principios Generales de la Interfaz</p> <p>Especificación del Comportamiento Dinámico de la Interfaz</p> <p>Especificación de Formatos de Impresión</p>	J-P	AS, UE
A8	Especificación del Plan de Pruebas (ASI10)	<p>Definición del Alcance de las Pruebas</p> <p>Definición de Requisitos del Entorno de Pruebas</p> <p>Definición de las Pruebas de Aceptación del Sistema</p> <p>Actualización del Plan de Pruebas</p>	J-P RS	AS, UE ES
A9		Presentación y aprobación del Documento de Análisis	AS	J-TI, J-P, UL

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Nº	Actividad	Tareas	Responsable	Participantes
	Presentación y Aprobación del Análisis del Sistema de Información (ASI11)	Clasificación y Catalogación de productos generados	RS	ES

Nota: La codificación ASI hace referencia a las actividades descritas en la metodología MÉTRICA Versión 3.

8.2.6 Artefactos


De entrada		De salida	
Código Formato	Descripción	Código Formato	Descripción
MCVDSS-EVS-0101	Informe de Viabilidad	MCVDSS-0002	Acta(s) de Reunión(es)
MCVDSS-EVS-0102	Catálogo de Requisitos	MCVDSS-ASI-0201	Documento de Análisis
		MCVDSS-EVS-0102	Catálogo de Requisitos (actualizado)
		MCVDSS-ASI-0202	Plan de Pruebas del Sistema
		MCVDSS-ASI-0203	Casos de Pruebas del Sistema
		MCVDSS-ASI-0204	Acta Aprobación del Prototipo del Sistema

8.3 Diseño del Sistema de Información (DSI)

8.3.1 Propósito

El propósito del proceso de Diseño del Sistema de Información (DSI) es la definición de la arquitectura del sistema y del entorno tecnológico que le va a dar soporte, junto con la especificación detallada de los componentes del sistema de información. A partir de dicha información, se generan todas las especificaciones de construcción relativas al propio sistema, así como la descripción técnica del plan de pruebas, la definición de los requisitos de implantación y el diseño de los procedimientos de migración y carga inicial, éstos últimos cuando proceda.

El propósito de la Interfaz de Seguridad en el proceso de Diseño del Sistema de Información (DSI) tiene como objetivo definir de manera detallada las funciones y mecanismos de seguridad que deben incorporarse en la arquitectura y el entorno tecnológico del sistema, asegurando que se minimicen o eliminen los riesgos lógicos identificados en fases anteriores. Esto implica traducir los requisitos de seguridad en especificaciones concretas que guíen la construcción del sistema, garantizando la coherencia con la política de seguridad de la organización y reforzando la protección del sistema y del proceso de desarrollo.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

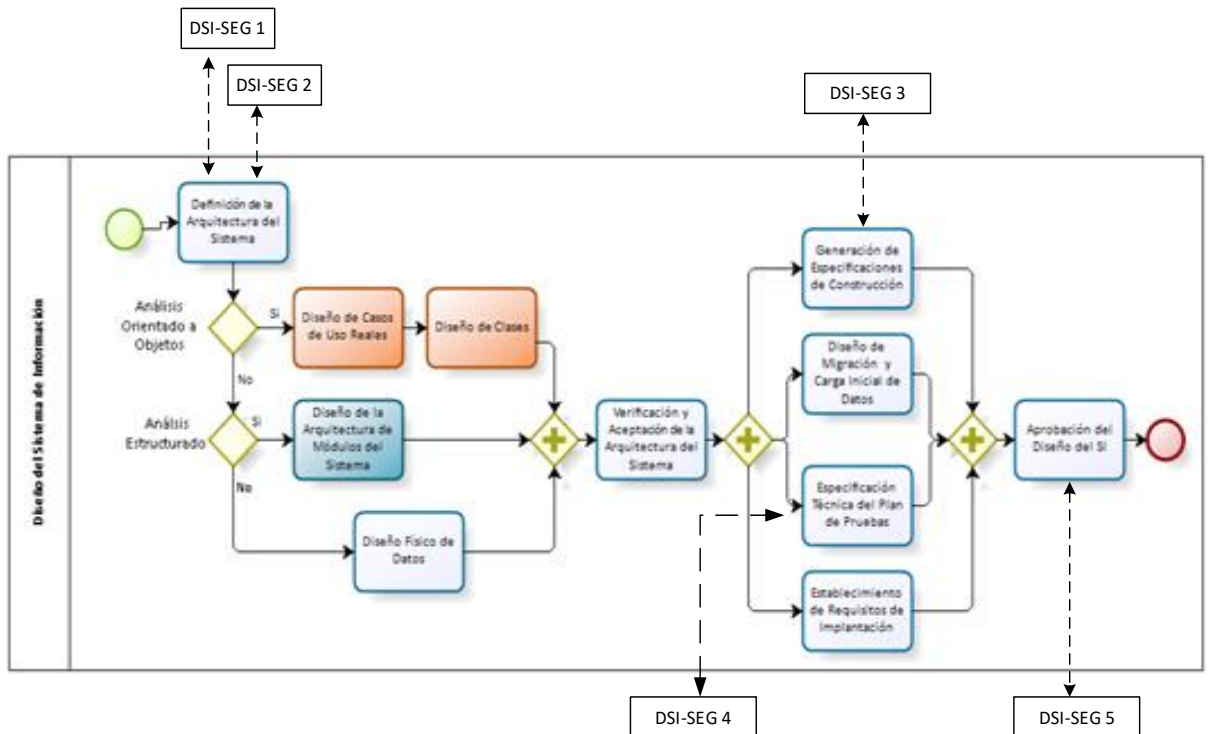
8.3.2 Resultados

Nº	Descripción del Resultado
1.	Se desarrolla, cumpliendo con la línea base, el diseño de arquitectura software que describe los elementos software que implementan los requerimientos.
2.	Se definen interfaces internas y externas para cada elemento del software.
3.	Se desarrolla un diseño detallado que describe las unidades del software que se pueden construir y probar.
4.	Se establecen la consistencia y correspondencia entre los requerimientos del software y el diseño del software.
5.	Se identifican condiciones de seguridad necesarias en el entorno de desarrollo (control de acceso, backups, entornos segregados)
6.	Se integran pruebas de seguridad en los planes de prueba: autenticación, integridad, ataques
7.	Se clasifican los documentos de diseño según nivel de seguridad (confidencial, inter SI no, restringido)
8.	Se detalla la arquitectura de seguridad del sistema incluyendo funciones y mecanismos de seguridad
9.	Se documentan los requisitos no funcionales relacionados con la seguridad

8.3.3 Roles

Abrev. Rol	Descripción del Rol
AF	Analista Funcional
AS	Analista(s) de Sistemas
ADS	Administrador de Servidores
ABD	Administrador de Base de Datos
DOC	Documentador
J-TI	Jefe de la OGTI
J-P	Jefe de Proyecto
UL	Usuario Líder (Jefe del usuario o su representante)
UE	Usuario(s) Experto(s)
AQA	Analista de Aseguramiento de la Calidad
EA	Especialista de Arquitectura
RS	Responsable de Seguridad
ES	Especialista de Seguridad


8.3.4 Diagrama del Subproceso



8.3.5 Lista de Actividades y Tareas

Nº	Actividad	Tareas	Responsable	Participantes
A1.	Definición de la Arquitectura del Sistema (DSI1)	Definición de niveles de arquitectura.	AS	EA, ES, DOC
		Identificación de Requisitos de Diseño y Construcción		
		Especificación de Excepciones.		
		Identificación de subsistemas de diseño funcionales y de soporte.		
		Especificación del Entorno Tecnológico		
		Especificación de Requisitos de Operación y Seguridad		
		Estudio de la Seguridad requerida en el diseño	RS	ES
Análisis de riesgos del entorno tecnológico				
A2.	<i>En el caso de Análisis Orientado a Objetos:</i> Diseño de Casos de Uso Reales (DSI3)	Diseño de la realización de los casos de uso	AS	UE
		a) Generar el diagrama de secuencia correspondiente a cada caso de uso.		
		b) Generar el diagrama de estado requerido para el caso de uso.		
	Revisión de la Interfaz de Usuario		EA, UE	
	Revisión de Subsistemas de Diseño e Interfaces			
A3.		Identificación de Clases Adicionales	AS	J-P, DOC

Nº	Actividad	Tareas	Respo nsable	Participa ntes
	<i>En el caso de Análisis Orientado a Objetos:</i> Diseño de Clases (DSI4)	Diseño de Asociaciones y Agregaciones		DOC, UE
		Identificación de Atributos de las Clases		
		Identificación de Operaciones de las Clases		
		Diseño de la Jerarquía		
		Descripción de Métodos de las Operaciones		
		Especificación de Necesidades de Migración y Carga Inicial de Datos		
A4.	<i>En el caso de Análisis Estructurado:</i> Diseño de la Arquitectura de Módulos del Sistema (DSI5)	Diseño de Módulos del Sistema	AS	J-P
		Diseño de Comunicaciones entre Módulos		
		Revisión de la Interfaz de Usuario		
A5.	Diseño Físico de Datos (DSI6)	Diseño del modelo físico de datos.	AS	J-P, EA, ABD
		Especificación del diccionario de bases de datos.		J-P, ES
		Optimización del modelo físico de datos.		J-P, EA, ES, ABD
		Especificación de la Distribución de Datos		J-P, EA
A6.	Verificación y Aceptación de la Arquitectura del Sistema (DSI7)	Verificación de las Especificaciones de Diseño	AS	RDS, ABD
		Análisis de Consistencia de las Especificaciones de Diseño		J-P, EA
		Aceptación de la Arquitectura del Sistema	J-P	AS
A7.	Generación de Especificaciones de Construcción (DSI8)	Especificación del Entorno de Construcción	AS	J-P, EA, ES, DOC
		Definición de Componentes y Subsistemas de Construcción		J-P, EA
		Elaboración de Especificaciones de Construcción		J-P
		Elaboración de Especificaciones del Modelo Físico de Datos	J-P, ABD	
		Identificación de Requisitos de Seguridad del entorno de construcción	RS	ES
A8.	Diseño de Migración y Carga Inicial de Datos (DSI9)	Especificación del Entorno de Migración	J-P	AS, EA, ES
		Diseño de Procedimientos de Migración y Carga Inicial		AS, EA
		Diseño Detallado de Componentes de Migración y Carga Inicial		AS
A9.	Especificación Técnica del Plan	Actualización del plan de pruebas: a) 1.- Estrategia de pruebas b) 2.- Cronograma	J-P	AS, EA, ES, AQA

 sunarp <small>Superintendencia Nacional de los Registros Públicos</small>	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Nº	Actividad	Tareas	Responsable	Participantes
	de Pruebas (DSI10)	c) 3.- Recursos, entre otros. Especificación de los casos de pruebas.		AQA, UE
A10.	Establecimiento de Requisitos de Implantación (DSI11)	Especificación de requisitos de documentación de usuario Especificación de Requisitos de Implantación Diseño de las pruebas de Seguridad	J-P	DOC, AS, UL, UE UL
A11.	Aprobación del Diseño del Sistema (DSI12)	Presentación y aprobación del diseño del sistema de información Clasificación y catalogación de productos de Seguridad generados	AS RS	J-TI, UL ES

Nota: La codificación DSI hace referencia a las actividades descritas en la metodología MÉTRICA Versión 3.

