



AGENCIA PARA LA REINCORPORACIÓN Y NORMALIZACIÓN (ARN)

GUÍA DE DESARROLLO DE SOFTWARE

BOGOTÁ D.C. NOVIEMBRE DE 2024

	GUÍA DE DESARROLLO DE SOFTWARE		CÓDIGO: TI-G-06
			FECHA 2024-11-14 VERSIÓN V- 2

TABLA DE CONTENIDO

1. OBJETIVOS	3
2. ALCANCE	3
3. TÉRMINOS Y DEFINICIONES	3
4. CONSIDERACIONES GENERALES	4
5. CONTENIDO Y DESARROLLO.....	5
5.1. FASES DE DESARROLLO Y METODOLOGÍA DE DESARROLLO	5
5.2. ESTÁNDARES DE PROGRAMACIÓN Y PRÁCTICAS RECOMENDADAS	11
5.3. CONTROL DE VERSIONES	14
5.4. ARQUITECTURA DEL SISTEMA DE INFORMACION MISIONAL	14
5.5. AMBIENTES DE DESARROLLO	15
5.6. PLAN DE CALIDAD DEL SOFTWARE	16
5.7. HERRAMIENTAS PARA GESTIÓN DE PROYECTOS DE DESARROLLO	23

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

1. OBJETIVOS

- Mejorar la calidad del software que se desarrolla en la Agencia, documentando recomendaciones, estándares y mejores prácticas aplicables al proceso.
- Servir como documento guía para conducir el proceso de desarrollo de software.

2. ALCANCE

Las recomendaciones aplican a los proyectos de software que ejecute la Agencia, y que contengan componentes de desarrollo de software.

3. TÉRMINOS Y DEFINICIONES

ARN: Agencia para la Reincorporación y Normalización.

ARPA: Aplicación de Apoyo a la Reincorporación y Procesos de Atención.

BUFFER DE MEMORIA: Es un espacio de memoria, en el que se almacenan datos de manera temporal.

CU: sigla usada para hacer referencia a los documentos de Caso de Uso.

GSI: grupo de Sistemas de Información de la Oficina de Tecnología de la Información.

NTC 5854: la Norma Técnica Colombiana (NTC) 5854 fue redactada y diseñada para establecer los requisitos de accesibilidad que deben cumplir los portales web del Estado Colombiano. Estos requisitos se agrupan en tres niveles de conformidad: A, AA, y AAA. Esta norma fue desarrollada empleando como documento de referencia “Las Pautas de Accesibilidad para el Contenido web (WCAG) 2.0 del 11 de diciembre de 2008”. El objetivo de esta norma es promover las buenas prácticas que permitan que el contenido de la web sea accesible a todos los usuarios independiente de su condición, para que puedan percibir, entender, navegar, interactuar y contribuir con los sitios web

	CÓDIGO: TI-G-06	
	FECHA 2024-11-14	VERSIÓN V- 2

PPR: Persona en proceso de Reintegración o Reincorporación.

RFC: la Solicitud de Cambio (Request for Change, RFC) es una requisición formal de Cambio en espera de ser implementada. Incluye detalles del Cambio propuesto, y puede estar en formato electrónico o en papel. Las siglas (en inglés) RFC a menudo se usan equivocadamente para referirse al Registro de Cambio o al Cambio mismo.

SARA: Sistema de Apoyo a la Reintegración.

SIRR: Sistema de Información para la Reintegración y la Reincorporación, es el sistema central de la Agencia para la Reincorporación y Normalización, donde se encuentra toda la información relacionada con las Personas en Proceso de Reintegración y su proceso de reintegración o reincorporación.

SOLID: Single responsibility, Open-closed, Liskov substitution, Interface segregation and Dependency inversion) es un acrónimo mnemónico introducido por Robert C. Martin¹² a comienzos de la década del 2000 que representa cinco principios básicos de la programación orientada a objetos y el diseño.¹

USUARIO FINAL: persona que utiliza las aplicaciones y sistemas de información de la entidad para apoyar sus actividades misionales y administrativas.

USUARIO PRIVILEGIADO: usuario de las aplicaciones y sistemas de información de la entidad que cuenta con permisos para realizar operaciones de consulta, creación, edición o eliminación de información.

USUARIOS EXTERNOS: personas que no hacen parte de la Agencia y que utilizan las aplicaciones y sistemas de información de la entidad. Puede ser ciudadanía en general o funcionarios de otras entidades públicas o privadas.

4. CONSIDERACIONES GENERALES

Este documento en su aplicabilidad es de competencia de los empleados públicos y contratistas del Grupo de Sistemas de Información de la Oficina de Tecnologías de la Información.

¹ Principios de SOLID, Antonio Leyva. Recuperado de: <https://devexperto.com/principio-responsabilidad-unica/>

