

**SALUD**  
SECRETARÍA DE SALUD



**MANUAL DE PROCEDIMIENTOS DE  
LABORATORIOS DE BIOLÓGICOS Y  
REACTIVOS DE MÉXICO, S.A. DE C.V.**

**BIRMEX**  
LABORATORIOS DE BIOLÓGICOS  
Y REACTIVOS DE MÉXICO,  
S.A. DE C.V.

**DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 1 de 19
	<b>1. Procedimiento de Planeación Estratégica.</b>		

## 1. PROPÓSITO

Establecer la funcionalidad del proceso de Planeación Estratégica de TIC, derivado del Manual Administrativo de Aplicación General en Materias de Tecnología de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), mediante la asignación de los roles identificados en el proceso y sus subprocesos, formalizando la asignación del rol a los responsables que participan en la ejecución de cada una de las tareas del proceso, con el fin de obtener la información, evidencias y entregables que generen las actividades ejecutadas durante el proceso.

## 2. ALCANCE

- 2.1 Obtener el mapa del proceso y de las actividades de los subprocesos involucrados, que permitan identificar la funcionalidad del proceso PE.
- 2.2 Identificar los roles o los actores que se requieren para que el proceso genere las evidencias y entregables que demuestren la funcionalidad del proceso.
- 2.3 Identificar a las áreas o personas que se harán responsables de los diferentes roles que requiere el proceso.
- 2.4 Formalizar las asignaciones de responsables de roles y actividades.
- 2.5 Establecer si es necesario entre las áreas identificadas que participarán con alguna responsabilidad en el proceso un OLA, acuerdo de operación, en el cual se especifiquen los servicios que se aportarán y los tiempos en los que se atenderán y los entregables comprometidos que requiere el proceso.
- 2.6 Identificar las capacitaciones que se requieran en las diferentes áreas o personas que asuman el rol asignado, para que se consideren en un programa de capacitación.
- 2.7 Identificar los indicadores de desempeño del proceso y registrarlos periódicamente para su evaluación posterior.
- 2.8 Identificar los indicadores de los servicios considerados y sus métricas.

## 3. POLÍTICAS DE OPERACIÓN, NORMAS Y LINEAMIENTOS

- 3.1 El Titular de la DTI es el responsable de la Planeación estratégica de TIC de la Institución. El titular de la DTI podrá designar como corresponsable de la Planeación estratégica de TIC en la Institución a un colaborador de un nivel inmediato inferior que le reporte directamente.
- 3.2 El Titular de la DTI deberá asegurarse que la Cartera Ejecutiva de Proyectos de TIC de la Institución cumpla con las disposiciones del Acuerdo.
- 3.3 El Grupo de trabajo para la dirección de TIC deberá apoyar la implementación, operación y mejora del SGSI, así como las acciones que realice el Grupo estratégico de seguridad de la información.
- 3.4 El Responsable de este proceso deberá asegurarse que el PETIC se integre en el sistema que para tales efectos informe la Unidad, habiendo cubierto previamente las autorizaciones correspondientes al interior de la Institución, tal y como lo establece el presente proceso.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>1. Procedimiento de Planeación Estratégica.</b>		Hoja: 2 de 19

#### 4. DESCRIPCIÓN DEL PROCEDIMIENTO

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director de Tecnologías de la Información (Soporte Administrativo)	1	Solicita la intervención del Director General de la Entidad, o el de un inmediato inferior que el Director designe.	Acta de Integración y forma de operación del grupo de trabajo para la dirección TIC  Informe de los resultados, recomendaciones y acuerdos del grupo de trabajo para la dirección TIC (Personal Operativo de la DTI)
	2	Establece el grupo de trabajo para la dirección TIC.	
	3	Formaliza mediante acta la integración y forma de operación del grupo de trabajo para la dirección TIC.	
	4	Define implementa y mantiene una adecuada organización al interior de la DTI.	
	5	Informa al Director General acerca de los resultados, recomendaciones y acuerdos del grupo de trabajo para la dirección TIC (Personal Operativo de la DTI).	
Director de Tecnologías de la Información (Grupo de trabajo para la dirección TIC)	6	Verifica que la dependencia cuente con una Cartera Ejecutiva de Proyectos de TIC actualizada.	
	7	Alinea las prioridades de la Cartera Ejecutiva de Proyectos de TIC con las prioridades institucionales y programas sensoriales.	
	8	Verifica que las principales inversiones en materia de TIC se encuentren alineadas a los objetivos estratégicos de la Institución.  ¿Las inversiones están alineadas con los objetivos?	
	9	No: Asegura que las principales inversiones en materia de TIC se encuentren alineadas a los objetivos estratégicos de la Institución.	
	10	Si: Establece la coordinación necesaria con el responsable del proceso ASI para la administración de riesgos y el SGSI.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>1. Procedimiento de Planeación Estratégica.</b>		Hoja: 3 de 19

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director de Tecnologías de la Información (Soporte Administrativo)	11	Identifica y categoriza el conjunto de proyectos TIC que integraran la Cartera Ejecutiva.	
Director de Tecnologías de la Información	12	Verifica que la Cartera Ejecutiva de Proyectos de TIC de la Institución cumpla con las disposiciones del Acuerdo. ¿La Cartera Ejecutiva de Proyectos TIC cumple con las disposiciones?	
	13	No: Asegura que la Cartera Ejecutiva de Proyectos de TIC cumpla con las disposiciones del acuerdo. Regresa actividad 12.	
	14	Si: Identifica máximo 7 proyectos de TIC que se consideren estratégicos.	PETIC
Director de Tecnologías de la Información (Soporte Administrativo)		Para conformar el PETIC, se aplica como criterio preferente para su identificación que aporten mayores beneficios a la población o cuenten con alto impacto en el cumplimiento de los objetivos institucionales, del Decreto y la EDN.  ¿Recursos de TIC alineados?	
	15	No: Asegura que la aplicación de Recursos TIC estén alineados al decreto y la EDN.	
	16	Si: Identifica los proyectos de TIC cuyo objetivo sea la contratación de bienes y servicios de TIC.	
		¿Los proyectos identificados son estratégicos o de contratación de bienes y servicios?	
	17	No: Genera reporte de proyectos que deben gestionarse en la ADP.	Reporte de proyectos que deben gestionarse en ADP
	18	Si: Integra la ficha técnica base para cada proyecto.	
	19	Categoriza los proyectos de la Cartera Ejecutiva.	

	<b>MANUAL DE PROCEDIMIENTOS</b>			Revisión: A
	<b>Dirección de Tecnologías de la Información</b>			Hoja: 4 de 19
	<b>1. Procedimiento de Planeación Estratégica.</b>			

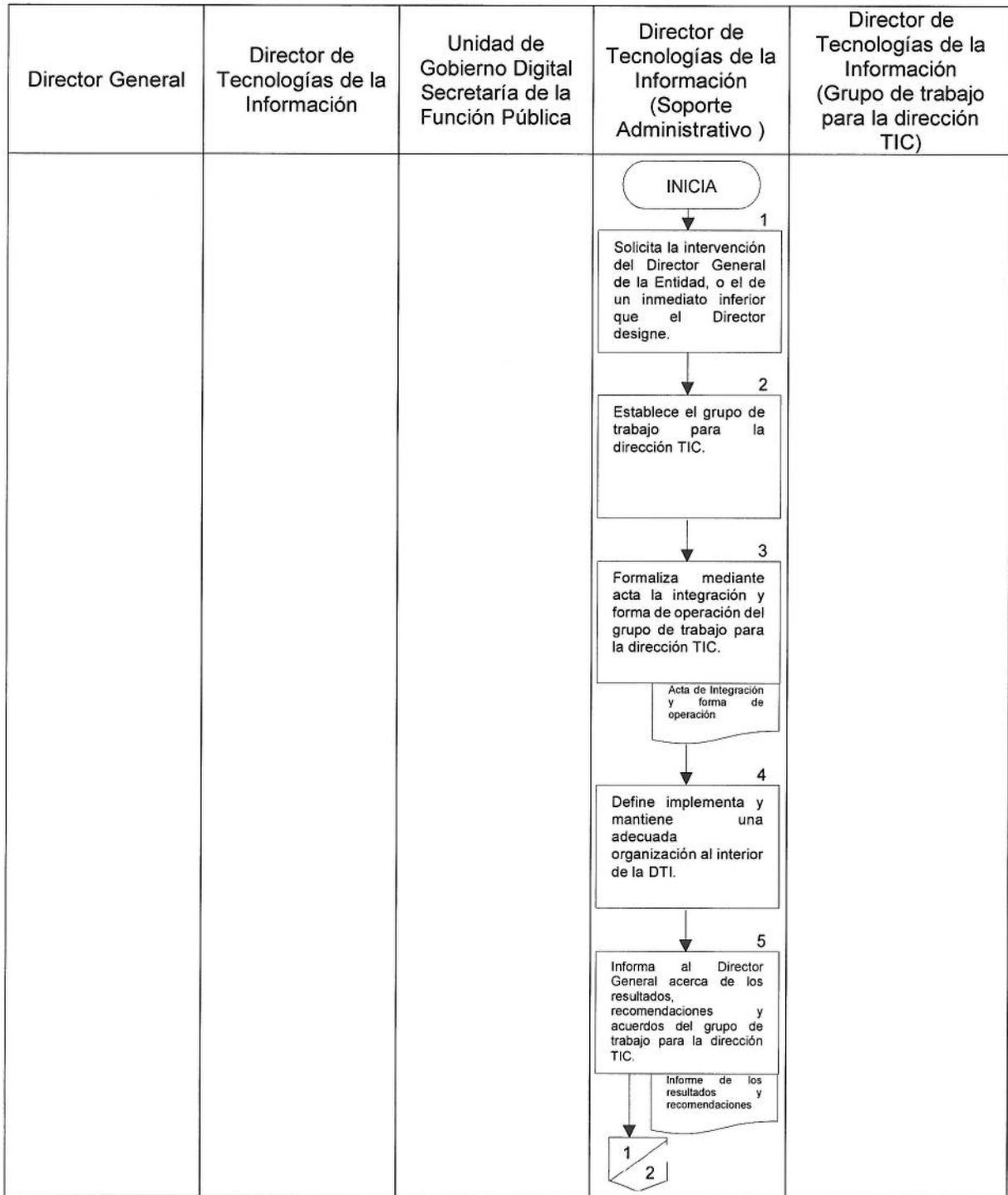
Responsable	No. Act.	Descripción de actividades	Documento o anexo
	20	Integra objetivos institucionales, metas nacionales, del programa y de la EDN.	PETIC
Director de Tecnologías de la Información	21	Revisa Cartera Ejecutiva de Proyectos de TIC para validarlo.	Cartera Ejecutiva de Proyectos de TIC
	22	Presenta Cartera Ejecutiva de Proyectos de TIC para autorización del titular de la Institución.	
Director General	23	Revisa la Cartera Ejecutiva de Proyectos de TIC.	Cartera Ejecutiva de Proyectos de TIC
		¿Autoriza la Cartera Ejecutiva de Proyectos de TIC?	
	24	No: Regresa a actividad 20.	
	25	Si: Autoriza e informa al Director de Tecnologías de la Información.	
Director de Tecnologías de la Información	26	Registra la Cartera Ejecutiva de Proyectos de TIC en el sistema informático.	Cartera Ejecutiva de Proyectos de TIC
Director de Tecnologías de la Información (Soporte Administrativo)	27	Verifica que se obtenga la autorización de la Cartera Ejecutiva de Proyectos de TIC por parte de la Unidad, utilizando para ello el sistema web al que se alude en el factor crítico anterior.	
		¿Cartera Ejecutiva de Proyectos de TIC integrada al sistema?	
	28	No: Asegura que la Cartera Ejecutiva de Proyectos de TIC se integre en el sistema informático.	
	29	Si: Verifica que se obtenga la autorización de la Cartera Ejecutiva de Proyectos de TIC por parte de la Unidad.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>1. Procedimiento de Planeación Estratégica.</b>		Hoja: 5 de 19

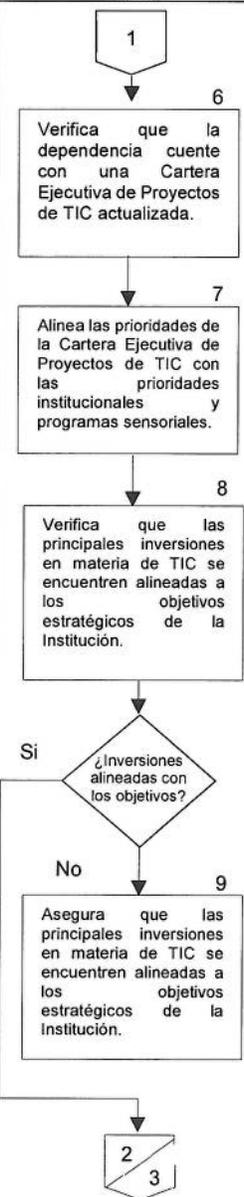
Responsable	No. Act.	Descripción de actividades	Documento o anexo
Unidad de Gobierno Digital Secretaría de la Función Pública	30	Revisa la Cartera Ejecutiva de Proyectos de TIC para autorizarla.	
		¿Autoriza la Cartera?	
	31	No: Regresa a actividad 21.	
	32	Si: Autoriza la Cartera e informa el Director de Tecnologías de la Información.	
Director de Tecnologías de la Información (Soporte Administrativo)	33	Difunde la Cartera Ejecutiva de Proyectos de TIC a todos los involucrados para su cumplimiento en la DTI y en la Institución.	
	34	Da seguimiento a la Cartera Ejecutiva de Proyectos de TIC y reportarlo a la Unidad.	Reporte Seguimiento del avance de la Cartera Ejecutiva de Proyectos de TIC
	35	Informa al grupo de trabajo para la dirección de TIC.	Tablero de Seguimiento de Planeación Estratégica
		TERMINA	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>1. Procedimiento de Planeación Estratégica.</b>		Hoja: 6 de 19

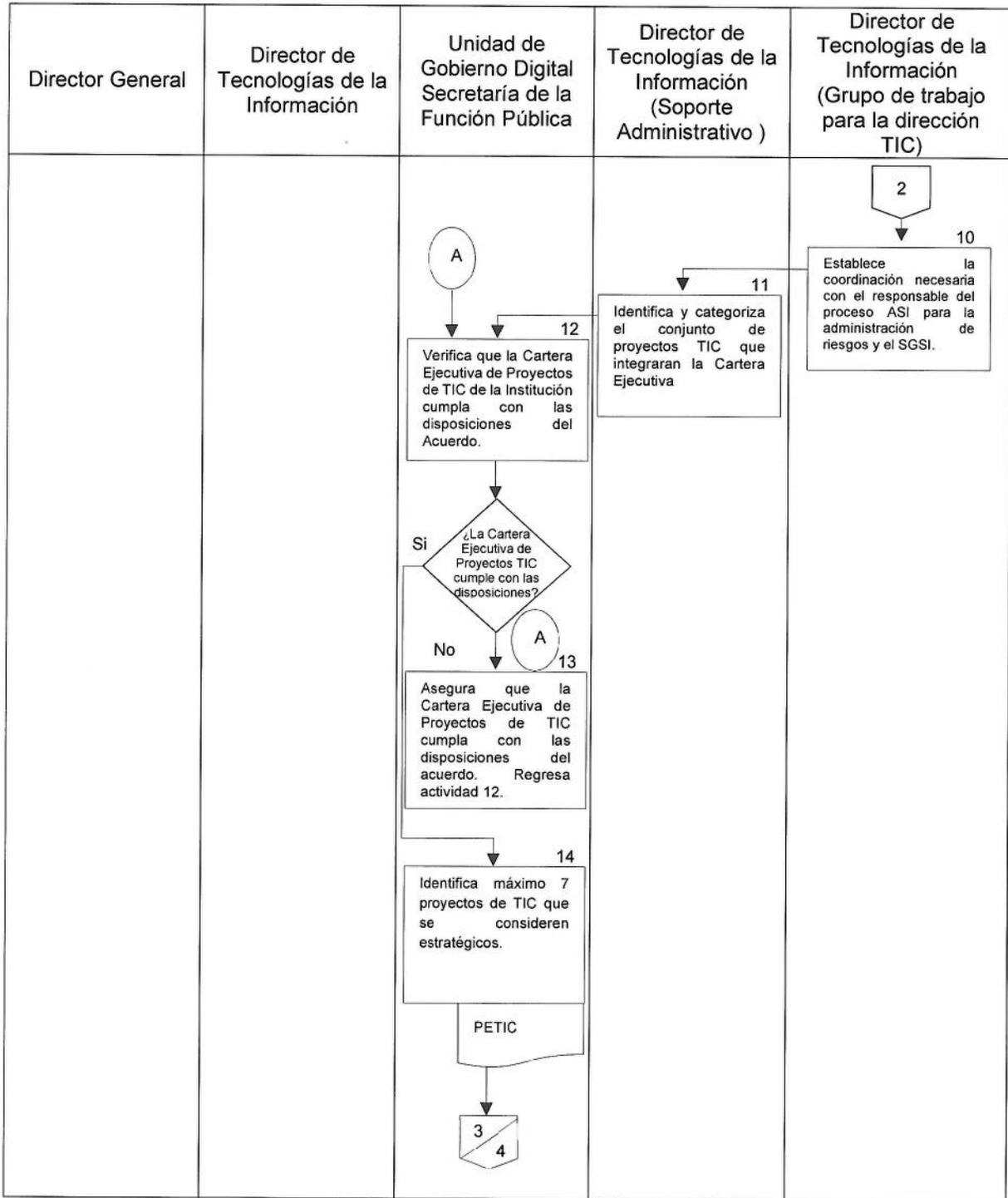
## 5. DIAGRAMA DE FLUJO



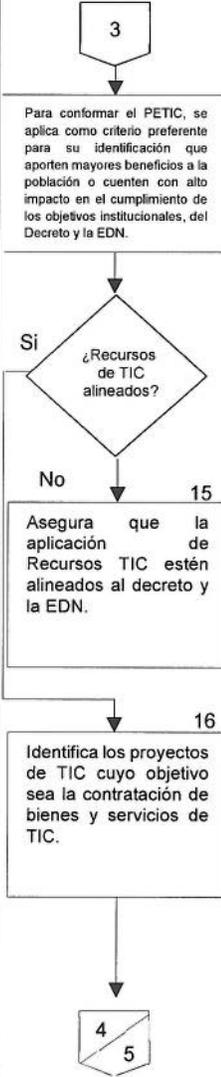
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 7 de 19
	<b>1. Procedimiento de Planeación Estratégica.</b>		

Director General	Director de Tecnologías de la Información	Unidad de Gobierno Digital Secretaría de la Función Pública	Director de Tecnologías de la Información (Soporte Administrativo )	Director de Tecnologías de la Información (Grupo de trabajo para la dirección TIC)
				 <pre> graph TD     1[1] --&gt; 6[6]     6 --&gt; 7[7]     7 --&gt; 8[8]     8 --&gt; D{¿Inversiones alineadas con los objetivos?}     D -- Si --&gt; 2_3[2/3]     D -- No --&gt; 9[9]     9 --&gt; 2_3   </pre>

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>1. Procedimiento de Planeación Estratégica.</b>		Hoja: 8 de 19



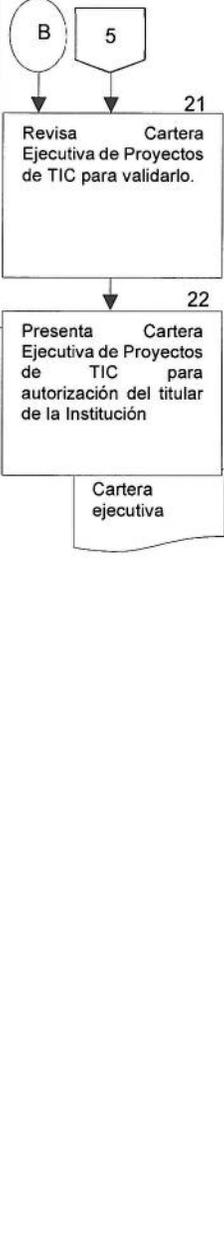
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 9 de 19
<b>1. Procedimiento de Planeación Estratégica.</b>			

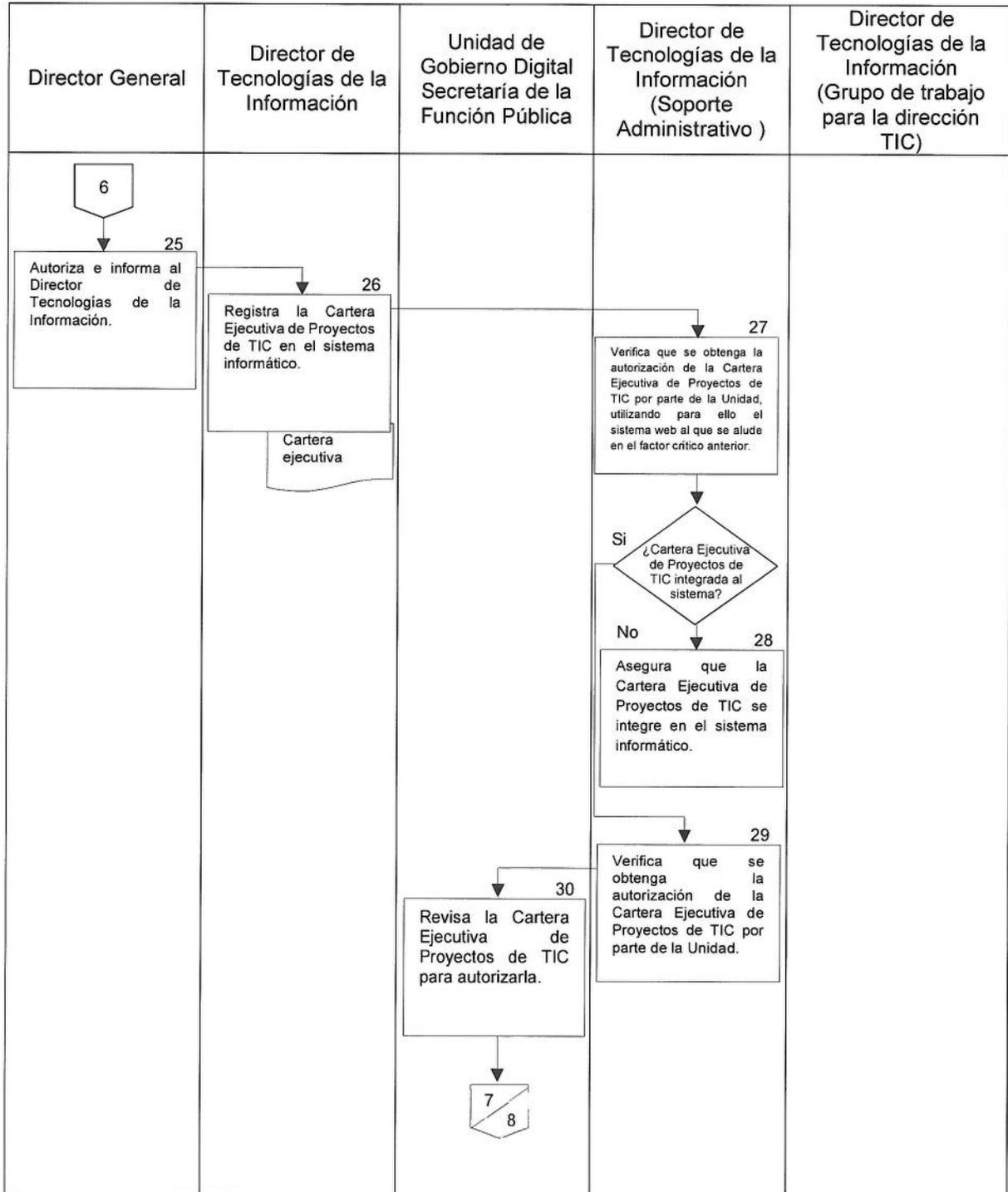
Director General	Director de Tecnologías de la Información	Unidad de Gobierno Digital Secretaría de la Función Pública	Director de Tecnologías de la Información (Soporte Administrativo )	Director de Tecnologías de la Información (Grupo de trabajo para la dirección TIC)
			 <pre> graph TD     3[3] --&gt; Text1[Para conformar el PETIC, se aplica como criterio preferente para su identificación que aporten mayores beneficios a la población o cuenten con alto impacto en el cumplimiento de los objetivos institucionales, del Decreto y la EDN.]     Text1 --&gt; Decision{¿Recursos de TIC alineados?}     Decision -- Si --&gt; Text2[Asegura que la aplicación de Recursos TIC estén alineados al decreto y la EDN.]     Decision -- No --&gt; Text3[Identifica los proyectos de TIC cuyo objetivo sea la contratación de bienes y servicios de TIC.]     Text2 -- 15 --&gt; 4_5[4/5]     Text3 -- 16 --&gt; 4_5   </pre>	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>1. Procedimiento de Planeación Estratégica.</b>		Hoja: 10 de 19

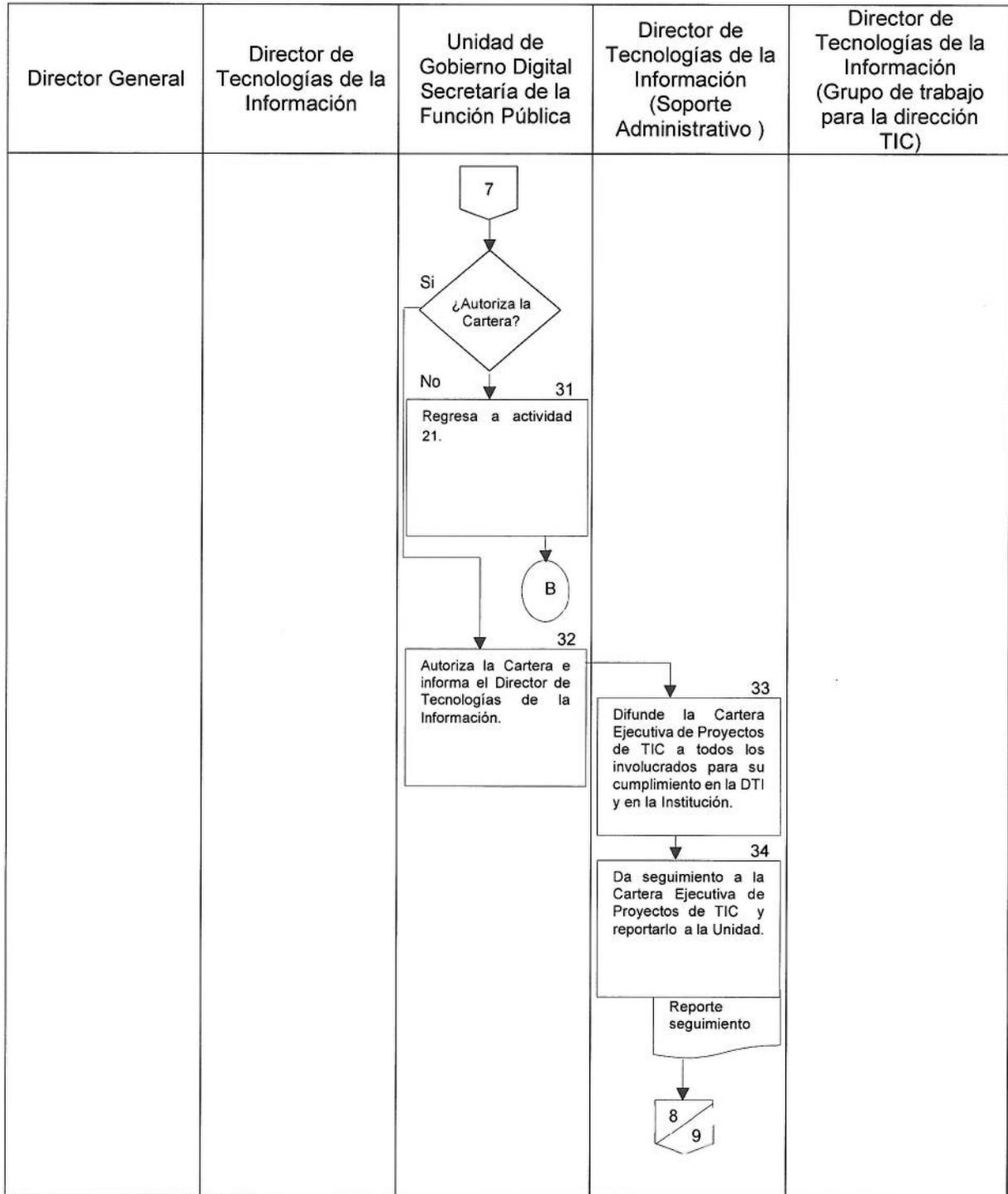
Director General	Director de Tecnologías de la Información	Unidad de Gobierno Digital Secretaría de la Función Pública	Director de Tecnologías de la Información (Soporte Administrativo )	Director de Tecnologías de la Información (Grupo de trabajo para la dirección TIC)
				

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 11 de 19
<b>1. Procedimiento de Planeación Estratégica.</b>			

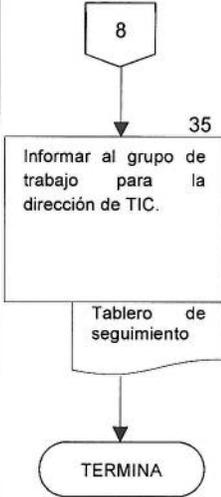
Director General	Director de Tecnologías de la Información	Unidad de Gobierno Digital Secretaría de la Función Pública	Director de Tecnologías de la Información (Soporte Administrativo )	Director de Tecnologías de la Información (Grupo de trabajo para la dirección TIC)
				



	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 13 de 19
<b>1. Procedimiento de Planeación Estratégica.</b>			



	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 14 de 19
<b>1. Procedimiento de Planeación Estratégica.</b>			

Director General	Director de Tecnologías de la Información	Unidad de Gobierno Digital Secretaría de la Función Pública	Director de Tecnologías de la Información (Soporte Administrativo )	Director de Tecnologías de la Información (Grupo de trabajo para la dirección TIC)
			 <pre> graph TD     8{{8}} --&gt; 35[35 Informar al grupo de trabajo para la dirección de TIC.]     35 --&gt; TS[Tablero de seguimiento]     TS --&gt; T([TERMINA])           </pre>	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>1. Procedimiento de Planeación Estratégica.</b>		Hoja: 15 de 19

## 6. DOCUMENTOS DE REFERENCIA

Nombre del documento	Código (cuando aplique)
6.1 Cartera Ejecutiva de Proyectos de TIC.	No aplica
6.2 EDN(Estrategia Digital Nacional).	No aplica

## 7. REGISTROS

Registros	Tiempo de conservación	Responsable de conservarlo	Código de registro o identificación única
Acta de integración y forma de operación del grupo de trabajo para la dirección de TIC	1 año o actualización	Director de Tecnologías de la Información.	No aplica
Cartera Ejecutiva de Proyectos de TIC	1 año	Director de Tecnologías de la Información.	No aplica
Tablero de Seguimiento de Planeación Estratégica	1 año	Director de Tecnologías de la Información.	No aplica
Informe de los resultados, recomendaciones y acuerdos del grupo de trabajo para la dirección TIC	1 año	Director de Tecnologías de la Información.	No aplica
Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC)	1 año	Director de Tecnologías de la Información.	No aplica
Reporte de proyectos que deben gestionarse en el ADP	3 meses	Director de Tecnologías de la Información.	No aplica
Reporte Seguimiento del avance de la Cartera Ejecutiva de Proyectos de TIC	3 meses	Director de Tecnologías de la Información.	No aplica

## 8. GLOSARIO DEL PROCEDIMIENTO

- 8.1 **Activos de TIC.**- los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.
- 8.2 **ACNF.**- proceso de administración de la configuración.
- 8.3 **ADP.**- proceso de administración de proyectos.
- 8.4 **ADS.**- proceso de administración de servicios.
- 8.5 **APCT.**- proceso de administración del presupuesto y las contrataciones.
- 8.6 **Aplicativo de Cómputo.**- el software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo a requerimientos previamente definidos.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>1. Procedimiento de Planeación Estratégica.</b>		Hoja: 16 de 19

- 8.7 **APRO.-** proceso de administración de proveedores;
- 8.8 **Arquitectura Empresarial.-** la información del estado actual y futuro de una Institución, a partir del análisis con perspectiva estratégica; considerando modelos de negocio, procesos, aplicativos y tecnologías de la información y comunicaciones;
- 8.9 **Arquitectura Orientada a Servicios.-** la metodología y marco de trabajo, para construir componentes de software reutilizables para la interoperabilidad de aplicativos de cómputo;
- 8.10 **AOP.-** proceso de administración de la operación;
- 8.11 **ASI.-** proceso de administración de la seguridad de la Información.
- 8.12 **Borrado Seguro.-** el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital.
- 8.13 **Cartera Ejecutiva de Proyectos de TIC.-** Conjunto total de proyectos de TIC que la institución propondrá a la Unidad para su seguimiento.
- 8.14 **Cartera Operativa de Proyectos de TIC.-** Conjunto total de proyectos que soportan la operación diaria de la DTI y no son considerados como estratégicos.
- 8.15 **Centro de Datos.-** el lugar físico en los que se ubiquen los activos de TIC y desde el que se proveen servicios de TIC.
- 8.16 **Cómputo en la Nube.-** al modelo de prestación de servicios digitales que permite a las Instituciones acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios.
- 8.17 **Dependencias.-** las Secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como a la Oficina de la Presidencia de la República y la Procuraduría General de la República; así como los Órganos Reguladores Coordinados en Materia Energética.
- 8.18 **Dominio Tecnológico.-** las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo.
- 8.19 **EDN.-** la Estrategia Digital Nacional contenida en el Objetivo número 5 del Programa.
- 8.20 **EIDA.-** el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, establecido mediante Acuerdo publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011.
- 8.21 **Entidades.-** los organismos descentralizados, empresas de participación estatal mayoritaria, instituciones nacionales de crédito, organizaciones auxiliares nacionales de crédito e instituciones nacionales de seguros y de fianzas, y fideicomisos públicos que en términos de la

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 17 de 19
	<b>1. Procedimiento de Planeación Estratégica.</b>		

Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales, sean considerados entidades de la Administración Pública Federal Paraestatal.