8.3.6 Artefactos

De entrada		De salida	
Código Formato	Descripción	Código Formato	Descripción
MCVDSS-ASI-0201	Documento de Análisis del Sistema	MCVDSS-DSI-0301	Documento de Diseño del Sistema
MCVDSS-EVS-0102	Catálogo de Requisitos	MCVDSS-00002	Acta(s) de Reunión(es)
MCVDSS-ASI-0202	Plan de Pruebas del Sistema	MCVDSS-EVS-0102	Catálogo de Requisitos (actualizado)
		MCVDSS-DSI-0302	Matriz de Trazabilidad
		MCVDSS-DSI-0303	Plan de Integración del Sistema
		MCVDSS-DSI-0304	Plan de Migración y Carga del Sistema
		MCVDSS-ASI-0202	Plan de Pruebas del Sistema (actualizado)

8.4 Construcción del Sistema de Información (CSI)

8.4.1 Propósito

El propósito del proceso de la Construcción del Sistema de Información (CSI) es generar el código de los componentes del Sistema de Información que reflejen de manera correcta el diseño del software y se elaboran todos los manuales de usuario final y de explotación con el objetivo de asegurar el correcto funcionamiento del Sistema para su posterior implantación. Para conseguir dicho objetivo, en este proceso se realizan las pruebas unitarias, las pruebas de integración de los subsistemas y componentes y las pruebas del sistema, de acuerdo al plan de pruebas establecido.

El propósito de la Interfaz de Seguridad en el proceso de la Construcción del Sistema de Información (CSI) tiene como objetivo garantizar que durante la codificación, generación y pruebas de los componentes del sistema se incorporen y verifiquen los mecanismos de seguridad definidos en fases anteriores. Esto asegura que el sistema desarrollado protege adecuadamente la información y los recursos, manteniendo la coherencia con la política de seguridad de la organización y minimizando riesgos lógicos como ataques, fallos o accesos no autorizados. Además, se refuerzan los controles de seguridad en el entorno de desarrollo para evitar filtraciones o manipulaciones indebidas.

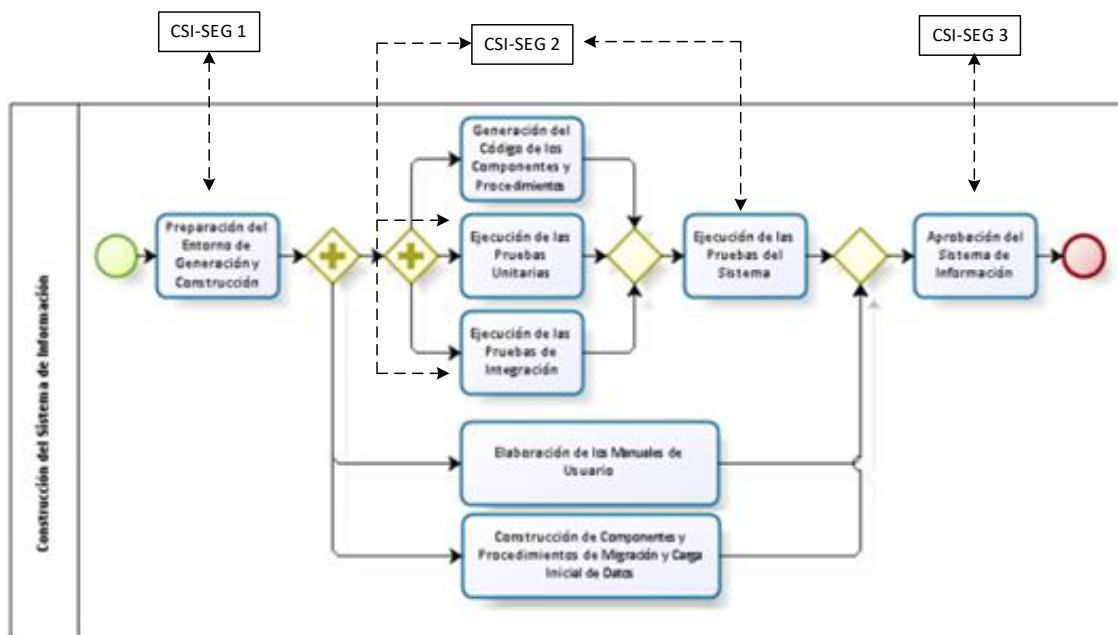
8.4.2 Resultados

Nº	Descripción del Resultado
1.	Se producen unidades del software definidas por el diseño.
2.	Se establece la consistencia y correspondencia entre los requerimientos del software, diseño y unidades del software.
3.	Se realiza la comprobación de las unidades del software contra los requerimientos y el diseño.
4.	Se desarrollan los criterios de verificación de los elementos del software para asegurar el cumplimiento con los requerimientos del software asignado a los elementos.
5.	Se verifican los elementos del software usando los criterios definidos.
6.	Se registran los resultados de las pruebas de integración.
7.	Se establece la consistencia y correspondencia entre el diseño del software y elementos del software.
8.	Se verifica la integración del software usando los criterios definidos.
9.	Se registran los resultados de la prueba.
10.	Se desarrolla la estrategia de regresión para reaplicar las pruebas al software integrado cuando se produce un cambio en los elementos del software.
11.	Se registran los resultados de las pruebas de seguridad de integración y de sistema realizadas.
12.	Se actualizan los manuales de usuario que incluyen procedimientos de operación, administración, seguridad y control de acceso
13.	Se desarrollan los procedimientos de migración y carga inicial de datos que cumplen con los requisitos de seguridad
14.	Se desarrolla planes de formación de seguridad para los usuarios finales y operación
15.	Se registran los productos generados indicando su nivel de seguridad (autenticación, confidencialidad, integridad, disponibilidad ACID)
16.	Se verifica que el código desarrollado cumpla con las directrices de codificación segura
17.	Se implementan registros de auditoría y log seguros
18.	Se registran los resultados de las pruebas de detección y mitigación de vulnerabilidades

8.4.3 Roles


Abrev. Rol	Descripción del Rol
AF	Analista Funcional
AS	Analista(s) de Sistemas
ADS	Administrador de Servidores
ABD	Administrador de Base de Datos
DOC	Documentador
J-TI	Jefe de la OGTI
J-P	Jefe de Proyecto
UL	Usuario Líder (Jefe del usuario o su representante)
UE	Usuario(s) Experto(s)
EA	Especialista de Arquitectura
AP	Analistas Programadores
AQA	Analista de Aseguramiento de la Calidad
AQC	Analista de Control de Calidad
RS	Responsable de Seguridad
ES	Especialista de Seguridad

8.4.4 Diagrama del Subproceso



8.4.5 Lista de Actividades y Tareas

Nº	Actividad	Tareas	Responsable	Participantes
A1	Preparación del Entorno de Generación y Construcción (CSI1)	Implantación de la base de datos física.	J-P	AS, AP, ABD
		Preparación del entorno de construcción.		AS, AP
		Estudio de la Seguridad requerida, supervisión de la Seguridad del entorno	RS	ES
A2	Generación del Código de los Componentes y Procedimientos (CSI2)	Generación del código de componentes.	AP	J-P, AS
		Generación del código de objetos de base de datos.		J-P, AS, ABD
		Documentación del código fuente implementado.		J-P, AS
A3	Ejecución de las Pruebas Unitarias (CSI3)	Preparación del entorno de las pruebas unitarias.	AP	J-P, AS, AQA
		Realización y evaluación de las Pruebas Unitarias		
		Estudio de los Resultados de Pruebas de Seguridad	RS	ES
A4	Ejecución de Pruebas de Integración (CSI4)	Preparación del Entorno de las Pruebas de Integración	AS	J-P, EA, AP
		Realización de las pruebas de integración.	AP	J-P, AS
		Evaluación del Resultado de las Pruebas de Integración	AS	J-P, AQA, AQC
		Estudio de los Resultados de Pruebas de Seguridad	RS	ES
A5	Ejecución de las Pruebas del Sistema (CSI5)	Preparación del Entorno de las Pruebas del Sistema.	AS	J-P, EA, AP
		Realización de las Pruebas del Sistema	AP	J-P, AS
		Evaluación del Resultado de las Pruebas del Sistema	AS	J-P, EA, AP
		Estudio de los Resultados de Pruebas de Seguridad	RS	ES
A6	Elaboración de los Manuales de Usuario (CSI6)	Elaboración de los manuales de usuario.	AP	DOC, J-P, AS
A7	Construcción de los Componentes y Procedimientos de Migración y Carga Inicial de Datos (CSI8)	Preparación del entorno de migración y carga Inicial de datos.	ABD	J-P, AS, AP, ES, EA
		Generación del código de los componentes y procedimientos de migración y carga inicial de datos.	AP	J-P, AS

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación:
		DI-001-2025-SUNARP-OTI

Nº	Actividad	Tareas	Responsable	Participantes
		Realización y evaluación de las pruebas de migración y carga inicial de datos.	AP	J-P, AS
A8	Aprobación del Sistema de Información (CSI9)	Presentación y aprobación del sistema de información.	AS	J-P, UL
		Clasificación y catalogación de productos generados de Seguridad	RS	ES

Nota: La codificación CSI hace referencia a las actividades descritas en la metodología MÉTRICA Versión 3.