	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

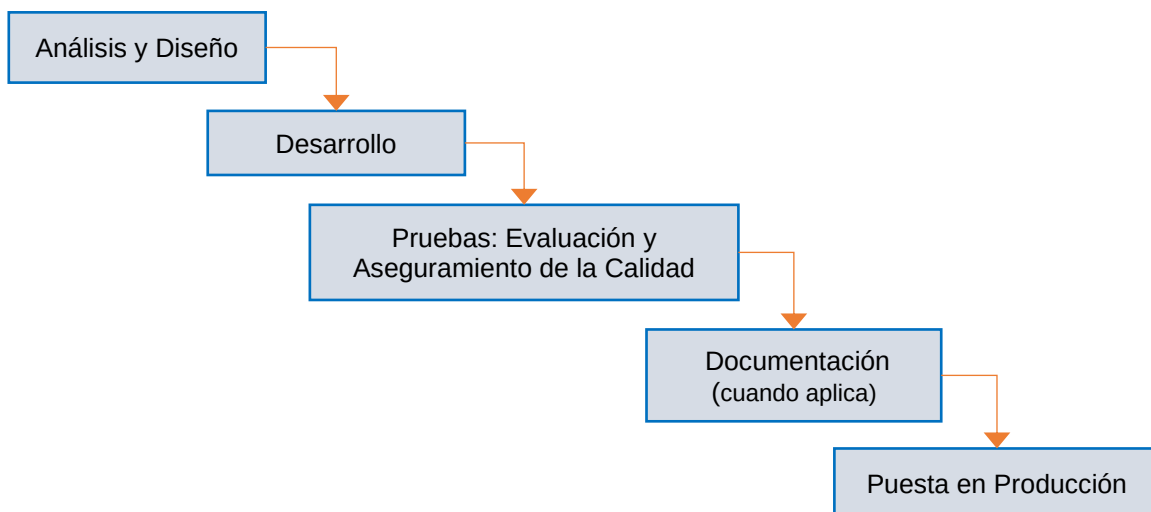
5. CONTENIDO Y DESARROLLO

5.1. FASES DE DESARROLLO Y METODOLOGÍA DE DESARROLLO

Dada las condiciones de la Agencia y su necesidad de mantener la seguridad de la información, se determina como metodología de desarrollo RUP (Proceso de Desarrollo Unificado) por ser un proceso de desarrollo de software formal que junto con el Lenguaje Unificado de Modelado UML, constituyen la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas de información. No obstante, lo anterior, se incorporan a la metodología elementos y prácticas de SCRUM como la gestión de backlogs, tareas, iteraciones y reuniones semanales de equipo.

En la oficina de Tecnologías de la Información – Grupo de Sistemas de Información, se establece que los proyectos de desarrollo de software para nuevas aplicaciones o funcionalidades y de mantenimiento de aplicaciones y/o funcionalidades existentes, deberán observar las siguientes fases del ciclo de vida de desarrollo de software, alineado con el TI-P-01 Procedimiento Atención a Requerimientos de Sistemas De Información:

Fases del Ciclo de Vida de Desarrollo de Software



Fuente: Propia de la OTI

Cuando se trate de implementación de nuevos sistemas de información o aplicaciones, estos proyectos pueden enmarcarse de acuerdo con lo indicado en

"Toda impresión física de este documento se considera Documento no Controlado.

La versión vigente se encuentra en el software para la administración de la planeación y la gestión"

Página 5 de

	CÓDIGO: TI-G-06	
	FECHA 2024-11-14	VERSIÓN V- 2

GUÍA DE DESARROLLO DE SOFTWARE

el documento TI-G-21 - Guía Gestión de Proyectos de Tecnologías de la Información, con el objetivo de que se pueda realizar seguimiento, así como establecer fases de implementación en las que se logre identificar las necesidades de aprovisionamiento de infraestructura, así como la gestión de riesgos asociados.

Por otro lado, también se podrán incluir otras metodologías, estándares y mejores prácticas que puedan aplicarse a proyectos de tecnologías emergentes como Automatización Robótica de procesos - RPA, Inteligencia Artificial entre otras conforme a las necesidades de la entidad.

5.1.1 Análisis y Diseño

En esta etapa los analistas del GSI se relacionan con los usuarios finales del sistema, se realizan mesas de trabajo a fin de definir los requisitos a cumplir por el proyecto o funcionalidad. Una vez que se recaban todos los requisitos, los analistas vuelven a reunirse con los usuarios para repasarlos en una etapa de verificación, realizando la estimación de esfuerzo de la solución propuesta, luego en caso de requerirse se plantea el diseño de la funcionalidad o aplicación y se documenta en los casos de uso respectivos que deben ser aprobados por los usuarios finales y contar con el aval del Administrador Funcional. Dentro de esta etapa se deben contemplar las siguientes recomendaciones de seguridad en la información:

- a. Nivel de confianza requerido con relación a la autenticación de usuario y los procesos de autenticación de usuario del negocio, al igual que para usuarios privilegiados o técnicos:

Aplicaciones con autenticación integrada con directorio activo: Esta autenticación se utiliza para aplicaciones de uso interno de la entidad, ya que se requiere que los usuarios cuenten con registro de usuario en el directorio activo, lo cual también les da acceso a los equipos y recursos de red de la entidad. Entre las aplicaciones que cuentan con este tipo de autenticación están el SIRR, SARA y ARPA.

Aplicaciones con autenticación integrada con el servicio ciudadano de Autenticación Digital: Esta autenticación se usa para aplicaciones que son utilizadas por usuarios externos a la entidad. Para hacer uso de esta autenticación se requiere que el usuario se registre previamente en el portal Gov.co. Este tipo de autenticación es utilizada principalmente para servicios que sean publicados en la Sede Electrónica de la entidad, como la consulta de notificaciones de participantes.

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

Autenticación con usuarios propios de la aplicación: En esta autenticación se permite el registro de usuarios en la base de datos de la aplicación, para lo cual se debe garantizar que las contraseñas se encuentren cifradas en la base de datos. Se utiliza únicamente en los casos en los que no sea posible utilizar la autenticación integrada con directorio activo y/o autenticación digital. Este tipo de autenticación es utilizada en SARA para consulta de entidades externas con las que se tienen convenios de intercambio de información.

Para este escenario de autenticación se deben tener en cuenta la Política de control de acceso detallado en su literal “Credenciales de acceso”, que se encuentra relacionada en TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información.