- 8.22 **ERISC.-** equipo de respuesta a incidentes de seguridad en TIC en la Institución;
- 8.23 **Estándar abierto:** a las especificaciones cuya utilización esté disponible de manera gratuita o que no suponga una dificultad de acceso, y que su uso y aplicación no esté condicionada al pago de un derecho de propiedad
- 8.24 **Herramienta de Gestión de la Política TIC.-** sistema web usado para llevar a cabo la comunicación de actividades de reporte establecidas en el Acuerdo, considerando el reporte de PETIC, la obtención del dictamen técnico que emite la Unidad, autorización por parte de la UPCP, la arquitectura empresarial, el MAAGTICSI, entre otros;
- 8.25 **Infraestructuras Críticas de Información.-** Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia.
- 8.26 **Infraestructuras de Información esenciales.-** Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de información, TIC y TO, cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación de las Instituciones.
- 8.27 **Infraestructura de TIC.-** el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC.
- 8.28 **Infraestructura Pasiva.-** elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de las dependencias o entidades, que sean necesarios para la instalación y operación de las redes, así como para la prestación de servicios de procesamiento de datos, de telecomunicaciones y radiodifusión.
- 8.29 **Instancias de Seguridad Nacional.-** las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquellas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional.
- 8.30 **Institución.-** las dependencias y entidades de la Administración Pública Federal, tal y como se definen en este Acuerdo.
- 8.31 **Lineamientos.-** los Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicados en el Diario Oficial de la Federación el 30 de enero de 2013.
- 8.32 **MAAGMAASSP.-** el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 18 de 19
	<b>1. Procedimiento de Planeación Estratégica.</b>		

- 8.33 **MAAGTICSI.-** el Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información. Anexo Único del presente Acuerdo.
- 8.34 **Niveles de servicio.-** el establecimiento en un lenguaje no técnico del servicio brindado, incluyendo al menos la definición, disponibilidad, calidad, tiempos de respuesta y solución.
- 8.35 **OPEC.-** proceso de operación de los controles de seguridad de la información y del erisc.
- 8.36 **PE.-** proceso de planeación estratégica.
- 8.37 **PETIC.-** el conjunto de proyectos que elaboran las Instituciones, conformado por un máximo de 7 proyectos estratégicos, en los términos establecidos en el presente Acuerdo.
- 8.38 **Portafolio de proyectos de TIC.-** es el total de los proyectos de TIC agrupados según su clasificación en Cartera Ejecutiva de Proyectos de TIC y Cartera Operativa de Proyectos de TIC que la Institución planea desarrollar, en los términos establecidos por el MAAGTICSI;
- 8.39 **Programa.-** el Programa para un Gobierno Cercano y Moderno 2013-2018, aprobado mediante Decreto publicado en el Diario Oficial de la Federación el 30 de agosto de 2013.
- 8.40 **Proyectos de TIC.-** el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC y que cuenta con presupuesto para su ejecución; considerando 2 tipos: proyectos operativos que soportan las actividades diarias de la DTI y proyectos estratégicos en los términos señalados en el presente Acuerdo.
- 8.41 **Retos Públicos.-** el modelo que fomenta la democratización del gasto público y la innovación, invitando a los emprendedores del país a plantear soluciones a retos de gobierno mediante el desarrollo de aplicativos tecnológicos web y móviles.
- 8.42 **SEGOB.-** la Secretaría de Gobernación.
- 8.43 **Seguridad de la información.-** la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.
- 8.44 **Seguridad Nacional.-** las acciones a las que se refiere el artículo 3 de la Ley de Seguridad Nacional.
- 8.45 **SFP.-** la Secretaría de la Función Pública.
- 8.46 **SHCP.-** la Secretaría de Hacienda y Crédito Público.
- 8.47 **Tecnologías Verdes.-** el conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las tecnologías de la información y comunicaciones, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías.
- 8.48 **TIC.-** las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		
	<b>1. Procedimiento de Planeación Estratégica.</b>		Hoja: 19 de 19

8.49 **Unidad:** la Unidad de Gobierno Digital de la SFP.

8.50 **DTIC:** la Dirección de Tecnologías de Información y Comunicaciones o área responsables

## 9. CAMBIOS DE VERSIÓN DEL PROCEDIMIENTO

Numero de revisión	Fecha de actualización	Descripción del cambio
0	No aplica	No aplica

## 10. ANEXOS DEL PROCEDIMIENTO

No aplica

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 1 de 17
	<b>2. Procedimiento para la Administración del Presupuesto y las Contrataciones.</b>		

## 1. PROPÓSITO

Establecer la funcionalidad del proceso de Administración del Presupuesto y las Contrataciones, derivado del Manual Administrativo de Aplicación General en Materias de Tecnología de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), mediante la asignación de los roles identificados en el proceso y sus subprocesos, formalizando la asignación del rol a los responsables que participan en la ejecución de cada una de las tareas del proceso, con el fin de obtener la información, evidencias y entregables que generen las actividades ejecutadas durante el proceso.

## 2. ALCANCE

- 2.1 Obtener el mapa del proceso y de las actividades de los subprocesos involucrados, que permitan identificar la funcionalidad del proceso APCT.
- 2.2 Identificar los roles o los actores que se requieren para que el proceso genere las evidencias y entregables que demuestren la funcionalidad del proceso.
- 2.3 Identificar a las áreas o personas que se harán responsables de los diferentes roles que requiere el proceso.
- 2.4 Formalizar las asignaciones de responsables de roles y actividades.
- 2.5 Establecer si es necesario entre las áreas identificadas que participarán con alguna responsabilidad en el proceso un OLA, acuerdo de operación, en el cual se especifiquen los servicios que se aportarán y los tiempos en los que se atenderán y los entregables comprometidos que requiere el proceso.
- 2.6 Identificar las capacitaciones que se requieran en las diferentes áreas o personas que asuman el rol asignado, para que se consideren en un programa de capacitación.
- 2.7 Identificar los indicadores de desempeño del proceso y registrarlos periódicamente para su evaluación posterior.
- 2.8 Identificar los indicadores de los servicios considerados y sus métricas.

## 3. POLÍTICAS DE OPERACIÓN, NORMAS Y LINEAMIENTOS

- 3.1 El responsable del seguimiento del presupuesto autorizado, de los procedimientos de contratación de TIC y de los contratos celebrados en materia de TIC, deberá ser designado por el titular de la DTI, y tener un nivel jerárquico inmediato inferior al de éste.
- 3.2 El responsable del proceso deberá asegurarse que éste se ejecute con apego a las disposiciones que en materia presupuestaria resulten aplicables, así como a los procesos de las unidades administrativas facultadas para administrar los recursos financieros y elaborar el anteproyecto anual de presupuesto de la Institución.
- 3.3 El responsable de este proceso deberá asegurarse que éste se efectúe con apego a las disposiciones en materia de adquisiciones y arrendamiento de bienes muebles y servicios, al Acuerdo por el que se expide el MAAGMAASSP, al Acuerdo y aquellas en materia presupuestaria, que resulten aplicables.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 2 de 17
	<b>2. Procedimiento para la Administración del Presupuesto y las Contrataciones.</b>		

- 3.4 El titular de la DTI, deberá designar a un representante con los conocimientos técnicos suficientes que permitan dar respuesta clara y precisa a las solicitudes de aclaración de los licitantes en las juntas de aclaraciones de los procedimientos de contratación a los que fuere convocada la DTI como área técnica.
- 3.5 Cuando otras áreas o unidades administrativas de la Institución diversas a la DTI, tengan asignados recursos financieros para la contratación de bienes o servicios de TIC necesarios para el cumplimiento de sus funciones, deberán contar previo al inicio del procedimiento de contratación de que se trate, con la aprobación por escrito de la DTI, por medio de un dictamen técnico.
- 3.6 En el supuesto a que se refiere la regla anterior, corresponderá al área o unidad administrativa de que se trate, fungir como área técnica, por lo que la DTI deberá proporcionar el apoyo técnico que le sea requerido por ésta.
- 3.7 En aquellos casos en que se integren o adicionen componentes de software a un aplicativo de cómputo o a un servicio de TIC ya existente, el responsable del proceso se deberá asegurar de que se consideren las siguientes pruebas: integrales, de funcionalidad, estrés, volumen, aceptación del usuario y de seguridad, con el propósito de comprobar que la funcionalidad del aplicativo de cómputo o servicio de TIC existente se mantiene inalterada y que la relativa al componente integrado o adicionado es consistente.
- 3.8 El responsable de este proceso deberá verificar que cada vez que se suscriba un contrato para la adquisición, arrendamiento o servicios de TIC, éste sea registrado en el sistema electrónico de compras gubernamentales denominado CompraNet, con apego a la normatividad aplicable, así como en la Herramienta de Gestión de la Política TIC, en un plazo no mayor a días 10 hábiles una vez firmado dicho contrato.
- 3.9 El titular de la DTI será el responsable de firmar electrónicamente el Estudio de Factibilidad, dentro de la Herramienta de Gestión de la Política TIC, así como de su trámite ante la Unidad.
- 3.10 El titular de la DTI deberá constatar que se revise el inventario de aplicaciones de la APF para determinar si existe, con el propósito de su reutilización, un aplicativo de cómputo de características similares a los requerimientos que la DTI reciba o que se generen dentro de la misma. En el caso de que en la revisión se haya determinado la existencia de algún aplicativo de cómputo susceptible de ser reutilizado, deberá dar aviso a la Unidad y gestionar dicha reutilización ante la DTI de la Institución responsable del aplicativo de cómputo de que se trate.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 3 de 17
	<b>2. Procedimiento para la Administración del Presupuesto y las Contrataciones.</b>		

#### 4. DESCRIPCIÓN DEL PROCEDIMIENTO

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director de Tecnologías de la Información (Soporte Administrativo)	1	Identifica los proyectos y servicios de TIC para lo que sea necesaria una asignación presupuestaria	
Director de Tecnologías de la Información (Soporte Administrativo con apoyo del Personal Operativo DTI).	2 3 4	2 Establece escenarios para el adecuado ejercicio del presupuesto destinado a las TIC 3 Estima los recursos presupuestarios de TIC, de acuerdo con los requerimientos previstos en los programas de aprovisionamiento y de mantenimiento de la infraestructura tecnológica de la DTI. 4 Presenta el presupuesto estimado de TIC al titular de la DTI para su autorización.	
Director de Tecnologías de la Información	5	Revisa presupuesto estimado de TIC  ¿Autoriza el presupuesto estimado de TIC?  No: Continuar en actividad 2 Si: Continuar en actividad 6	
Titulares de las Unidades Administrativas	6	Reciben el presupuesto estimado de TIC del ejercicio siguiente	
Director de Tecnologías de la Información (Soporte Administrativo con apoyo del Personal Operativo)	7 8 9 10 11	7 Gestiona ante la unidad administrativa facultada las constancias de suficiencia presupuestaria para sustentar la contratación de bienes y servicios de TIC que sean requeridos por la DTI. 8 Elabora listado de bienes y servicios de TIC a contratar por la DTI 9 Reporta a la Unidad de Gobierno Digital de la SFP 10 Verifica la posibilidad de llevar a cabo contrataciones consolidadas y de utilizar contratos marco u otras estrategias de contratación. 11 Asegura que para cada contratación que se prevea, se elabore el Estudio de Factibilidad	Listado de bienes y Servicios de TIC  Listado de bienes y Servicios de TIC  Estudio de Factibilidad

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 4 de 17
	<b>2. Procedimiento para la Administración del Presupuesto y las Contrataciones.</b>		

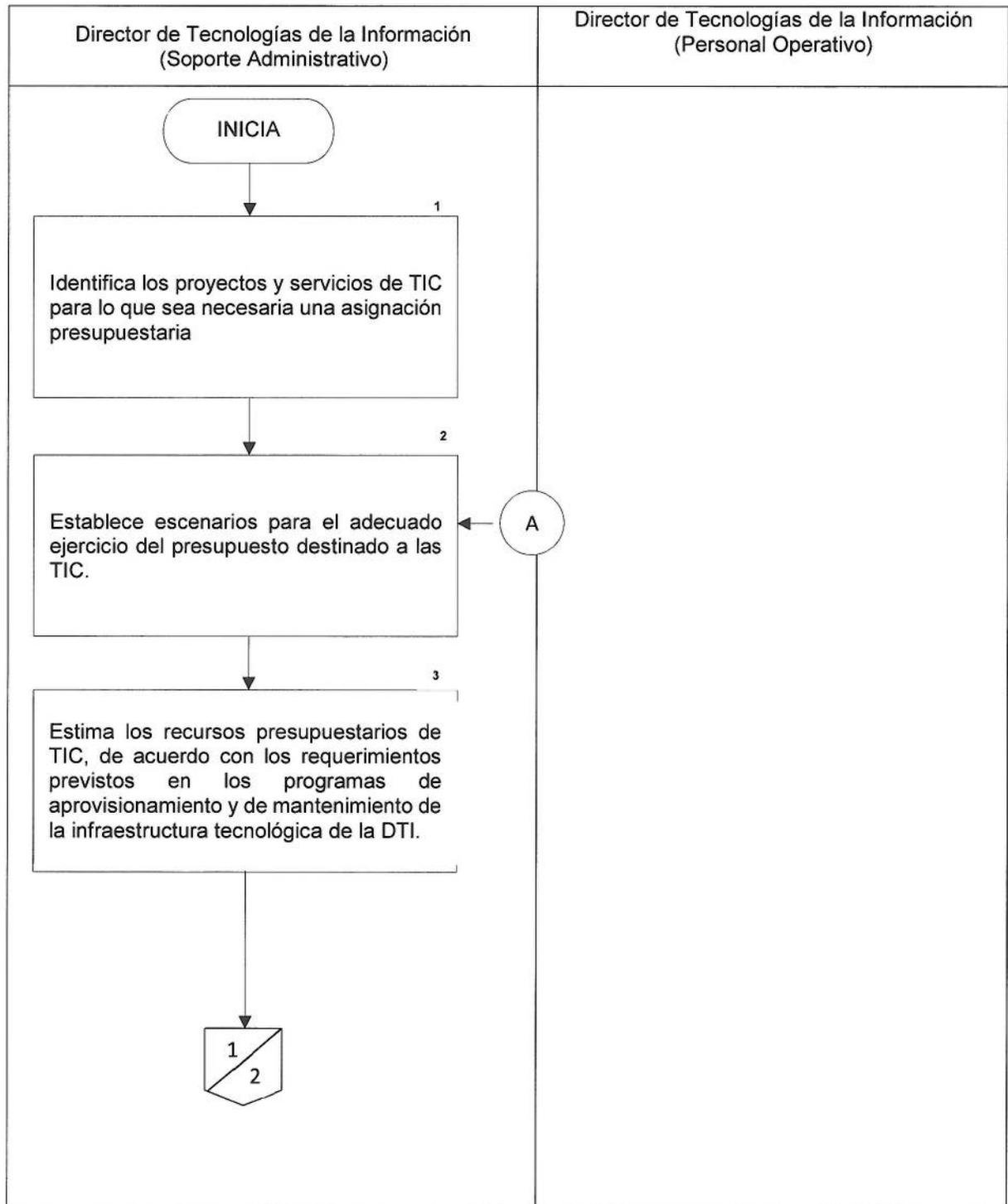
Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director de Tecnologías de la Información (Soporte Administrativo con apoyo del Personal Operativo)	12	Propone la estrategia de contratación para los proyectos de TIC autorizados	Estrategias de contratación para los proyectos TIC
	13	Define acciones para proveer al área de adquisiciones los elementos técnicos necesarios	Anexo Técnico
	14	Verifica que la documentación soporte que deba entregarse al área contratante de la Institución se encuentre debidamente integrada, en términos de lo señalado en el numeral 4.2.1.1.8 del MAAGMAASSP, y particularmente que el anexo técnico que elabore la DTI contenga las especificaciones y requerimientos técnicos del bien o servicio de TIC que se pretenda contratar.  ¿Documentación debidamente integrada?  No: Continuar en actividad 15 Si: Continuar en actividad 16	
	15	Identifica los documentos soporte que no estén integrados de acuerdo a los lineamientos de MAAGMAASSP. Regresa Actividad 14	
	16	Integra los requerimientos técnicos en materia de TIC para que se lleve a cabo la investigación de mercado correspondiente.	
	17	Verifica que ésta contenga los criterios de calidad, de aceptación y los niveles de servicio esperados respecto de los bienes y servicios de TIC que se pretenden contratar.  ¿La información contiene criterios de calidad, aceptación y niveles de servicio esperados?  No: Continuar en actividad 16 Si: Continuar en actividad 18	

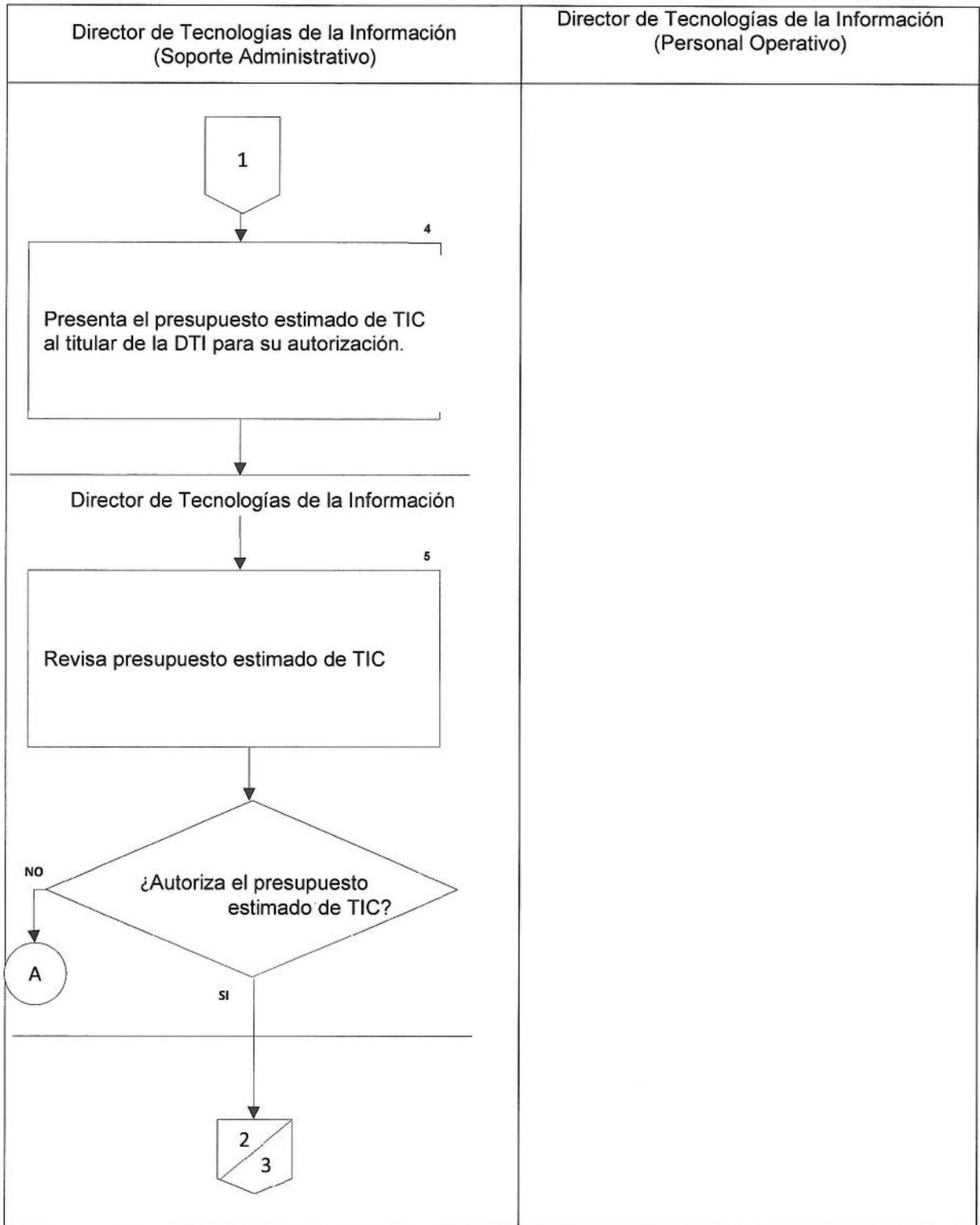
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: <b>5</b> de 17
	<b>2. Procedimiento para la Administración del Presupuesto y las Contrataciones.</b>		

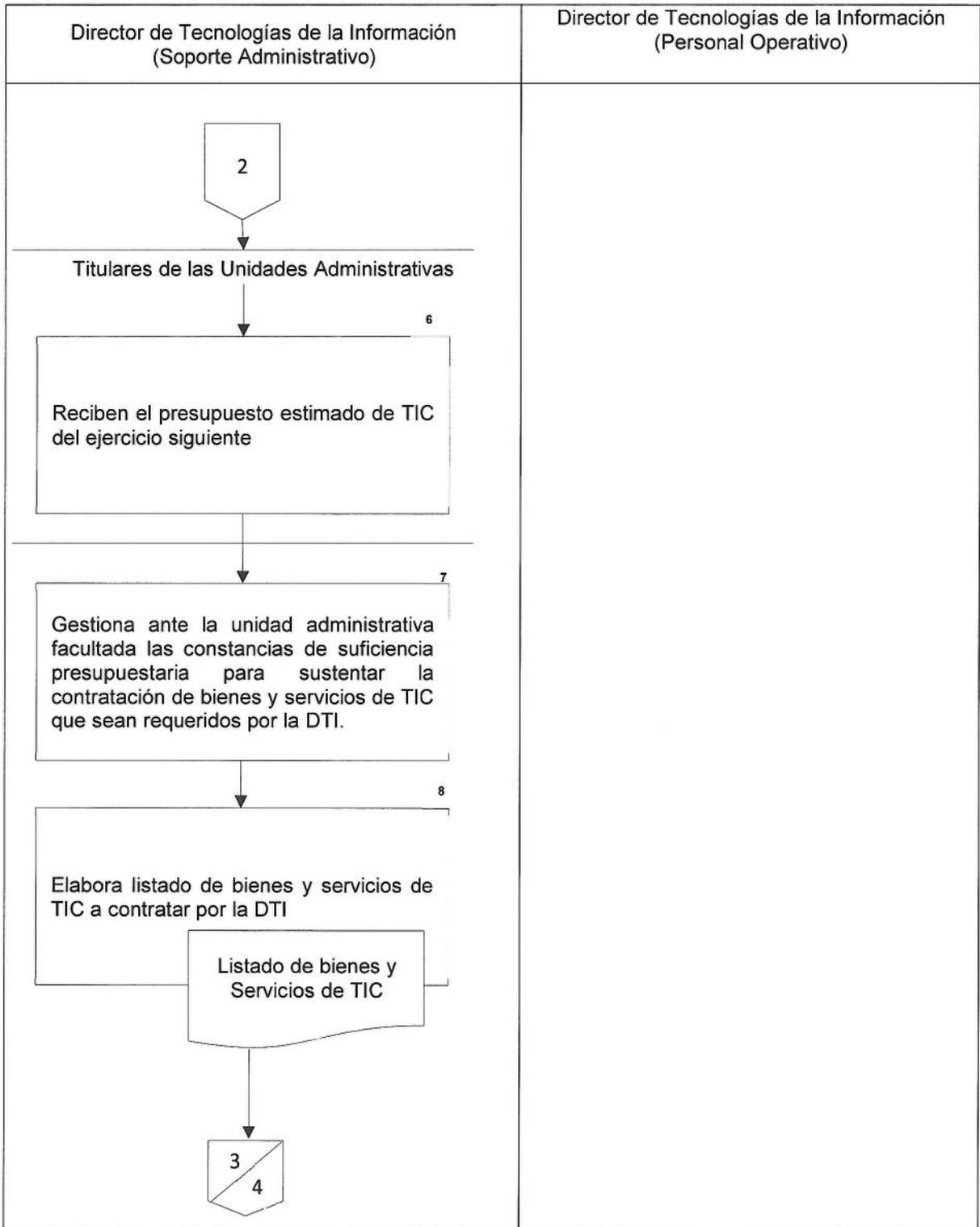
Responsable	No. Act.	Descripción de actividades	Documento o anexo
	18	Participa con el área contratante en la elaboración de la investigación de mercado	Estudio de Mercado
Director de Tecnologías de la Información (Soporte Administrativo con apoyo del Personal Operativo)	19	Apoya al área contratante en la elaboración e integración del proyecto	
	20	Mantiene informados a los responsables del seguimiento al ejercicio del presupuesto autorizado para las contrataciones de TIC	
Director de Tecnologías de la Información (Personal Operativo)	21	Participa en las juntas de aclaraciones que se lleven a cabo, apoyando al área contratante	
	22	Analiza y evalúa la propuesta técnica de las proposiciones que presenten los licitantes con apoyo del área de Adquisiciones  TERMINA	

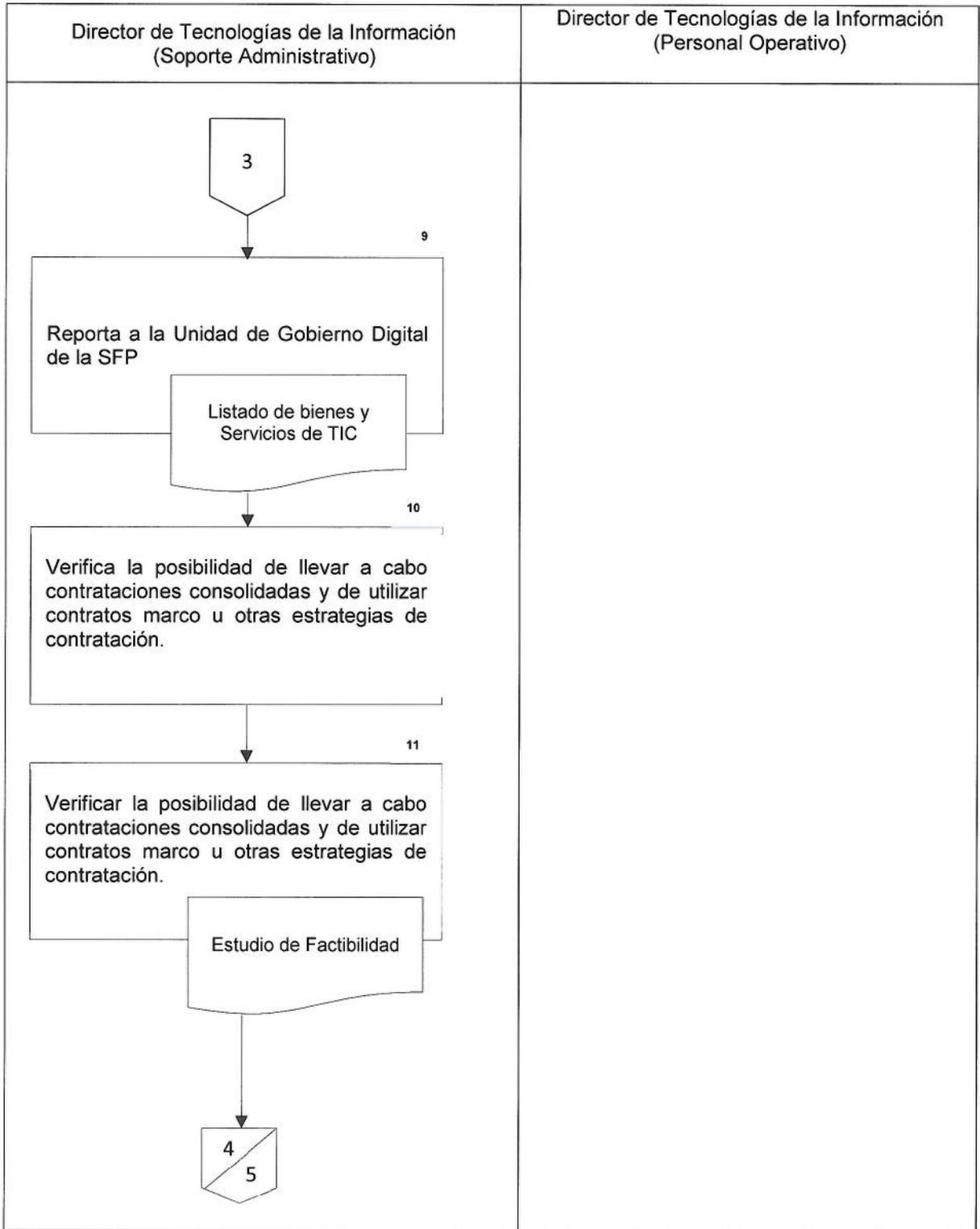
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información <b>2. Procedimiento para la Administración del Presupuesto y las Contrataciones.</b>		Hoja: 6 de 17