8.4.6 Artefactos


De entrada		De salida	
Código Formato	Descripción	Código Formato	Descripción
MCVDSS-ASI-0201	Documento de Análisis del Sistema	MCVDSS-CSI-0401	Plan de Implantación
MCVDSS-DSI-0301	Documento de Diseño del Sistema	MCVDSS-00002	Acta(s) de Reunión(es)
MCVDSS-EVS-0102	Catálogo de Requisitos	MCVDSS-CSI-0402	Manual de Usuario
MCVDSS-DSI-0302	Matriz de Trazabilidad	MCVDSS-CSI-0403	Manual de Soporte Técnico del Sistema
MCVDSS-DSI-0303	Plan de Integración del Sistema	MCVDSS-CSI-0404	Manual de Operaciones del Sistema
MCVDSS-DSI-0304	Plan de Migración y Carga del Sistema	MCVDSS-CSI-0405	Reporte de Pruebas del Sistema
MCVDSS-ASI-0202	Plan de Pruebas del Sistema	MCVDSS-CSI-0406	Acta de Pruebas de Aceptación del Sistema / Regresión
MCVDSS-DSI-0305	Casos de Pruebas del Sistema		

8.5 Implantación y Aceptación del Sistema de Información (IAS)

8.5.1 Propósito

El propósito del proceso de Implantación y Aceptación del Sistema de Información (IAS) es la entrega (instalación) y aceptación del sistema en su totalidad, y la realización de todas las actividades necesarias para el paso a producción del mismo.

El propósito de la Interfaz de Seguridad en el proceso de Implantación y Aceptación del Sistema (IAS) tiene como objetivo garantizar que el sistema de información, una vez construido, cumpla con todos los requisitos de seguridad establecidos. Esto implica reforzar los procedimientos de seguridad y control de accesos, verificar mediante pruebas que las funciones y mecanismos de seguridad adicionales están correctamente implementados, y asegurar que el sistema pueda operar de forma segura en su entorno productivo. Además, se busca que los acuerdos de nivel de servicio (SLA) contemplen los aspectos de seguridad antes de la puesta en producción.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

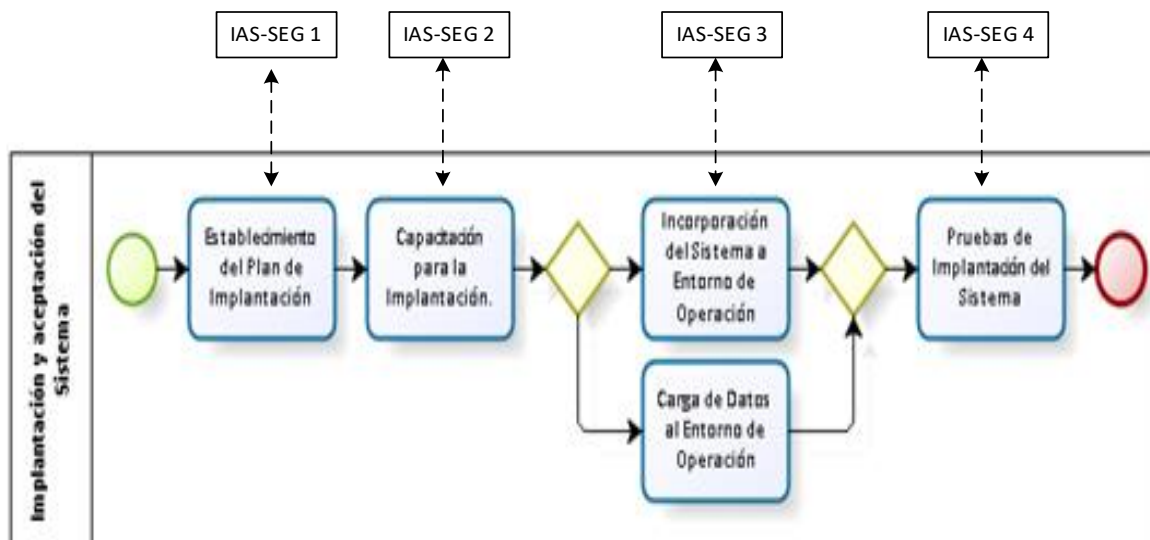
8.5.2 Resultados

Nº	Descripción del Resultado
1.	Se desarrolla una estrategia de instalación de software.
2.	Se desarrollan los criterios de instalación del software para demostrar el cumplimiento con los requerimientos de instalación del software.
3.	Se instala el producto software en el ambiente designado.
4.	Se asegura que el producto del software está listo para el uso en su ambiente proyectado.
5.	Se verifican y validan los requisitos de seguridad a través de pruebas específicas durante la implantación
6.	Se registran los resultados de las pruebas y detección de posibles incidencias relacionadas con la seguridad
7.	Se registran los requisitos de seguridad en los SLA
8.	Se refuerzan los controles de seguridad durante el proceso de implantación para proteger la información y los recursos
9.	Se elaboran manuales operativos seguros
10.	Se elaboran un plan de respuesta a incidentes
11.	Se verifican que los mecanismos de seguridad están activos y documentados
12.	Se registran las incidencias o debilidades detectadas

8.5.3 Roles


Abrev. Rol	Descripción del Rol
AS	Analista(s) de Sistemas
ABD	Administrador de Base de Datos
J-P	Jefe de Proyecto
UL	Usuario Líder (Jefe del usuario o su representante)
UE	Usuario(s) Experto(s)
AP	Analistas Programadores
EI	Equipo de Implantación
RS	Responsable de Seguridad
ES	Especialista de Seguridad

8.5.4 Diagrama del Subproceso



8.5.5 Lista de Actividades y Tareas

Nº	Actividad	Tareas	Responsable	Participantes
A1.	Establecimiento del Plan de Implantación (IAS1)	Definición del Plan de Implantación	J-P	AS, EI, UL
		Especificación del equipo de implantación.	J-P	AS, AP, EI, UL
		Estudio de la Seguridad requerida en el proceso	RS	ES
A2.	Capacitación para la Implantación (IAS2)	Preparación de la capacitación del equipo de implantación.	J-P	EI, UL
		Formación del Equipo de Implantación.		
		Preparación de la Formación a Usuarios Finales		
		Seguimiento de la Formación a Usuarios Finales		
		Formación necesaria para la implantación	RS	ES
A3.	Incorporación del Sistema al Entorno de Operación (IAS3)	Preparación de la instalación.	J-P	EI
		Realización de la instalación.	RS	ES
		Revisión y Supervisión de medidas de Seguridad del entorno de Operación		
A4.	Carga de Datos al Entorno de Operación (IAS4)	Migración y carga inicial de datos.	J-P	EI, ABD, UE
A5.	Pruebas de Implantación del Sistema (IAS5)	Preparación de las Pruebas de Implantación	J-P	EI
		Realización de las Pruebas de Implantación del Sistema	EI	J-P

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación:
		DI-001-2025-SUNARP-OTI

Nº	Actividad	Tareas	Responsable	Participantes
		Evaluación del resultado de las Pruebas de Implantación	J-P	EI
		Estudio de resultados de pruebas de Seguridad de implantación del sistema	RS	ES
		Revisión de medidas de Seguridad en el entorno de producción		

Nota: La codificación IAS hace referencia a las actividades descritas en la metodología MÉTRICA Versión 3.

8.5.6 Artefactos

De entrada		De salida	
Código Formato	Descripción	Código Formato	Descripción
MCVDSS-CSI-0401	Plan de Implantación	MCVDSS-IAS-0501	Plan de Implantación (actualizado)
MCVDSS-CSI-0402	Manual de Usuario	MCVDSS-00002	Acta(s) de Reunión(es)
MCVDSS-CSI-0403	Manual de Soporte Técnico del Sistema	MCVDSS-CSI-0405	Reporte de Pruebas del Sistema (de la implementación)
MCVDSS-CSI-0404	Manual de Operaciones del Sistema	MCVDSS-CSI-0403	Manual de Soporte Técnico del Sistema (actualizado)
MCVDSS-CSI-0405	Reporte de Pruebas del Sistema	MCVDSS-CSI-0404	Manual de Operaciones del Sistema (actualizado)
MCVDSS-CSI-0406	Acta de Pruebas de Aceptación del Sistema / Regresión	MCVDSS-DSI-0304	Plan de Migración y Carga del Sistema (actualizado)
MCVDSS-DSI-0304	Plan de Migración y Carga del Sistema	MCVDSS-IAS-0502	Acta de Capacitación a Usuarios Finales
		MCVDSS-IAS-0503	Acta de Conformidad General & Pase a Producción


8.6 Mantenimiento del Sistema de Información (MSI)

8.6.1 Propósito

El propósito del proceso de Mantenimiento del Sistema de Información (MSI) es la obtención de una nueva versión de un sistema de información a partir de las peticiones de mantenimiento que los usuarios realizan con motivo de un problema detectado en el sistema, o por la necesidad de una mejora del mismo.

El tipo de mantenimiento que se atienden son:

- **Correctivo:** son aquellos cambios precisos para corregir errores del producto software.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

- Evolutivo: son las incorporaciones, modificaciones y eliminaciones necesarias en un producto software para cubrir la expansión o cambio en las necesidades del usuario.

El propósito de la Interfaz de Seguridad en el proceso de Mantenimiento del Sistema de Información (MSI) tiene como objetivo asegurar que durante la evolución, corrección y adaptación del sistema se mantenga y refuerce la protección de la información y los recursos. Esto implica gestionar adecuadamente los riesgos de seguridad derivados de los cambios, garantizar la continuidad de los controles de acceso y protección, y mantener la integridad, confidencialidad y disponibilidad del sistema durante todo su ciclo de vida.