Autenticación biométrica: En esta autenticación se permite el registro de datos biométricos en la base de datos de la aplicación. Se utiliza en ARPA para validar el registro de la asistencia por parte de la población objeto. En estos casos se aplican las siguientes recomendaciones:

- Considerar lo estipulado en la Resolución 5633 de 2016 de la Registraduría Nacional y sus anexos 1 y 2.
- Cumplir con las disposiciones legales relacionadas con la protección de datos personales de acuerdo con documento DE-M-06 Manual de Protección de Datos Personales.
- Determinar y validar las demás características contribuyen con el cumplimiento de del documento TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información en la política relacionada a control de acceso.

- b. Definir las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad, integridad;

El sistema debe contar con medidas preventivas y reactivas para garantizar la confidencialidad y la integridad de la información del sistema. El sistema debe contar con los siguientes mecanismos:

- **Confidencialidad:** El sistema debe garantizar que el acceso a la información tenga varios niveles de confidencialidad, por lo tanto, el sistema debe contar con:

Transporte seguro: La información debe viajar por un canal seguro para el transporte de los datos a través de internet y así asegurar la confidencialidad de la información, por lo que deberá ser capaz de

	CÓDIGO: TI-G-06	
	FECHA 2024-11-14	VERSIÓN V- 2

GUÍA DE DESARROLLO DE SOFTWARE

operar en HTTPs.

Autorización: El sistema deberá tener políticas de acceso a la información mediante roles para impedir que los usuarios tengan acceso a información o procesos no autorizados.

- **Integridad:** El sistema debe tener mecanismos que impidan realizar modificaciones no autorizadas a la información para evitar que la información pierda exactitud. Para esto, el sistema debe contar con mecanismos de validación de la información, que permitan que durante las transacciones de datos en los procesos del sistema, se realicen las validaciones del lado del cliente y del lado del servidor para garantizar la exactitud de la información.
 - **Disponibilidad:** El sistema debe garantizar la disponibilidad de la información a las personas que cuenten con los privilegios de acceso.
- c. Definir los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso y seguimiento, y de no repudio;
- Dentro de los documentos de Arquitectura de nuevos proyectos o aplicaciones se deberá contemplar un ítem donde se definan los requisitos de ingreso, seguimiento y de no repudio.
- d. Establecer los requisitos exigidos por otros controles de seguridad, (interfaces con el ingreso o seguimiento, o los sistemas de detección de fuga de datos).

En los documentos de caso de uso se debe documentar en el apartado 3. Actores y Permisos, los roles, permisos y nivel de acceso a la información que deberán tener los usuarios para acceder a la aplicación.

- e. Una vez finalizada la etapa de requerimientos los casos de uso, o arquitectura deben ser cargados en el repositorio <http://otidocs.acr.int/sites/OTI>, adicionalmente los casos de uso deben ser incluidos en el inventario de casos de uso.
- f. Los casos deben ser nombrados según la siguiente nomenclatura: CU-SISTEMA-MODULO-XXXX

	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

CU	Que corresponde a la sigla caso de uso
Sistema	Corresponde a una sigla que corresponde al sistema o ambiente donde se desarrollara el caso de uso (SIRR SARA, INTRANET)
Módulo	Nombre que referencia al módulo a desarrollar (Jurídica, Plan de Trabajo, etc.)
Consecutivo	Número Consecutivo compuesto por 4 dígitos de los casos de uso por módulo

Ejemplo: CU-SIR-PLANDETRABAJO-0001

- g. El requerimiento debe ser documentado en el formato de caso de uso “TI-F-03 Formato Caso de Uso”, publicado en SAPYG.

Una vez documentado el caso de uso, éste es validado y aprobado (mediante firma electrónica o correo electrónico) por el usuario solicitante, el administrador funcional del SIRR, el jefe o coordinador del área solicitante y el coordinador del grupo de sistemas de información, asegurando la pertinencia y exactitud del requerimiento.

5.1.2 Desarrollo

Esta etapa se refiere al desarrollo del software según las definiciones realizadas en los documentos de casos de uso aprobados y firmados, durante en la etapa de análisis y diseño.

En la construcción del software se deberán tener en cuenta las recomendaciones que se describen en el ítem **5 Estándares de programación y prácticas recomendadas** del presente documento.

Para el caso del desarrollo de reportes a través de la herramienta de Reporting Services se deben nombrar los informes con el código del caso de uso con el que se especificó, a partir de la publicación de la presente guía.

Una vez finalizado el desarrollo se debe realizar el empaquetamiento y la preparación del despliegue en ambiente de pruebas, con lo cual el desarrollador deberá solicitar caso a la mesa de ayuda con el fin de asegurar:

- a. Realizar la preparación del ambiente de pruebas:
 - Se debe realizar la instalación, publicación o despliegue del software desarrollado o modificado en los servidores de aplicación y/o base de datos.

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

b. Preparación de los datos y estructuras de pruebas:

- Se debe verificar si se requiere preparar datos del ambiente productivo al ambiente de pruebas.
- Realizar ajustes en la configuración de roles, en caso de que sea requerido para el funcionamiento del software en el ambiente de pruebas.

5.1.3 Pruebas y Aseguramiento de la Calidad

Dentro de esta etapa se contemplan dos eventos:

- Prueba de los desarrollos realizados tratados en detalle en el capítulo 7. PLAN DE CALIDAD DEL SOFTWARE del presente documento.
- Validación y aprobación de las actas de cierre por parte del jefe de área o coordinador del área solicitante, el administrador funcional, el coordinador del grupo de sistemas de información o sus delegados y los profesionales que participaron en el requerimiento. Para lo anterior se debe aplicar el formato TI-F-02 Acta de Cierre de Funcionalidad o Requerimiento.

5.1.4 Documentación

En esta fase se crean los instructivos de usuario de las funcionalidades (cuando se requiere) o aplicaciones desarrolladas, estos documentos deben ser publicados en el portal SIRR.