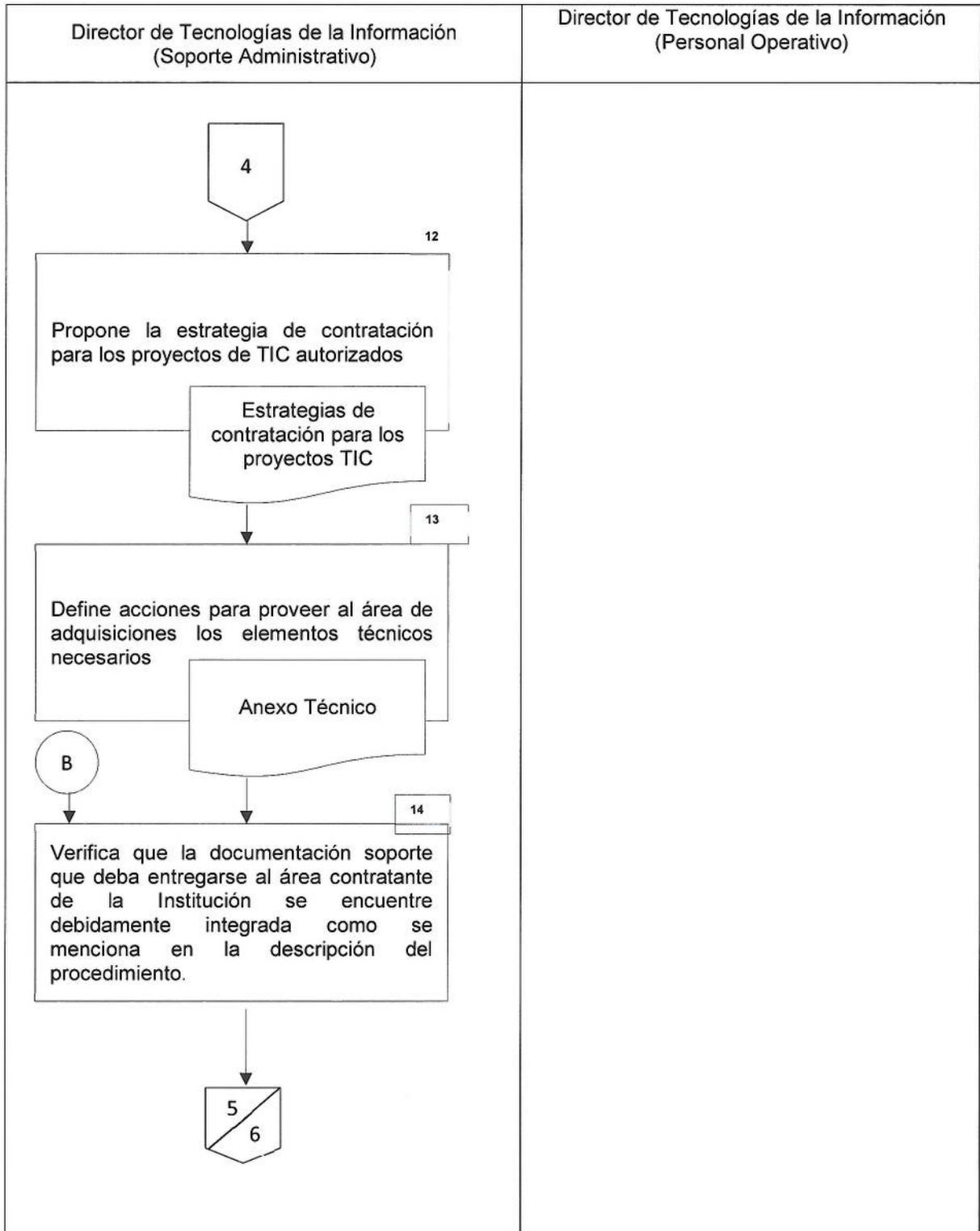
## 5. DIAGRAMA DE FLUJO

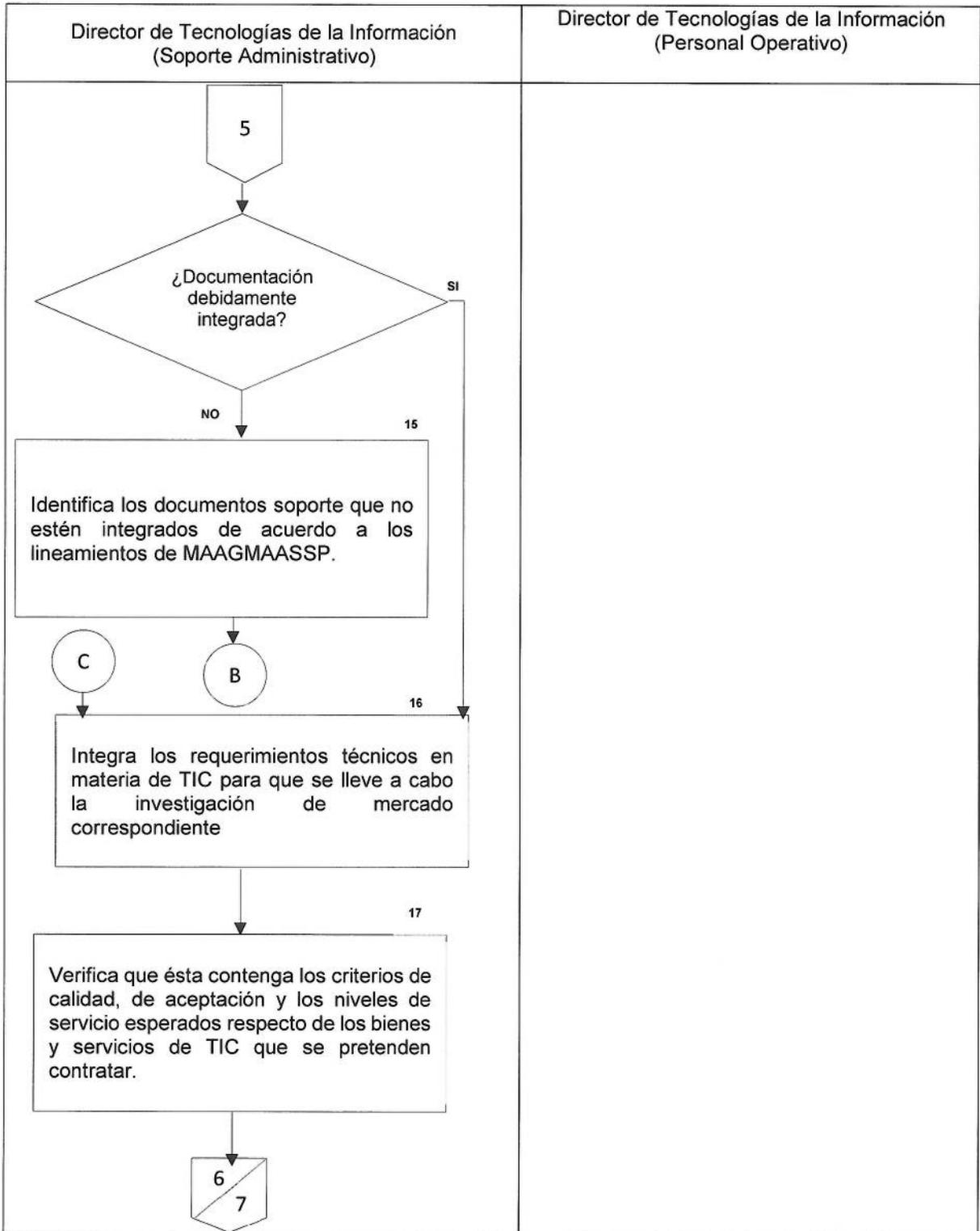


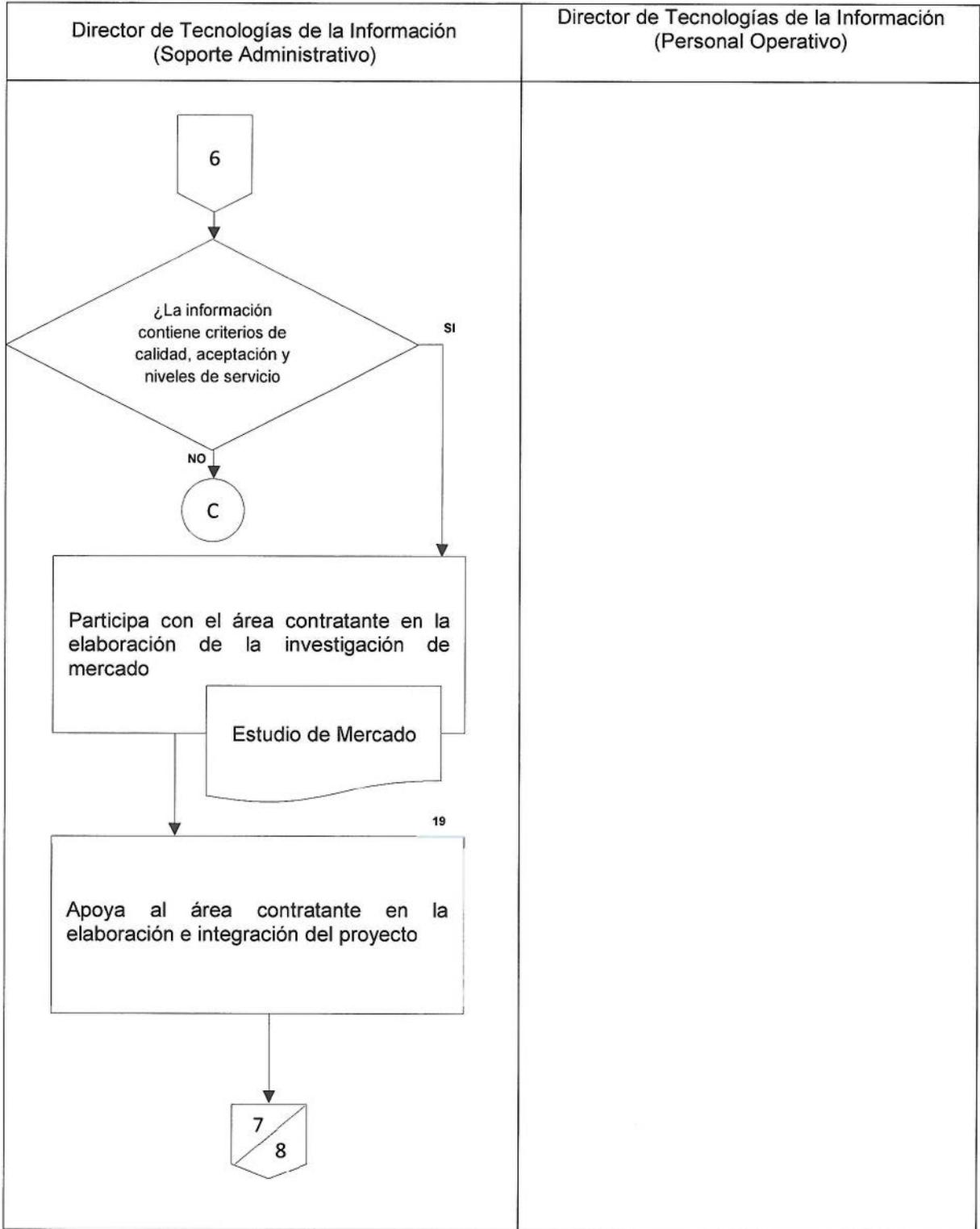


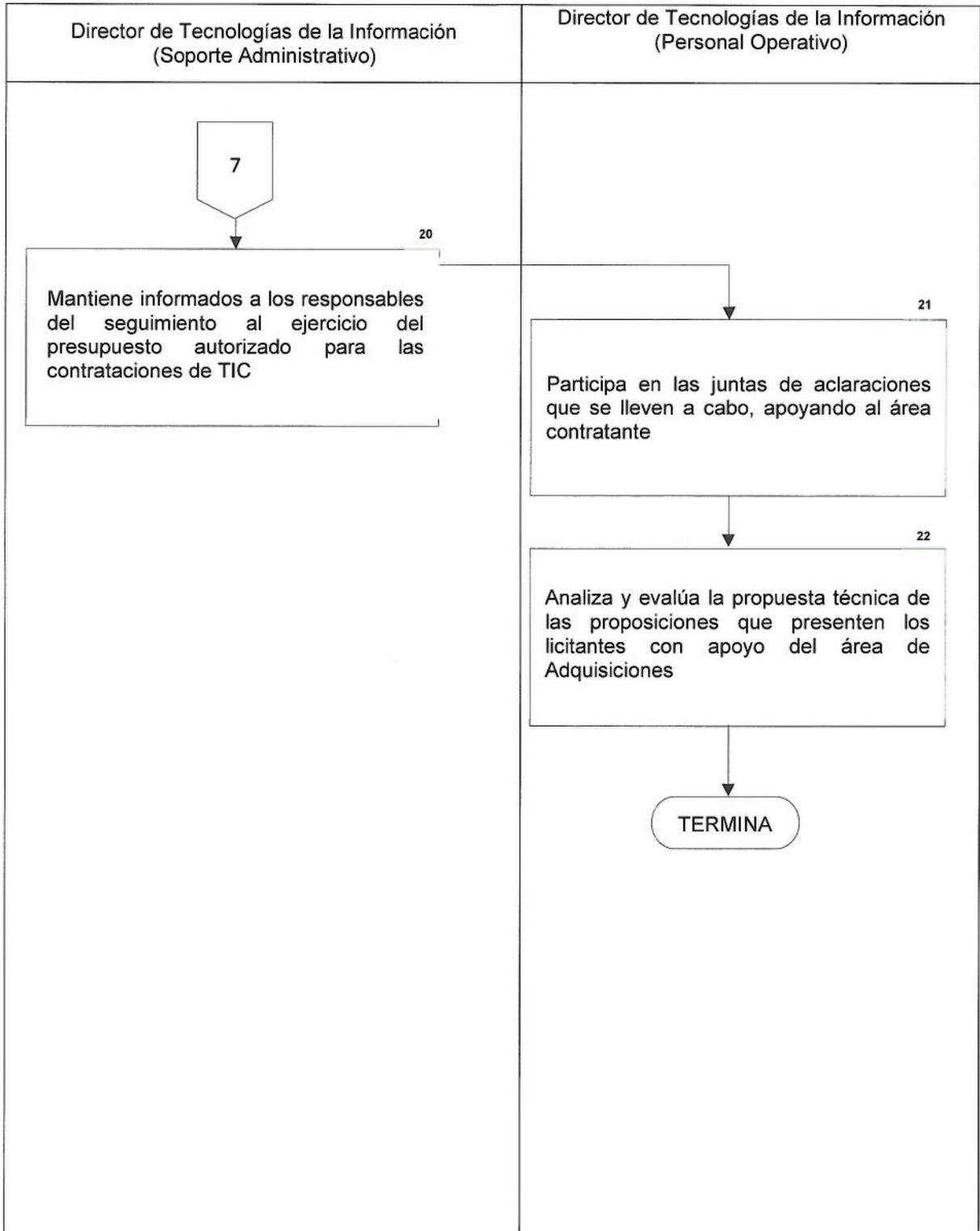












	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 14 de 17
	<b>2. Procedimiento para la Administración del Presupuesto y las Contrataciones.</b>		

## 6. DOCUMENTOS DE REFERENCIA

Nombre del documento	Código (cuando aplique)
No aplica	No aplica

## 7. REGISTROS

Registros	Tiempo de conservación	Responsable de conservarlo	Código de registro o identificación única
No aplica	No aplica	No aplica	No aplica

## 8. GLOSARIO DEL PROCEDIMIENTO

- 8.1 **Activos de TIC:** los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.
- 8.2 **ACNF:** proceso de administración de la configuración;
- 8.3 **ADP:** proceso de administración de proyectos;
- 8.4 **ADS:** proceso de administración de servicios;
- 8.5 **APCT:** proceso de administración del presupuesto y las contrataciones;
- 8.6 **Aplicativo de Cómputo:** el software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo a requerimientos previamente definidos;
- 8.7 **APRO:** proceso de administración de proveedores;
- 8.8 **Arquitectura Empresarial:** la información del estado actual y futuro de una Institución, a partir del análisis con perspectiva estratégica; considerando modelos de negocio, procesos, aplicativos y tecnologías de la información y comunicaciones;
- 8.9 **Arquitectura Orientada a Servicios:** la metodología y marco de trabajo, para construir componentes de software reutilizables para la interoperabilidad de aplicativos de cómputo;
- 8.10 **AOP:** proceso de administración de la operación;
- 8.11 **ASI:** proceso de administración de la seguridad de la Información.
- 8.12 **Borrado Seguro:** el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital;
- 8.13 **Cartera Ejecutiva de Proyectos de TIC:** Conjunto total de proyectos de TIC que la institución propondrá a la Unidad para su seguimiento;
- 8.14 **Cartera Operativa de Proyectos de TIC:** Conjunto total de proyectos que soportan la operación diaria de la DTI y no son considerados como estratégicos;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 15 de 17
	<b>2. Procedimiento para la Administración del Presupuesto y las Contrataciones.</b>		

- 8.15 **Centro de Datos:** el lugar físico en los que se ubiquen los activos de TIC y desde el que se proveen servicios de TIC;
- 8.16 **Cómputo en la Nube:** al modelo de prestación de servicios digitales que permite a las Instituciones acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios;
- 8.17 **Dependencias:** las Secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como a la Oficina de la Presidencia de la República y la Procuraduría General de la República; así como los Órganos Reguladores Coordinados en Materia Energética;
- 8.18 **Dominio Tecnológico:** las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo;
- 8.19 **EDN:** la Estrategia Digital Nacional contenida en el Objetivo número 5 del Programa;
- 8.20 **EIDA:** el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, establecido mediante Acuerdo publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011;
- 8.21 **Entidades:** los organismos descentralizados, empresas de participación estatal mayoritaria, instituciones nacionales de crédito, organizaciones auxiliares nacionales de crédito e instituciones nacionales de seguros y de fianzas, y fideicomisos públicos que en términos de la Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales, sean considerados entidades de la Administración Pública Federal Paraestatal;
- 8.22 **ERISC:** equipo de respuesta a incidentes de seguridad en TIC en la Institución;
- 8.23 **Estándar abierto:** a las especificaciones cuya utilización esté disponible de manera gratuita o que no suponga una dificultad de acceso, y que su uso y aplicación no esté condicionada al pago de un derecho de propiedad
- 8.24
- 8.25 **Herramienta de Gestión de la Política TIC:** sistema web usado para llevar a cabo la comunicación de actividades de reporte establecidas en el Acuerdo, considerando el reporte de PETIC, la obtención del dictamen técnico que emite la Unidad, autorización por parte de la UPCP, la arquitectura empresarial, el MAAGTICSI, entre otros;
- 8.26 **Infraestructuras Críticas de Información:** Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia.
- 8.27 **Infraestructuras de Información esenciales:** Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de información, TIC y TO, cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación de las Instituciones.
- 8.28 **Infraestructura de TIC:** el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 16 de 17
	<b>2. Procedimiento para la Administración del Presupuesto y las Contrataciones.</b>		

- 8.29 Infraestructura Pasiva:** elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de las dependencias o entidades, que sean necesarios para la instalación y operación de las redes, así como para la prestación de servicios de procesamiento de datos, de telecomunicaciones y radiodifusión;
- 8.30 Instancias de Seguridad Nacional:** las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquellas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional;
- 8.31 Institución:** las dependencias y entidades de la Administración Pública Federal, tal y como se definen en este Acuerdo;
- 8.32 Lineamientos:** los Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicados en el Diario Oficial de la Federación el 30 de enero de 2013;
- 8.33 MAAGMAASSP:** el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público;
- 8.34 MAAGTICSI:** el Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información. Anexo Único del presente Acuerdo;
- 8.35 Niveles de servicio:** el establecimiento en un lenguaje no técnico del servicio brindado, incluyendo al menos la definición, disponibilidad, calidad, tiempos de respuesta y solución.
- 8.36 OPEC:** proceso de operación de los controles de seguridad de la información y del erisc;
- 8.37 PE:** proceso de planeación estratégica;
- 8.38 PETIC:** el conjunto de proyectos que elaboran las Instituciones, conformado por un máximo de 7 proyectos estratégicos, en los términos establecidos en el presente Acuerdo;
- 8.39 Portafolio de proyectos de TIC:** es el total de los proyectos de TIC agrupados según su clasificación en Cartera Ejecutiva de Proyectos de TIC y Cartera Operativa de Proyectos de TIC que la Institución planea desarrollar, en los términos establecidos por el MAAGTICSI;
- 8.40 Programa:** el Programa para un Gobierno Cercano y Moderno 2013-2018, aprobado mediante Decreto publicado en el Diario Oficial de la Federación el 30 de agosto de 2013;
- 8.41 Proyectos de TIC:** el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC y que cuenta con presupuesto para su ejecución; considerando 2 tipos: proyectos operativos que soportan las actividades diarias de la DTI y proyectos estratégicos en los términos señalados en el presente Acuerdo;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 17 de 17
	<b>2. Procedimiento para la Administración del Presupuesto y las Contrataciones.</b>		

8.42 **Retos Públicos:** el modelo que fomenta la democratización del gasto público y la innovación, invitando a los emprendedores del país a plantear soluciones a retos de gobierno mediante el desarrollo de aplicativos tecnológicos web y móviles;

8.43 **SEGOB:** la Secretaría de Gobernación;

8.44 **Seguridad de la información:** la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma;

8.45 **Seguridad Nacional:** las acciones a las que se refiere el artículo 3 de la Ley de Seguridad Nacional;

8.46 **SFP:** la Secretaría de la Función Pública;

8.47 **SHCP:** la Secretaría de Hacienda y Crédito Público;

8.48 **Tecnologías Verdes:** el conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las tecnologías de la información y comunicaciones, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías;

8.49 **TIC:** las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video;

8.50 **Unidad:** la Unidad de Gobierno Digital de la SFP;

8.51 **DTIC:** la Dirección de Tecnologías de Información y Comunicaciones o área responsables de las TIC en la Institución.

## 9. CAMBIOS DE VERSIÓN DEL PROCEDIMIENTO

Numero de revisión	Fecha de actualización	Descripción del cambio
0	No aplica	No aplica

## 10. ANEXOS DEL PROCEDIMIENTO

No aplica

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 1 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		

## 1. PROPÓSITO

Establecer la funcionalidad del proceso de Administración de Servicios, derivado del Manual Administrativo de Aplicación General en Materias de Tecnología de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), mediante la asignación de los roles identificados en el proceso y sus subprocesos, formalizando la asignación del rol a los responsables que participan en la ejecución de cada una de las tareas del proceso, con el fin de obtener la información, evidencias y entregables que generen las actividades ejecutadas durante el proceso.

## 2. ALCANCE

- 2.1 Obtener el mapa del proceso y de las actividades de los subprocesos involucrados, que permitan identificar la funcionalidad del proceso ADS.
- 2.2 Identificar los roles o los actores que se requieren para que el proceso genere las evidencias y entregables que demuestren la funcionalidad del proceso
- 2.3 Identificar a las áreas o personas que se harán responsables de los diferentes roles que requiere el proceso.
- 2.4 Formalizar las asignaciones de responsables de roles y actividades.
- 2.5 Establecer si es necesario entre las áreas identificadas que participarán con alguna responsabilidad en el proceso un OLA, acuerdo de operación, en el cual se especifiquen los servicios que se aportarán y los tiempos en los que se atenderán y los entregables comprometidos que requiere el proceso.
- 2.6 Identificar las capacitaciones que se requieran en las diferentes áreas o personas que asuman el rol asignado, para que se consideren en un programa de capacitación.
- 2.7 Identificar los indicadores de desempeño del proceso y registrarlos periódicamente para su evaluación posterior.
- 2.8 Identificar los indicadores de los servicios considerados y sus métricas.

## 3. POLÍTICAS DE OPERACIÓN, NORMAS Y LINEAMIENTOS

- 3.1 El responsable de este proceso deberá ser designado por el titular de la DTI, y tener un nivel jerárquico inmediato inferior al de éste.
- 3.2 El Responsable del proceso Administración de Servicios (ADS) deberá asegurarse que el hardware y el software de recuperación utilizado en la aplicación del programa de continuidad sea funcional, para restablecer, probar y renovar los respaldos al menos semestralmente.
- 3.3 El Responsable del proceso Administración de Servicios (ADS) deberá asegurarse que los servicios de TIC y las soluciones tecnológicas que provea la DTI para oficios electrónicos al interior de la Institución y entre instituciones, cumplan con lo que se establece tanto en los Lineamientos para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión, así como en los Documentos Técnicos de Interoperabilidad vigentes y los aplicables que expida la Subcomisión de Interoperabilidad de la CIDGE, derivados del Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b> <b>3. Procedimiento para la Administración de Servicios.</b>		Hoja: 2 de 21

- 3.4 El responsable del diseño de servicios de TIC, conjuntamente con el Responsable de la planeación estratégica de la DTI, deberán asegurarse que el diseño de nuevas soluciones tecnológicas y servicios de TIC incluya, de ser el caso, aquellos datos que permitan cumplir con la normatividad técnica de domicilios geográficos que para dicho fin emite el INEGI.
- 3.5 El responsable del diseño de servicios de TIC, conjuntamente con el responsable de la planeación estratégica de la DTI, deberán asegurarse que se cumpla, para el Cifrado de Datos, como mínimo con estándares tales como 3DES de triple llave, AES-128, AES-192 y AES-256, así como redes con protocolos seguros para su envío.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>3. Procedimiento para la Administración de Servicios.</b>		Hoja: 3 de 21

#### 4. DESCRIPCIÓN DEL PROCEDIMIENTO

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director de Tecnologías de la Información (Personal Operativo)	1	Coordina la actualización constante del catálogo de servicios de TIC	Catálogo de Servicios de TIC  Catálogo de Servicios de TIC
	2	Asegura que los datos se mantengan en el repositorio de configuraciones del ACNF, se encuentren registrados en la Herramienta de Gestión de la Política TIC	
	3	Mantiene informados a los responsables sobre los cambios al catálogo de servicios	
Director de Tecnologías de la Información (Soporte Administrativo)	4	Asigna un responsable del diseño de TIC para cada servicio	
Director de Tecnologías de la Información (Responsable del diseño de servicios de TIC)	5	Define y coordinar con los involucrados los requerimientos del servicio de TIC	Análisis de requerimientos  Análisis de Impacto al negocio
	6	Realiza un análisis de los requerimientos asociados al servicio de TIC	
	7	Verifica infraestructura, capacidad, componentes y servicios de TIC existentes	
	8	Efectúa análisis de impacto al negocio	
	9	Verifica que la solución para el servicio de TIC que se hubiere seleccionado se encuentre alineada al programa de tecnología, a los objetivos institucionales y a las líneas de acción de la EDN. ¿La solución está alineada a la EDN? No: Continuar en la actividad 8 Si: Continuar en la actividad 10	
	10	Define y da seguimiento al desarrollo y mantenimiento de los servicios, así como la evaluación periódica de estos a través de una hoja de ruta de servicios (roadmap).	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 4 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		

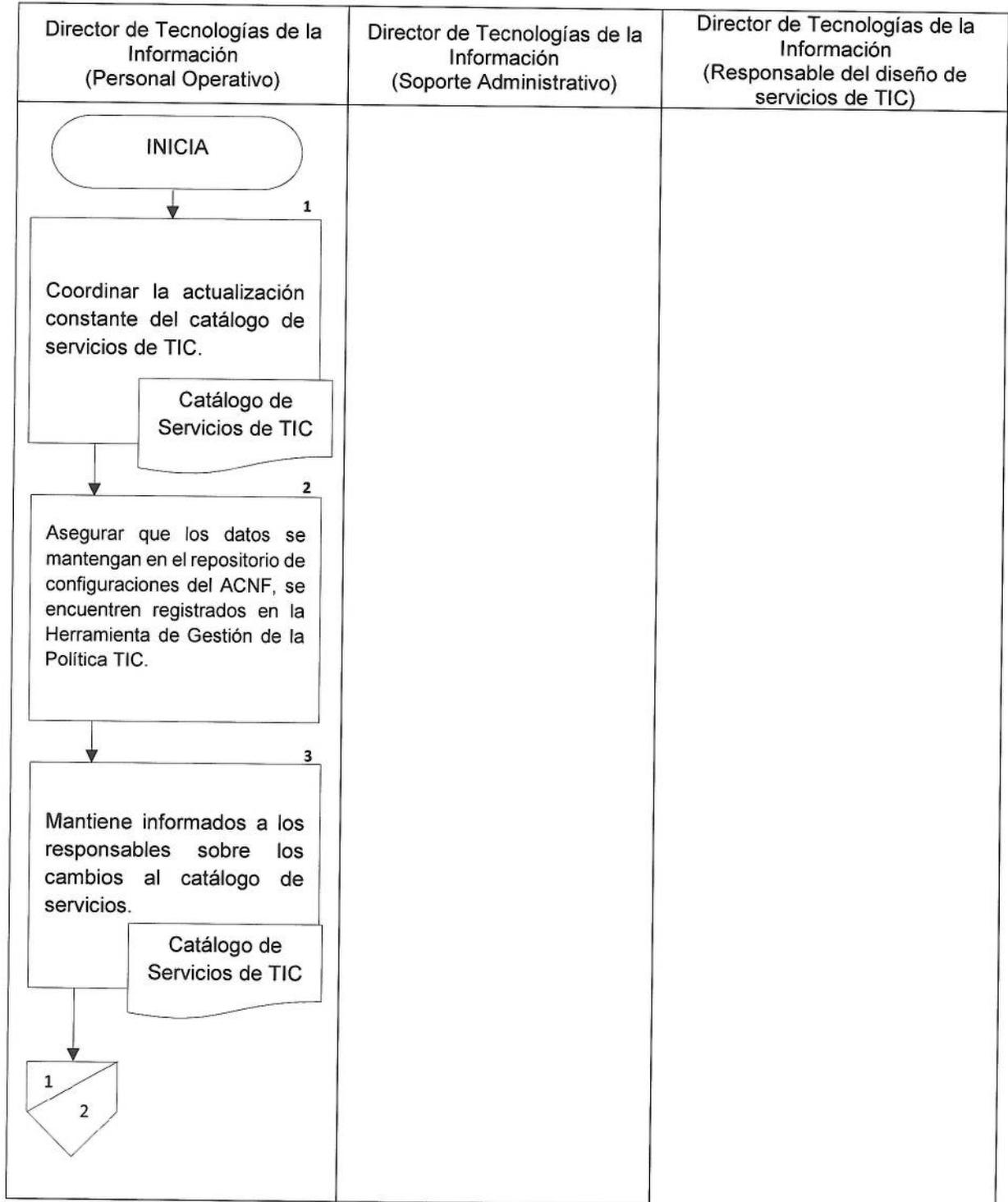
Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director de Tecnologías de la Información (Responsable del diseño de servicios de TIC)	11	Evalúa y selecciona, en coordinación con la unidad administrativa solicitante, la solución más adecuada, así como la capacidad técnica y administrativa requerida por la Institución para la operación dicha solución.	
	12	Integra el expediente del diseño de TIC	
	13	Actualiza el portafolio de servicios TIC con la información del expediente del servicio de TIC diseñado.	
Director de Tecnologías de la Información (Soporte Administrativo con apoyo de personal operativo)	14	Determina el balance entre la demanda de los servicios y la capacidad de infraestructura TIC	Programa de Capacidad
	15	Establece escenarios para diversas proyecciones de demanda de los servicios	
	16	Determina los componentes de infraestructura necesarios para cumplir los requerimientos	
	17	Identifica los activos de TIC que requieren actualizarse, mejorarse o sustituirse	
	18	Elabora el programa de capacidad	
	19	Monitorea el rendimiento actual y la capacidad utilizada	
	20	Obtiene información de los incidentes que se han presentado por falta de capacidad	
	21	Evalúa los niveles de la capacidad y rendimiento de la infraestructura	
	22	Verifica, al menos trimestralmente, la capacidad y rendimiento de la infraestructura de TIC, para determinar si es suficiente para prestar los servicios de TIC con los niveles de servicio acordados ¿La infraestructura es suficiente? No: continuar en actividad 23 Sí: continuar en actividad 25	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 5 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		

