

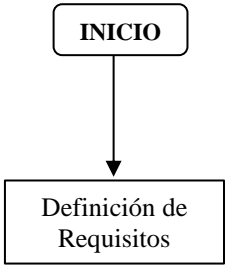
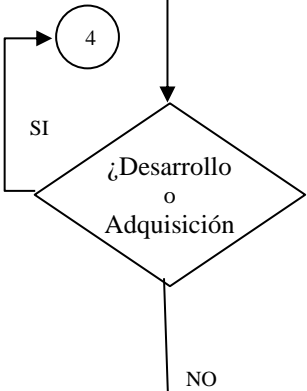
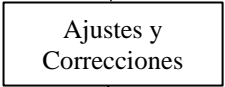
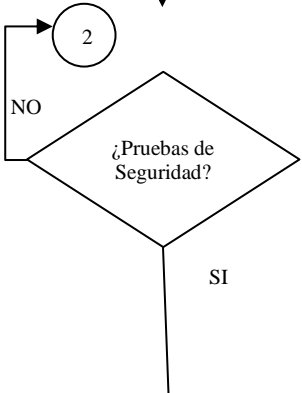
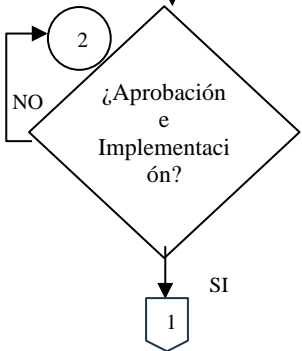
	GESTIÓN DE TICS	CÓDIGO	E-GTIC-PR-013
		VERSIÓN	01
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE	PÁGINA	1 DE 3
		VIGENTE DESDE	20/02/2025

1. INFORMACIÓN GENERAL DEL PROCEDIMIENTO	
OBJETIVO	Establecer los lineamientos para la gestión de la seguridad de la información en los sistemas desarrollados internamente o adquiridos a terceros, garantizando la confidencialidad, integridad y disponibilidad de la información.
ALCANCE	Este procedimiento aplica a todo el ciclo de vida del software dentro de la entidad, incluyendo adquisición, desarrollo, pruebas, implementación, mantenimiento y actualizaciones, considerando ambientes de desarrollo, pruebas y producción. Este procedimiento también aplica a sistemas existentes que sean actualizados o modificados.

2. GLOSARIO	
Término	Definición
Ambiente de Desarrollo	Es la infraestructura tecnológica (hardware y software) que permite desarrollar todos los elementos o componentes para ofrecer un servicio de Tecnologías de la Información
Ambiente de Pruebas	Es la infraestructura tecnológica (hardware y software) que permite probar todos los elementos o componentes para ofrecer un servicio de Tecnologías de la Información
Ambiente de Producción	Sistema operativo donde el software es usado por los usuarios finales.
Ambiente de Producción Integridad	Propiedad que asegura que la información no ha sido alterada de forma no autorizada.
Confidencialidad	Garantía de que la información solo es accesible por personas autorizadas.
Disponibilidad	Proporción del tiempo que el sistema está en ejecución. La capacidad de un servicio de Tecnologías de la información y comunicaciones- Tic u otro elemento de configuración para realizar su función acordada cuando sea necesaria
Disponibilidad: Ciclo de Vida del Software	Conjunto de fases desde la concepción hasta la obsolescencia de un sistema
Integridad	Garantía de exactitud y fiabilidad de la información.
OTIC	Oficina Tecnologías de la Información y Comunicaciones
Pruebas de Seguridad	Conjunto de fases desde la concepción hasta la obsolescencia de un sistema. Evaluaciones realizadas para identificar vulnerabilidades en el software antes de su implementación.
Sistema operativo donde el software es usado por los/las usuarios/as finales.	Sistema operativo donde el software es usado por los/las usuarios/as finales.

3. CONDICIONES GENERALES	
No.	Descripción
1	Se deben identificar y documentar los requerimientos de seguridad desde la fase de adquisición o desarrollo del software, en conformidad con estándares como ISO 27001 y la Ley 1581 de 2012. Estos requisitos deben incluir medidas de control de acceso, encriptación y auditoría de registros. Cada sistema tiene unas particularidades, y eso se determina en un documento (no codificado) de requisitos del sistema
2	Todo software debe someterse a pruebas de seguridad antes de su implementación. Estas pruebas deben incluir análisis de vulnerabilidades y pruebas de penetración, siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información del Estado. Los hallazgos deben documentarse y corregirse antes de su puesta en producción.
3	Se debe garantizar la separación entre los entornos de desarrollo, pruebas y producción. Esto debe incluir la implementación de controles de acceso específicos para cada ambiente y el uso de datos anonimizados en pruebas para evitar riesgos de seguridad
4	Cualquier modificación en el software debe quedar registrado en el formato SOLICITUD DESARROLLO Y/O ACTUALIZACIÓN DE SOFTWARE – INTERNO- E-GTIC-FT-009-. Todas las modificaciones deben ser documentadas y aprobadas por los/as responsables designados/as, en el formato de REGISTRO DE RESULTADO DE PRUEBAS- SOLICITUD DESARROLLO Y/O ACTUALIZACIÓN DE SOFTWARE E-GTIC-FT-018 antes de su implementación.
5	Se deben aplicar medidas de seguridad en todo mantenimiento correctivo y evolutivo del software. Esto incluye la aplicación de parches de seguridad según las recomendaciones del fabricante, la validación de cambios en un entorno de pruebas antes de su implementación y la documentación de todas las acciones realizadas.
6	Debe existir un procedimiento formal para reportar, analizar y solucionar incidentes de seguridad relacionados con el software. Todo incidente debe registrarse en la mesa de ayuda Aranda Service Desk de la entidad y será atendido conforme a la Política de Gestión de Incidentes de Seguridad de la Información. En casos críticos, se debe seguir un proceso de escalamiento definido.