De requerirse capacitación complementaria a la documentación, esta deberá ser coordinada por el área usuaria. En caso de que la dependencia usuaria requiera la capacitación del apoyo de los profesionales de la OTI que participaron del proyecto o desarrollo, deberá solicitarlo a través de caso registrado en el Centro de Servicios por vía correo electrónico <Soporte@reincorporacion.gov.co>.

5.1.5 Despliegue y Puesta en Producción

En esta fase se crea la solución de la nueva funcionalidad o aplicación y se solicita la publicación en ambiente productivo al Grupo de Infraestructura y Soporte a través de un registro en la herramienta de mesa de ayuda en el marco de la gestión de cambios y con el diligenciamiento del formato TI-F-05 Requerimiento de Cambio (RFC).

	CÓDIGO: TI-G-06	
	FECHA 2024-11-14	VERSIÓN V- 2

5.2. ESTÁNDARES DE PROGRAMACIÓN Y PRÁCTICAS RECOMENDADAS

En este apartado se referencian los principios, estándares y mejores prácticas para la construcción de sistemas, los cuales deberán ser observados en las actividades de implementación de sistemas de información.

También se definen las condiciones de seguridad que se deben observar diferenciadas para los nuevos sistemas y para el mantenimiento a los sistemas existentes.

5.2.1 Estándar de Seguridad de Aplicaciones WEB

Los nuevos sistemas de información en las fases de diseño y construcción deben considerar las recomendaciones del Estándar de Verificación de Seguridad en Aplicaciones, actualmente el estándar vigente es OWASP. Las consideraciones de seguridad que apliquen a los nuevos sistemas se deben registrar en el formato **TI-F-15 Verificación de requisitos de seguridad de la información en aplicaciones de software**.

Para el mantenimiento de sistemas existentes se deberán incluir verificaciones de seguridad en su justa medida para garantizar que los sistemas conserven sus condiciones de seguridad, las cuales deben ser documentadas de acuerdo con lo establecido en el numeral 7- Plan de calidad de software del presente documento.

La información de detalle del proyecto OWASP y el estándar, puede consultarse en el sitio web oficial: https://www.owasp.org/index.php/Sobre_OWASP

5.2.2 SOLID

Con el propósito de que los diseños de software sean más comprensibles, flexibles y mantenibles se recomienda, en los casos en los que aplique, la aplicación de los 5 principios SOLID:

- Principio de Responsabilidad Única (Single Responsibility Principle)
- Principio Open/Closed (Open/Closed Principle)
- Principio de Sustitución de Liskov (Liskov Substitution Principle)
- Principio de Segregación de Interfaces (Interface Segregation Principle)
- Principio de Inversión de Dependencias (Dependency Inversion Principle)

5.2.3 Especificaciones de Codificación para Aplicaciones WEB

- HTML 5: <https://html.spec.whatwg.org/multipage/>

	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

- CSS 3.0: <https://www.w3.org/Style/CSS/specs.en.html>
- ECMAScript: <https://www.ecma-international.org/publications-and-standards/standards/ecma-262/>
- WCAG 2.1: <https://www.w3.org/TR/WCAG21/>
- Norma técnica nacional de accesibilidad web NTC 5854: <http://ntc5854.accesibilidadweb.org/>

Para las **aplicaciones desarrolladas para escritorio de Windows** como lo es la aplicación ARPA, deben cumplir los lineamientos de accesibilidad documentados por Microsoft en su página:

<https://docs.microsoft.com/es-es/windows/uwp/design/accessibility/accessibility-overview>

5.2.4 Estándares de Codificación de Lenguajes de Programación

Teniendo en cuenta que las tecnologías utilizadas en la ARN son herramientas de Microsoft, se ha propuesto la implementación de la guía de Convenciones de código de C# propuesta por Microsoft en su página:

<https://docs.microsoft.com/es-es/dotnet/csharp/programming-guide/inside-a-program/coding-conventions> para los desarrollos en SIRR, ARPA y SARA.

Igualmente se tendrá en cuenta la siguiente documentación para nombrar los objetos, clases y demás componentes del código:

<https://docs.microsoft.com/en-us/dotnet/standard/design-guidelines/capitalization-conventions>

Algunos ejemplos de la notación a utilizar son:

Identificador	Case	Ejemplo	Descripción
Clase	Pascal	Actividad, Persona, Programación	Utilizar nombres que identifiquen la entidad desde el punto de vista del desarrollador; los nombres deberán reflejar escenarios de uso. No usar guion bajo en los nombres de clases.

	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

Identificador	Case	Ejemplo	Descripción
Tipo de enumeración	Pascal	TipoDocumento	Usar sustantivos para los nombres, no utilizar prefijos.
Valores de enumeración	Pascal	Cédula, TarjetaIdentidad, RegistroCivil	Usar sustantivos para los nombres, no utilizar prefijos.
Evento	Pascal	OnClickEnrolar_Click	No utilizar abreviaturas, se debe colocar la palabra On, seguida del nombre del control, la descripción del evento y finalmente la acción del evento, separada por _.
Excepción	Pascal	FileNotFoundException	Termina el nombre con la palabra "Exception".
Constantes	Pascal	NOMBRE_REPOSITARIO	El nombre debe ser en letras mayúsculas y usar guion _ cuando el nombre está conformado por más de una palabra.
Interfaz	Pascal	I Actividad	Nombrar interfaces con sustantivos o adjetivos que describan el funcionamiento y utilizar como prefijo la letra I.
Método	Pascal	ConsultarActividades, ReprogramarActividad	Los nombres de los métodos deben ser verbos para describir la acción del método y facilitar a los desarrolladores la comprensión de lo que hace el método
Espacio de nombres	Pascal	ACR.SIPAS.Model	<Compañía>.<Proyecto>.<Funcionalidad>
Parámetro	Camel	nombres, apellidos, fecha Actividad	Utilizar nombres descriptivos y significativos.
Propiedad	Pascal	Edad, EsCabezaFamilia	Asignar nombres a las propiedades mediante un sustantivo o un adjetivo. Denomine las propiedades booleanas con una frase afirmativa.