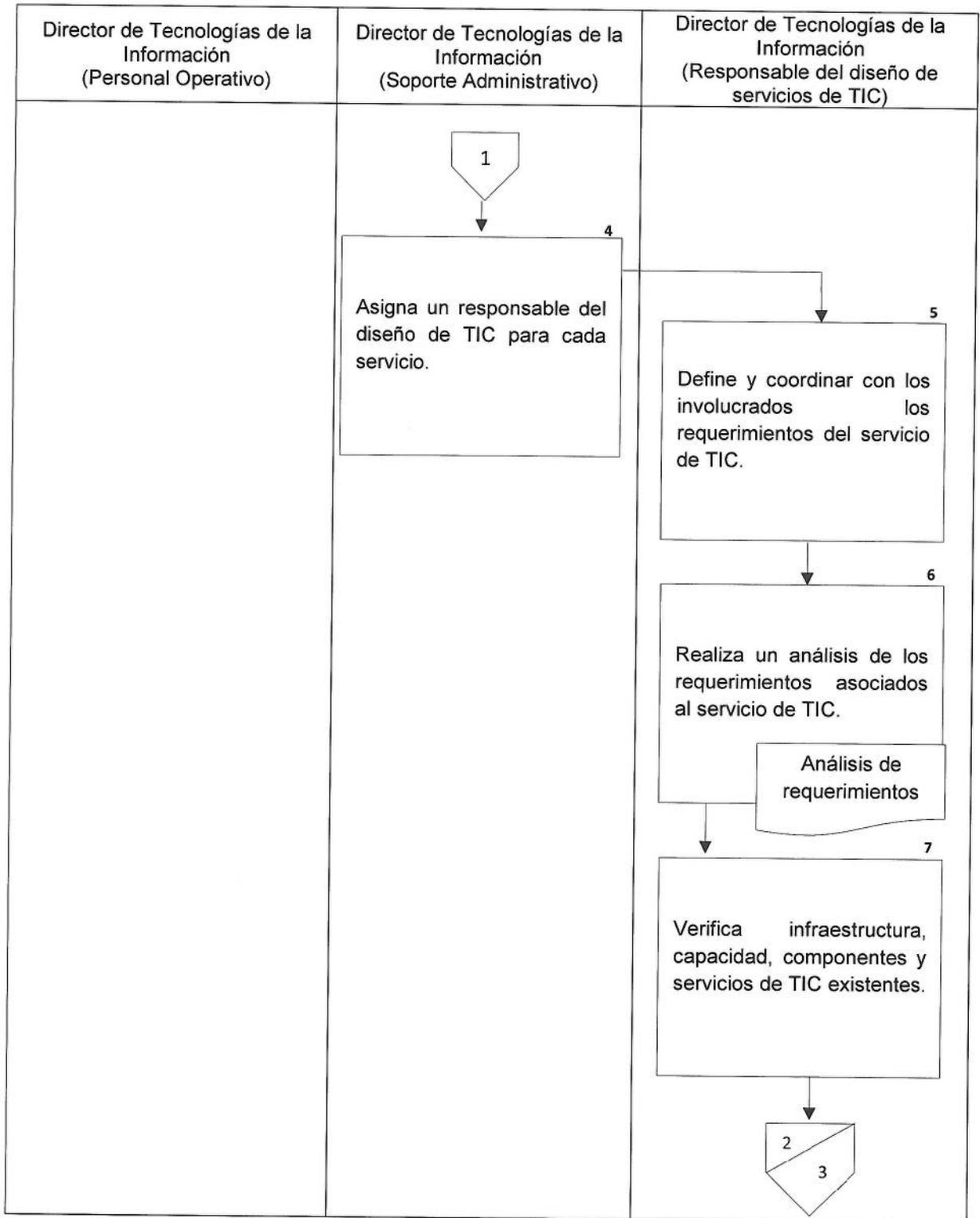
Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director de Tecnologías de la Información (Soporte Administrativo con apoyo de personal operativo)	23	Identifica las tendencias de las cargas de trabajo de los componentes de la infraestructura, en condiciones normales y de contingencia, así como determinar sus proyecciones, para que sean incluidas en el programa de capacidad.	Programa de Capacidad
	24	Define las acciones a implementar cuando la capacidad y rendimiento de la infraestructura de TIC no estén en el nivel requerido	
	25	Incluye en los programas de continuidad las características de capacidad y rendimiento de cada componente de infraestructura de TIC	
	26	Mantiene informados a los responsables de procesos de la DTI	
Director de Tecnologías de la Información (Responsable del diseño de servicios de TIC)	27	Efectúa el análisis de impacto al negocio, en el que se identifiquen las funciones, actividades, áreas o unidades administrativas, así como los servicios que proporciona la Institución que podrían resultar afectados como consecuencia de la interrupción de uno o más servicios de TIC, así como el alcance de las consecuencias que se generarían.	Análisis de Impacto al Negocio
	28	Elabora el programa de continuidad	Programa de Continuidad
	29	Integra definiciones en el programa de continuidad	
	30	Efectúa pruebas de recuperación al programa de continuidad	Programa de Continuidad
	31	Actualiza el programa de continuidad con las medidas correctivas que se definan sobre los hallazgos e incidentes encontrados en las pruebas	
	32	Revisa el contenido del programa de continuidad	
Director de Tecnologías de la Información (Personal Operativo DTI)	33	Mantiene actualizados y bajo resguardo los respaldos de información considerados por la Institución y ser aprobados por el Titular de la DTI.	
TERMINA			

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 6 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		

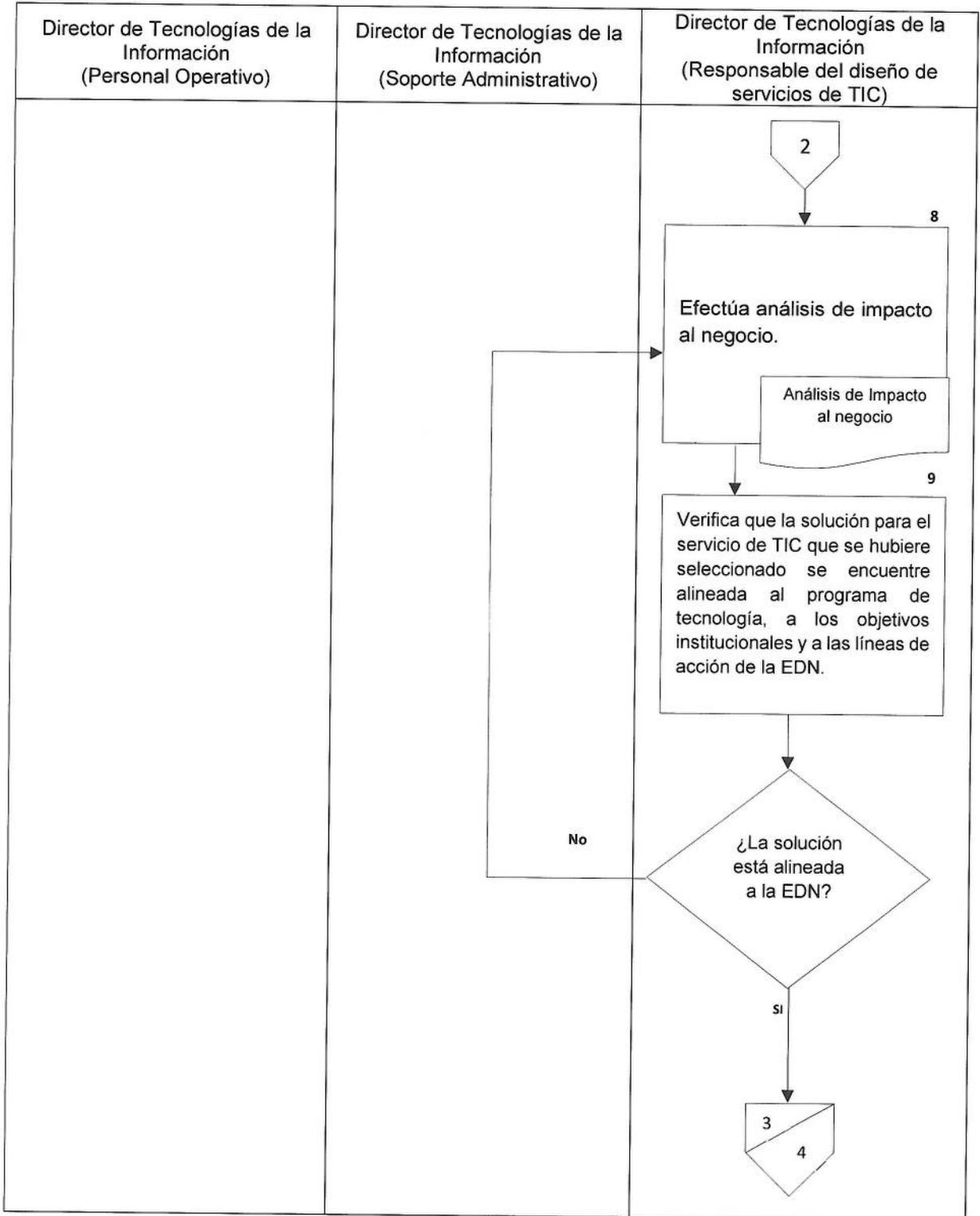
## 5. DIAGRAMA DE FLUJO



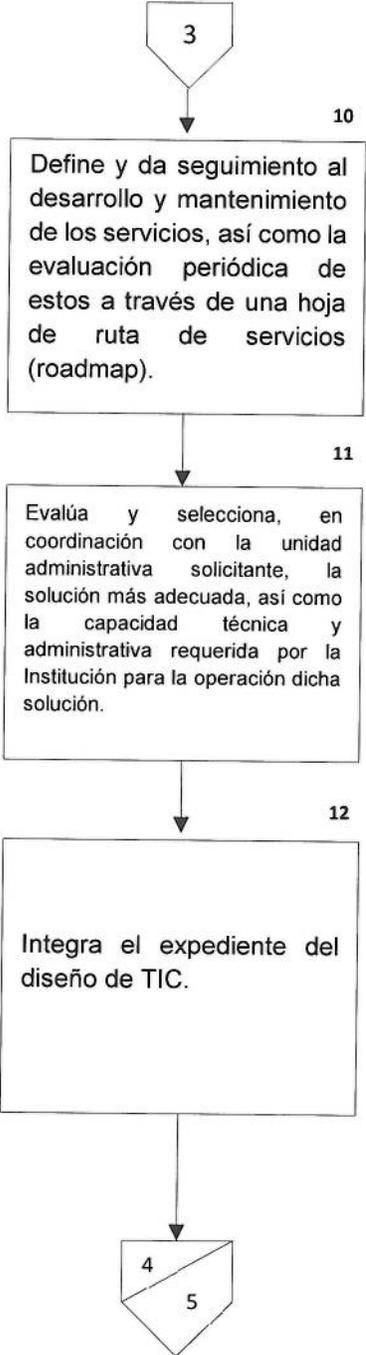
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 7 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		

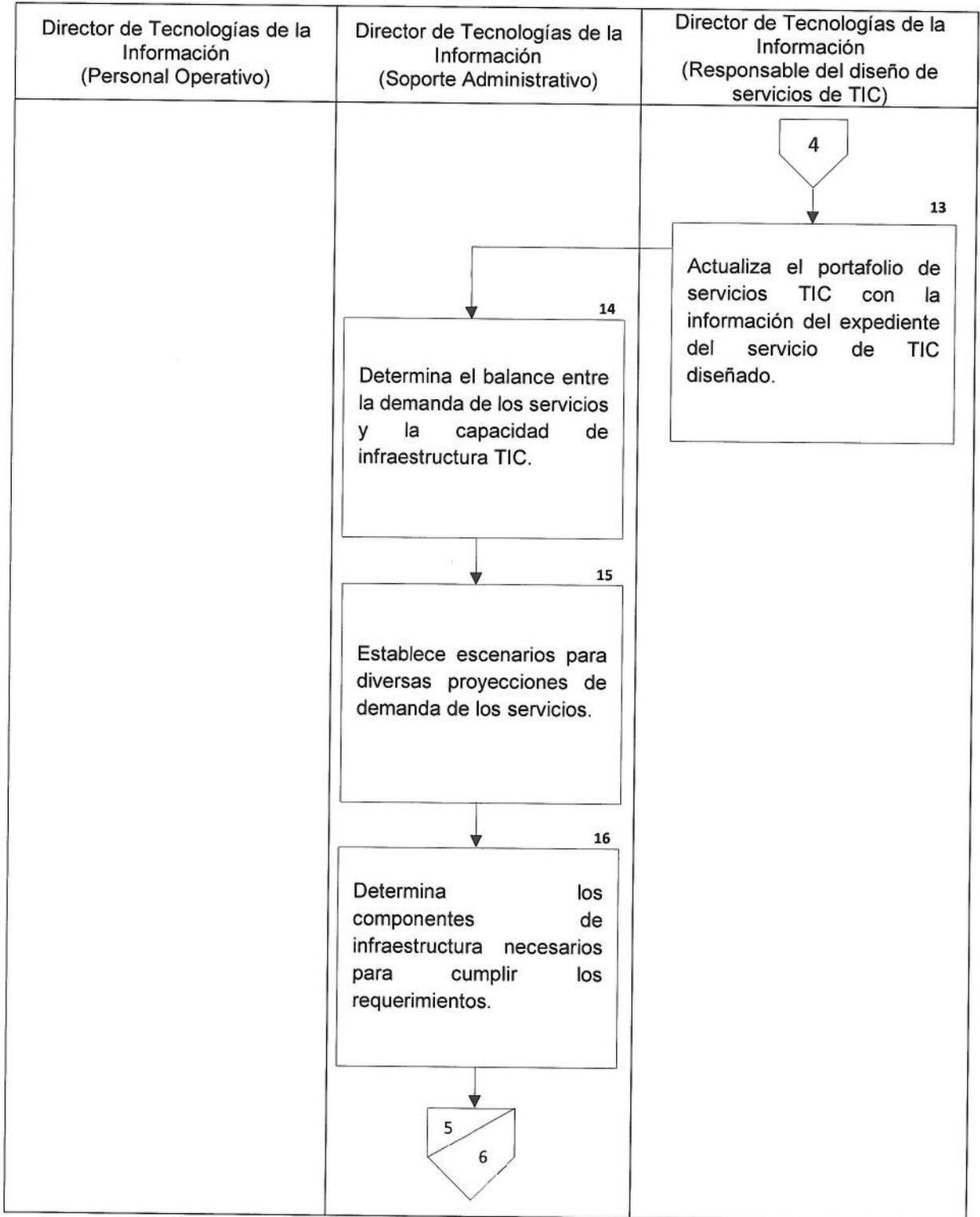


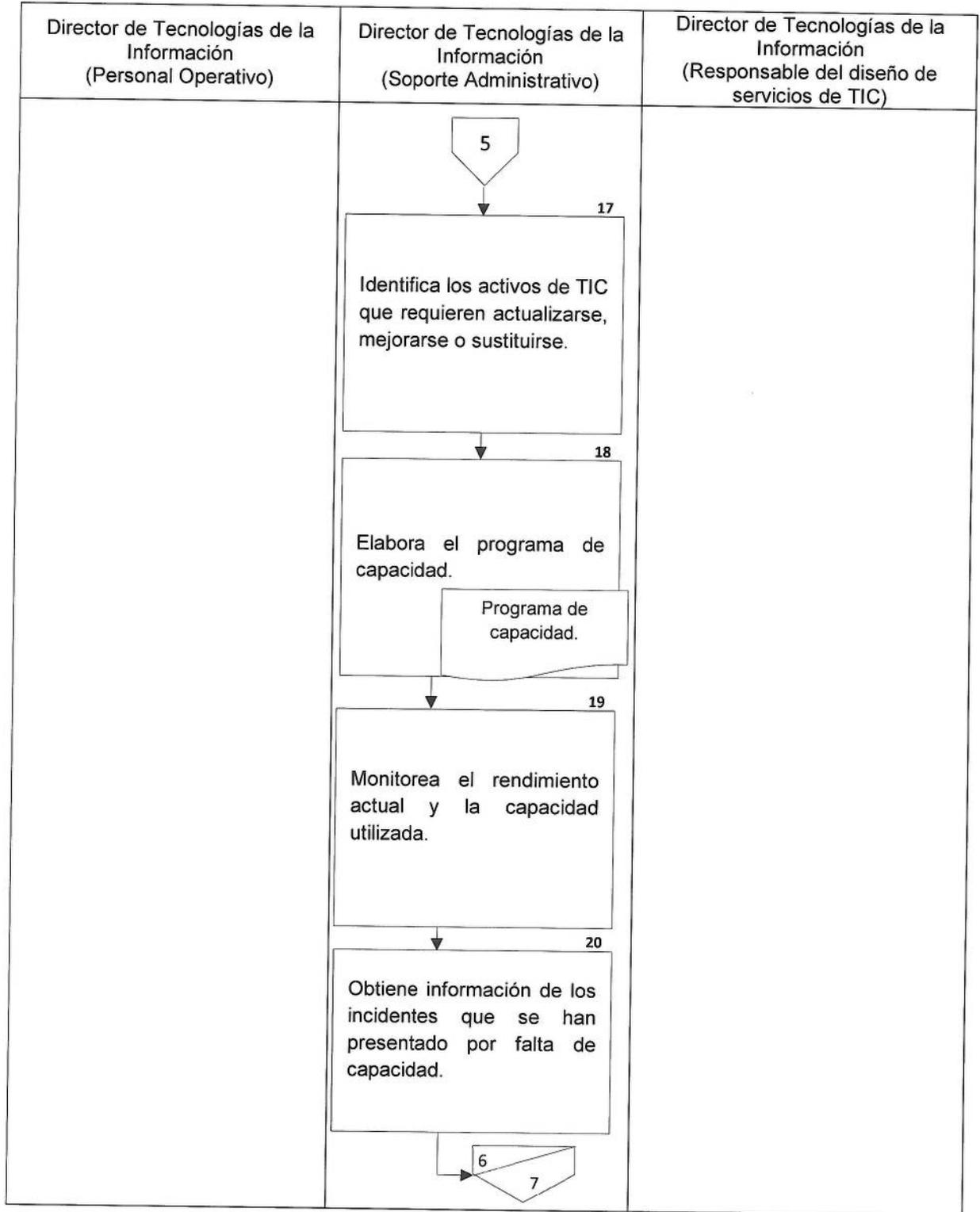
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 8 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		



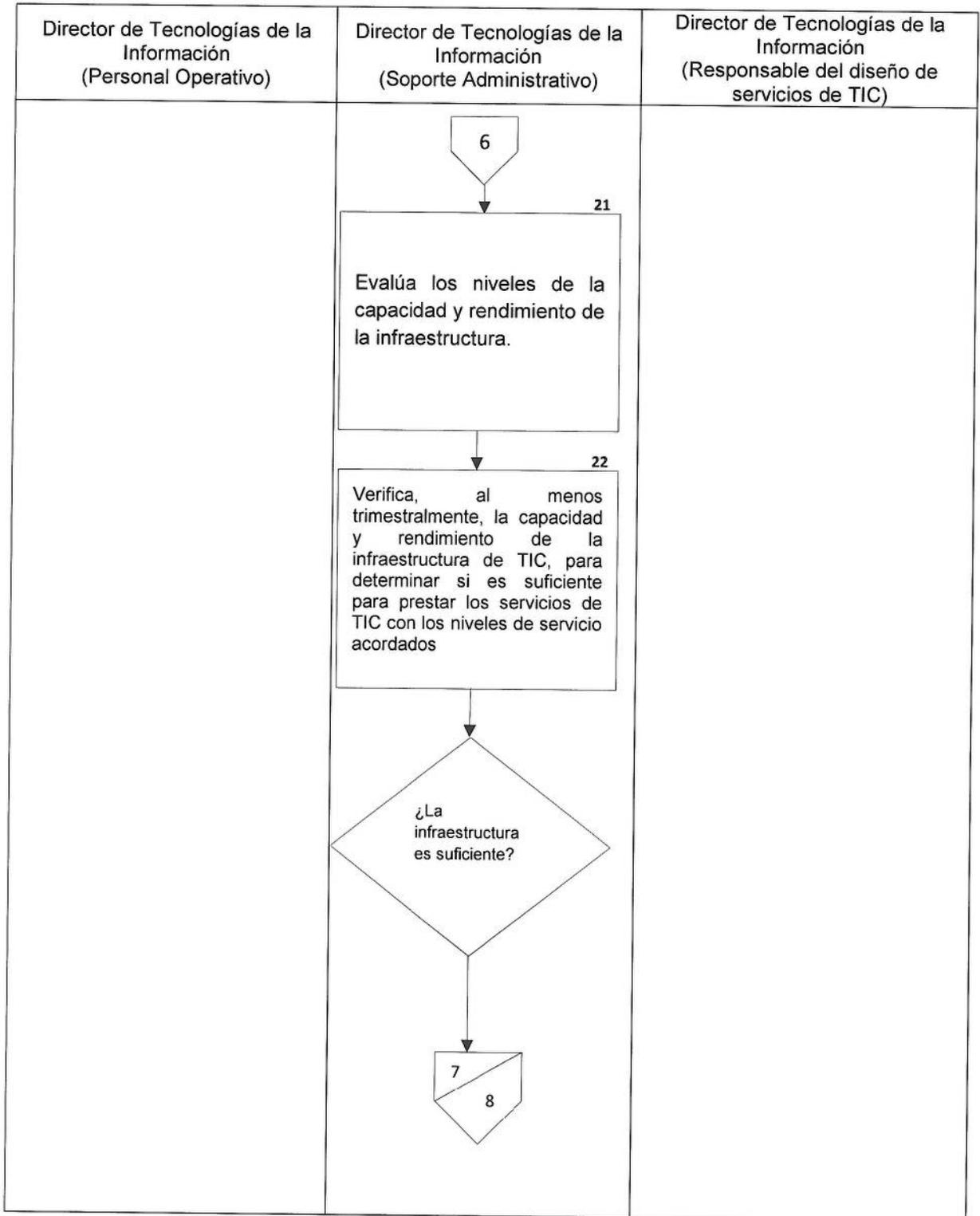
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>3. Procedimiento para la Administración de Servicios.</b>		Hoja: 9 de 21

Director de Tecnologías de la Información (Personal Operativo)	Director de Tecnologías de la Información (Soporte Administrativo)	Director de Tecnologías de la Información (Responsable del diseño de servicios de TIC)
		<div style="text-align: center;">  <pre> graph TD     3{{3}} --&gt; 10[Define y da seguimiento al desarrollo y mantenimiento de los servicios, así como la evaluación periódica de estos a través de una hoja de ruta de servicios (roadmap).]     10 --&gt; 11[Evalúa y selecciona, en coordinación con la unidad administrativa solicitante, la solución más adecuada, así como la capacidad técnica y administrativa requerida por la Institución para la operación dicha solución.]     11 --&gt; 12[Integra el expediente del diseño de TIC.]     12 --&gt; 45{{4 5}}           </pre> </div>

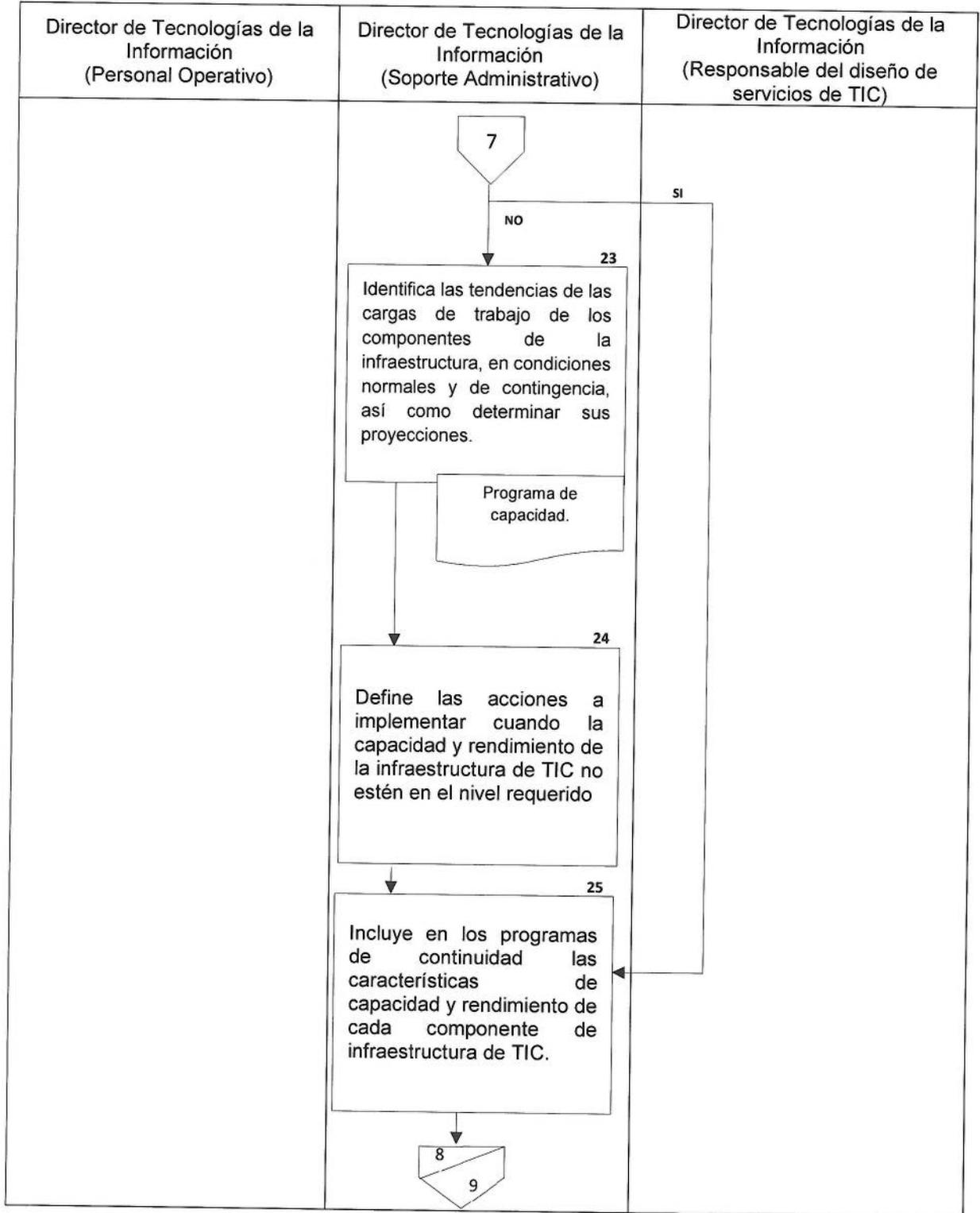


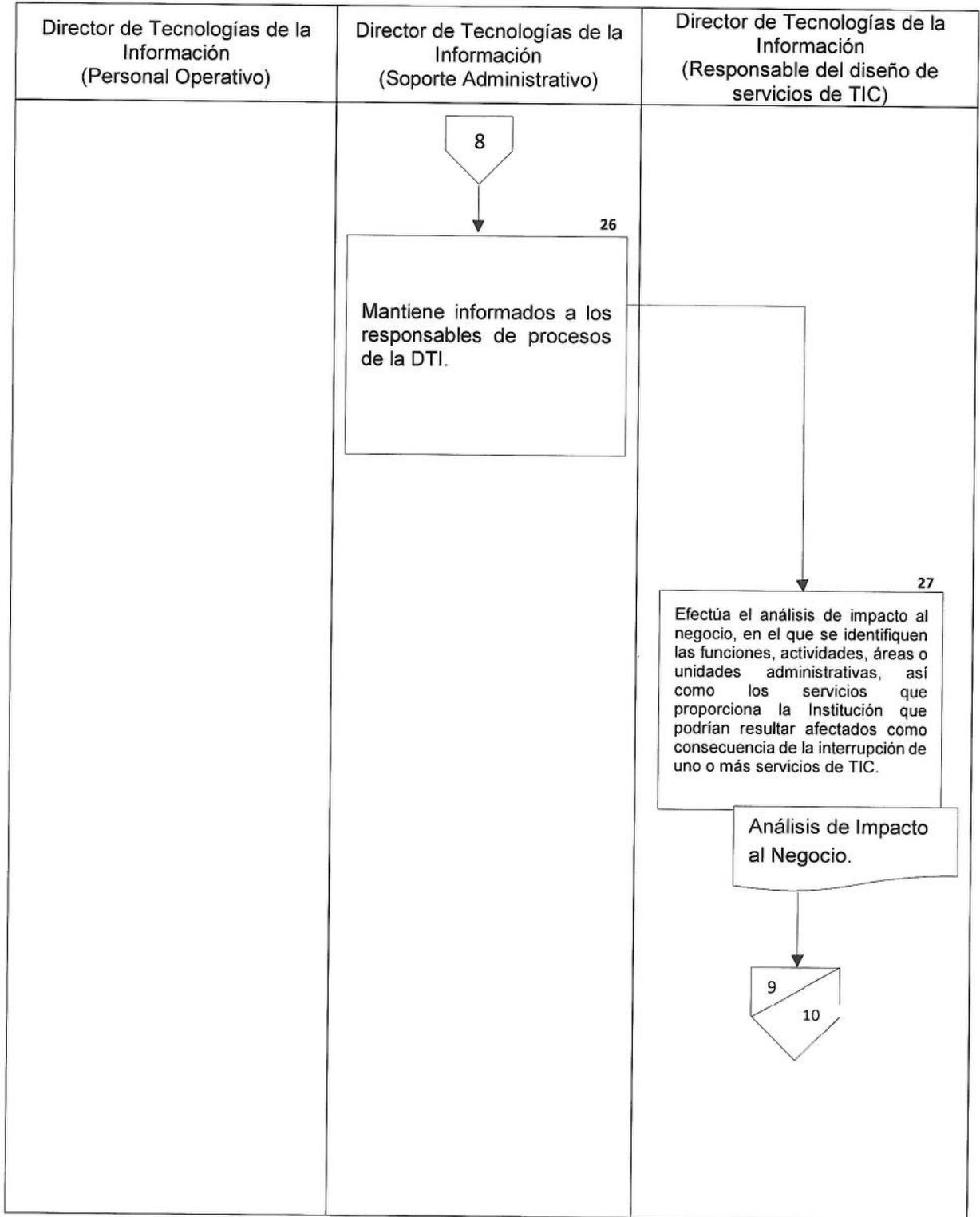


	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 12 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		