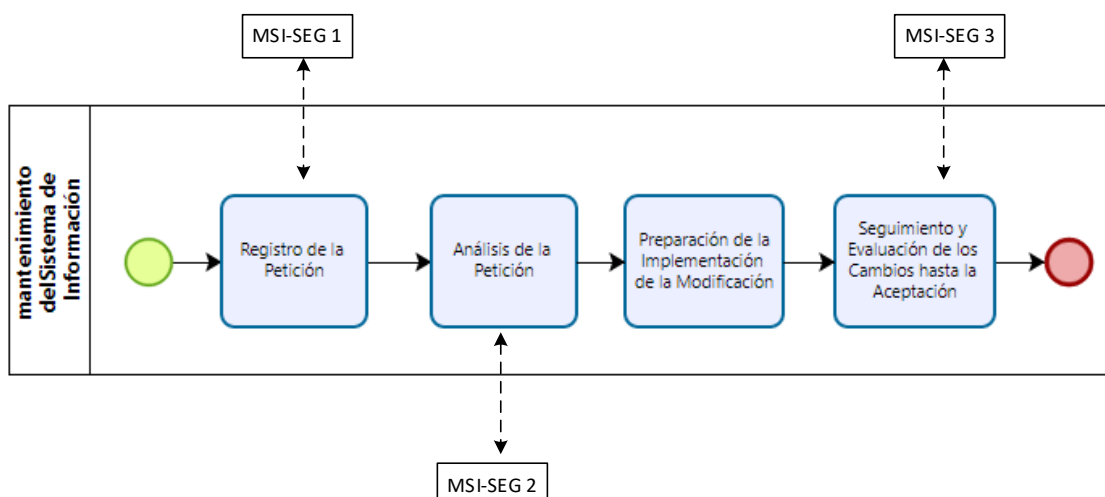
8.6.2 Resultados

Nº	Descripción del Resultado
1.	Se desarrolla una estrategia de mantenimiento para manejar la modificación, migración y retiro de productos de acuerdo con la estrategia de release, véase (Software Release Management en los <i>términos y definiciones</i>).
2.	Se identifica el impacto de los cambios en la organización, funcionamientos o interfaces del sistema existente.
3.	Se actualiza la documentación del software del sistema/software afectado según sea necesario.
4.	Se desarrollan los productos modificados con pruebas asociadas que demuestren que los requerimientos no son los acordados.
5.	Se migran las actualizaciones del producto al ambiente del cliente.
6.	Se retiran los productos de su uso, a solicitud, de una manera controlada que minimiza la perturbación a los clientes.
7.	Se comunica la modificación del sistema/software a todas las partes afectadas.
8.	Se identifica y se supervisa los riesgos operacionales para la introducción y funcionamiento del producto.
9.	Se opera el producto en su ambiente proyectado de acuerdo con los requerimientos.
10.	Se desarrollan los criterios para el uso operacional que demuestra el cumplimiento con los requerimientos acordados.
11.	Se actualizan y verifican los mecanismos y funciones de seguridad conforme a las modificaciones realizadas en el sistema
12.	Se documentan las acciones de mantenimiento relacionadas con la seguridad, incluyendo registro de cambios, pruebas y validaciones
13.	Se realiza la gestión de incidentes y vulnerabilidades de seguridad detectadas durante el mantenimiento
14.	Se actualiza el inventario de vulnerabilidades
15.	Se evalúa el impacto en seguridad antes de aprobar los cambios
16.	Se documentan las lecciones aprendidas

8.6.3 Roles

Abrev. Rol	Descripción del Rol
AS	Analista(s) de Sistemas
J-P	Jefe de Proyecto
UL	Usuario Líder (Jefe del usuario o su representante)
UE	Usuario(s) Experto(s)
AP	Analistas Programadores
DOC	Documentador
RS	Responsable de Seguridad
ES	Especialista de Seguridad

8.6.4 Diagrama del Subproceso



8.6.5 Lista de Actividades y Tareas

Nº	Actividad	Tareas	Responsable	Participantes
A1.	Registro de la Solicitud de Mantenimiento (MSI1)	Registro de la Solicitud de Mantenimiento.	AS	DOC
		Asignación de la Solicitud		AP
		Estudio de la seguridad requerida en el proceso	RS	ES
A2.	Análisis de la Solicitud de Mantenimiento (MSI2)	Verificación y Estudio de la Petición.	AS	AP, UE
		Estudio de la propuesta de solución		
		Estudio de la petición	RS	ES
		Análisis de las funciones y mecanismos de Seguridad afectados		

 sunarp <small>Superintendencia Nacional de los Registros Públicos</small>	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP- OTI
--	--	---

A3.	Preparación de la Implementación de Modificación (MSI3)	Identificación de Elementos Afectados	J-P	AS, AP
		Establecimiento del Plan de Acción		
		Especificación del Plan de Pruebas de Regresión		
A4.	Seguimiento y Evaluación de los Cambios hasta Aceptación (MSI4)	Seguimiento de los Cambios	J-P	AS, AP
		Realización de las Pruebas de Regresión		AS, AP
		Solicitud de Pase a producción y Cierre de la Petición	AS	J-P, UL
		Clasificación y catalogación de los productos generados de Seguridad	RS	ES

8.6.6 Artefactos

De entrada		De salida	
Código Formato	Descripción	Código Formato	Descripción
MCDVSS-MSI-0600	Solicitud de Mantenimiento	MCDVSS-MSI-0601	Plan de Mantenimiento
MCDVSS-EVS-0102	Catálogo de Requisitos	MCDVSS-EVS-0102	Catálogo de Requisitos (de mantenimiento)
MCDVSS-CSI-0402	Manual de Usuario	MCDVSS-00002	Acta(s) de Reunión(es)
		MCDVSS-CSI-0405	Reporte de Pruebas del Sistema (de mantenimiento)
		MCDVSS-CSI-0406	Acta de Pruebas de Aceptación del Sistema / Regresión (de mantenimiento)
		MCDVSS-CSI-0402	Manual de Usuario (actualizado)
		MCDVSS-MSI-0602	Acta de Conformidad
		MCDVSS-MSI-0603	Solicitud de Pase a Producción

IX. DISPOSICIONES COMPLEMENTARIAS


- Todas las coordinaciones requeridas para el uso de la presente Metodología se realizarán a través de la Oficina de Tecnologías de la Información (OTI – Sunarp).
- La presente Metodología y los formatos de los artefactos están sujetos a la mejora continua; cuando se identifique una oportunidad de mejora deberá ser canalizada al Jefe de la OTI para evaluar la propuesta de cambio.
- La presente directiva debe estar considerada en los términos de referencia que requieran el servicio de desarrollo o mantenimiento de un software.

X. ANEXOS

Anexo	Código	Descripción
Anexo 1	MCVDSS-0001	Solicitud formal
Anexo 2	MCVDSS-0002	Modelo Acta de Reunión
Anexo 3	MCVDS-EVS-0101	Informe de Viabilidad Técnica
Anexo 4	MCVDSS-EVS-0102	Catálogo de Requisitos
Anexo 5	MCVDSS-EVS-0103	Acta de Aplicabilidad
Anexo 6	MCVDSS-ASI-0201	Documento de Análisis
Anexo 7	MCVDSS-ASI-0202	Plan de Pruebas del Sistema
Anexo 8	MCVDSS-ASI-0203	Casos de Pruebas del Sistema
Anexo 9	MCVDSS-ASI-0204	Acta Aprobación del Prototipo del Sistema
Anexo 10	MCVDSS-DSI-0301	Documento de Diseño del Sistema
Anexo 11	MCVDSS-DSI-0302	Matriz de Trazabilidad
Anexo 12	MCVDSS-DSI-0303	Plan de Integración del Sistema
Anexo 13	MCVDSS-DSI-0304	Plan de Migración y Carga del Sistema
Anexo 14	MCVDSS-CSI-0401	Plan de Implantación
Anexo 15	MCVDSS-CSI-0402	Manual de Usuario
Anexo 16	MCVDSS-CSI-0403	Manual de Soporte Técnico del Sistema
Anexo 17	MCVDSS-CSI-0404	Manual de Operaciones del Sistema
Anexo 18	MCVDSS-CSI-0405	Reporte de Pruebas del Sistema
Anexo 19	MCVDSS-CSI-0406	Acta de Pruebas de Aceptación del Sistema / Regresión
Anexo 20	MCVDSS-IAS-0501	Plan de Implantación (actualizado)
Anexo 21	MCVDSS-IAS-0502	Acta de Capacitación a Usuarios Finales
Anexo 22	MCVDSS-IAS-0503	Acta de Conformidad General & Pase a Producción
Anexo 23	MCVDSS-MSI-0600	Solicitud de Mantenimiento
Anexo 24	MCVDSS-MSI-0601	Plan de Mantenimiento
Anexo 25	MCVDSS-MSI-0602	Acta de Conformidad de Mantenimiento
Anexo 26	MCVDSS-MSI-0603	Solicitud de Pase a Producción

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 1 MCVDSS-0001 - Solicitud Formal

	Oficina de Tecnologías de la Información	Código: MCVDSS-0001 Versión: 1.0
	Solicitud de Implementación / Mantenimiento	Fecha: 01/01/2025 Página: 1 de 3

INDICACIONES: Por favor completar los <datos o información> que se solicita entre los símbolos <_>

Solicitud de Implementación / Mantenimiento

1. Generalidades

1.1. Identificación de solicitud de cambio:

Solicitud de I/M N°:	SC-00y-20XX	NOTA: debe ser numerado por la OTI
Descripción abreviada de la solicitud:	<Nombre del Proyecto / Sistema / Módulo / Proceso / Componente/Servicio>	

1.2. Información del Solicitante:

Nombre:	<Apellidos y nombres>
Área:	<Área/Oficina, Sede/Zona Registral>
Cargo:	<Cargo>
Correo electrónico:	<Correo electrónico Institucional>
Teléfono:	<Anexo>
Fecha de solicitud:	<dd/mm/20yy>

1.3. Personal de contacto para coordinar requerimientos:

Apellidos y Nombres	Correo	Teléfono	Función, Rol, etc.
< Apellidos y Nombres 1 >	< email institucional >	< anexo >	< Cargo, función, rol, etc. >
< Apellidos y Nombres 2 >	< email institucional >	< anexo >	< Cargo, función, rol, etc. >
< Apellidos y Nombres 3 >	< email institucional >	< anexo >	< Cargo, función, rol, etc. >
< Apellidos y Nombres 4 >	< email institucional >	< anexo >	< Cargo, función, rol, etc. >

2. Información de la solicitud

Necesidad N° 1:		<i>NOTA: Copiar este cuadro para cada solicitud</i>	
Tipo de cambio:	Rutinario ()	Normal ()	Urgente ()
Clasificación:	Aplicación ()		Infraestructura TI ()
Tipo de Requerimiento.:	Requerimiento Funcional () <i>(Define qué debe hacer un sistema)</i>		Requerimiento No Funcional () <i>(Define cómo debe ser el sistema)</i>
Situación actual o problema:	<Describe la situación que motiva la presente solicitud.> <Para hacerlo más descriptivo no olvide adjuntar captura de pantalla actual, mencionar mensajes de error recientes, reportes, registros, referencia a documentos como reglamentos, etcétera, que debería corregirse, mejorarse o cambiarse>		
Requerimiento:	<Describe el requerimiento de manera sencilla, clara, concisa, completa, consistente, comprensible y sin mezclar varios requerimientos en uno> <El requerimiento especifica lo que el sistema informático debe hacer (o ser) y en algunos casos lo que no debe hacer. Describe alternativamente el (los) servicio(s) que debe proporcionar el sistema, la manera en que debe reaccionar a determinadas		

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 2 MCVDSS-0002 – Modelo de Acta de Reunión

	Oficina de Tecnologías de la Información	Código: MCVDSS-0002 Versión: 1.0 Fecha: 01/01/2025 Página: 1 de 2
Acta de Reunión		
SC-00y-20XX – SUNARP/OTI		