5.2.4 Estándar de Nombramiento y Codificación de Base de Datos

Para los diseños y desarrollos que impliquen creación de bases de datos, tablas, procedimientos almacenados u otros objetos de base de datos se deberán seguir los lineamientos que para este efecto defina el Grupo de Infraestructura y Soporte.

5.2.5 Recomendación para el Nombramiento de los Reportes

Los reportes desarrollados deben ser nombrados con el mismo código de caso de uso documentado para su desarrollo siguiendo la codificación descrita en el literal 4.1.1 f) de este documento.

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

5.3. CONTROL DE VERSIONES

El control de versiones del código fuente debe protegerse mediante el uso del repositorio de código fuente.

- Librerías de fuentes de programas: Todo código desarrollado o actualizado debe alojarse en el servidor <http://azuredevops.reincorporacion.gov.co:8080> a través de la herramienta de control de versiones Team Foundation Server en el proyecto OTI/ACR ubicándolo en el espacio correspondiente a la aplicación o proyecto al que pertenezca.
- Al realizar una entrada en el repositorio, el código fuente de los programas y las librerías de las fuentes de los programas se debe escribir una descripción corta del código y si es una actualización o control de cambio se debe escribir un comentario del cambio realizado, adicionalmente el código desarrollado se debe enlazar a la tarea de desarrollo asignada en el Azure DevOps.
- Solo los funcionarios y contratistas del Grupo de Sistemas de Información están autorizados para crear, consultar y actualizar nuevos proyectos y/o código fuente. El acceso a los proyectos se controla a través el panel de control del Azure DevOps donde se configuran los usuarios y/o grupos que podrán acceder a los proyectos.
- Todos los Plug-Ing y Stored Procedure después de desarrollados deben ser registrados en el archivo Inventario de Plug-Ins y SP publicado en la ruta: <http://otidocs.acr.int/sites/OTI/Documentos%20compartidos/OTI/GASI/Desarrollos%20Internos/Inventario%20de%20Plug-Ins%20y%20Stored%20Procedure>

5.4. ARQUITECTURA DEL SISTEMA DE INFORMACION MISIONAL

5.4.1 SIRR

Se referencia a continuación la ubicación del documento de línea base del servicio del SIRR.

<http://intracr/portal/GIYS/Documentos/Sistemas%20de%20Informaci%C3%B3n%20ARN/Sistema%20misional/SIRR/LINEA%20BASE%20SERVICIO%20SIRR.pdf>

Por otro lado, aplica la documentación oficial de Microsoft CRM Dynamics

	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

<https://www.microsoft.com/es-ES/dynamics/crm-customer-center/microsoft-dynamics-365-user-guides.aspx>

5.4.2 ARPA

La Arquitectura planteada para ARPA se encuentra documentada en el Documento de Diseño ACR_ModernizacionSIPAS_Disenio_V5 ubicado en la ruta: http://otidocs.acr.int/sites/OTI/Documentos%20compartidos/OTI/GASI/Desarrollos%20Internos/ARPA/Documentación%20Modernización%20SIPAS/ACR_ModernizacionSIPAS_Disenio_V5.docx

Y en el documento de arquitectura de ARPA después de la refactorización, ubicado en la ruta: <http://otidocs.acr.int/sites/OTI/Documentos%20compartidos/OTI/GASI/Desarrollos%20Internos/ARPA/Documentos%20de%20Dise%C3%B1o%20para%20Refactorizaci%C3%B3n%20ARPA%20V6/Documento%20Arquitectura%20ARPA.docx>

5.4.3 SARA

La Arquitectura planteada para SARA se encuentra documentada en el Documento Arquitectura SARA ubicado en la ruta: <http://otidocs.acr.int/sites/OTI/Documentos%20compartidos/OTI/GASI/Desarrollos%20Internos/SARA%20V2/Documento%20Arquitectura%20SARA.docx>

5.5. AMBIENTES DE DESARROLLO

- **SIRR**

En el documento de línea base del SIRR se encuentran documentados los ambientes del SIRR, entre ellos el de desarrollo

<http://intracr/portal/GIYS/Documentos/Sistemas%20de%20Informaci%C3%B3n%20ARN/Sistema%20misional/SIRR/LINEA%20BASE%20SERVICIO%20SIRR.pdf>

- **ARPA**

En el documento de Arquitectura de ARPA se encuentra la descripción de los ambientes:

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

http://otidocs.acr.int/sites/OTI/Documentos%20compartidos/OTI/GASI/Desarrollos%20Internos/ARPA/Documentación%20Modernización%20SIPAS/ACR_ModernizacionSIPAS_Disenio_V5.docx

<http://otidocs.acr.int/sites/OTI/Documentos%20compartidos/OTI/GASI/Desarrollos%20Internos/ARPA/Documentos%20de%20Dise%C3%B1o%20para%20Refactorizaci%C3%B3n%20ARPA%20V6/Documento%20Arquitectura%20ARPA.docx>

- **SARA**

En el documento de Arquitectura de SARA en el ítem 5. vista de despliegue se describen el ambiente de desarrollo:

<http://otidocs.acr.int/sites/OTI/Documentos%20compartidos/OTI/GASI/Desarrollos%20Internos/SARA%20V2/Documento%20Arquitectura%20SARA.docx>

5.6. PLAN DE CALIDAD DEL SOFTWARE

5.6.1 Principales Objetivos del Aseguramiento de la Calidad del Software

- Mejorar la calidad del software monitoreando apropiadamente tanto los productos de software como el proceso de desarrollo que los genera.
- Asegurar el cumplimiento de los estándares y procedimientos establecidos para el software y el proceso de software establecidos.