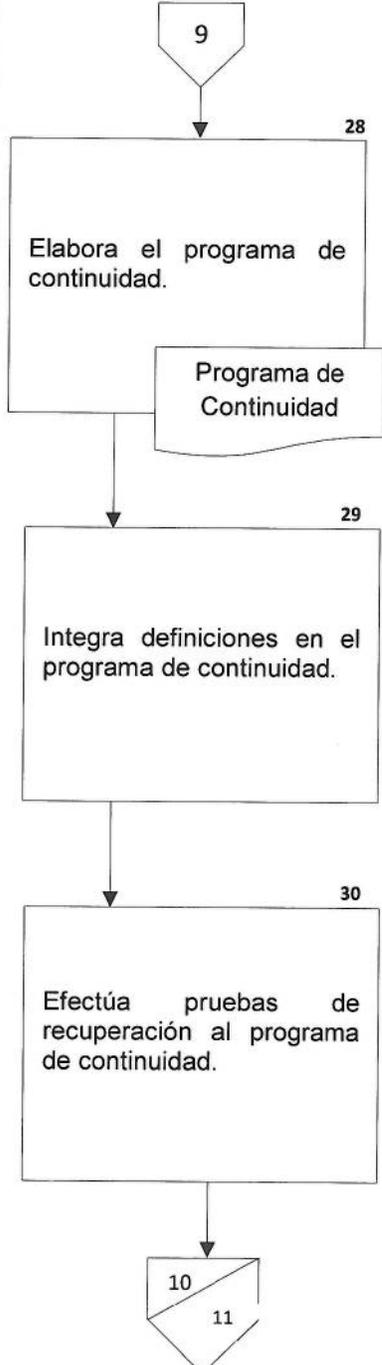


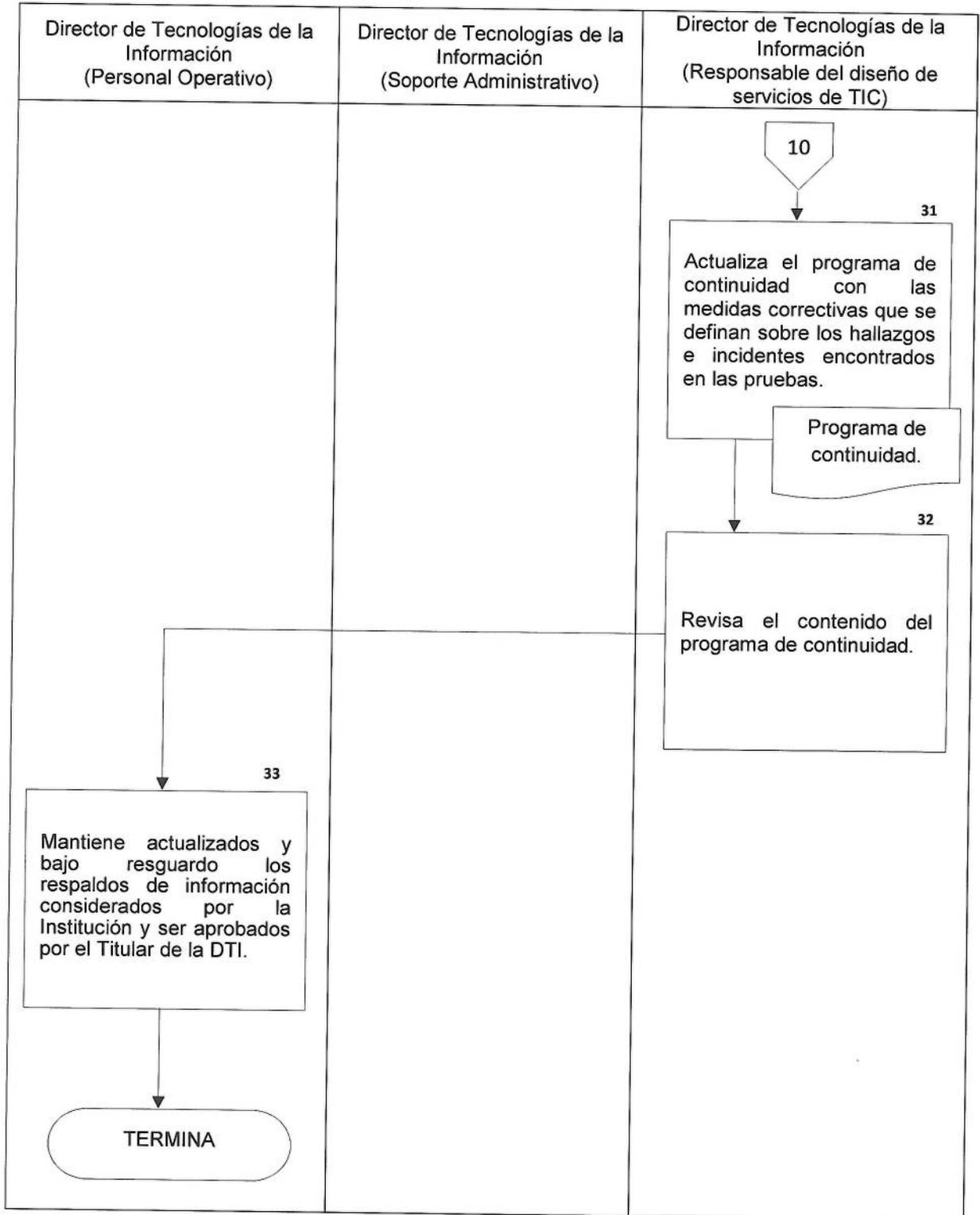
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 13 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		





	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 15 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		

Director de Tecnologías de la Información (Personal Operativo)	Director de Tecnologías de la Información (Soporte Administrativo)	Director de Tecnologías de la Información (Responsable del diseño de servicios de TIC)
		 <pre> graph TD     9[9] --&gt; 28[28: Elabora el programa de continuidad.]     28 --&gt; PC[Programa de Continuidad]     PC --&gt; 29[29: Integra definiciones en el programa de continuidad.]     29 --&gt; 30[30: Efectúa pruebas de recuperación al programa de continuidad.]     30 --&gt; 10_11[10/11] </pre>



	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 17 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		

## 6. DOCUMENTOS DE REFERENCIA

Nombre del documento	Código (cuando aplique)
6.1 Repositorio (ACNF).	No aplica
6.2 Lineamientos para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión.	No aplica
6.3 Documento Técnico de Interoperabilidad de los Sistemas Automatizados de Control de Gestión (DTISACG).	No aplica
6.4 Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.	No aplica
6.5 Normatividad técnica de domicilios geográficos (INEGI).	No aplica
6.6 Manual para la aplicación y difusión de la Norma Técnica sobre Domicilios Geográficos.	No aplica
6.7 Estándares para el cifrado de datos AES-128, AES-192 y AES-256.	No aplica
6.8 EDN(Estrategia Digital Nacional).	No aplica

## 7. REGISTROS

Registros	Tiempo de conservación	Responsable de conservarlo	Código de registro o identificación única
Catálogo de Servicios de TIC	4 meses	Responsable del Proceso	N/A
Análisis de Impacto al negocio	6 meses	Responsable del Proceso	N/A
Oportunidades identificadas para mejorar capacidad	3 meses	Responsable del Proceso	N/A
Niveles de servicio alcanzados	3 meses	Responsable del Proceso	N/A
Análisis de requerimientos	4 meses	Responsable del Proceso	N/A
Programa de Capacidad	3 meses	Responsable del Proceso	N/A
Programa de Continuidad	6 meses	Responsable del Proceso	N/A

## 8. GLOSARIO DEL PROCEDIMIENTO

- 8.1 Activos de TIC:** los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.
- 8.2 ACNF:** proceso de administración de la configuración.
- 8.3 ADP:** proceso de administración de proyectos.
- 8.4 ADS:** proceso de administración de servicios.
- 8.5 APCT:** proceso de administración del presupuesto y las contrataciones.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		
	<b>3. Procedimiento para la Administración de Servicios.</b>		Hoja: 18 de 21

- 8.6 Aplicativo de Cómputo:** el software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo a requerimientos previamente definidos.
- 8.7 APRO:** proceso de administración de proveedores.
- 8.8 Arquitectura Empresarial:** la información del estado actual y futuro de una Institución, a partir del análisis con perspectiva estratégica; considerando modelos de negocio, procesos, aplicativos y tecnologías de la información y comunicaciones.
- 8.9 Arquitectura Orientada a Servicios:** la metodología y marco de trabajo, para construir componentes de software reutilizables para la interoperabilidad de aplicativos de cómputo.
- 8.10 AOP:** proceso de administración de la operación.
- 8.11 ASI:** proceso de administración de la seguridad de la Información.
- 8.12 Borrado Seguro:** el proceso mediante el cual se elimina de manera permanente y de forma irre recuperable la información contenida en medios de almacenamiento digital.
- 8.13 Cartera Ejecutiva de Proyectos de TIC:** Conjunto total de proyectos de TIC que la institución propondrá a la Unidad para su seguimiento.
- 8.14 Cartera Operativa de Proyectos de TIC:** Conjunto total de proyectos que soportan la operación diaria de la DTI y no son considerados como estratégicos.
- 8.15 Centro de Datos:** el lugar físico en los que se ubiquen los activos de TIC y desde el que se proveen servicios de TIC.
- 8.16 Cómputo en la Nube:** al modelo de prestación de servicios digitales que permite a las Instituciones acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios.
- 8.17 CMDB:** Base de Datos de la Gestión de la Configuración.
- 8.18 Dependencias:** las Secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como a la Oficina de la Presidencia de la República y la Procuraduría General de la República; así como los Órganos Reguladores Coordinados en Materia Energética.
- 8.19 Dominio Tecnológico:** las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo.
- 8.20 EDN:** la Estrategia Digital Nacional contenida en el Objetivo número 5 del Programa.
- 8.21 EIDA:** el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, establecido mediante Acuerdo publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 19 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		

- 8.22 Entidades:** los organismos descentralizados, empresas de participación estatal mayoritaria, instituciones nacionales de crédito, organizaciones auxiliares nacionales de crédito e instituciones nacionales de seguros y de fianzas, y fideicomisos públicos que en términos de la Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales, sean considerados entidades de la Administración Pública Federal Paraestatal.
- 8.23 ERISC:** equipo de respuesta a incidentes de seguridad en TIC en la Institución.
- 8.24 Estándar abierto:** a las especificaciones cuya utilización esté disponible de manera gratuita o que no suponga una dificultad de acceso, y que su uso y aplicación no esté condicionada al pago de un derecho de propiedad.
- 8.25 Herramienta de Gestión de la Política TIC:** sistema web usado para llevar a cabo la comunicación de actividades de reporte establecidas en el Acuerdo, considerando el reporte de PETIC, la obtención del dictamen técnico que emite la Unidad, autorización por parte de la UCP, la arquitectura empresarial, el MAAGTICSI, entre otros.
- 8.26 Infraestructuras Críticas de Información:** Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia.
- 8.27 Infraestructuras de Información esenciales:** Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de información, TIC y TO, cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación de las Instituciones.
- 8.28 Infraestructura de TIC:** el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC.
- 8.29 Infraestructura Pasiva:** elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de las dependencias o entidades, que sean necesarios para la instalación y operación de las redes, así como para la prestación de servicios de procesamiento de datos, de telecomunicaciones y radiodifusión.
- 8.30 Instancias de Seguridad Nacional:** las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquellas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional.
- 8.31 Institución:** las dependencias y entidades de la Administración Pública Federal, tal y como se definen en este Acuerdo.
- 8.32 Lineamientos:** los Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicados en el Diario Oficial de la Federación el 30 de enero de 2013.
- 8.33 MAAGMAASSP:** el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 20 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		

- 8.34 MAAGTICSI:** el Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información. Anexo Único del presente Acuerdo.
- 8.35 Niveles de servicio:** el establecimiento en un lenguaje no técnico del servicio brindado, incluyendo al menos la definición, disponibilidad, calidad, tiempos de respuesta y solución.
- 8.36 OPEC:** proceso de operación de los controles de seguridad de la información y del erisc.
- 8.37 PE:** proceso de planeación estratégica.
- 8.38 PETIC:** el conjunto de proyectos que elaboran las Instituciones, conformado por un máximo de 7 proyectos estratégicos, en los términos establecidos en el presente Acuerdo.
- 8.39 Portafolio de proyectos de TIC:** es el total de los proyectos de TIC agrupados según su clasificación en Cartera Ejecutiva de Proyectos de TIC y Cartera Operativa de Proyectos de TIC que la Institución planea desarrollar, en los términos establecidos por el MAAGTICSI.
- 8.40 Programa:** el Programa para un Gobierno Cercano y Moderno 2013-2018, aprobado mediante Decreto publicado en el Diario Oficial de la Federación el 30 de agosto de 2013.
- 8.41 Proyectos de TIC:** el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC y que cuenta con presupuesto para su ejecución; considerando 2 tipos: proyectos operativos que soportan las actividades diarias de la DTI y proyectos estratégicos en los términos señalados en el presente Acuerdo.
- 8.42 Retos Públicos:** el modelo que fomenta la democratización del gasto público y la innovación, invitando a los emprendedores del país a plantear soluciones a retos de gobierno mediante el desarrollo de aplicativos tecnológicos web y móviles.
- 8.43 SEGOB:** la Secretaría de Gobernación.
- 8.44 Seguridad de la información:** la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.
- 8.45 Seguridad Nacional:** las acciones a las que se refiere el artículo 3 de la Ley de Seguridad Nacional.
- 8.46 SFP:** la Secretaría de la Función Pública.
- 8.47 SHCP:** la Secretaría de Hacienda y Crédito Público.
- 8.48 Tecnologías Verdes:** el conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las tecnologías de la información y comunicaciones, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 21 de 21
	<b>3. Procedimiento para la Administración de Servicios.</b>		

**8.49 TIC:** las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

**8.50 Unidad:** la Unidad de Gobierno Digital de la SFP.

**8.51 DTIC:** la Dirección de Tecnologías de Información y Comunicaciones o área responsables de las TIC en la Institución.

## 9. CAMBIOS DE VERSIÓN DEL PROCEDIMIENTO

Numero de revisión	Fecha de actualización	Descripción del cambio
0	No Aplica	No aplica

## 10. ANEXOS DEL PROCEDIMIENTO

No aplica

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 1 de 11
	<b>4. Procedimiento para la Administración de la configuración.</b>		

## 1. PROPÓSITO

Establecer la funcionalidad del proceso de Administración de la Configuración, derivado del Manual Administrativo de Aplicación General en Materias de Tecnología de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), mediante la asignación de los roles identificados en el proceso y sus subprocesos, formalizando la asignación del rol a los responsables que participan en la ejecución de cada una de las tareas del proceso, con el fin de obtener la información, evidencias y entregables que generen las actividades ejecutadas durante el proceso.

## 2. ALCANCE

- 2.1 Obtener el mapa del proceso y de las actividades de los subprocesos involucrados, que permitan identificar la funcionalidad del proceso ACNF.
- 2.2 Identificar a las áreas o personas que se harán responsables de los diferentes roles que requiere el proceso.
- 2.3 Formalizar las asignaciones de responsables de roles y actividades.
- 2.4 Establecer si es necesario entre las áreas identificadas que participarán con alguna responsabilidad en el proceso un OLA, acuerdo de operación, en el cual se especifiquen los servicios que se aportarán y los tiempos en los que se atenderán y los entregables comprometidos que requiere el proceso.
- 2.5 Identificar las capacitaciones que se requieran en las diferentes áreas o personas que asuman el rol asignado, para que se consideren en un programa de capacitación.
- 2.6 Identificar los indicadores de desempeño del proceso y registrarlos periódicamente para su evaluación posterior.
- 2.7 Identificar los indicadores de los servicios considerados y sus métricas.

## 3. POLÍTICAS DE OPERACIÓN, NORMAS Y LINEAMIENTOS

- 3.1 El responsable de este proceso es responsable de la administración del repositorio de configuraciones.
- 3.2 El responsable de este proceso deberá mantener una verificación continua del repositorio de configuraciones a fin de constatar que éste se encuentre actualizado.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 2 de 11
	<b>4. Procedimiento para la Administración de la configuración.</b>		

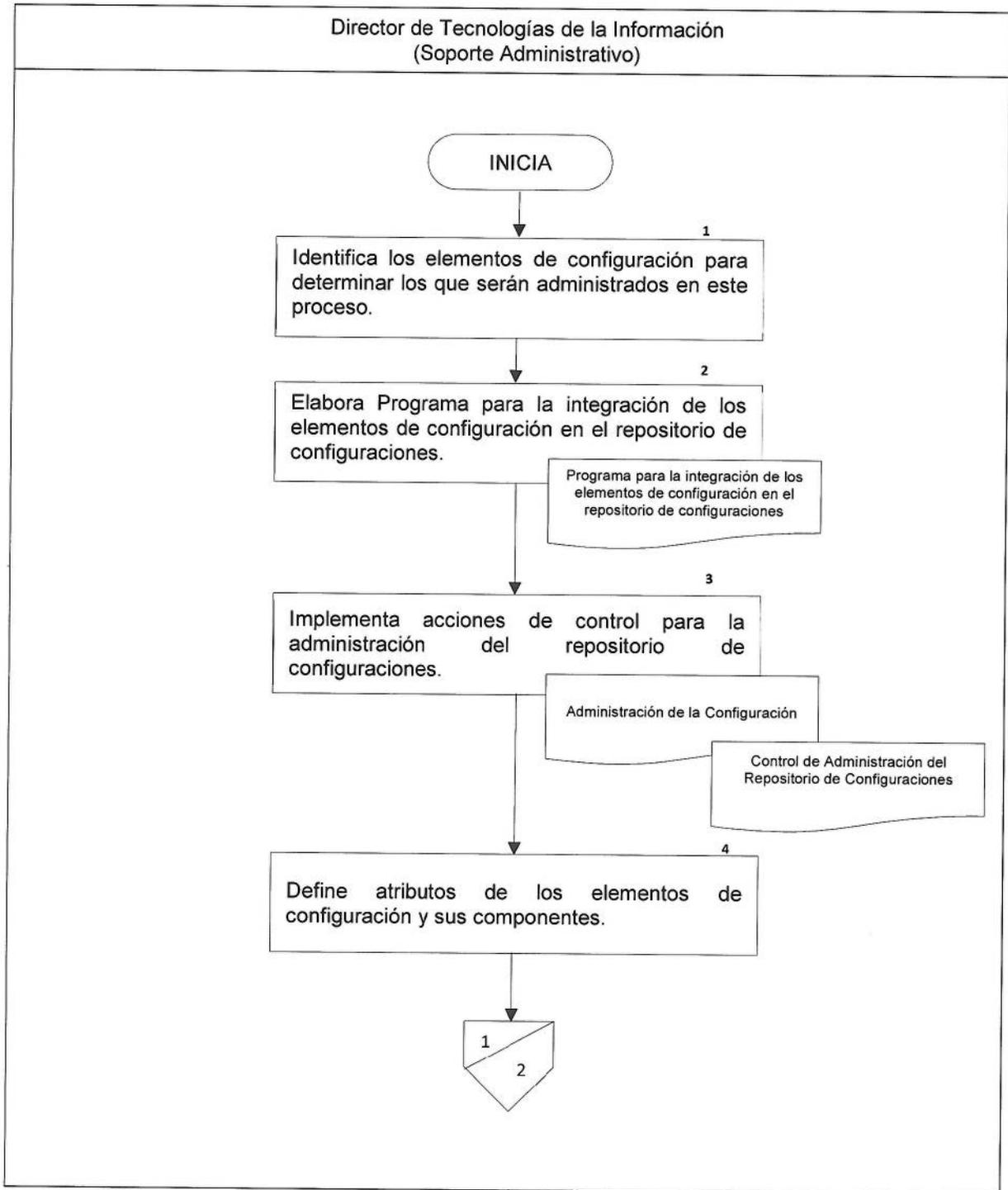
#### 4. DESCRIPCIÓN DEL PROCEDIMIENTO

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director de Tecnologías de la Información (Soporte Administrativo)	1	Identifica los elementos de configuración para determinar, de acuerdo a las necesidades y recursos con los que cuenta la DTI, los que serán administrados en este proceso.	
	2	Elabora Programa para la integración de los elementos de configuración en el repositorio de configuraciones	Programa para la integración de los elementos de configuración en el repositorio de configuraciones
	3	Implementa acciones de control para la administración del repositorio de configuraciones	Administración de la Configuración
	4	Define atributos de los elementos de configuración y sus componentes.	Control de Administración del Repositorio de Configuraciones
	5	Define atributos mínimos para conformar las líneas base de los elementos de configuración, así como los que no requieren.	
	6	Define nomenclatura de los elementos de configuración y sus componentes.	
	7	Identifica la relación funcional y de dependencia entre los elementos de configuración y sus componentes, así como su relación con elementos de otros procesos y sistemas.	
	8	Integra un catálogo que permita identificar los diferentes estados en que pueden encontrarse los elementos de configuración o sus componentes.	

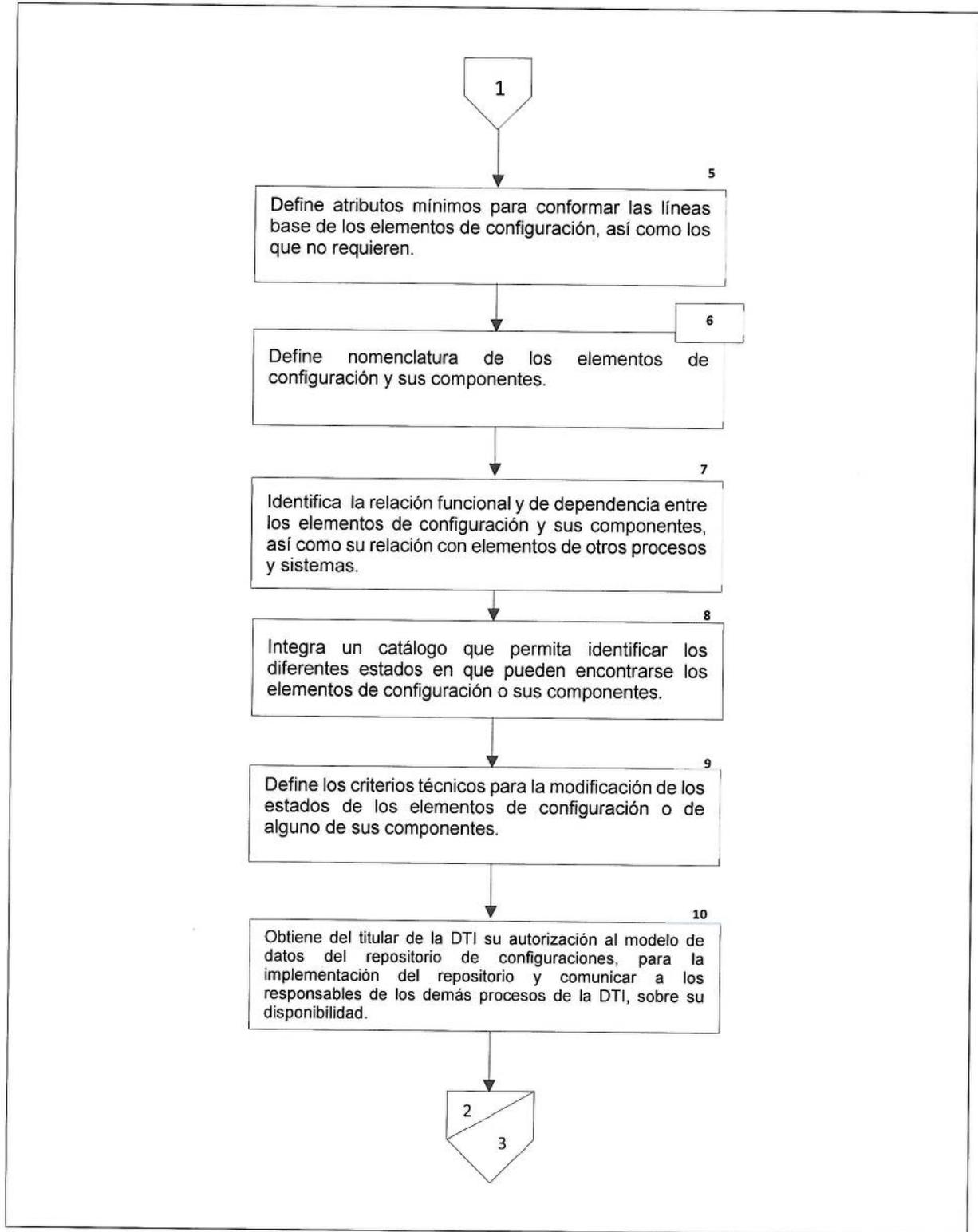
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 3 de 11
	<b>4. Procedimiento para la Administración de la configuración.</b>		

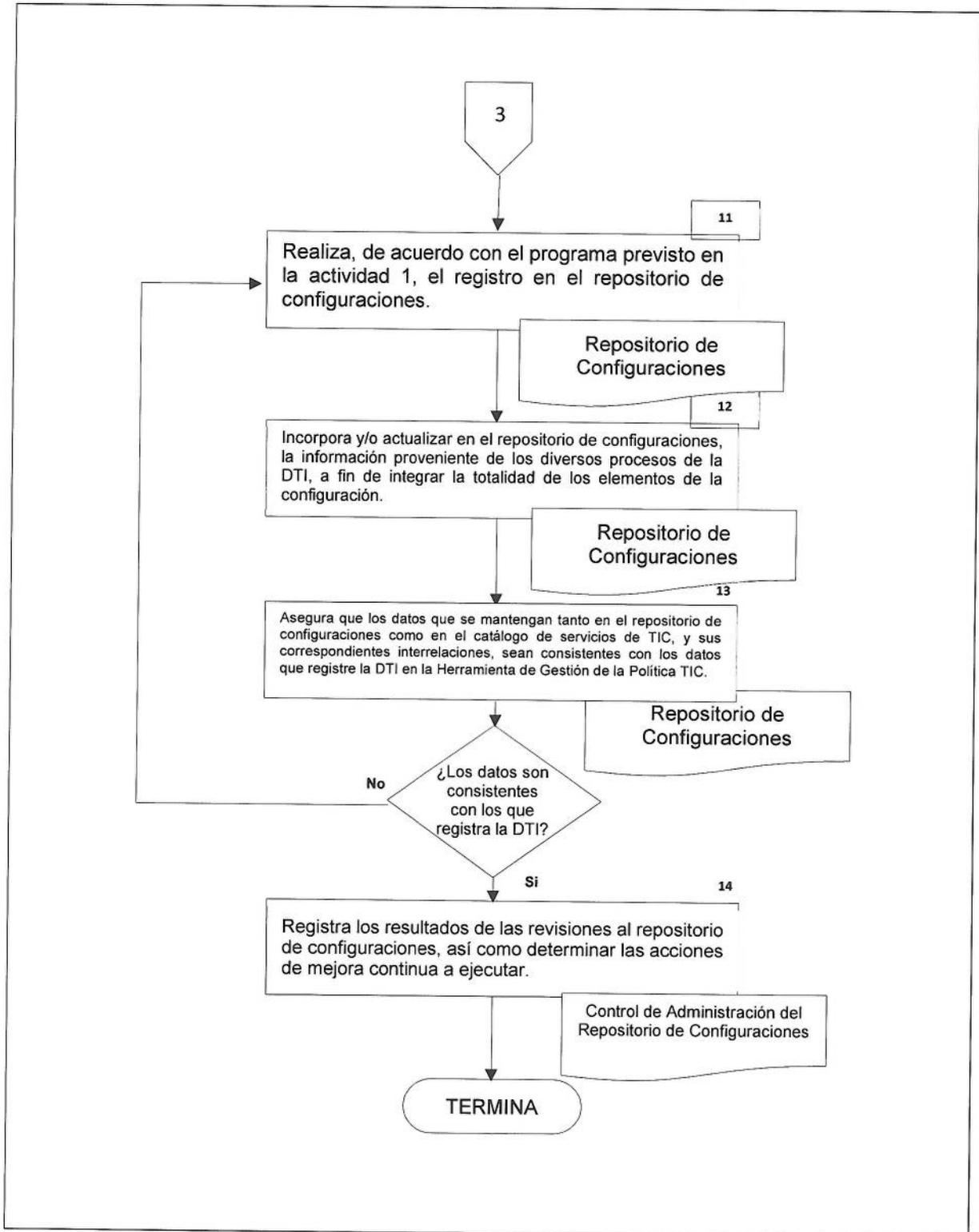
Responsable	No. Act.	Descripción de actividades	Documento o anexo
	9	Define los criterios técnicos para la modificación de los estados de los elementos de configuración o de alguno de sus componentes.	
Director de Tecnologías de la Información (Soporte Administrativo)	10	Obtiene del titular de la DTI su autorización al modelo de datos del repositorio de configuraciones, para la implementación del repositorio y comunicar a los responsables de los demás procesos de la DTI, sobre su disponibilidad.	
	11	Realiza, de acuerdo con el programa previsto en la actividad 1, el registro en el repositorio de configuraciones.	Repositorio de Configuraciones
	12	Incorpora y/o actualizar en el repositorio de configuraciones, la información proveniente de los diversos procesos de la DTI, a fin de integrar la totalidad de los elementos de la configuración.	Repositorio de Configuraciones
	13	Asegura que los datos que se mantengan tanto en el repositorio de configuraciones como en el catálogo de servicios de TIC, y sus correspondientes interrelaciones, sean consistentes con los datos que registre la DTI en la Herramienta de Gestión de la Política TIC.  ¿Los datos son consistentes con los que registra la DTI?  No: Continuar en actividad 11 Si: Continuar en actividad 14	Repositorio de Configuraciones
	14	Registra los resultados de las revisiones al repositorio de configuraciones, así como determinar las acciones de mejora continua a ejecutar  TERMINA	Control de Administración del Repositorio de Configuraciones

## 5. DIAGRAMA DE FLUJO



	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 5 de 11
<b>4. Procedimiento para la Administración de la configuración.</b>			





	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 7 de 11
	<b>4. Procedimiento para la Administración de la configuración.</b>		

## 6. DOCUMENTOS DE REFERENCIA

Nombre del documento	Código (cuando aplique)
6.1 Soluciones tecnológicas y sus componentes, así como la información funcional y técnica de los mismo y la relativa a diversos ambientes arquitectura tecnológica de DTI.	No aplica
6.2 Catálogo de servicios(ADS)	No aplica
6.3 Lineamientos para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión.	No aplica
6.4 Documento Técnico de Interoperabilidad de los Sistemas Automatizados de Control de Gestión (DTISACG).	No aplica
6.5 Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.	No aplica

## 7. REGISTROS

Registros	Tiempo de conservación	Responsable de conservarlo	Código de registro o identificación única
7.1 Programa para integración de los elementos de configuración en repositorio de configuraciones	6 meses	Responsable del proceso	No aplica
7.2 Control de Administración del Repositorio de Configuraciones	6 meses	Responsable del proceso	No aplica
7.3 Repositorio de Configuraciones	6 meses	Responsable del proceso	No aplica
7.4 Registro de resultados de los cambios realizados en el repositorio de configuraciones	6 meses	Responsable del proceso	No aplica

## 8. GLOSARIO DEL PROCEDIMIENTO

- 8.1 Activos de TIC.-** los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.
- 8.2 ACNF.-** proceso de administración de la configuración.
- 8.3 ADP.-** proceso de administración de proyectos.
- 8.4 ADS.-** proceso de administración de servicios.
- 8.5 APCT.-** proceso de administración del presupuesto y las contrataciones.
- 8.6 Aplicativo de Cómputo.-** el software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo a requerimientos previamente definidos.
- 8.7 APRO.-** proceso de administración de proveedores.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 8 de 11
	<b>4. Procedimiento para la Administración de la configuración.</b>		

- 8.8 Arquitectura Empresarial.-** la información del estado actual y futuro de una Institución, a partir del análisis con perspectiva estratégica; considerando modelos de negocio, procesos, aplicativos y tecnologías de la información y comunicaciones.
- 8.9 Arquitectura Orientada a Servicios.-** la metodología y marco de trabajo, para construir componentes de software reutilizables para la interoperabilidad de aplicativos de cómputo.
- 8.10 AOP.-** proceso de administración de la operación.
- 8.11 ASI.-** proceso de administración de la seguridad de la Información.
- 8.12 Borrado Seguro.-** el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital.
- 8.13 Cartera Ejecutiva de Proyectos de TIC.-** Conjunto total de proyectos de TIC que la institución propondrá a la Unidad para su seguimiento.
- 8.14 Cartera Operativa de Proyectos de TIC.-** Conjunto total de proyectos que soportan la operación diaria de la DTI y no son considerados como estratégicos.
- 8.15 Centro de Datos.-** el lugar físico en los que se ubiquen los activos de TIC y desde el que se proveen servicios de TIC.
- 8.16 Cómputo en la Nube.-** al modelo de prestación de servicios digitales que permite a las Instituciones acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios.
- 8.17 CMDB.-** Base de Datos de la Gestión de la Configuración.
- 8.18 Dependencias.-** las Secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como a la Oficina de la Presidencia de la República y la Procuraduría General de la República; así como los Órganos Reguladores Coordinados en Materia Energética.
- 8.19 Dominio Tecnológico.-** las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo.
- 8.20 EDN.-** la Estrategia Digital Nacional contenida en el Objetivo número 5 del Programa.
- 8.21 EIDA.-** el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, establecido mediante Acuerdo publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011.
- 8.22 Entidades.-** los organismos descentralizados, empresas de participación estatal mayoritaria, instituciones nacionales de crédito, organizaciones auxiliares nacionales de crédito e instituciones nacionales de seguros y de fianzas, y fideicomisos públicos que en términos de la Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales, sean considerados entidades de la Administración Pública Federal Paraestatal.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 9 de 11
	<b>4. Procedimiento para la Administración de la configuración.</b>		

**8.23 ERISC.-** equipo de respuesta a incidentes de seguridad en TIC en la Institución.

**8.24 Estándar abierto.-** a las especificaciones cuya utilización esté disponible de manera gratuita o que no suponga una dificultad de acceso, y que su uso y aplicación no esté condicionada al pago de un derecho de propiedad.