CONVOCATORIA	
Requerimiento:	<Nombre del Proyecto / Sistema / Módulo / Proceso / Componente/Servicio>
Solicitud N°:	<SC-002-20YY>
Convocado por:	<Ap. Nombres> – <u>Responsable</u> del Proyecto
Asunto:	<Motivo de la reunión en el marco del requerimiento >
Referencia:	<Documento(s) de Referencia >
Fecha:	dd/mm/20YY
Hora:	hh:mm am/pm a hh:mm am/pm
Lugar:	Sede Central – Sunarp - Sala de reuniones de la <u>OTI</u>

AGENDA
1. Informe del estado de la capacitación del <Nombre del Proyecto / Sistema / Módulo / Proceso / Componente/Servicio>.
2. Aprobación de actividades subsiguientes en el ...
3. Otros puntos relacionados

DESARROLLO DE LA REUNIÓN	
Inicio de la reunión: 03:00 p.m.	
N°	Acción
<Descripción de la participación de los asistentes, pudiendo incluir antecedentes, supuestos, entre otros temas considerados en la agenda o por los asistentes>	
1	<u>Apertura</u> de la reunión El <u>Jefe</u> de la <u>OTI</u> expone lo siguiente: Informa la agenda de la reunión. Informa que... Informa que...
2	<u>Informe</u> de ... El <u>Responsable</u> de Desarrollo de la Sunarp, expone lo siguiente: Realiza un breve recuento de las actividades ... Informa que la mencionada ...: Informa que corresponde continuar ...
3

ACUERDOS DE LA REUNIÓN				
Los aquí presentes, luego de deliberar y evaluar todo lo acontecido en la reunión, acuerdan lo siguiente:				
N°	Temas	Acuerdo	Responsable(s)	Fecha Término

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 3 MCVDSS-EVS-0101 – Informe de Viabilidad Técnica

	Oficina de Tecnologías de la Información	Código: MCVDSS-EVS-0101 Versión: 1.0
	Estudio de Viabilidad del Sistema	Fecha: 01/01/2025 Página: 4 de 10
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Estudio de Viabilidad del Sistema

INDICACIONES:


- Por favor completar los <datos o información> que se solicita entre los símbolos <_ _ >
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

I. GENERALIDADES DEL REQUERIMIENTO

Producto:	Descripción General del Sistema(s) involucrado(s)
Descripción general de la solicitud:	<Realizar una descripción gráfica o textual correspondiente al Contexto del Sistema involucrado. Será tomado como punto de partida para el desarrollo del Modelo de Casos de Uso, dentro del proceso ASJ.>
Contexto del Sistema:	<Descripción gráfica o textual del Contexto del Sistema.> <Contiene una descripción del contexto del sistema realizada mediante un diagrama simple o de manera textual, el cual será tomado como punto de partida para el desarrollo del Modelo de Casos de Uso, dentro del proceso ASJ.>
Estructura Organizativa	<Contiene la descripción gráfica o textual de los interesados en el presente requerimiento.>
Objetivos generales del Estudio de Viabilidad:	<Establecen los objetivos generales del Estudio de Viabilidad, teniendo en cuenta las restricciones identificadas anteriormente.>

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 4 MCVDSS-EVS-0102 – Catálogo de Requisitos

	Oficina de Tecnologías de la Información	Código: MCVDSS2-EVS-0102 Versión: 1.0
Catálogo de Requisitos		Fecha: 01/01/2025 Página: 4 de 14
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Catálogo de Requisitos

INDICACIONES: Por favor completar los <datos o información> que se solicita entre los símbolos <_ _>

1. INTRODUCCIÓN

<Descripción general de la solicitud >

2. ALCANCE DEL SISTEMA:

ALCANCE	<Descripción somera y concisa del alcance que se ha identificado y que queda establecido>
Unidades organizativas involucradas:	<Identificar las unidades organizativas afectadas por el sistema, así como su estructura y responsables de las mismas.

<Analizar si los productos intermedios (informes, análisis, matrices) requieren niveles especiales de seguridad en cuanto a autenticación, confidencialidad, integridad y disponibilidad.>

Ejemplos:

- Aplicar firma digital a los informes de evaluación para garantizar autenticidad.
- Cifrar los documentos de análisis económico con datos presupuestales (confidencialidad).
- Mantener registros hash (SHA-256) de los productos generados para verificar integridad.

Estudio de la Seguridad requerida en el proceso:

<Evaluar si durante el proceso es necesario aplicar controles de seguridad a los productos intermedios generados (informes, análisis, matrices, etc.), considerando:

- La naturaleza del sistema de información.
- El impacto de un posible acceso no autorizado, alteración o pérdida de estos productos.
- El contexto en que se desarrollan las actividades

Ejemplos a considerar:

1. Producto: Informe de análisis de alternativas de solución

- **Confidencialidad:** Alta (puede contener información estratégica o sensible del negocio).
- **Integridad:** Alta (una alteración podría desvirtuar el análisis técnico o financiero).
- **Disponibilidad:** Media (requiere acceso durante reuniones de decisión).
- **Control recomendado:** Firma digital del responsable, almacenamiento en sistema con control de versiones.

2. Producto: Modelo de Costes del Sistema


- **Confidencialidad:** Media (detalles financieros internos).
- **Integridad:** Alta (los datos sirven para decisiones de inversión).
- **Disponibilidad:** Media.
- **Control recomendado:** Control de acceso por perfil, respaldo automatizado.

3. Producto: Estudio de Impacto Organizativo


- **Confidencialidad:** Alta (puede implicar reorganización, reasignación de funciones, etc.).

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 5
MCVDSS-EVS-0103 – Acta de Aplicabilidad

	Oficina de Tecnologías de la Información Acta de Aprobación de Requisitos y de la Solución SC-00y-20XX – SUNARP/OTI	Código: MCVDSS-EVS-0103 Versión: 1.0 Fecha: 01/01/2025 Página: 1 de 3
---	---	--

CONVOCATORIA	
Requerimiento:	<Nombre del Proyecto / Sistema / Módulo / Proceso / Componente/Servicio>
Solicitud N°:	<SC-00y-20YY>
Convocado por:	<Ap. Nombres> – Responsable del Proyecto
Asunto:	<Motivo de la reunión en el marco del requerimiento >
Referencia:	<Documento(s) de Referencia >
Fecha:	dd/mm/20YY
Hora:	hh:mm am/pm a hh:mm am/pm
Lugar:	Sede Central – Sunarp - Sala de reuniones de la OTI

AGENDA	
1.	Informe del estado de la capacitación del <Nombre del Proyecto / Sistema / Módulo / Proceso / Componente/Servicio>.
2.	Aprobación de requisitos ...
3.	Aprobación de la solución propuesta ...
4.	Otros puntos relacionados


DESARROLLO DE LA REUNIÓN	
Inicio de la reunión: 03:00 p.m.	
N°	Tema
Acción	
<Descripción de la participación de los asistentes, pudiendo incluir antecedentes, supuestos, entre otros temas considerados en la agenda o por los asistentes>	
1	<u>Apertura</u> de la reunión El <u>Jefe</u> de la <u>OTI</u> expone lo siguiente: Informa la agenda de la reunión. Informa que... Informa que...
2	Informe de ... El Responsable de Desarrollo de la Sunarp, expone lo siguiente: Realiza un breve recuento de las actividades ... Informa que la mencionada ...: Informa que corresponde continuar ...
3

ACUERDOS DE LA REUNIÓN	
Los aquí presentes, luego de deliberar y evaluar todo lo acontecido en la reunión, acuerdan lo siguiente:	
<Descripción de los acuerdos de los participantes, pudiendo incluir antecedentes, supuestos, entre otros temas previos considerados por los participantes de la reunión>	
SOBRE LOS REQUISITOS:	
ALCANCE: <Ámbito, Conceptualizaciones, Referencias>	
DESCRIPCIÓN: <Funcional, Procedimental, Necesidades/ Problemas, Objetivos>	
ANTECEDENTES:	

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 6
MCVDSS-ASI-0201 – Documento de Análisis

	Oficina de Tecnologías de la Información	Código: MCVDSS-ASI-0201 Versión: 1.0
	Análisis del Sistema de Información	Fecha: 01/01/2025 Página: 4 de 18
SC-00y-20XX - <Proyecto/Sistema/Módulo>		

Análisis del Sistema de Información

INDICACIONES:

- Por favor completar los <datos o información> que se solicita entre los símbolos <_>
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

I. DEFINICIÓN DEL SISTEMA

I.1. Determinación del Alcance del Sistema:

Alcance del Sistema de Información	<Definido en el Informe de Viabilidad> <Aprobado en el Acta ____> <Ver documento: ____>
Requisitos del Sistema de Información	<Definido en el Catálogo de Requisitos> <Aprobado en el Acta ____> <Ver documento: ____>


I.2. Identificación del Entorno Tecnológico:

Servidor de Aplicaciones:	HARDWARE: <Tipo de Procesador> <Tamaño de Memoria> <Tipo de Servidor:_(Ejemplo: <u>OAS</u> , <u>GLASSFISH</u> , otro)> SOFTWARE DE BASE: <Sistema Operativo> <Motor de Base de Datos> <Software de Programación> COMUNICACIONES: <Protocolo de Comunicaciones> <Web: <u>HTTP</u> / <u>HTTPS</u> / <u>SQL</u> / <u>FTP</u> > <Cliente servidor: <u>Nº</u> de puerto> CONSIDERACIONES: <Almacenar datos o imágenes> <Capturar el IP Cliente> <Enviar Correos> <Cantidad estimada de usuarios> <Cantidad de conexiones mínimas y máximas> <Nivel de concurrencia> < <u>JDK</u> > < <u>JRE</u> > <Web/Cliente servidor>
Seguridad:	<Estándares Adoptados> <Web <u>Services</u> > <Aplicaciones> <Certificado Digital> <Cifrado de objetos> <Autenticación <u>Multifactor MFA</u> >

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 7
MCVDSS-ASI-0202 – Plan de Pruebas del Sistema

	Oficina de Tecnologías de la Información	Código: MCVDSS-ASI-0202 Versión: 1.0
Plan de Pruebas del Sistema		Fecha: 01/01/2025 Página: 5 de 17
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Plan de Pruebas del Sistema

INDICACIONES:

- Por favor completar los <datos o información> que se solicita entre los símbolos <_ _ >
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