5.6.2 Definiciones

Calidad: “Propiedad o conjunto de propiedades inherentes a una cosa, que permiten apreciarla como igual, mejor o peor que las restantes de su especie” (Real Academia Española)

Calidad del Software: “Grado con el cual el cliente o usuario percibe que el software satisface sus expectativas”. IEEE

5.6.3 Modelo de Calidad

	CÓDIGO: TI-G-06	
	FECHA 2024-11-14	VERSIÓN V- 2

GUÍA DE DESARROLLO DE SOFTWARE

El Grupo de Sistemas de Información ha diseñado una metodología para asegurar la calidad del desarrollo realizado por el grupo el cual busca cumplir los atributos de calidad en las funcionalidades desarrolladas:

- Adecuación: Capacidad del producto para proporcionar un conjunto de funciones para tareas y objetivos de usuarios especificados.
- Exactitud: Capacidad del producto de software para proporcionar los resultados o efectos acordados con el grado necesario de precisión.
- Interoperabilidad: Capacidad del producto de software para interactuar con uno o más sistemas especificados.
- Seguridad: Capacidad del producto de software para garantizar la disponibilidad, la integridad, la confidencialidad y la autenticación.
- Cumplimiento funcional: Capacidad del producto de software para adherirse a normas, convenciones o regulaciones en leyes y prescripciones similares relacionadas con la funcionalidad.

Para el cumplimiento de estos atributos se consideran dos fases para la evaluación del producto de software: Pruebas Internas y Pruebas de calidad externa.

- **Prueba de calidad interna**

Toma en cuenta todas las características del producto software desarrollado, debe ser medido y evaluado tomando en cuenta los requisitos especificados y aprobados por el usuario, y realizando las siguientes actividades:

- Análisis del requerimiento especificado.
- Identificación de escenarios de pruebas.
- Ejecución y documentación de pruebas.
- Informar y documentar los errores detectados.
- Revalidar correcciones.

Este proceso lo llevará un funcionario del grupo de sistemas de información para lo cual se realizará un plan de ejecución, realización de pruebas (Test Case) y documentará los errores detectados (Bug) en la herramienta establecida (Test Manager) asociada a una tarea en la plataforma de Azure DevOps. Cuando lo amerite, y dependiendo de la complejidad o impacto del requerimiento se deberán realizar pruebas de integración para verificar que todas las interacciones con otras funcionalidades relacionadas operan correctamente.

	CÓDIGO: TI-G-06	
	FECHA 2024-11-14	VERSIÓN V- 2

GUÍA DE DESARROLLO DE SOFTWARE

Pruebas de seguridad: Las pruebas de seguridad hacen parte de las pruebas de calidad internas y buscan identificar vulnerabilidades que permitan a posibles atacantes acceder a información confidencial y/o afectar el funcionamiento normal de las aplicaciones. El analista de pruebas debe validar el alcance de las pruebas de acuerdo con la aplicación que se va a probar teniendo en cuenta si es una aplicación desarrollada *in house* como SARA o ARPA o si se trata de una personalización del CRM como en el caso del SIRR. Se debe tener en cuenta que en los casos en los que el formulario está expuesto a internet, estas pruebas deben ser mucho más exhaustivas y detalladas ya que la exposición y riesgo son mayores.

Cuando se trate de implementación de un nuevo sistema de información o aplicación, es necesario considerar pruebas de carga, estrés, concurrencia, seguridad y verificación de estándares; así como documentarlas en el formato de **“Verificación de requisitos de seguridad de la información en aplicaciones web externas y tercerizadas”** publicado en el sistema SAPYG dentro del proceso de Gestión de tecnologías de la información, previo a su puesta en producción, registro de información que queda incluida en <http://otidocs.acr.int/sites/OTI> y se relaciona en la tarea de la herramienta DevOps.

Para el caso de mantenimientos aditivos o correctivos a sistemas de información existentes, las pruebas de seguridad están orientadas a la separación de funciones y roles e integridad y confidencialidad de acuerdo con lo especificado en los casos de uso y podrán incluir los siguientes pasos:

- **Verificación de la autenticación y autorización:** se debe llevar a cabo la validación de permisos indicados en CU, comprobando que un rol especificado pueda llevar a cabo la tarea indicada (consulta, creación, edición o eliminación) dentro de la funcionalidad y comprobando que cualquier otro rol no especificado en el CU no tenga los permisos. También se puede intentar acceder a recursos sin estar autenticado o realizar acciones no autorizadas.
- **Comprobación de la configuración de roles:** Se debe comprobar dentro de la aplicación la configuración establecida de acuerdo con el CU para el/los roles indicados. Si existen diferencias entre los roles configurados respecto a los especificados en el CU, se debe reportar al analista, para confirmar si se deben realizar actualizaciones en el CU o corrección en la configuración de la aplicación.
- **Validar la entrada de datos:** Es importante verificar de acuerdo con las reglas establecidas en el caso de uso si el formulario implementa

	CÓDIGO: TI-G-06	
	FECHA 2024-11-14	VERSIÓN V- 2

mecanismos de validación y filtrado de datos en el lado del cliente y del servidor. Para esto se puede probar introduciendo datos maliciosos, como caracteres especiales o cadenas demasiado largas, para comprobar si se manejan correctamente.