**8.25 Herramienta de Gestión de la Política TIC.-** sistema web usado para llevar a cabo la comunicación de actividades de reporte establecidas en el Acuerdo, considerando el reporte de PETIC, la obtención del dictamen técnico que emite la Unidad, autorización por parte de la UPCP, la arquitectura empresarial, el MAAGTICSI, entre otros.

**8.26 Infraestructuras Críticas de Información.-** Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia.

**8.27 Infraestructuras de Información esenciales.-** Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de información, TIC y TO, cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación de las Instituciones.

**8.28 Infraestructura de TIC.-** el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC.

**8.29 Infraestructura Pasiva.-** elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de las dependencias o entidades, que sean necesarios para la instalación y operación de las redes, así como para la prestación de servicios de procesamiento de datos, de telecomunicaciones y radiodifusión.

**8.30 Instancias de Seguridad Nacional.-** las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquellas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional.

**8.31 Institución.-** las dependencias y entidades de la Administración Pública Federal, tal y como se definen en este Acuerdo.

**8.32 Lineamientos.-** los Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicados en el Diario Oficial de la Federación el 30 de enero de 2013.

**8.33 MAAGMAASSP.-** el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público.

**8.34 MAAGTICSI.-** el Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información. Anexo Único del presente Acuerdo.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 10 de 11
	<b>4. Procedimiento para la Administración de la configuración.</b>		

- 8.35 Niveles de servicio.-** el establecimiento en un lenguaje no técnico del servicio brindado, incluyendo al menos la definición, disponibilidad, calidad, tiempos de respuesta y solución.
- 8.36 OPEC.-** proceso de operación de los controles de seguridad de la información y del erisc.
- 8.37 PE.-** proceso de planeación estratégica.
- 8.38 PETIC.-** el conjunto de proyectos que elaboran las Instituciones, conformado por un máximo de 7 proyectos estratégicos, en los términos establecidos en el presente Acuerdo.
- 8.39 Portafolio de proyectos de TIC.-** es el total de los proyectos de TIC agrupados según su clasificación en Cartera Ejecutiva de Proyectos de TIC y Cartera Operativa de Proyectos de TIC que la Institución planea desarrollar, en los términos establecidos por el MAAGTICSI.
- 8.40 Programa.-** el Programa para un Gobierno Cercano y Moderno 2013-2018, aprobado mediante Decreto publicado en el Diario Oficial de la Federación el 30 de agosto de 2013.
- 8.41 Proyectos de TIC.-** el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC y que cuenta con presupuesto para su ejecución; considerando 2 tipos: proyectos operativos que soportan las actividades diarias de la DTI y proyectos estratégicos en los términos señalados en el presente Acuerdo.
- 8.42 Retos Públicos.-** el modelo que fomenta la democratización del gasto público y la innovación, invitando a los emprendedores del país a plantear soluciones a retos de gobierno mediante el desarrollo de aplicativos tecnológicos web y móviles.
- 8.43 SEGOB:** la Secretaría de Gobernación.
- 8.44 Seguridad de la información.-** la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.
- 8.45 Seguridad Nacional.-** las acciones a las que se refiere el artículo 3 de la Ley de Seguridad Nacional.
- 8.46 SFP.-** la Secretaría de la Función Pública.
- 8.47 SHCP.-** la Secretaría de Hacienda y Crédito Público.
- 8.48 Tecnologías Verdes.-** el conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las tecnologías de la información y comunicaciones, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías.
- 8.49 TIC.-** las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.
- 8.50 Unidad.-** la Unidad de Gobierno Digital de la SFP.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 11 de 11
	<b>4. Procedimiento para la Administración de la configuración.</b>		

**8.51 DTIC.-** la Dirección de Tecnologías de Información y Comunicaciones o área responsables de las TIC en la Institución.

## 9. CAMBIOS DE VERSIÓN DEL PROCEDIMIENTO

Numero de revisión	Fecha de actualización	Descripción del cambio
0	No aplica	No aplica

## 10. ANEXOS DEL PROCEDIMIENTO

No aplica

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 1 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

## 1. PROPÓSITO

Establecer la funcionalidad del proceso de Administración de la Seguridad de la Información, derivado del Manual Administrativo de Aplicación General en Materias de Tecnología de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), mediante la asignación de los roles identificados en el proceso y sus subprocesos, formalizando la asignación del rol a los responsables que participan en la ejecución de cada una de las tareas del proceso, con el fin de obtener la información, evidencias y entregables que generen las actividades ejecutadas durante el proceso.

## 2. ALCANCE

- 2.1 Obtener el mapa del proceso y de las actividades de los subprocesos involucrados, que permitan identificar la funcionalidad del proceso ASI.
- 2.2 Identificar los roles o los actores que se requieren para que el proceso genere las evidencias y entregables que demuestren la funcionalidad del proceso.
- 2.3 Identificar a las áreas o personas que se harán responsables de los diferentes roles que requiere el proceso.
- 2.4 Formalizar las asignaciones de responsables de roles y actividades.
- 2.5 Establecer si es necesario entre las áreas identificadas que participarán con alguna responsabilidad en el proceso un OLA, acuerdo de operación, en el cual se especifiquen los servicios que se aportarán y los tiempos en los que se atenderán y los entregables comprometidos que requiere el proceso.
- 2.6 Identificar las capacitaciones que se requieran en las diferentes áreas o personas que asuman el rol asignado, para que se consideren en un programa de capacitación.
- 2.7 Identificar los indicadores de desempeño del proceso y registrarlos periódicamente para su evaluación posterior.
- 2.8 Identificar los indicadores de los servicios considerados y sus métricas.

## 3. POLÍTICAS DE OPERACIÓN, NORMAS Y LINEAMIENTOS

- 3.1 El responsable de la seguridad de la información en la Institución está a cargo de este proceso y en su caso, podrá auxiliarse de los servidores públicos que considere necesarios, debiendo para ello notificar por escrito a cada uno para que conozcan los roles que desempeñarán, actividades y responsabilidades.
- 3.2 En el caso en que el Director General tenga un nivel jerárquico equivalente o inferior a director general, el servidor público que designe como responsable de la seguridad de la información en la Institución deberá tener un nivel inmediato inferior a éste.
- 3.3 El responsable de este proceso se deberá asegurar que las acciones y productos que sean resultado de su ejecución, sean consecuentes con lo previsto en el Acuerdo por el que se emiten las Disposiciones en Materia de Control Interno y se expide el Manual Administrativo de Aplicación

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 2 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

General en Materia de Control Interno, en lo relativo a la administración de riesgos y seguridad de la información, y de que los mismos se comuniquen al coordinador de control interno de la Institución que se designe conforme a lo establecido en dicho ordenamiento.

- 3.4 En caso de que la Institución cuente con infraestructuras críticas de información, el responsable de la seguridad de la información se asegurará de que el análisis de riesgos previsto en este proceso se enfoque a éstas; y en caso de que no se cuente con dichas infraestructuras, que el análisis se oriente a los activos de información clave de la Institución.
- 3.5 El responsable de este proceso deberá establecer el equipo de respuesta a incidentes de seguridad de TIC (ERISC) y definir los roles y responsabilidades de sus integrantes, así como asegurarse de que éstos conozcan las reglas de operación del mismo y la guía técnica de atención a incidentes.
- 3.6 El responsable de la seguridad de la información de la Institución será quien mantendrá comunicación con el Centro para la atención de cualquier incidente de seguridad de la información que implique una amenaza a la Seguridad Nacional y designará un enlace para que se coordine con los ERISC de las demás Instituciones en la atención de otros incidentes que así lo requieran.
- 3.7 El responsable de la seguridad de la información de las Instituciones que tengan el carácter de instancia de Seguridad Nacional, deberá coordinarse con las diversas instancias de Seguridad Nacional involucradas cuando se presente un incidente de seguridad que supere su capacidad de respuesta.
- 3.8 El grupo estratégico de seguridad de la información deberá asegurar que se integre al SGSI un control de seguridad para evitar intrusiones a la infraestructura de TIC, incluyendo ataques externos vía Internet, Intranet o Extranet.
- 3.9 El grupo estratégico de seguridad de la información deberá asegurarse de que se integren al SGSI, controles de seguridad en los equipos del ambiente operativo y de comunicaciones de la Institución, para efectuar la revisión a las bitácoras internas de los mismos, con la finalidad de identificar intentos de ataques o de explotación de vulnerabilidades.
- 3.10 El responsable de este proceso deberá hacer del conocimiento de las autoridades competentes, los intentos de violación a los controles de seguridad y los incidentes de seguridad, incluido el acceso no autorizado a la infraestructura y servicios de TIC y a la información contenida en éstos, para que se determinen, en su caso, las responsabilidades que correspondan conforme a las disposiciones jurídicas aplicables.
- 3.11 El grupo estratégico de seguridad de la información deberá constatar que los controles de seguridad que se hayan establecido para el repositorio de configuraciones, se implementen de igual manera, para activos y elementos de configuración de los ambientes de desarrollo, pruebas y preproducción.
- 3.12 El grupo estratégico de seguridad de la información deberá coordinarse con los responsables de los procesos de la DTI, para que se implementen controles de seguridad que impidan que el código de las soluciones tecnológicas, sus componentes y productos, y demás elementos relacionados, se copien, envíen, transmitan o difundan por cualquier medio, con fines distintos a su desarrollo.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 3 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

- 3.13 El grupo estratégico de seguridad de la información deberá coordinarse con los responsables de los procesos de la DTI, para que se implementen controles de seguridad orientados a que las herramientas para el desarrollo de las soluciones tecnológicas, sus componentes y productos, únicamente estén disponibles para los involucrados en su desarrollo y a la conclusión de éste, tales herramientas sean borradas de modo seguro de cualquier equipo del ambiente de trabajo.
- 3.14 El grupo estratégico de seguridad de la información deberá constatar que, como parte de los mecanismos que se establezcan para el ambiente operativo, se implemente un control para la elaboración y conservación de bitácoras de seguridad para los sistemas identificados como parte de una infraestructura de información esencial y/o crítica. En estas bitácoras se registrará el usuario, nombre de equipo, dirección IP, hora de entrada y salida del sistema, así como el tipo de consulta o cambios realizados en la configuración de las aplicaciones. Estas bitácoras tendrán un tiempo mínimo de almacenamiento de un año.
- 3.15 El grupo estratégico de seguridad de la información de Instituciones que tengan el carácter de instancia de Seguridad Nacional, deberá recomendar que en los procedimientos de contratación de soluciones tecnológicas o servicios de TIC prevista, se incluyan los requerimientos de continuidad de la operación, niveles de servicio y tiempos de respuesta a interrupciones, en concordancia con la criticidad de los procesos institucionales que los bienes o servicios objeto de las contrataciones soportarán.
- 3.16 El grupo estratégico de seguridad de la información deberá implementar mecanismos para asegurar que los sistemas y aplicativos para desplegar los servicios de TIC que se desarrollen o adquieran, cumplan con los controles previstos en el Proceso de Administración de la Seguridad de la Información (ASI).
- 3.17 El responsable de este proceso deberá coordinarse con los responsables de la administración de los servicios de TIC y con aquellos responsables de la operación de los mismos, a fin de que los acuerdos de nivel de servicio SLA y los acuerdos de nivel operacional OLA sean determinados y considerados en función de los programas de continuidad y de contingencia de la DTI y del proceso.
- 3.18 El responsable de este proceso deberá enviar a la Unidad un informe semestral, en los meses de julio del año al que corresponda y en enero del año siguiente. El informe deberá ser elaborado por el responsable del ERISC-OPEC, y contendrá el Proceso ASI con el estado que guarda su cumplimiento y la información relativa a la operación de los controles de seguridad mínimos (establecidos en la actividad ASI 6), así como de aquellos derivados del análisis de riesgos.
- 3.19 El responsable de la seguridad de la información de la Institución, podrá considerar a los equipos y/o activos de información, de propósito específico, de control, de monitoreo o industriales, como un dominio tecnológico de TO y de esta manera integrar sus controles de seguridad al SGSI.
- 3.20 Los servidores públicos de la DTI y los usuarios están obligados a operar en un ambiente de trabajo que garantice la confidencialidad, integridad y disponibilidad de la información, de acuerdo a lo previsto en el presente manual.
- 3.21 El responsable de este proceso deberá efectuar las actualizaciones que deriven de la ejecución de los factores críticos de las actividades del presente proceso.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		Hoja: 4 de 74

#### 4. DESCRIPCIÓN DEL PROCEDIMIENTO

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director General	1	Designa al responsable de la seguridad de la información en la Institución, quien deberá tener nivel jerárquico mínimo de director general o equivalente.	
Director General Adjunto de Administración y Finanzas	2	Informa al Centro sobre su designación y de la del enlace responsable de mantener comunicación con los ERISC de otras Instituciones.	Documento de Integración y operación del grupo estratégico e seguridad de la información
	3	Establece el grupo estratégico de seguridad de la información (GESI), que estará integrado por servidores públicos que conozcan los procesos institucionales y que cuenten con conocimientos en materia de seguridad de la información, mediante el documento de integración y operación del grupo estratégico de seguridad de la información.	
	4	Dirige y coordina al grupo estratégico de seguridad de la información y da seguimiento a las acciones establecidas por el mismo.	
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI)	5	Coordina la elaboración y actualización del catálogo de infraestructuras de información esencial y, en su caso, críticas.	Catálogo de infraestructuras críticas
	6	Establece, conjuntamente con los responsables de los procesos de la DTI, así como en su caso con los servidores públicos que corresponda, los mecanismos para garantizar la protección de las infraestructuras de información esenciales y/o críticas que éstos tengan bajo su responsabilidad.	
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director	7	Vigila que los controles de seguridad de la información que se definan e implementen, consideren los mecanismos establecidos en el punto	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 5 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			

Responsable	No. Act.	Descripción de actividades	Documento o anexo
de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI)		anterior, así como el análisis de riesgos que se indica a partir de la actividad 62.	
	8	Constata que se efectúe la implementación del SGSI en la Institución y que se lleven a cabo revisiones al mismo en periodos no mayores a un año, a fin de verificar su cumplimiento.	
	9	Da seguimiento a las acciones de mejora continua derivadas de las revisiones al SGSI.	
	10	Realiza un diagnóstico de los requerimientos de seguridad de la información de la Institución, considerando la participación de las unidades administrativas usuarias de la información, para establecer adecuadamente el alcance del SGSI.	
	11	Define el alcance del SGSI, de manera tal que establezca límites de protección desde la perspectiva institucional, para proporcionar la seguridad requerida a los activos de información.	
	12	Genera las estrategias específicas de seguridad de la información, que permitan cumplir con la misión, visión y objetivos de la Institución.	
	13	Desarrolla reglas técnicas para verificar que los controles de seguridad de la información que se definan operen según lo esperado.	
	14	Define métricas para evaluar el grado de cumplimiento de los requerimientos de seguridad identificados para los activos de información.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 6 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI)	15	Elabora las reglas técnicas que contengan las acciones para la adecuada operación del SGSI.	Documento de definición del SGSI
	16	Diseña en coordinación con las diferentes áreas administrativas de la Institución, la estrategia de seguridad de la información que será implementada al interior de la misma, así como efectuar su revisión al menos una vez al año. Dicha estrategia será la base para establecer el SGSI.	
	17	Integra el documento de definición del SGSI e incluir en éste el programa de implementación del SGSI que se desarrolle.	
Director General Adjunto de Administración y Finanzas	18	Hace del conocimiento al Director General el documento de definición del SGSI, que ya incluya el programa de implementación desarrollado.	Documento de definición del SGSI
	19	Asegura que se presente a la unidad administrativa responsable de la capacitación en la Institución, una propuesta para que se integren al programa de capacitación institucional, los cursos necesarios para difundir los conceptos e importancia de la seguridad de la información, así como la estructura y alcances del SGSI.	Propuesta capacitación conceptos e importancia de la seguridad de la información
	20	Da a conocer el SGSI, y su programa de implementación, a los servidores públicos de la Institución involucrados con el mismo.	
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de	21	Elabora un programa de evaluaciones del SGSI, integrarlo al documento de definición del SGSI y difundirlo en la Institución.	Documento de definición del SGSI

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 7 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Comercialización (Grupo Estratégico de Seguridad de la información - GESI)			
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI)	22	Elabora, prueba y mantiene actualizada una directriz rectora de respuesta a incidentes, la cual deberá contener al menos: a) El rol y el servidor público asignado a éste, quien puede iniciar las tareas de respuesta a incidentes. b) El mecanismo de notificación, escalamiento y atención de incidentes en la Institución. c) Los mecanismos de interacción con otras Instituciones u organizaciones externas. d) Los criterios técnicos de obtención de indicios, preservación de evidencias, e investigación de incidentes, considerando lo establecido en las disposiciones jurídicas aplicables.	Documento de resultados de análisis de riesgos
	23	Con apoyo de las unidades administrativas, ejecuta los programas de implementación para el manejo de riesgos y de implementación del SGSI, de acuerdo a lo que se establece en el documento de definición del SGSI.	
	24	Da seguimiento a la ejecución del programa de implementación del SGSI y actualizar el avance del mismo.	Documento de definición del SGSI
	25	Elabora un informe de resultados de la implementación del SGSI e integrarlo al documento de definición del SGSI.	Documento de definición del SGSI
	26	Asegura que los controles de seguridad se hayan implementado de acuerdo a lo previsto en el documento de definición del SGSI y su programa de implementación del SGSI.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 8 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
	27	Elabora un programa de evaluaciones del SGSI, integrarlo al documento de definición del SGSI y difunde en la Institución.	Documento de definición del SGSI
Director General Adjunto de Administración y Finanzas	28	Hace del conocimiento del órgano interno de control en la Institución y/o, cuando corresponda, de las autoridades que resulten competentes, el incumplimiento al SGSI a efecto de que se determinen, en su caso, las responsabilidades que procedan en términos de los ordenamientos legales aplicables.	
Departamento de Informática (Soporte Administrativo)	29	Obtiene los datos necesarios para verificar la eficiencia y eficacia de los controles implementados, de acuerdo al programa de evaluaciones del SGSI recibido del grupo estratégico de seguridad de la información.	Documento de definición del SGSI  Intentos de violaciones e incidentes de seguridad  Documento de definición del SGSI
	30	Mide la efectividad de los controles de seguridad implementados.	
	31	Efectúa, con base en el programa de evaluaciones del SGSI, la evaluación del SGSI.	
	32	Registra la información de los intentos de violaciones e incidentes de seguridad, hayan sido exitosos o no, así como efectuar el análisis y evaluación de dicha información.	
	33	Documenta las acciones de revisión del SGSI que hayan resultado, mediante la elaboración de un informe de revisión del SGSI, integrarlo al documento de definición del SGSI y enviarlo al grupo estratégico de seguridad de la información.	
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director	34	Designa su equipo de trabajo, para conformar el catálogo de infraestructuras de información esenciales y, en su caso, críticas, el	Acta de integración del Equipo de trabajo para la identificación de infraestructuras de

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 9 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI)		responsable del equipo deberá ser funcionario público con nivel mínimo de Director General Adjunto u homólogo con conocimientos en seguridad de la información y análisis de riesgos.	información esenciales y/o críticas (ETIIIEC)
DTI Soporte Administrativo, DGAC Soporte Administrativo, DGACAC Soportes Administrativos, Control de Calidad de Materias Primas y Envases (Equipo de trabajo para la identificación de infraestructuras de información esenciales y/o críticas -ETIIIEC)	35	Analiza los procesos existentes y determinar cuáles de éstos son críticos y enlistarlos, considerando como tales aquellos de los que depende la Institución para alcanzar sus objetivos, en los niveles de servicio que tenga establecidos, derivado de sus atribuciones. Dicho análisis se realizará considerando al menos los siguientes elementos: i) Proveedores del proceso. ii) Insumos del proceso. iii) Eventos de inicio que disparan la ejecución del proceso. iv) Subprocesos o actividades que lo conforman. v) Actores que intervienen en su ejecución. vi) Productos o servicios que genera. vii) Evento de fin del proceso. viii) Clientes o usuarios del proceso. ix) Activos de información involucrados en el proceso.	
	36	Analiza los diagramas de los procesos, a fin de identificar las interdependencias que existan entre éstos, así como con otros fuera de la Institución.	
	37	Enlista y describe las actividades de cada proceso crítico, así como los factores de éxito para que el proceso se lleve a cabo de manera adecuada	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 10 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
	38	Identifica y enlista las actividades que resultan críticas para la operación del proceso.	
	39	Identifica, a partir de los procesos críticos identificados y enlistados en el factor crítico anterior, aquellos que se encuentren vinculados con la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a lo que señalan los artículos 3 y 5 de la Ley de Seguridad Nacional.	
DTI Soporte Administrativo, DGAC Soporte Administrativo, DGACAC Soportes Administrativos, Control de Calidad de Materias Primas y Envases (Equipo de trabajo para la identificación de infraestructuras de información esenciales y/o críticas -ETIIIEC)		¿Se identifican procesos críticos que se encuentren vinculados a la Ley de Seguridad Nacional?  No: Continuar en actividad 40 Si: Continuar en actividad 41	
	40	Adapta y aplica los puntos del 41 al 54 con perspectiva a nivel Entidad.	
	41	Identifica los activos de información involucrados en los procesos de Seguridad Nacional.	
	42	Efectúa valoración de activos de información, en términos de la posible pérdida de su confidencialidad, integridad o disponibilidad, para identificar aquellos que deban considerarse como activos de información clave y registrar los resultados.	
	43	Utiliza como parámetros para identificar la criticidad de una infraestructura, los tipos de impacto que podrían ocurrir ante la presentación de un incidente.	
	44	Determina el nivel de criticidad de cada infraestructura mediante la identificación de su interdependencia y el nivel de impacto que tenga con cada una de las infraestructuras con las que se relacione.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 11 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
	45	Revisa los resultados obtenidos.	
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI)	46	Verifica los resultados obtenidos por el equipo de trabajo y constatar que las infraestructuras de información esenciales y/o críticas que hubieren identificado, efectivamente tengan ese carácter.	
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI) con apoyo del Equipo de trabajo para la identificación de infraestructuras de información esenciales y/o críticas (ETIIIEC).	47	Elabora el catálogo de infraestructuras de información esenciales y/o críticas, con base en la información verificada en el paso anterior.	Catálogo de infraestructuras críticas
	48	Asigna el sector y subsector que corresponda cada infraestructura identificada.	
	49	Verifica que el catálogo de infraestructuras de información esenciales y/o críticas incorpore los datos de identificación, señalando su descripción, componentes, sector y subsector, Institución y ubicación y las matrices de la infraestructura con respecto de sus activos clave, y los impactos que le fueron determinados.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 12 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			

Responsable	No. Act.	Descripción de actividades	Documento o anexo
	50	Incluye en el catálogo de infraestructuras de información esencial y/o crítica en un mapa de localización geográfica, en donde se muestre su ubicación.	Catálogo de infraestructuras críticas
	51	Incluye en el catálogo de infraestructuras de información esenciales y/o críticas, la información de los miembros y roles del equipo de trabajo para la identificación de infraestructuras de información esenciales y/o críticas (ETIIIEC).	
Director General Adjunto de Administración y Finanzas	52	Presenta a la aprobación del Director General, el catálogo de infraestructuras de información esencial y/o crítica elaborado.	Catálogo de infraestructuras críticas
	53	Asegura de que se observe lo establecido en la Ley de Seguridad Nacional, en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su Reglamento y demás disposiciones aplicables, para la clasificación y resguardo de la información generada.	
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI)	54	Revisa, por lo menos una vez al año, el catálogo de infraestructuras de información esenciales y/o críticas de la institución, y el equipo efectúe las acciones para su actualización.	Catálogo de infraestructuras críticas
	55	Define estrategias, metodologías y herramientas que se usarán para administrar los riesgos.	
	56	Integra el marco normativo que resulte aplicable a los riesgos identificados.	
	57	Establece de las reglas para medir la efectividad de los controles en la gestión de los riesgos.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 13 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
	58	Define la forma y periodicidad con las que se informará a los grupos y equipos de trabajo, a las áreas y unidades administrativas de la Institución y externos involucrados, sobre los riesgos a los que se encuentran expuestos los procesos y servicios que utilizan.	
	59	Define de consideraciones sobre riesgos de TIC y seguridad a la información que coadyuven en la toma de decisiones estratégicas de la Institución.	
	60	Somete a consideración y aprobación del Director General Adjunto de Administración y Finanzas, las definiciones efectuadas en los pasos anteriores. ¿Se aprueban las definiciones?  No: Continuar en actividad 55 Si: Continuar en actividad 61	
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI)	61	Establece la directriz de administración de riesgos con las actividades anteriores.	Acta de Integración del Equipo de Trabajo para realizar análisis de riesgos. (ETRAR)
	62	Integra a su equipo de trabajo de análisis de riesgos, el cual deberá: a) Tener un responsable, quien deberá ser un funcionario público de nivel mínimo de Director General Adjunto u homólogo con conocimientos necesarios de seguridad de la información y análisis de riesgos. b) La conformación del equipo se hará con servidores públicos que, preferentemente, deberán tener conocimientos en TIC, seguridad de la información y seguridad física; así como por aquellos que se considere puedan aportar mayor capacidad de análisis y alcance de objetivos. c) Que los integrantes del equipo cuenten con al menos un año de experiencia y conocimientos en el área en la cual se desempeñan.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 14 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
		<p>d) Se delimite el objetivo y alcance del análisis de riesgos que se efectuará por el equipo de trabajo.</p> <p>e) Se seleccione al líder del equipo y se haga de su conocimiento que su rol será el de interpretar y difundir instrucciones, coordinar tareas y materializar resultados.</p> <p>f) Integrar, en caso de ser necesario, más de un equipo de trabajo de análisis de riesgos, para efectuar el adecuado acopio de información e integración que deriva del análisis de riesgos que se efectúa en esta actividad.</p>	
DTI Soporte Administrativo, DGAC Soporte Administrativo, DGACAC Soportes Administrativos, Control de Calidad de Materias Primas y Envases, con apoyo de las diversas unidades administrativas de la Institución. (Equipo de trabajo para realizar análisis de riesgos - ETRAR)	63	Identifica los procesos críticos, recopilando la información siguiente: a) La de aquellos procesos de los que la Institución dependa para alcanzar sus objetivos y niveles de servicio comprometidos, derivada de la identificación realizada conforme la actividad 35, en los casos en que la Institución no hubiere identificado procesos críticos vinculados con la Seguridad Nacional. b) La obtenida como resultado del desarrollo de la actividad 35, por haberse identificado procesos críticos vinculados con la Seguridad Nacional.	Relación de elementos que se pretenden proteger
	64	Identifica los activos de información y consultar a los responsables de éstos, para identificar y elaborar una relación de los elementos que se pretenden proteger ante la posible materialización de amenazas.	
	65	Integra, a la relación de activos de información, las características de los mismos que pudieran ser aprovechadas para poner en riesgo la confidencialidad, integridad y disponibilidad de éstos, considerando, asimismo, las características del ambiente y de la Institución en que se ubican. Considerar como	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 15 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
		vulnerabilidad la ausencia y/o falla de controles.	
	66	Integra a los responsables de la administración, operación y, en su caso, resguardo de los activos de información en el proceso de identificación de vulnerabilidades.	
	67	Registra las posibles amenazas, que en caso de materializarse, tendrían efectos negativos sobre la seguridad en uno o varios de los activos de información.	Documento de resultados de análisis de riesgos
	68	Identifica y registra los agentes que podrían materializar una amenaza.	Documento de resultados de análisis de riesgos
DTI Soporte Administrativo, DGAC Soporte Administrativo, DGACAC Soportes Administrativos, Control de Calidad de Materias Primas y Envases, con apoyo de las diversas unidades administrativas de la Institución. (Equipo de trabajo para realizar análisis de riesgos - ETRAR)	69	Define los escenarios de riesgo, para lo cual es necesario efectuar los cálculos para establecer el valor del riesgo para cada escenario, utilizando la fórmula: $R=PI$ ; en la que "P" es la probabilidad de ocurrencia de la amenaza, e "I" es el impacto ocasionado por la materialización de la misma.	
	70	Establece las variables complementarias que se indican en el formato del producto "Documento de resultados del análisis de riesgos", ya que éstas determinan el valor final del riesgo, utilizando la tabla denominada "Probabilidad de ocurrencia contra impacto".	Documento de resultados del análisis de riesgos
	71	Integra en el "Documento de resultados del análisis de riesgos", el resultado de la identificación y evaluación de los escenarios de riesgo.	Documento de resultados de análisis de riesgos
	72	Define la estrategia de seguridad para cada riesgo, seleccionando alguna de las establecidas: evitar, mitigar o reducir, financiar o asumir y transferir o compartir, debiendo evaluarse en este mismo orden.	Documento de resultados del análisis de riesgos