1. INTRODUCCIÓN

<El presente documento detalla el Plan de Pruebas para el sistema, alineado con los principios de la Metodología Métrica 3. Este plan establece los objetivos, el alcance, la estrategia, los recursos y el cronograma para las actividades de prueba del sistema, garantizando que el producto final cumpla con los requisitos funcionales y no funcionales establecidos.>

Proyecto/Sistema/Módulo		Tipo de Proyecto/Sistema/Módulo
Documentos	Disponibles	Observaciones
	<input checked="" type="radio"/> SI <input type="radio"/> No	
	<input type="radio"/> SI <input type="radio"/> No	
	<input type="radio"/> SI <input type="radio"/> No	
	<input type="radio"/> SI <input checked="" type="radio"/> No	
Responsable de Control de Calidad:		
Equipo de Pruebas:		

1.1. Objetivo del Plan de Pruebas

<El objetivo principal de este Plan de Pruebas es:

- Verificar que el sistema cumpla con todas las especificaciones y requisitos funcionales y no funcionales.
- Identificar, registrar y gestionar la corrección de defectos (bugs) en el software.
- Asegurar la calidad del sistema antes de su despliegue en el entorno de producción.>



Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 8 MCVDSS-ASI-0203 – Casos de Prueba del Sistema

	Oficina de Tecnologías de la Información	Código: MCVDSS-ASI-0203
	Casos de Prueba del Sistema	Versión: 1.0 Fecha: 01/01/2025 Página: 4 de 10
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Casos de Prueba del Sistema

INDICACIONES:

- Por favor completar las <datos o información> que se solicita entre los símbolos <_>
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

1. CASOS DE PRUEBAS FUNCIONALES

La lista de requisitos obtenidos durante el diseño y sus correspondientes casos de prueba son:

<Para cada requisito funcional debería desarrollar los casos y procedimientos de prueba correspondientes>

Id. RD	Requisito de Diseño (RD)	Id. CP	Descripción del Caso de Prueba (CP)

<CONTENIDO DE CADA CAMPO:

- *Id RD: es el identificador de requisito en el diseño*
- *Nombre del Requisito: Nombre del requisito funcional sobre el que se diseña el caso de prueba.*
- *Id-CP: es el identificador de caso de prueba*
- *Descripción del caso de prueba: Descripción detallada del caso de prueba.>*


Los casos de prueba en el diseño son:

<Para cada caso de prueba colocar lo siguiente:>

Caso de prueba:		<Id-CP>		
Elemento a probar:		<Indique el módulo que será probado o el Id-RD>		
Nº	Acción requerida	Datos de entrada	Datos de salida	Resultado esperado / Observación
1				
2				
3				
...				
Necesidades del entorno:				


Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 9

MCVDSS-ASI-0204 – Acta Aprobación del Prototipo del Sistema

	Oficina de Tecnologías de la Información Acta de Aprobación del Prototipo del Sistema	Código: MCVDSS-ASI-0204 Versión: 1.0 Fecha: 01/01/2025 Página: 1 de 2
SC-00y-20XX – SUNARP/OTI		

CONVOCATORIA		
Requerimiento:	<Nombre del Proyecto / Sistema / Módulo / Proceso / Componente/Servicio>	
Solicitud N°:	<SC-00y-20YY>	
Convocado por:	<Ap. Nombres> – Responsable del Proyecto	
Asunto:	<Motivo de la reunión en el marco del requerimiento >	
Referencia:	<Documento(s) de Referencia >	
Fecha:	dd/mm/20YY	Hora: hh:mm am/pm a hh:mm am/pm
Lugar:	Sede Central – Sunarp - Sala de reuniones de la OTI	

AGENDA
<ol style="list-style-type: none"> 1. Informe del estado de la capacitación del <Nombre del Proyecto / Sistema / Módulo / Proceso / Componente/Servicio>. 2. Aprobación del prototipo ... 3. Otros puntos relacionados


DESARROLLO DE LA REUNIÓN		
Inicio de la reunión: hh:mm am/pm		
N°	Tema	Acción
<Descripción de los acuerdos de los participantes, pudiendo incluir antecedentes, supuestos, entre otros temas previos considerados por los participantes de la reunión>		
DESCRIPCIÓN:		
<Funcional, Alcance, Objetivos, Valor Incorporado, Beneficios>		
CONSIDERACIONES / OBSERVACIONES:		
<Descripción de las consideraciones / observaciones>		

ACUERDOS DE LA REUNIÓN
Los aquí presentes, luego de deliberar y evaluar todo lo acontecido en la reunión, acuerdan lo siguiente:
<Descripción de los acuerdos de los participantes, pudiendo incluir antecedentes, supuestos, entre otros temas previos considerados por los participantes de la reunión>
PROTOTIPO DEL SISTEMA:
<Descripción de las pantallas por módulo, bajo el siguiente esquema:
Módulo: nombre del módulo 1
Nombre de la pantalla: nombrePantalla
Descripción de la pantalla: detalle de las funcionalidades de la pantalla

Clasificación: **Uso Interno**, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 10
MCVDSS-DSI-0301 – Documento de Diseño del Sistema

	Oficina de Tecnologías de la Información	Código: MCVDSS-DSI-0301 Versión: 1.0
	Diseño del Sistema de Información	Fecha: 04/06/2025 Página: 4 de 20
SC-00y-20XX - <Proyecto/Sistema/Módulo>		

Diseño del Sistema de Información

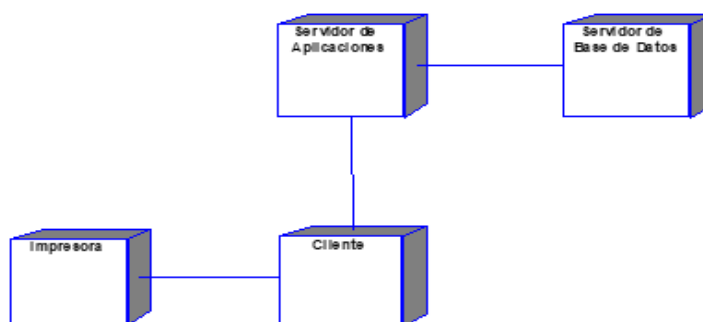
INDICACIONES:

- Por favor completar los <datos o información> que se solicita entre los símbolos <_ _>
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

I. DEFINICIÓN DE LA ARQUITECTURA DEL SISTEMA

I.1. Definición de Niveles de Arquitectura:

Los nodos que formarán parte del sistema son:



.<Diagrama de Nodos>

<Identificar los niveles involucrados en el sistema, colocar el diagrama de nodos respectivo y completar la Tabla siguiente:>

Nodos	Descripción los Nodos Involucrados	Relación	Tipo
Base de Datos	Motor de Base de Datos donde se guardará la información del sistema.	Servidor de Aplicaciones	Bidireccional
Cliente	PC donde el cliente se conectará a la aplicación a través de un navegador de Internet.	Servidor de Aplicaciones	Bidireccional
Servidor de Correos	Servidor utilizado para el envío de las notificaciones creadas en la aplicación	Servidor de Aplicaciones	Unidireccional
Impresora	Utilizado por el cliente para imprimir información relevante que considere pertinente	Cliente	Unidireccional

Los nodos del sistema están organizados en los siguientes niveles:

<Colocar los niveles considerados para los nodos definidos>

- Nivel 1: Cliente
- Nivel 2: Servidor de Aplicaciones
- Nivel 3: Base de Datos y Servidor de Correos

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 11
MCVDSS-DSI-0302 – Matriz de Trazabilidad

		Oficina General de Tecnologías de la Información									Código: MCVDS2-DSI-0302	
		Matriz de Trazabilidad									Versión: 1.0	
											Página: 1 de 1	
Identificación	Sub identificación	Descripción del requisito	Versión	Estado actual	Última fecha estado registrado	Criterios de aceptación	Nivel de complejidad	Diseño del producto	Desarrollo del producto	Estrategia de pruebas	Interesado (Stakeholder) dueño del requisito	Nivel de prioridad
Página 1												

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 12 MCVDSS-DSI-0303 – Plan de Integración del Sistema

	Oficina de Tecnologías de la Información	Código: MCVDSS-DSI-0303 Versión: 1.0
	Plan de Integración del Sistema	Fecha: 01/01/2025 Página: 4 de 12
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Plan de Integración del Sistema

INDICACIONES:

- Por favor completar los <datos o información> que se solicita entre los símbolos <_ _>
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

1. ALCANCE DE LAS PRUEBAS

1.1. Propósito

<El presente documento describe el Plan de Integración de los componentes de software <colocar el nombre del sistema desarrollado>

1.2. Referencia

<Se deberá listar la documentación a utilizar para la realización y ejecución del presente plan.>

1.3. Roles y Recursos

Recursos			
Rol	Responsabilidades específicas o comentarios	Necesario	Mínimo
Gestor de prueba			
Diseñador de prueba			
Probador			
...			

2. ESTRATEGIAS DE INTEGRACIÓN

2.1. Tipo de integración

<Seleccionar el tipo de integración a realizar. Entre ellos pueden ser:

- Integración descendente, es una estrategia de integración incremental a la construcción, en el cual se integran los módulos moviéndose en dirección hacia abajo por la jerarquía comenzando por el módulo principal.
- Integración ascendente, es donde la construcción empieza desde los módulos más bajos hacia el módulo principal, el procesamiento requerido de los módulos subordinados siempre está disponible y elimina la necesidad de resguardo.

En algunos de los casos se puede combinar ambas estrategias.>

Tipo de Integración	Realizable	Observaciones
	<input checked="" type="radio"/> SI <input type="radio"/> No	
	<input checked="" type="radio"/> SI <input type="radio"/> No	
	<input checked="" type="radio"/> SI <input type="radio"/> No	
	<input checked="" type="radio"/> SI <input type="radio"/> No	

Clasificación: **Uso Interno**, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 13
MCVDSS-DSI-0303 – Plan de Migración y Carga del Sistema

	Oficina de Tecnologías de la Información	Código: MCVDSS-DSI-0304 Versión: 1.0
	Plan de Migración y Carga del Sistema	Fecha: 01/01/2025 Página: 4 de 10
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Plan de Migración y Carga del Sistema

INDICACIONES:

- Por favor completar los <datos o información> que se solicita entre los símbolos <_ _>
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

1. ALCANCE DE LAS PRUEBAS

1.1. Propósito

< Está tarea se realiza si es necesaria una migración de datos de otros sistemas, o una carga inicial de información.>

1.2. Referencia

<Se deberá listar la documentación a utilizar para la realización y ejecución del presente plan.>

1.3. Roles y Recursos

Recursos			
Rol	Responsabilidades específicas o comentarios	Necesario	Mínimo

2. ESTRATEGIAS DE MIGRACIÓN Y CARGA

Se especifican las necesidades de migración o carga inicial de los datos requeridos por el sistema.