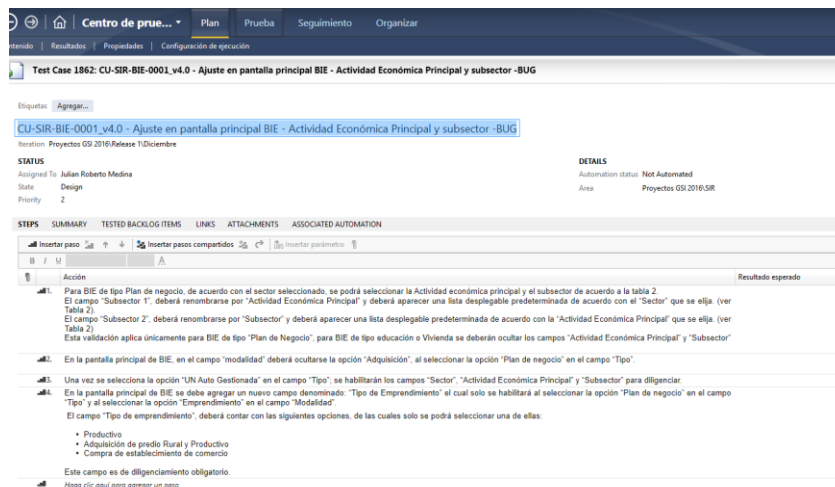
- **Explorar la gestión de errores:** Se puede validar la gestión de errores del formulario introduciendo datos incorrectos o incompletos y observar cómo se manejan los errores. Los mensajes de error no deben revelar información sensible y deben ser claros para el usuario sin proporcionar pistas a posibles atacantes.
- **Prueba de inyección de código:** Se puede validar si un formulario es vulnerable a la inyección de código intentando ingresar datos maliciosos en los campos del formulario. Por ejemplo, se puede probar la inyección de SQL ingresando 'OR '1'='1 en un campo de búsqueda y verificar si se obtiene una respuesta inesperada.
- **Realiza pruebas de cross-site scripting (XSS):** Para comprobar si el formulario presenta esta vulnerabilidad se puede probar ingresando scripts o etiquetas HTML en campos donde se muestre contenido en el navegador. Se debe comprobar si el formulario filtra o escapa correctamente estos datos para evitar ataques XSS.
- **Prueba de cabeceras seguras:** En servicios en línea expuestos en internet que van sobre HTTP, deben realizarse las siguientes pruebas:
 - Content Security Policy
 - Cookies seguras
 - Cross-origin Resource Sharing
 - HTTP Public Key Pinning
 - HTTP Strict Transport Security
 - Redirection
 - Referrer Policy
 - Subresource Integrity
 - X-Content-Type-Options
 - X-Frame-Options
 - X-XSS-Protection

Todos los sistemas de información serán sujetos de evaluación de seguridad conforme al plan de evaluación de vulnerabilidades determinado.

Ejemplo de documentación de Set de Pruebas en el Test Manager:

	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

Imagen No1. Ejemplo de uso del Test Manager



Fuente: Azure DevOps

• Prueba de calidad externa

Desde una visión externa enfocadas a la ejecución del producto, es evaluada en un ambiente simulado. Esperando eliminar la mayor cantidad de fallas posibles durante las pruebas, sin afectar la arquitectura del software. En este proceso se involucra al usuario solicitante o funcionarios asignados por el solicitante con el propósito de que de un aval del producto desarrollado mediante la firma o aprobación electrónica de un Acta de Cierre (formato *TI-F-02 Acta de cierre de funcionalidad o requerimiento*). Si llegase a fallar el software, el solicitante o el analista de pruebas deben reportar los hallazgos identificados durante las pruebas realizadas para su revisión.

En este proceso se podrá involucrar a algunos asistentes de información cuando los productos desarrollados posean características que requieran ser probados en un ambiente similar al de los usuarios en cuanto a recursos ubicación geográfica entre otros.

5.6.4 Consideraciones de la Etapa de Pruebas

- Todos los desarrollos deben superar la etapa de pruebas antes de pasar a Producción, se incluyen los controles de cambio y soportes que se resuelvan con ajustes al Software.

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

- b. El desarrollador debe informar al líder del proyecto asignado, la terminación del desarrollo para la asignación del inicio de la etapa de pruebas, con el propósito de realizar la asignación correspondiente en Azure DevOps.
- c. Todas las pruebas deben ser documentadas en el TestManager y relacionadas a la tarea de pruebas asignada en el Azure DevOps.
- d. Todos los desarrollos y controles de cambio que impliquen ajustes o creación de nuevos roles se deben incluir en la solución generada para publicar en los ambientes de pruebas y producción.
- e. Siempre se deberá tener en cuenta el flujo de la etapa de pruebas en este documento.

5.6.4 Ambiente de Pruebas y Capacitación

El ambiente de pruebas de los diferentes sistemas de información, son administrados por el grupo de Infraestructura y Soporte, quienes realizarán las publicaciones y la asignación de los roles a los usuarios genéricos, para ello los desarrolladores deberán realizar la solicitud con los correspondientes RFC, a través de la herramienta establecida (ARANDA). Algunas actividades de configuración podrán estar en manos del equipo de pruebas. Este ambiente también puede disponerse para capacitaciones requeridas sobre los diferentes sistemas.