	GESTIÓN DE TICS	CÓDIGO	E-GTIC-PR-013
		VERSIÓN	01
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE	PÁGINA	2 DE 3
		VIGENTE DESDE	20/02/2025

No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	PUNTO DE CONTROL	REGISTRO	TIEMPO
1		Definir detalladamente los requerimientos de seguridad.	Ingeniero responsable de la seguridad perimetral de la OTIC		Documento de Requisitos del sistema	Max: 5 días Min: 3 días Prom: 4 días
2		Gestionar la adquisición y/o desarrollo de software, considerando los requisitos de seguridad definidos SI: Si la implementación cumple con las medidas de seguridad establecidas, avanza a la fase de pruebas paso 4. Si NO se solicita corrección y ajustes paso 3	Desarrollador / Proveedor	X	Informe de Desarrollo	Max: 5 días Min: 3 días Prom: 2,5 días
3		Realizar correcciones y ajustes solicitados	Desarrollador / Proveedor		Informe de Desarrollo	Max: 5 días Min: 5 días Prom: 10 días
4		Realizar pruebas para validar la seguridad del software. SI: el software supera las pruebas se continúa con la aprobación paso 5 NO: Si el software no supera las pruebas se requieren correcciones y nuevas pruebas, se devuelve a paso 2	Ingeniero responsable de la seguridad perimetral de la OTIC	X	Informe de Pruebas	Max: 10 días Min: 7 días Prom: 8,5 días
5		Realizar validación final y despliegue en producción. SI: La validación es exitosa, implementar software en producción NO: Ajustar y realizar correcciones, se devuelve a paso 2	Ingeniero responsable de pruebas de software	X	ACTA A-GDO-FT-004	Max: 2 días Min: 5 días Prom: 3,5 días

	GESTIÓN DE TICS		CÓDIGO	E-GTIC-PR-013		
			VERSIÓN	01		
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE		PÁGINA	3 DE 3		
			VIGENTE DESDE	20/02/2025		
No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	PUNTO DE CONTROL	REGISTRO	TIEMPO
6		<p>Registrar los cambios en el formato REGISTRO DE RESULTADO DE PRUEBAS- SOLICITUD DESARROLLO Y/O ACTUALIZACIÓN DE SOFTWARE E-GTIC-FT-018</p> <p>SI se aprueba un cambio, se documenta en el formato Registro de Cambios y se aplica.</p> <p>NO, se ajusta antes de su implementación.</p>	Equipo de Desarrollo de la OTIC	X	Registro de Cambios	<p>Max: 3 días</p> <p>Min: 1 día</p> <p>Prom: 2 días</p>

5.CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA (DD/MM/AAAA)	ELABORÓ
01	Se crea el PROCEDIMIENTO ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE con el objetivo de establecer los lineamientos para la gestión de la seguridad de la información en los sistemas desarrollados internamente o adquiridos a terceros, garantizando la confidencialidad, integridad y disponibilidad de la información. Este procedimiento también aplica a sistemas existentes que sean actualizados o modificados en el Instituto Distrital Para la Protección de la Niñez y a Juventud IDIPRON/ Oficina de TICS, tomando como base los lineamientos recomendados en Norma la ISO IEC 27001 de 2013 Numeral 14.1.1 de la misma, para la gestión de incidentes.	20/02/2025	<p>JHON CABRERA Contratista Oficina De Tics</p> <p>YEIMMY ROCIO CARDENAS Técnico operativo Código 314 grado 03</p>

6. REVISIÓN Y APROBACIÓN

	NOMBRE	CARGO	FECHA (DD/MM/AAAA)
REVISÓ	SANDRA PATRICIA GUERRERO RAMIREZ	CONTRATISTA GESTIÓN DE TICS	20/02/2025
APROBACIÓN LÍDER DE PROCESO	LUIS CARLOS OCAMPO RAMOS	JEFE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIÓN	20/02/2025