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		Hoja: 16 de 74

Responsable	No. Act.	Descripción de actividades	Documento o anexo
	73	Obtiene la relación de riesgos que requieren atención, su prioridad y estrategia de seguridad.	
	74	Elabora la lista de escenarios de riesgo, cuya acción de seguridad implica el uso de controles o la modificación de un proceso para evitar, mitigar o reducir, financiar o asumir y transferir o compartir los riesgos.	
	75	Compara el costo del control que se proponga contra el impacto que se podría ocasionar por la materialización del riesgo.	
DTI Soporte Administrativo, DGAC Soporte Administrativo, DGACAC Soportes Administrativos, Control de Calidad de Materias Primas y Envases, con apoyo de las diversas unidades administrativas de la Institución. (Equipo de trabajo para realizar análisis de riesgos - ETRAR)	76	Verifica el costo-beneficio de controles de seguridad, debiendo definir los valores indicados en éste, para cada escenario de riesgo.	
	77	Elabora el análisis del costo-beneficio de controles de seguridad e integrar los datos en el "Documento de resultados del análisis de riesgos".	Documento de resultados de análisis de riesgos
	78	Integra la lista de controles recomendados, para un adecuado tratamiento de los riesgos detectados en el orden de prioridad establecido, indicando además los requerimientos para su implementación.	Documento de resultados de análisis de riesgos
	79	Incluye, de ser el caso, el nivel de riesgo residual de cada escenario.	Documento de resultados de análisis de riesgos
	80	Elabora e integra las declaraciones de aplicabilidad con los controles necesarios, de acuerdo a los resultados obtenidos.	Documento de resultados de análisis de riesgos
	81	Elabora e incluye las propuestas para los programas de mitigación de riesgos, considerando los controles establecidos en las declaraciones de aplicabilidad.	Documento de resultados de análisis de riesgos

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		Hoja: 17 de 74

Responsable	No. Act.	Descripción de actividades	Documento o anexo
	82	Elabora e incluye un programa de contingencia a los riesgos, considerando, de ser el caso, la intervención del ERISC.	Documento de resultados de análisis de riesgos
	83	Obtiene del grupo estratégico de seguridad de la información, la aprobación del "Documento de resultados del análisis de riesgos"	Documento de resultados de análisis de riesgos
		¿Se aprueba el documento?  No: Continuar en actividad 55 Si: Continuar en actividad 84	
	84	Envía a los responsables de los procesos en las diversas áreas y unidades administrativas de la Institución para su revisión.	Documento de resultados de análisis de riesgos
DTI Soporte Administrativo, DGAC Soporte Administrativo, DGACAC Soportes Administrativos, Control de Calidad de Materias Primas y Envases, con apoyo de las diversas unidades administrativas de la Institución. (Equipo de trabajo para realizar análisis de riesgos - ETRAR)	85	Selecciona de entre los controles recomendados por el grupo estratégico de seguridad de la información, contenidos en el "Documento de resultados del análisis de riesgos", aquéllos a implementar de acuerdo a las capacidades y recursos de las áreas y unidades administrativas involucradas.	
	86	Justifica ante el grupo estratégico de seguridad de la información las razones por las cuales existan controles recomendados no seleccionados.	
	87	Elabora e integra en el "Documento de resultados del análisis de riesgos", el programa de implementación para el manejo de riesgos, de acuerdo a los resultados de la selección efectuada en la actividad 85.	Documento de resultados de análisis de riesgos
	88	Incluye la asignación de responsables de la implementación de cada control, integrando éstas al "Documento de resultados del análisis de riesgos" y los datos necesarios para su	Documento de resultados de análisis de riesgos

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 18 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
		implementación, así como documentarse conjuntamente con la implementación de las acciones y controles del SGSI.	
	89	En el programa de implementación para el manejo de riesgos se establece un responsable de la implementación de cada uno de los riesgos a manejar.	
	90	Obtiene del grupo estratégico de seguridad de la información la aprobación del programa de implementación elaborado.  ¿Se aprueba el programa?  No: Continuar en actividad 87 Si: Continuar en actividad 91	
	91	Verifica su adecuada integración con las demás actividades de implementación o mejora de los controles de seguridad y las acciones del SGSI.	
		¿El programa está integrado con las demás actividades de implementación, mejora de los controles de seguridad y acciones del SGSI? No: Continuar en actividad 87 Si: Continuar en actividad 92	
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo	92	Cuida que el análisis de riesgos se realice o actualice conforme a las actividades anteriores, al menos una vez al año, o bien, en caso de un cambio en los procesos, activos de información o cuando se detecte una nueva amenaza o vulnerabilidad a la seguridad de la información y/o los activos de TIC que la soportan.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		Hoja: 19 de 74

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Estratégico de Seguridad de la información - GESI)	93	Asegura que se obtengan los productos de este proceso debidamente actualizados.	Documento de definición del SGSI
	94	Asegura que se documente la mejora continua que resulte necesaria, derivada de la actividad 92.	
	95	Integra al SGSI los controles mínimos de seguridad de la información.	
	96	Asegura que los servidores y estaciones de trabajo, cuenten con software actualizado para detección y protección contra programas para vulnerar la seguridad de los dispositivos de TIC y TO, así como su información y los servicios que proveen. El software debe emitir reportes sobre el estado de actualización de los componentes sobre los que tienen cobertura.	
	97	Designa personal en las áreas relacionadas con el manejo, administración y gestión de los activos de información de la Institución, con apego a las disposiciones jurídicas aplicables y considerando los procedimientos que, en su caso, se tengan implementados en el área o unidad administrativa de que se trate.	
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI)	98	Instala en los equipos de cómputo de los usuarios, incluyendo los móviles que se conecten a la red de datos, las herramientas antivirus y aquellas necesarias para prevenir ataques por la vulnerabilidad que el uso de estos equipos conlleva.	
	99	Asegura el borrado seguro de dispositivos de almacenamiento que por algún motivo necesiten ser reparados, reemplazados o asignados a otro usuario; y mantiene evidencia auditable del proceso.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 20 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
	100	Garantiza la asignación, revocación, supresión o modificación de los privilegios de acceso a la información otorgados a servidores públicos de la Institución y de otras Instituciones, así como al personal de los proveedores de servicios u otros usuarios, al inicio o término de su empleo, cargo o comisión, relación contractual o de cualquier otra naturaleza, o bien, cuando por algún motivo el nivel de privilegios de acceso asignado cambie.	
	101	Instala mecanismos de cifrado de datos en los dispositivos electrónicos móviles que contengan información considerada como reservada o sensible para la Institución.	
	102	Cuenta con registros de auditoría y bitácoras de seguridad en los sistemas identificados como críticos, así como con las condiciones de seguridad que impidan borrar o alterar éstos.	
	103	Implementa mecanismos de TIC Y TO para impedir la conexión a redes inalámbricas externas que se encuentren al alcance de los dispositivos electrónicos institucionales.	
	104	Instala en los componentes de los servicios de correo electrónico, herramientas actualizadas de protección contra correos electrónicos no deseados o no solicitados.	
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de	105	Establece el mecanismo para garantizar la eliminación o modificación de los privilegios de acceso a la información del personal interno y proveedores de servicios, cuando terminen su relación contractual o cuando por algún motivo	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 21 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI)		el nivel de privilegios de accesos asignados cambie.	
	106	Define los controles de seguridad necesarios para salvaguardar los activos de TIC y TO, los activos de información y las infraestructuras de información esenciales de la Institución y, en su caso, las críticas, proporcionales a su valor e importancia.	
		CONDICIÓN: ¿Se aplican los controles de seguridad? NO: Continuar en actividad 107 SI: Continuar en actividad 109	
	107	Los controles de seguridad aplicarán a los activos de TIC y TO, activos de información e infraestructuras de información esenciales y/o críticas que técnica y/o normativamente les corresponda, y de ser el caso, el GESI justifica la no aplicabilidad de los mismos.	
	108	En aquellos que se haya definido la no aplicabilidad de los controles de este factor crítico, se definen e implementan los controles que deriven de la ejecución del análisis de riesgos.	
	109	Documenta los controles determinados conforme al paso 107, incluyendo su definición detallada e integrarlos al documento de definición del SGSI.	
	110	Elabora conjuntamente con los responsables de los procesos institucionales involucrados, el programa de implementación del SGSI e integrarlo al mismo documento. El programa de implementación deberá incluir el nombre del responsable de la implementación de cada uno de los	Documento de definición del SGSI

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 22 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

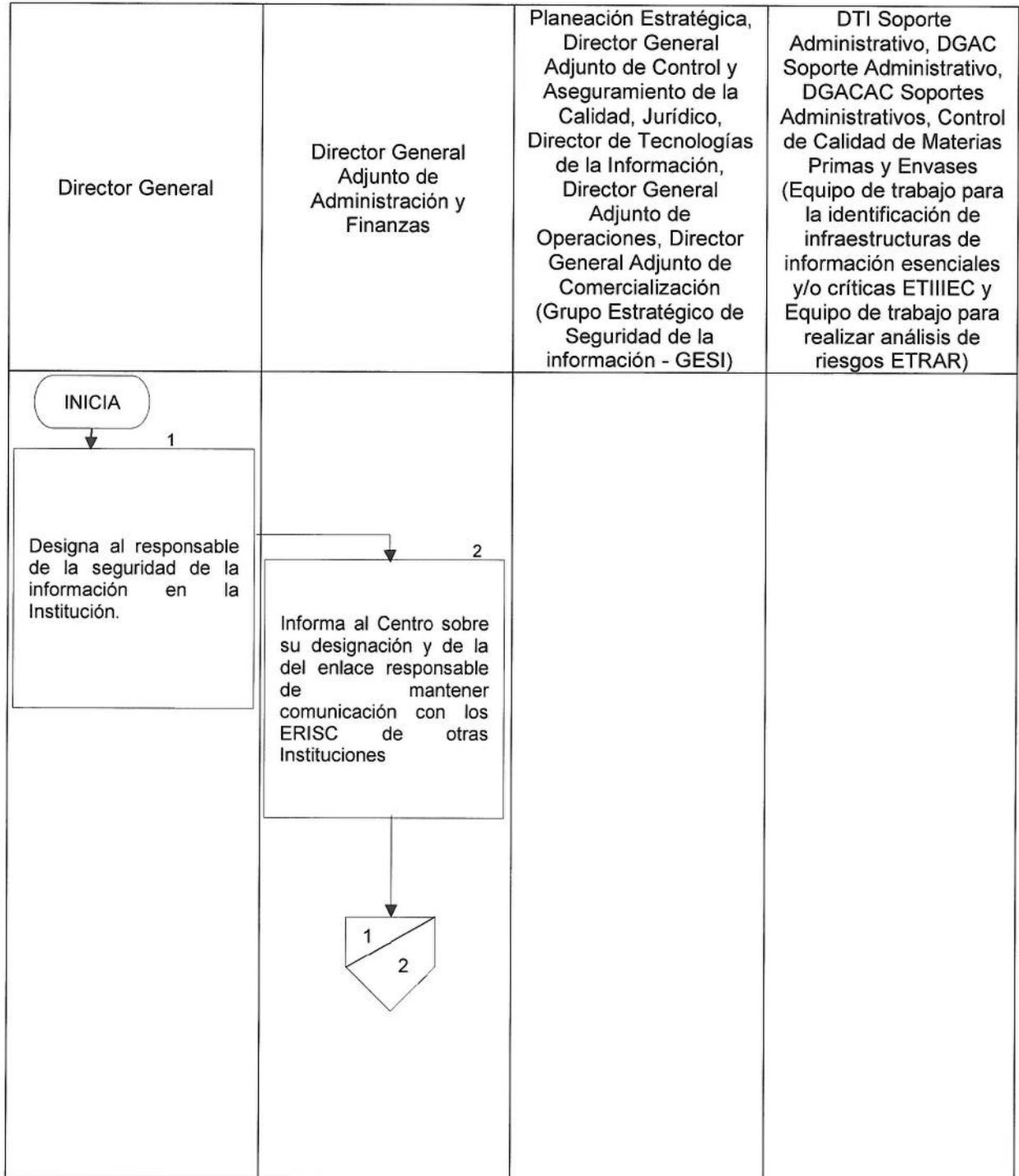
Responsable	No. Act.	Descripción de actividades	Documento o anexo
		controles de seguridad del SGSI que se hayan establecido.	
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI)	111	Mejora el SGSI	Implementación de la mejora al SGSI
	112	Constata que las actualizaciones de seguridad en todos los componentes de la infraestructura tecnológica de la Institución se apliquen, a fin de hacer del conocimiento del titular de la misma el cumplimiento de los controles de seguridad establecidos.	
	113	Obtiene, de la evaluación del SGSI, los datos sobre su desempeño, a fin de definir y documentar las acciones correctivas y preventivas para ajustar el mismo, e integrarlas al documento de definición del SGSI.	Documento de definición del SGSI
	114	Elabora el documento de implementación de la mejora al SGSI e integrarlo al documento de definición del SGSI. El documento de implementación debe utilizarse para la planeación y el seguimiento de las acciones de mejora, ya sean preventivas o correctivas.	Documento de definición del SGSI
	115	Comunica las mejoras que deberán aplicarse al SGSI al responsable del grupo de trabajo para la implementación de la seguridad de la información, por medio del documento de definición del SGSI, en lo relativo a los resultados de la evaluación del SGSI y la implementación al SGSI.	
	116	Vigila y registra las observaciones necesarias respecto a la implementación de las mejoras mediante un informe de seguimiento a las acciones de mejora al SGSI que deberá integrarse al documento de definición del SGSI.	Documento de definición del SGSI

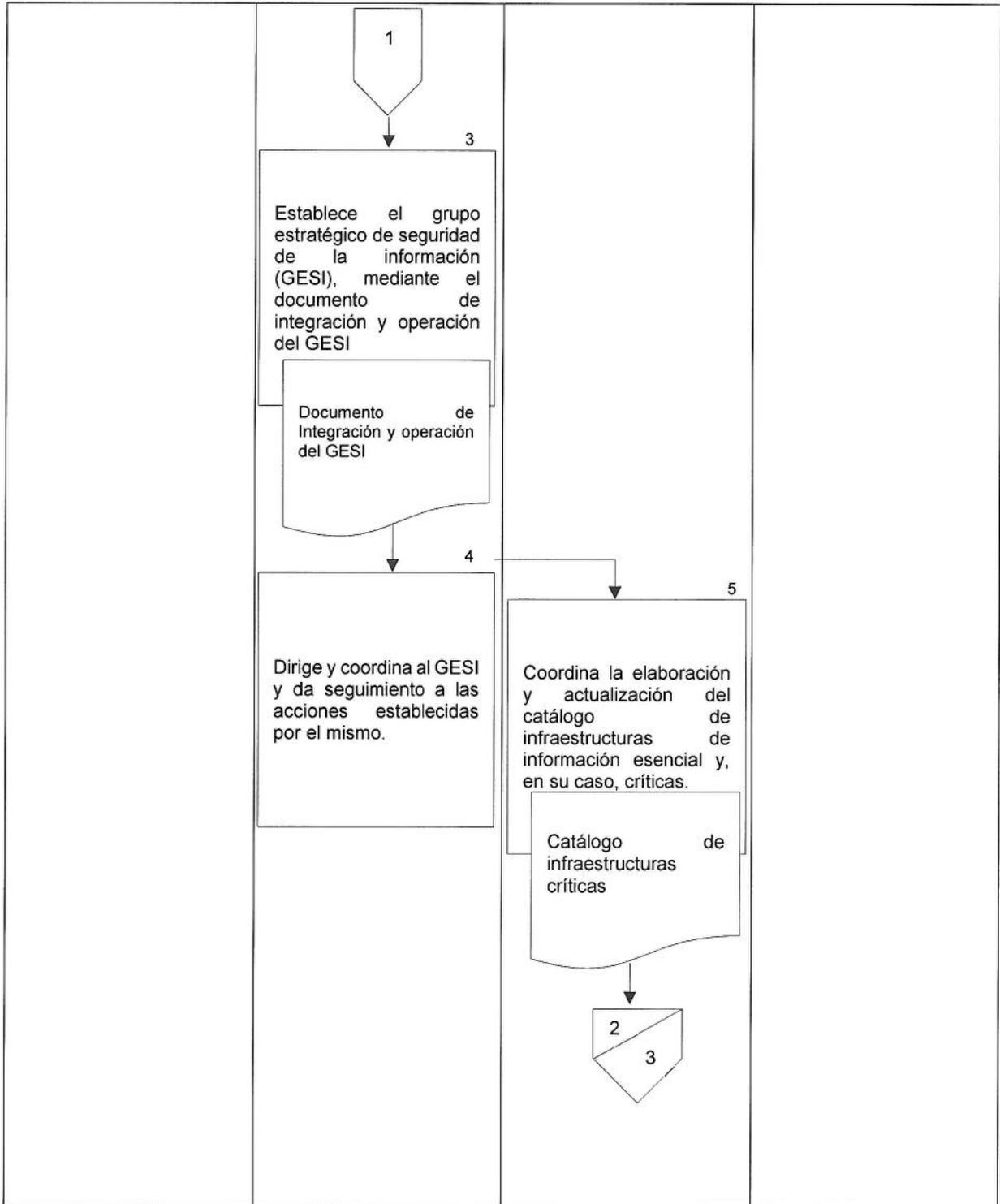
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 23 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Planeación Estratégica, Director General Adjunto de Control y Aseguramiento de la Calidad, Jurídico, Director de Tecnologías de la Información, Director General Adjunto de Operaciones, Director General Adjunto de Comercialización (Grupo Estratégico de Seguridad de la información - GESI)	117	Aplica las acciones correctivas y preventivas a los controles de seguridad de la información, indicados por el grupo estratégico de seguridad de la información.	Documento de definición del SGSI
	118	Documenta el resultado de la aplicación de la mejora, para cada uno de los controles de seguridad de la información que resultaron impactados, incluyendo las mejoras del SGSI aplicadas.	
	119	Actualiza el informe de seguimiento a las acciones de mejora al SGSI e integrarlo en el documento de definición del SGSI.	
	120	Verifica el contenido del informe de seguimiento a las acciones de mejora al SGSI; actualizar el programa de evaluaciones del SGSI, integrarlo en el documento de definición del SGSI y enviar éste al grupo estratégico de seguridad de la información para su revisión.	
		TERMINA	

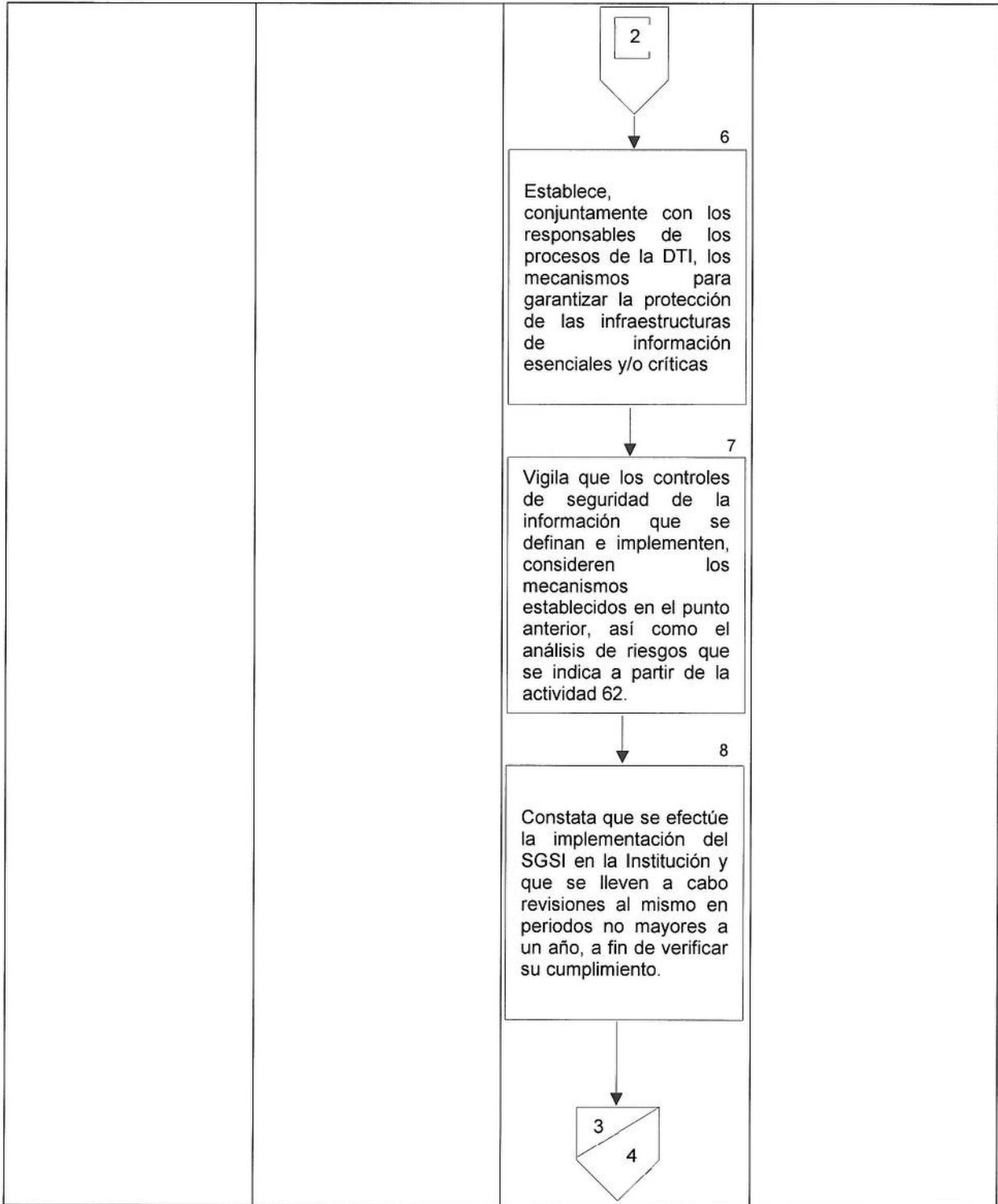
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 24 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			

## 5. DIAGRAMA DE FLUJO

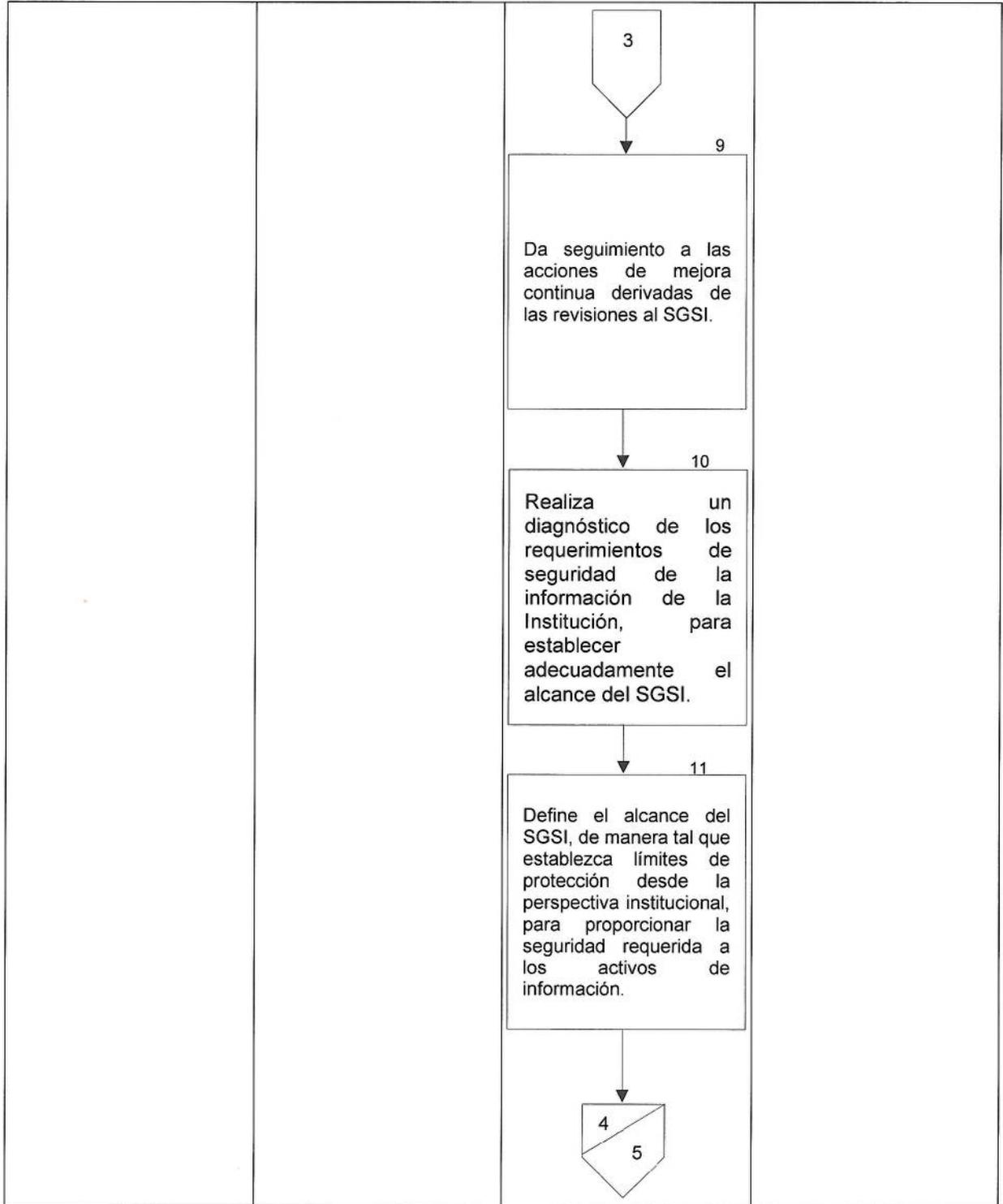




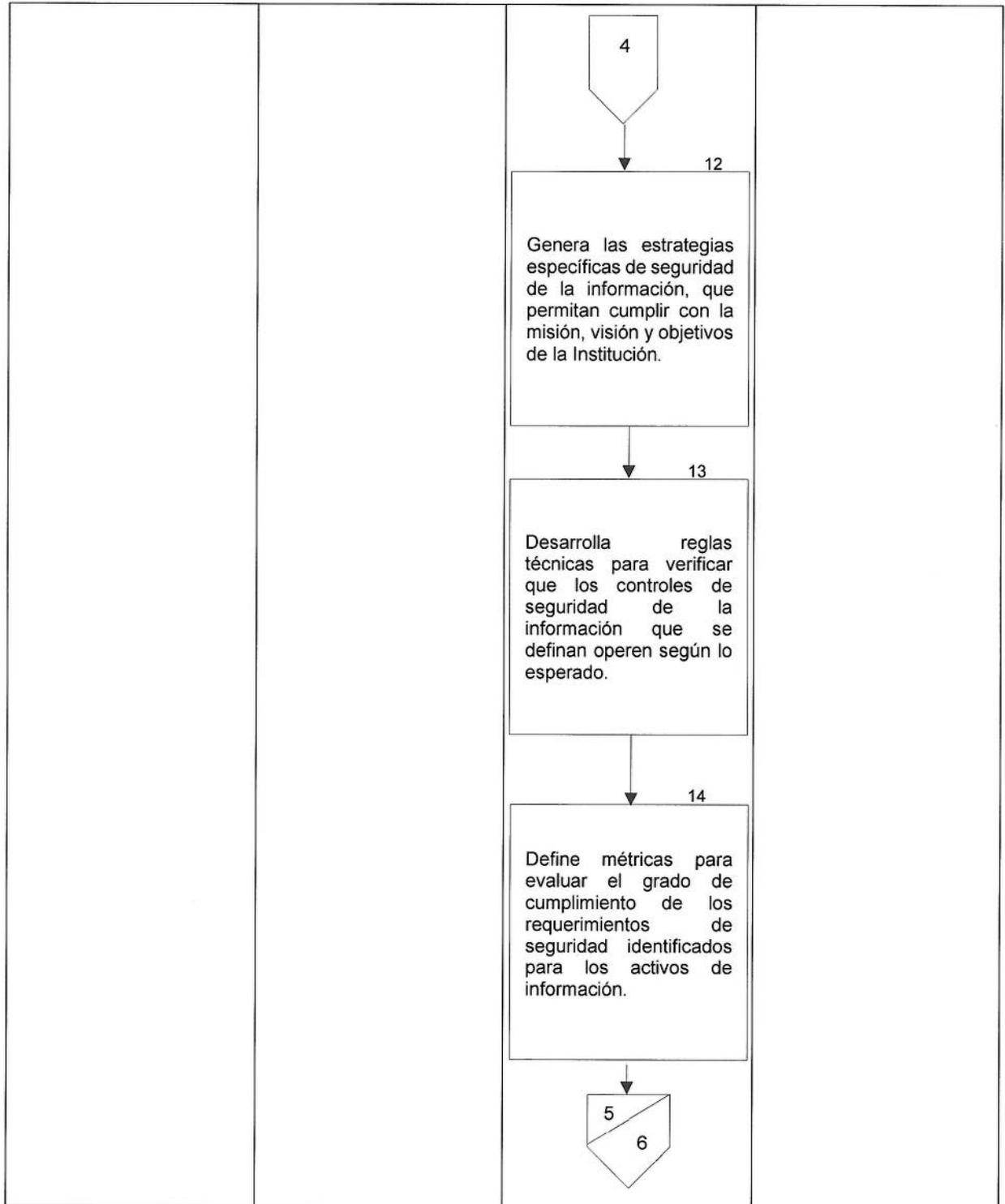
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 26 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