2.1. Especificación del entorno de migración y carga inicial de datos

<Se evalúa las necesidades de infraestructura, principalmente relacionadas con el modelo físico de datos, espacio de almacenamiento, ubicación.>

A continuación se describen los requisitos, herramientas o utilidades de software específicas para el entorno de migración y carga:

- ...
- ...

2.2. Definición de procedimientos de migración y carga inicial

Los procedimientos asociados a la migración y carga inicial de datos están relacionados con la preparación, la realización y la posterior verificación del proceso. Entre ellos se encuentran los siguientes:

<Si esta sección no aplica, colocar "No aplica" y justificar, a continuación ejemplos para cada tipo de procedimiento.>

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 14
MCVDSS-CSI-0401 – Plan de Implantación del Sistema

	Oficina de Tecnologías de la Información	Código: MCVDSS-CSI-0401 Versión: 1.0
Plan de Implantación del Sistema		Fecha: 01/01/2025 Página: 4 de 17
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Plan de Implantación del Sistema

INDICACIONES:

- Por favor completar los <datos o información> que se solicita entre los símbolos <_ _ >
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

1. ALCANCE DE LAS PRUEBAS

1.1. Propósito

< Establecer los lineamientos y tareas necesarias para instalar y probar el sistema de software desarrollado, para que la transición a los usuarios se realice efectiva y eficientemente>

<Definir las pruebas a realizar en la implantación:

- Las pruebas de implantación, cubre desde el diseño interno hasta aspectos tales como comunicaciones, comprueba que el sistema pueda generar volúmenes de información requeridos, si se ajusta a los tiempos deseados y que los procedimientos de respaldo, seguridad e interfaces con otros sistemas funcionen correctamente. (describir que es lo que se va implantar)
- Las pruebas de aceptación, tienen como objetivo validar que el sistema se ajusta a sus necesidades, las pruebas son realizadas por los usuarios. (describir que es lo que se va implantar).>

1.2. Referencia

<Se deberá listar la documentación a utilizar para la realización y ejecución del presente plan.>

1.3. Roles, Responsabilidades y Recursos

Rol	Responsabilidades específicas o comentarios	Recursos	
		Necesario	Mínimo
Gestor de prueba			
Diseñador de prueba			
Probador			
...			

2. REQUISITOS DE IMPLANTACIÓN

<Opcional. Se especifican los requisitos relacionados a los siguientes aspectos:


- Capacitación
- Infraestructura
- Instalación

<Si no se requiere debe indicarlo y justificar>


N°	Requisitos de Implantación	Descripción
----	----------------------------	-------------

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 15
MCVDSS-CSI-0402 – Manual de Usuario del Sistema

	Oficina de Tecnologías de la Información	Código: MCVDSS-CSI-0402 Versión: 1.0
Manual de Usuario del Sistema		Fecha: 01/01/2025 Página: 4 de 10
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Manual de Usuario del Sistema

INDICACIONES:

- Por favor completar los <datos o información> que se solicita entre los símbolos <_ _>
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

- I. Objetivo del Sistema**
 <Describir los objetivos del sistema>

- II. ALCANCE DEL SISTEMA**
 <Descripción del alcance>

- III. DESCRIPCIÓN GENERAL DEL SISTEMA**
 <Descripción del sistema considerando los puntos principales del mismo>
 <Descripción del acceso y seguridad del sistema>

- IV. FUNCIONALIDAD DEL SISTEMA**
 <Nombre de la funcionalidad 1>
 <Explicación de la funcionalidad 1>

 <Nombre de la funcionalidad 2>
 <Explicación de la funcionalidad 2>

- V. CONSULTAS Y REPOTES**
 <Nombre de la consulta o reporte 1>
 <Descripción>
 <Forma de obtención>

 <Nombre de la consulta o reporte 2>
 <Descripción>
 <Forma de obtención>

- VI. GLOSARIO DE TÉRMINOS**
 <Desarrollar un glosario de términos>

- VII. GLOSARIO DE PROBLEMAS FRECUENTES**
 <Describir los problemas frecuentes del software>

- VIII. DESCRIPCIÓN DE PERFILES**
 <Descripción de los distintos perfiles de usuarios>

Clasificación: *Uso Interno*, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 16
MCVDSS-CSI-0403 – Manual de Soporte Técnico del Sistema

	Oficina de Tecnologías de la Información Manual de Soporte Técnico	Código: MCVDSS-CSI-0403 Versión: 1.0 Fecha: 01/01/2025 Página: 4 de 10
<i>SC-002-20XX - <Proyecto/Sistema/Módulo></i>		

Manual de Soporte Técnico

INDICACIONES:

- Por favor completar las <datos o información> que se solicita entre los símbolos <__>
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

I. PROPÓSITO

<El presente documento describe las pautas a seguir para la solución de incidencias e instalación y configuración del sistema informático <colocar el nombre del sistema desarrollado>.>

II. ASISTENCIA DE MESA DE AYUDA Y SOPORTE TÉCNICO

II.1. DESCRIPCIÓN DEL PROCEDIMIENTO PARA LA ATENCIÓN INCIDENCIAS

II.1.1. PROBLEMA <AL INGRESAR AL APLICATIVO>

II.1.1.1. Verificar ingreso correcto al sistema

El link de ingreso al aplicativo es:

<<http://nombresistema.sunarp.gob.pe/inicio>>



II.1.1.2. Acciones en caso de error de acceso al sistema:

<Describir la acción a tomar>.

II.1.2. PROBLEMA <AL ACCEDER CON UN USUARIO AL APLICATIVO>

II.1.2.1. Error de ingreso de usuario


<Describir el error>.

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.

Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 17
MCVDSS-CSI-0404 – Manual de Operaciones del Sistema

	Oficina de Tecnologías de la Información	Código: MCVDSS-CSI-0404 Versión: 1.0
Manual de Operaciones del Sistema		Fecha: 01/01/2025 Página: 4 de 10
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Manual de Operaciones del Sistema

INDICACIONES:

- Por favor completar los <datos o información> que se solicita entre los símbolos <_ >
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

I. PROPÓSITO

< El presente documento describe los procedimientos a ejecutar del sistema <colocar el nombre del sistema desarrollado> por el operador del Centro de Cómputo >

II. DESCRIPCIÓN DE LOS PROCEDIMIENTOS EN LOTE (BATCH)

II.1. PROCEDIMIENTO DE BASE DE DATOS

<En esta actividad se debe listar los procedimientos de base de datos que tiene desarrollado el sistema >.

Ítem	Sistema	Procedimientos	Entorno de Ejecución	Horario	Periodicidad	Responsable de Ejecución	Responsable de desarrollo

II.2. PROCEDIMIENTO DE OPERACIONES


<En esta actividad se debe listar los procedimientos que ejecutaran los operadores de base de datos>.

Ítem	Sistema	Procedimientos	Entorno de Ejecución	Horario	Periodicidad	Responsable de Ejecución	Responsable de desarrollo

Clasificación: **Uso Interno**, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 18 MCVDSS-CSI-0405 – Reporte de Pruebas del Sistema

	Oficina de Tecnologías de la Información	Código: MCVDSS-CSI-0405 Versión: 1.0
Reporte de Pruebas del Sistema		Fecha: 01/01/2025 Página: 4 de 10
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Reporte de Pruebas del Sistema

INDICACIONES:

- Por favor completar las <datos o información> que se solicita entre los símbolos <_ _>
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

1. DATOS GENERALES

Proyecto:	<Indicar el nombre del proyecto (código si tiene) y nombre referencial o alias>		
Tipo de prueba:	<Tipo de pruebas a ejecutar: funcional, integración, regresión, carga, migración, etc.>		
Responsable:	<Indicar nombre del revisor(es)>	Rol:	<Rol que desempeña el responsable>
Lugar:	<Indicar el lugar de la revisión>	Fecha:	<Indicar la fecha de la revisión>
Hora Inicio:	<Indicar hora de inicio de la revisión>	Hora Fin:	<Indicar la hora de fin de la revisión>

Recursos			
Rol	Responsabilidades específicas o comentarios	Necesario	Mínimo

2. REPORTE DE PRUEBAS

Id. Prueba	Nombre de la prueba ejecutada	Resultado	Comentario / Id Anomalía
<Id del caso de prueba>		<OK/ No OK>	<Si presenta una anomalía generar un id y detallar en el la sección 2.>

3. ANOMALÍAS (DEFECTOS) DETECTADAS

Id Anomalía	Descripción de la anomalía	Función afectada	Tipo anomalía (**)	Id. Prueba	Criticidad (*)	Responsable	Fecha cierre anomalía
		<Función o requisito afectado>				<Nombre del responsable de levantar la anomalía>	<dd/mm/yy>
<Si desea puede colocar un gráfico relacionado a la anomalía de la fila anterior>							

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 20
MCVDSS-IAS-0501 – Plan de Implantación del Sistema (actualizado)

	Oficina de Tecnologías de la Información	Código: MCVDSS-IAS-0501 Versión: 1.0
	Plan de Implantación del Sistema <i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>	Fecha: 01/01/2025 Página: 4 de 14

Plan de Implantación del Sistema

INDICACIONES:

- Por favor completar los <datos o información> que se solicita entre los símbolos <_ >
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

1. PROPÓSITO

<Establecer los lineamientos y tareas necesarias para instalar y probar el sistema de software desarrollado, para que la transición a los usuarios se realice efectiva y eficientemente.>

<Definir las pruebas a realizar en la implantación:

- Las pruebas de implantación, cubre desde el diseño interno hasta aspectos tales como comunicaciones, comprueba que el sistema pueda generar volúmenes de información requeridos, si se ajusta a los tiempos deseados y que los procedimientos de respaldo, seguridad e interfaces con otros sistemas funcionen correctamente. (describir que es lo que se va implantar)
- Las pruebas de aceptación, tienen como objetivo validar que el sistema se ajusta a sus necesidades, las pruebas son realizadas por los usuarios. (describir que es lo que se va implantar). >

2. REFERENCIA

<Se deberá listar la documentación a utilizar para la realización y ejecución del presente plan.>

3. ROLES Y RESPONSABILIDADES


Rol	Responsabilidades específicas	Responsable
Gestor de Pruebas	Supervisar y dirigir el trabajo... <ul style="list-style-type: none"> Revisar y aprobar el Plan de Pruebas. Revisar y aprobar los Casos de Prueba. Elaborar el Acta de Conformidad de Pruebas. 	■
Diseñador de Pruebas	Identificar, priorizar e implementar los casos de prueba. Responsabilidades: <ul style="list-style-type: none"> Elaborar el Plan de Pruebas. Diseñar los Casos de Prueba. 	■
...