- **SIRR**

Se referencia al documento de línea base del SIRR en el cual se documenta la configuración de los ambientes, entre ellos, el ambiente de pruebas:

<http://intracr/portal/GIYS/Documentos/Sistemas%20de%20Informaci%C3%B3n%20ARN/Sistema%20misional/SIRR/LINEA%20BASE%20SERVICIO%20SIRR.pdf>

- **ARPA**

En el documento de Arquitectura de ARPA se encuentra la descripción de los ambientes:

http://otidocs.acr.int/sites/OTI/Documentos%20compartidos/OTI/GASI/Desarrollos%20Internos/ARPA/Documentación%20Modernización%20SIPAS/ACR_ModernizacionSIPAS_Disenio_V5.docx

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE DESARROLLO DE SOFTWARE	CÓDIGO: TI-G-06	
		FECHA 2024-11-14	VERSIÓN V- 2

<http://otidocs.acr.int/sites/OTI/Documentos%20compartidos/OTI/GASI/Desarrollos%20Internos/ARPA/Documentos%20de%20Dise%C3%B1o%20para%20Refactorizaci%C3%B3n%20ARPA%20V6/Documento%20Arquitectura%20ARPA.docx>

- **SARA**

En el documento de Arquitectura de SARA en el ítem 5. Vista de Despliegue se describen el ambiente de desarrollo:

<http://otidocs.acr.int/sites/OTI/Documentos%20compartidos/OTI/GASI/Desarrollos%20Internos/SARA%20V2/Documento%20Arquitectura%20SARA.doc>
X

5.6.5 Manejo de Datos en Ambiente de Pruebas

Para contar con los datos necesarios en los ambientes de pruebas, se debe realiza copia de la base de datos del ambiente productivo cada mes o cuando el grupo de desarrollo lo considere necesario para lo cual realizará solicitud al administrador de bases de datos a través de Soporte la herramienta establecida.

Dentro del procedimiento de replicar la base de datos de producción a pruebas se realiza una reducción de esta excluyendo documentos adjuntos relacionados a las PPR, igualmente se realiza un shrink y se correrá procedimiento encargado de enmascarar o modificar los datos sensibles de las PPR como son Nombre, Identificación y datos de ubicación. Igualmente se correrá procedimiento para modificar los new_name de las entidades donde se reflejan los datos de las PPR.

5.6.6 Usuarios de Prueba

Para el desarrollo de las pruebas tanto internas como con los interesados, se deben utilizar los usuarios genéricos a los cuales se les asignarán los roles requeridos para las interactuar con las funcionalidades.

- **Gestión de Contraseñas:**

La administración de los usuarios y contraseñas está a cargo del Grupo de Infraestructura y Soporte, quienes deben informar al coordinador del Grupo de Sistemas de Información siempre que se actualicen las contraseñas de estos usuarios y esté será el encargado de replicar a los funcionarios y contratistas de su grupo.

	CÓDIGO: TI-G-06	
	FECHA 2024-11-14	VERSIÓN V- 2

Se recomienda que la información del ambiente de pruebas SIRR sea actualizado con una periodicidad mensual o según necesidad, para lo cual el Coordinador del Grupo de Sistemas de Información generara solicitud a través de suporte@reincorporacion.gov.co al Grupo de Sistemas de Información.

5.7. HERRAMIENTAS PARA GESTIÓN DE PROYECTOS DE DESARROLLO

5.7.1 Herramientas de Gestión

El grupo de Apoyo a Sistemas de Información utiliza para la gestión y control del desarrollo de software varias herramientas que de manera articulada brindan la información de trazabilidad de cada requerimiento desde su solicitud inicial hasta la entrega del producto implementado.

La primera herramienta corresponde a la implementada por la mesa de ayuda, pues allí es donde se radican de manera inicial los requerimientos por parte de los usuarios. Cuando los requerimientos llegan a la OTI por SIGOB o a través de un acta de trabajo o por correo electrónico al buzón del coordinador del Grupo de Sistemas de Información, entonces se debe reenviar el requerimiento a suporte@reincorporacion.gov.co para se cree el caso en la herramienta de la mesa de ayuda.

Por cada requerimiento recibido se debe crear un grupo de tareas (Backlog) en la plataforma Azure DevOps que es la segunda herramienta utilizada para la gestión de desarrollo. Según la complejidad del caso se crean una o varias tareas para el análisis y diseño, el desarrollo, las pruebas, y la documentación y entrega del producto implementado.

El caso abierto en la herramienta de mesa de ayuda se debe cerrar indicando el id de la tarea creada en el TFS. Y en la descripción de las tareas se debe hacer referencia al id del caso en la mesa de ayuda.

Como complemento a lo anterior, también se puede utilizar el Microsoft Project para facilitar el control general del cronograma de actividades o gestión de proyectos. Esto para cuando el requerimiento solicitado corresponda a desarrollos que demanden esfuerzos, recursos y tiempos de entrega mayores, a criterio de la coordinación del Grupo de Sistemas de Información.

	CÓDIGO: TI-G-06	
	FECHA 2024-11-14	VERSIÓN V- 2

5.7.2 Infraestructura de las Herramientas de Gestión

Las herramientas utilizadas se encuentran implementadas en la siguiente infraestructura:

- **Aranda:** Es una herramienta de mesa de ayuda diseñada para optimizar la gestión de incidencias y solicitudes en entornos empresariales. Permite a los usuarios reportar problemas y hacer seguimiento de su resolución a través de un sistema intuitivo. La plataforma facilita la organización de tareas, la asignación de responsables y el monitoreo del rendimiento del equipo de soporte. Además, incluye funcionalidades como la creación de bases de datos de conocimiento, informes analíticos y la integración con otras herramientas, lo que mejora la eficiencia en la atención al cliente y la satisfacción del usuario.
- **Azure DevOps:** Es una plataforma integral de Microsoft que facilita la colaboración y gestión de proyectos en equipos de desarrollo de software. Ofrece un conjunto de herramientas para la planificación, desarrollo, pruebas y entrega continua de aplicaciones, incluyendo Azure Boards para la gestión de tareas, Azure Repos para control de versiones, Azure Pipelines para integración y entrega continua, y Azure Test Plans para la gestión de pruebas. Su capacidad de integración con otros servicios y herramientas, así como su enfoque en metodologías ágiles, permite a los equipos mejorar su eficiencia y productividad a lo largo del ciclo de vida del desarrollo de software.