4. REQUISITOS DE IMPLANTACIÓN


<Se especifican los requisitos relacionados a los siguientes aspectos: (Opcional)

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 22
MCVDSS-IAS-0503 – Acta de Conformidad General & Pase a Producción

	Oficina de Tecnologías de la Información Acta de Conformidad General & Pase a Producción	Código: MCVDSS-IAS-0503 Versión: 1.0 Fecha: 01/01/2025 Página: 1 de 2
SC-00y-20XX - <Proyecto/Sistema/Módulo>		

CONVOCATORIA	
Requerimiento:	<Nombre del Proyecto / Sistema / Módulo / Proceso / Componente/Servicio>
Solicitud N°:	<SC-002-20YY>
Convocado por:	<Ap. Nombres> – <u>Responsable</u> del Proyecto
Asunto:	<Motivo de la reunión en el marco del requerimiento >
Referencia:	<Documento(s) de Referencia >
Fecha:	dd/mm/20YY Hora: hh:mm am/pm a hh:mm am/pm
Lugar:	Sede Central – Sunarp - Sala de reuniones de la <u>OTI</u>

AGENDA	
1.	Informe del estado de la capacitación del <Nombre del Proyecto / Sistema / Módulo / Proceso / Componente/Servicio>.
2.	Aprobación de la implementación ...
3.	Otros puntos relacionados

DESARROLLO DE LA REUNIÓN	
Inicio de la reunión: hh:mm am/pm	
N°	Tema Acción
< SOLICITANTE: >	
<RESPONSABLE: <Nombre Completo del <u>Responsable</u> del Requerimiento>	
CARGO/ROL: <Nombre del Cargo/Rol>	
UNIDAD ORGÁNICA: <Descripción de la Unidad Orgánica>	
>	
< DESCRIPCIÓN: >	
<Funcional, Alcance, Objetivos, Valor Incorporado, Beneficios>	
< CONSIDERACIONES / OBSERVACIONES: >	
<Descripción de las consideraciones / observaciones>	


CONVOCADOS / ASISTENTES					
Fin de la reunión: hh:mm am/pm. Los asistentes firman en señal de conformidad con el acta.					
N°	Nombre	Cargo	Oficina	Asistencia	Firma
1		Responsable de Desarrollo	<u>OTI</u>	(Si)	
2		Analista de Sistemas	<u>OTI</u>	(Si)	
4		Jefe del Área Usuaría	<u>DTR</u>	(Si)	
5		Usuario Líder	<u>DTR</u>	(Si)	

Clasificación: **Uso Interno**, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 23
MCVDSS-MSI-0600 – Solicitud de Cambios y/o Mantenimiento

	Oficina de Tecnologías de la Información Solicitud de Cambios y/o Mantenimiento del Sistema	Código: MCVDSS-MSI-0600 Versión: 1.0 Fecha: 01/01/2025 Página: 1 de 2
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Solicitud de Cambios del Sistema

1. Generalidades

1.1. Identificación de la solicitud:

Solicitud N°:	<SC-00x-20YY>
Descripción abreviada de la solicitud:	<Breve descripción de la solicitud>
Fecha de la Solicitud:	dd/mm/20YY
Referencia:	<Indicar los documentos de gestión relacionados al proyecto>

1.2. Información del Solicitante:

Nombre:	<Apellidos y nombres>
Área:	<Área/Oficina, Sede/Zona Registral>
Cargo:	<Cargo>
Correo electrónico:	<Correo electrónico Institucional>
Teléfono:	<Anexo>

2. Información del requerimiento

Requerimiento N°1:	<i>NOTA: Copiar este cuadro para cada requerimiento</i>	
Tipo de requerimiento: Ajuste software existente <input type="checkbox"/> Nuevo componente a software existente <input type="checkbox"/>	Clasificación: Sistema Registral <input type="checkbox"/> Sistema Administrativo <input type="checkbox"/>	Prioridad: Alta <input type="checkbox"/> Media <input type="checkbox"/> Baja <input type="checkbox"/>
REQUERIMIENTO <Describe el requerimiento de manera sencilla, clara, concisa, completa, consistente, comprensible y sin mezclar varios requerimientos en uno> <El requerimiento especifica lo que el sistema informático debe hacer (o ser) y en algunos casos lo que no debe hacer. Describe alternativamente el (los) servicio(s) que debe proporcionar el sistema, la manera en que debe reaccionar a determinadas entradas y de cómo se debe comportar en		

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 24
MCVDSS-MSI-0601 – Plan de Mantenimiento del Sistema

	Oficina de Tecnologías de la Información	Código: MCVDSS-MSI-0601 Versión: 1.0
Plan de Mantenimiento del Sistema		Fecha: 01/01/2025 Página: 4 de 12
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Plan de Mantenimiento del Sistema

INDICACIONES:

- Por favor completar los <datos o información> que se solicita entre los símbolos <_ _>
- Los puntos a los que se hace referencia en el presente documento, no necesariamente deben ser aplicados en su totalidad, se desarrollarán de acuerdo al tipo de proyecto. (En esos casos sólo colocar "No Aplica")

1. ALCANCE DE LAS PRUEBAS

1.1. Propósito

<Identifica los elementos necesarios para el mantenimiento del sistema informático <nombre del sistema>>

1.2. Referencia

<Se deberá listar la documentación a utilizar para la realización y ejecución del presente plan.>

1.3. Roles, Responsabilidades y Recursos

Rol	Responsabilidades específicas	Responsable

2. RECURSOS

2.1. Herramientas

<A continuación se lista las herramientas involucradas en el mantenimiento del sistema a realizar.>

2.2. Hardware y software

< A continuación se lista el hardware y software involucrados en el mantenimiento del sistema a realizar.>

3. DESCRIPCIÓN DEL SISTEMA

3.1. Descripción del sistema

<Se presenta una lista con una breve descripción de todos los componentes y artefactos relevantes del sistema que son de utilidad para poder hacer el mantenimiento correspondiente


4. PROCESOS Y PROCEDIMIENTOS

4.1. Solicitud del requerimiento de mantenimiento

<Completar el formato de <MCVDSS-EVS-0102 - Catálogo de Requisitos N° nnnn>, y referenciar en esta sección>

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 25
MCVDSS-MSI-0602 – Acta de Conformidad de Mantenimiento del Sistema

	Oficina de Tecnologías de la Información Acta de Conformidad de Mantenimiento	Código: MCVDSS-MSI-0602 Versión: 1.0 Fecha: 01/01/2025 Página: 1 de 2
SC-00y-20XX - <Proyecto/Sistema/Módulo>		

CONVOCATORIA	
Requerimiento:	<Nombre del Proyecto / Sistema / Módulo / Proceso / Componente/Servicio>
Solicitud N°:	<SC-00X-20YY>
Convocado por:	<Ap. Nombres> – Responsable del Proyecto
Asunto:	<Motivo de la reunión en el marco del requerimiento>
Referencia:	<Documento(s) de Referencia >
Fecha:	dd/mm/20YY
Lugar:	Sede Central – Sunarp - Sala de reuniones de la <u>OTI</u>


AGENDA	
1.	Informe del estado de la capacitación del <Nombre del Proyecto / Sistema / Módulo / Proceso / Componente/Servicio>.
2.	Aprobación de actividades de mantenimiento ...
3.	Otros puntos relacionados

DESARROLLO DE LA REUNIÓN	
Inicio de la reunión: hh:mm am/pm	
N°	Tema
Acción	
<Descripción de los acuerdos de los participantes, pudiendo incluir antecedentes, supuestos, entre otros temas previos considerados por los participantes de la reunión>	
DESCRIPCIÓN:	
<Funcional, Alcance, Objetivos, Valor Incorporado, Beneficios, otros que consideren, sobre los cuales se da conformidad>	
AVANCES IMPLEMENTADOS:	
<Descripción de los Avances del Servicio Informático prestado al Área Usuaria >	
CONSIDERACIONES / OBSERVACIONES:	
<Descripción de las consideraciones / observaciones>	

ACUERDOS DE LA REUNIÓN	
Los aquí presentes, luego de deliberar y evaluar todo lo acontecido en la reunión, acuerdan lo siguiente:	


Clasificación: **Uso Interno**, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

	DIRECTIVA QUE APRUEBA LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO	Codificación: DI-001-2025-SUNARP-OTI
---	--	--

Anexo N° 26

MCVDSS-MSI-0603 – Solicitud de Pase a Producción del Sistema

	Oficina de Tecnologías de la Información	Código: MCVDSS-MSI-0603 Versión: 1.0
Solicitud de Pase a Producción		Fecha: 01/01/2025 Página: 1 de 3
<i>SC-00y-20XX - <Proyecto/Sistema/Módulo></i>		

Nombre del Proyecto y/o Requerimiento:	
---	--

Fecha del pase a producción:	
Responsable del pase a producción:	
Documento que originó el proyecto:	
Fecha del documento que origino el proyecto:	
Área usuaria:	

1. DIAGRAMA DE CONTEXTO
 <Se debe indicar los sistemas que participan en el pase a producción>

2. SISTEMAS INVOLUCRADOS QUE SE VERÁN AFECTADOS

Sistemas:	
-----------	--

3. LISTA DE PERSONAL DE DESARROLLO QUE HA TRABAJADO LA NUEVA VERSIÓN
 <Se debe listar el personal que ha participado en la modificación/adequación del sistema>

4. LISTA DE OBJETOS DE BASE DE DATOS AFECTADOS
 <Se debe listar todos los objetos de BD (procedimientos, funciones, etc.) que forman parte del sistema>

5. CONFORMIDAD DE LOS RESPONSABLES DEL ÁREA DE BASE DE DATOS
 <Se debe listar el personal que ha dado la conformidad en la modificación/adequación de objetos de BD del sistema>

6. DESCRIPCIÓN DE LAS FUNCIONALIDADES IMPLEMENTADAS
 <Se debe realizar una descripción detallada de las nuevas funcionalidades>

7. RUTA EN DONDE SE UBICA EL EAR / EJECUTABLE / SCRIPTS
 <Se debe listar el personal que ha participado en la modificación/adequación del sistema>

Clasificación: Uso Interno, no debe ser divulgado a terceros sin la autorización de la Sunarp.
 Copia no controlada, el uso de un documento obsoleto es responsabilidad del usuario, sírvase verificar su vigencia.

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.