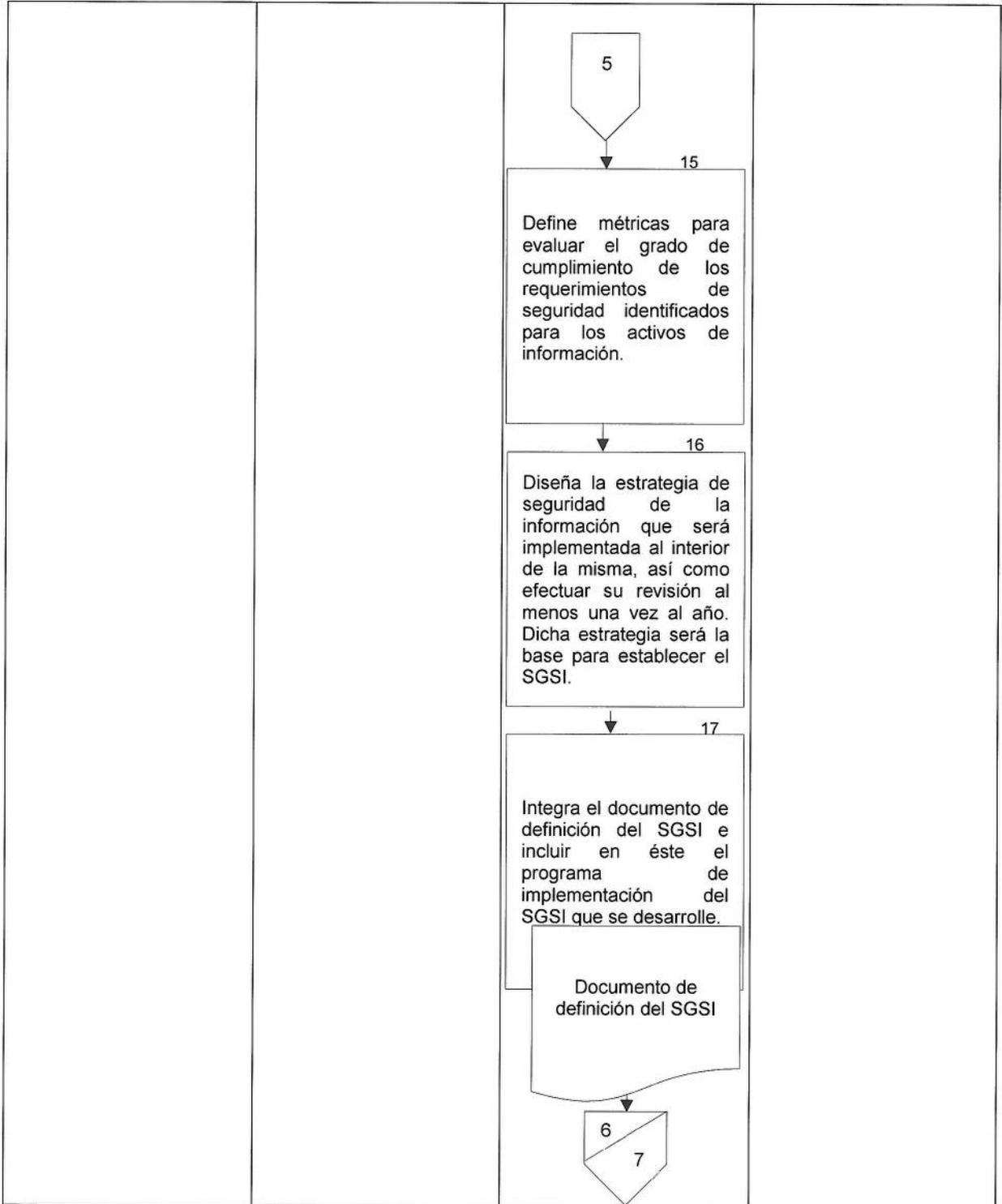
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		Hoja: 27 de 74



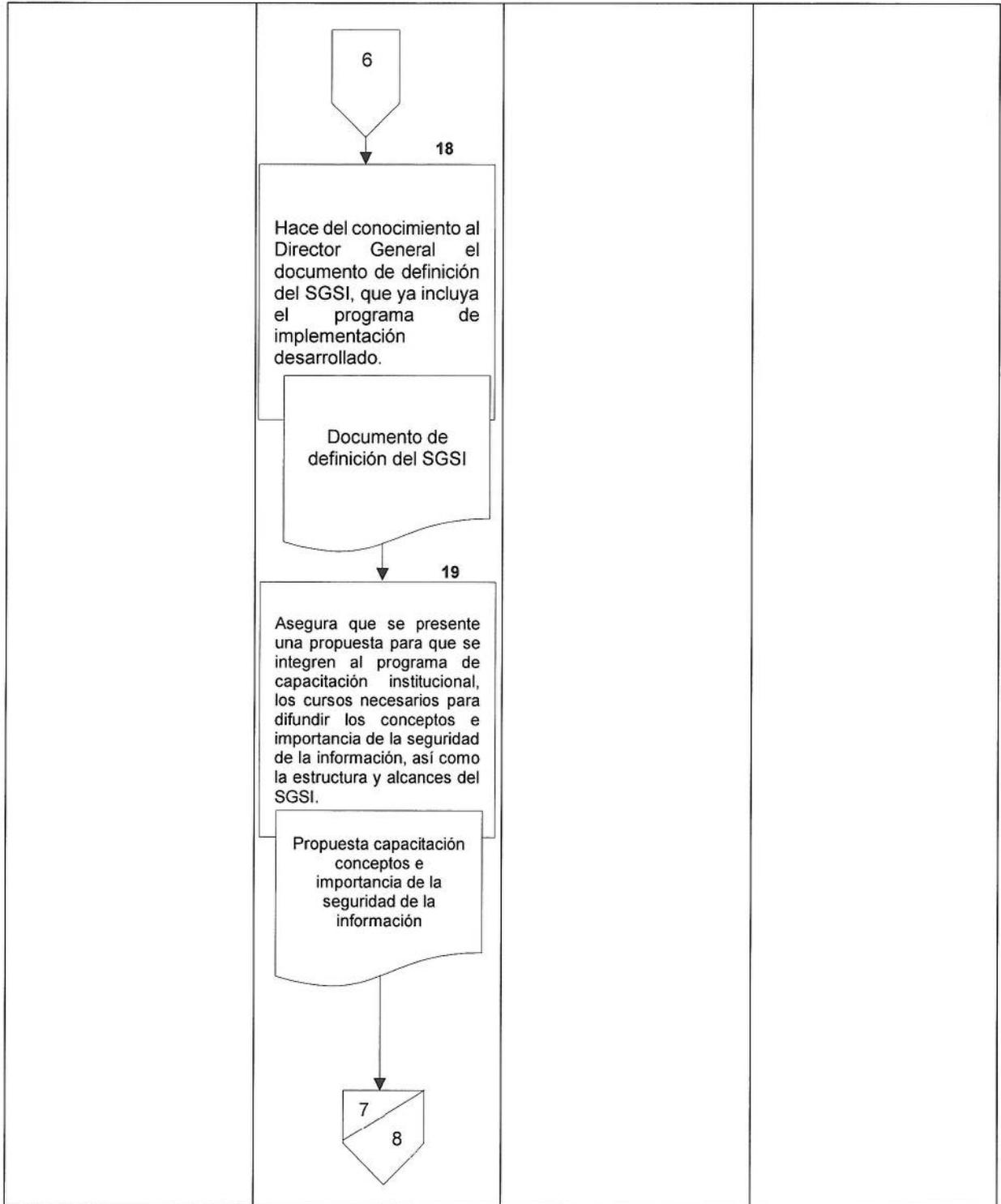
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 28 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



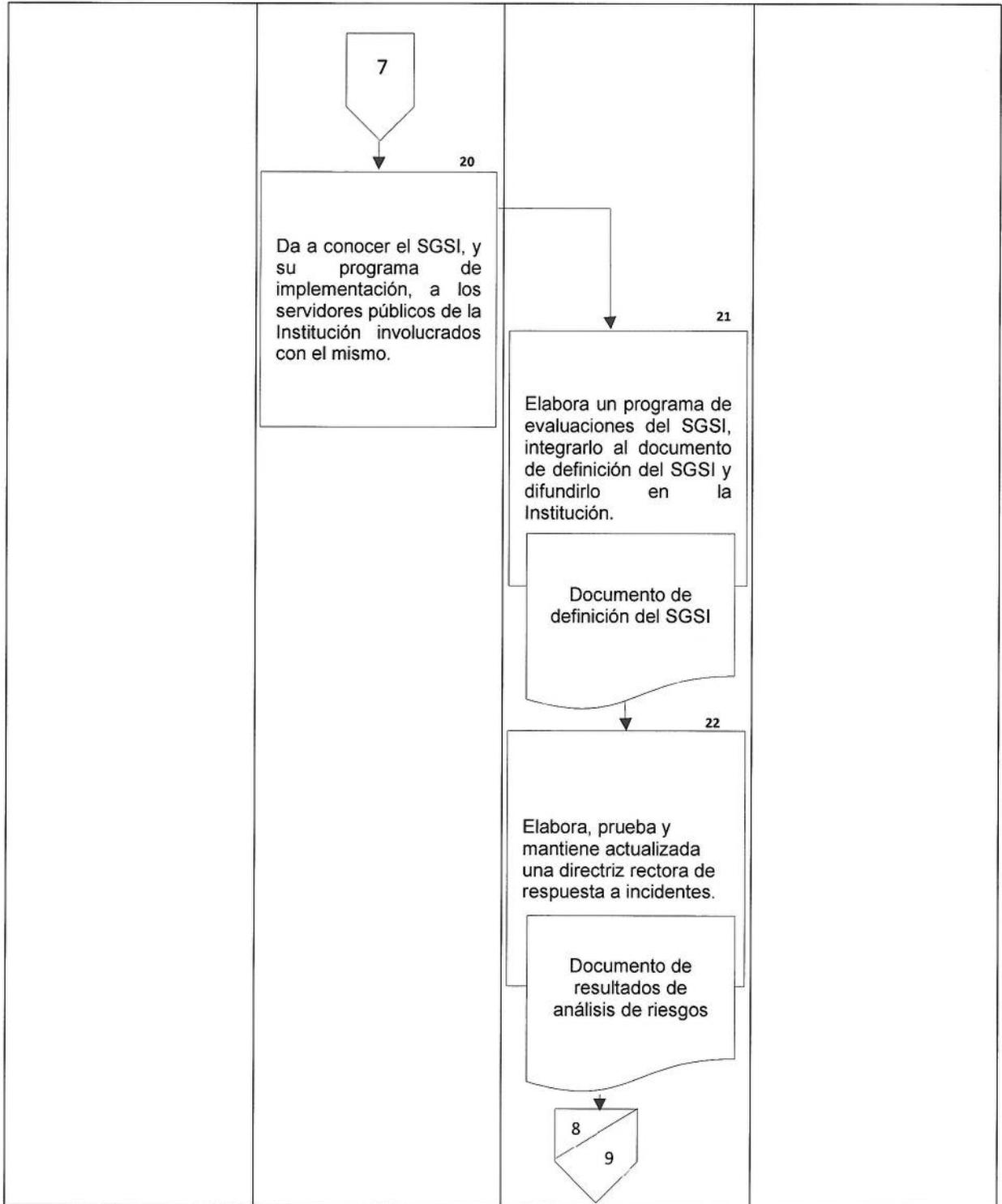
	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>UNIVERSIDAD DE GUATEMALA</small> <small>INSTITUTO DE INVESTIGACIONES Y RECURSOS HUMANOS</small> <small>UNIVERSIDAD</small>	Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 29 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



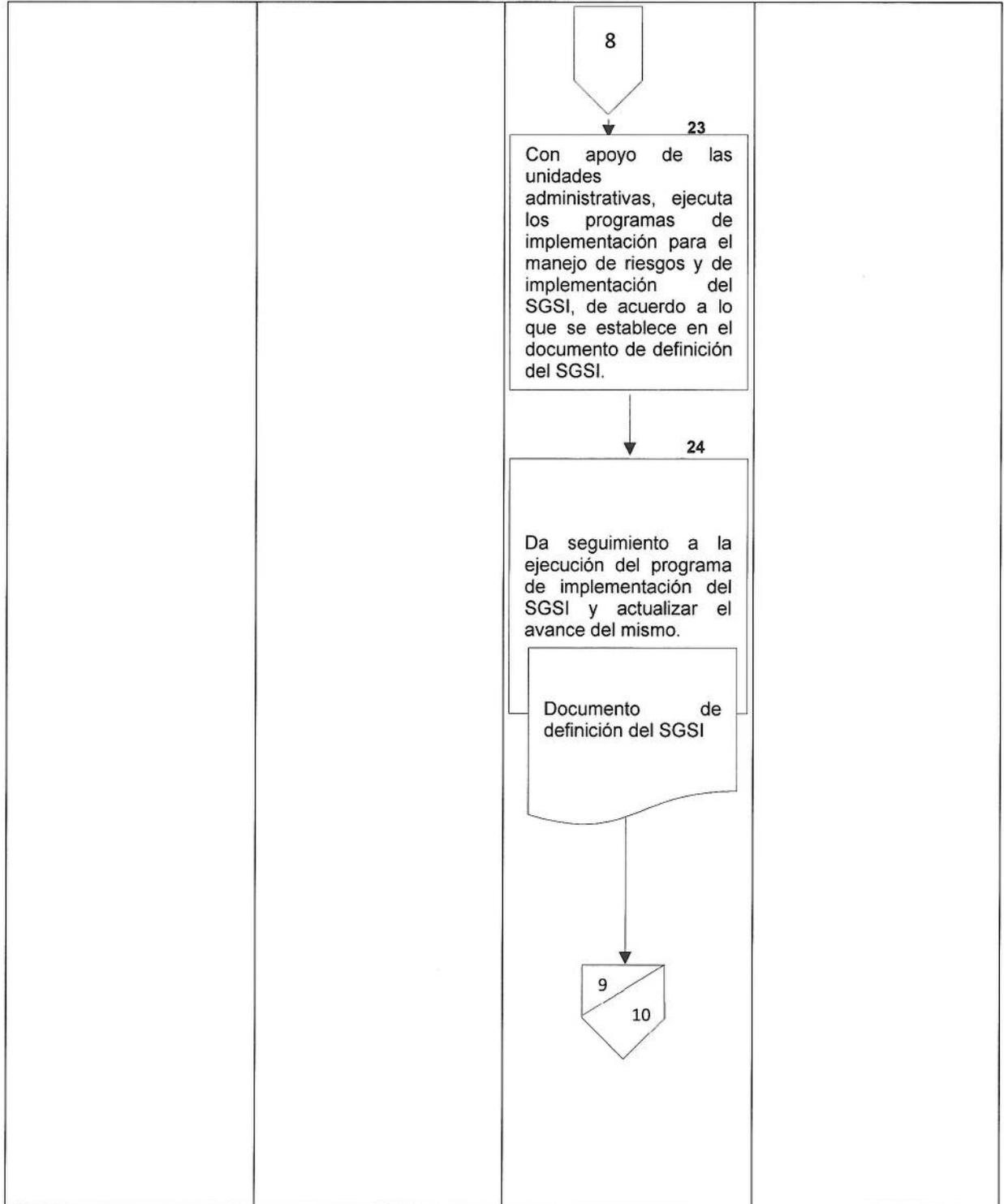
	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>ADMINISTRACIÓN DE PROCESOS Y RESULTADOS DE SERVICIOS</small>	Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 30 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



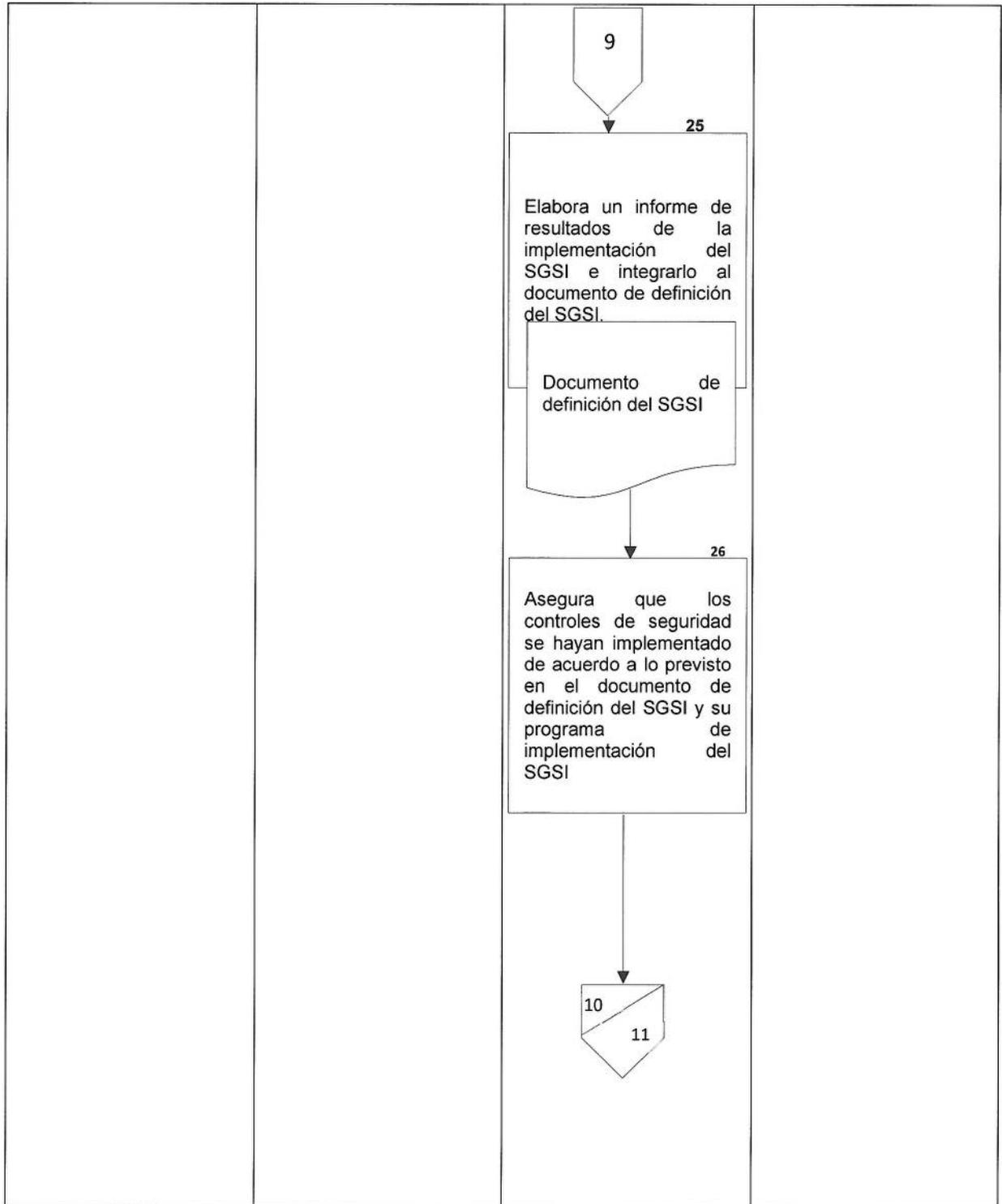
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 31 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			

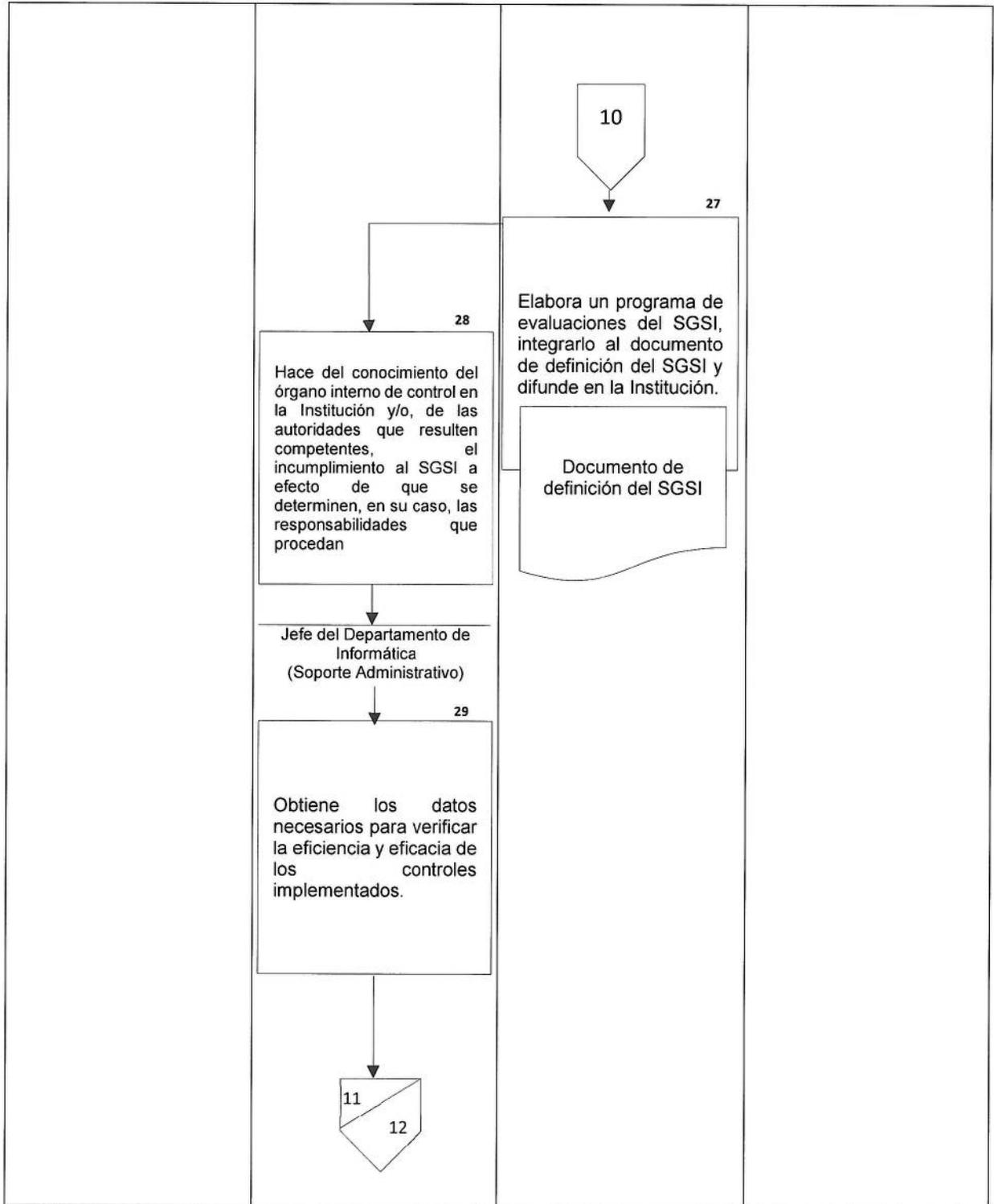


	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 32 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			

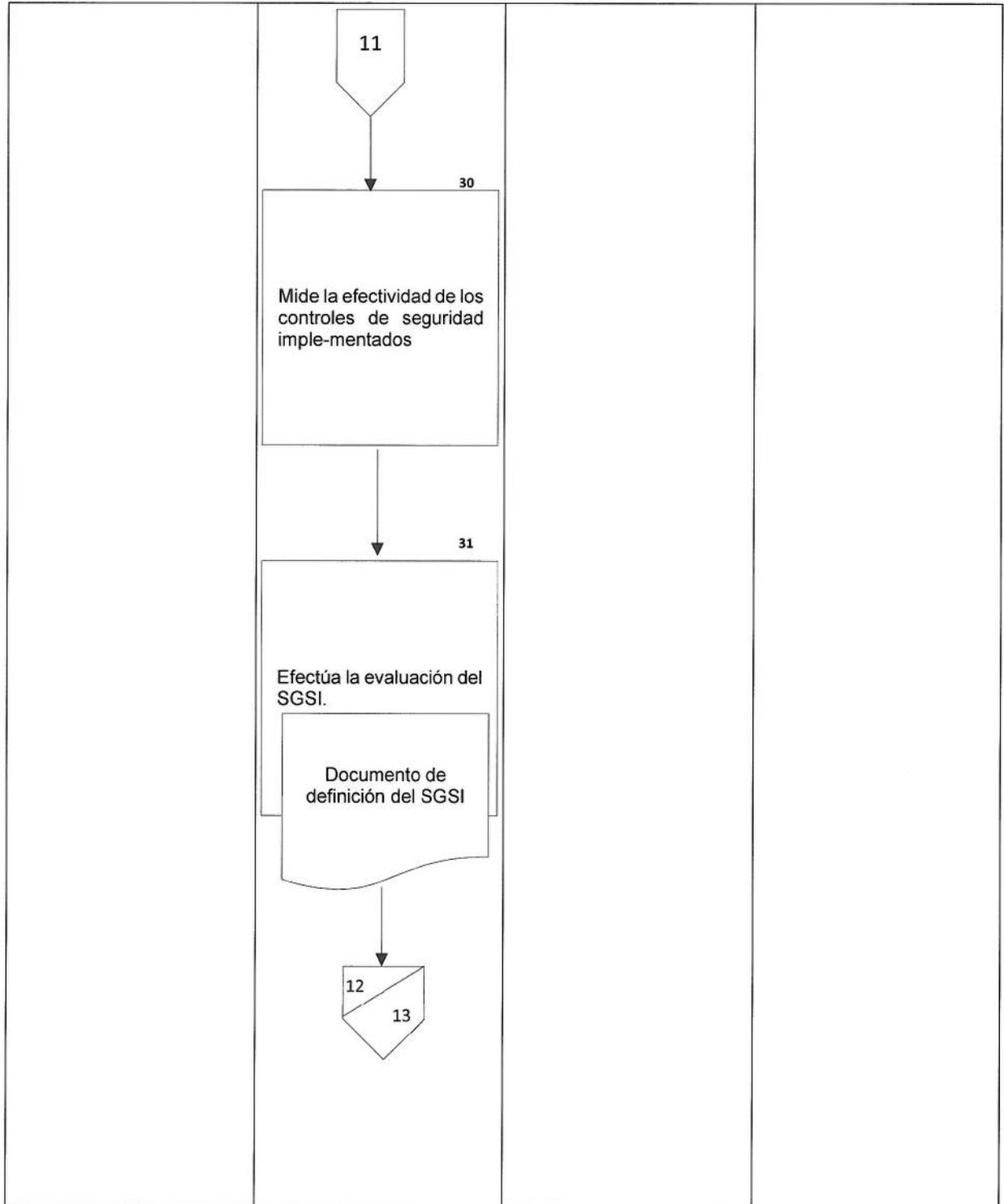


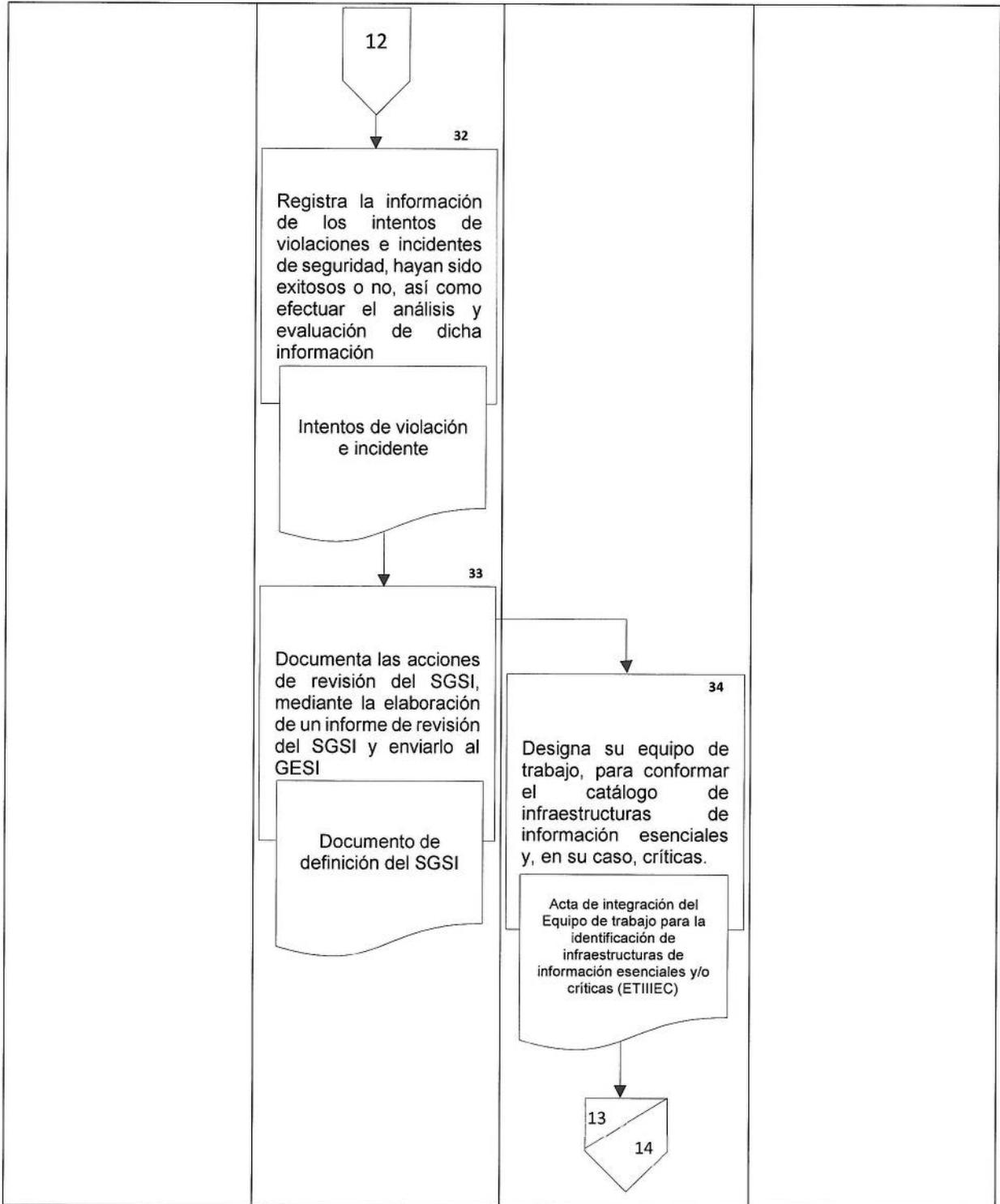
	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>COMUNIDAD DE SALUD BIRMEX Y SEGURIDAD DE LA INFORMACIÓN</small>	Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 33 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



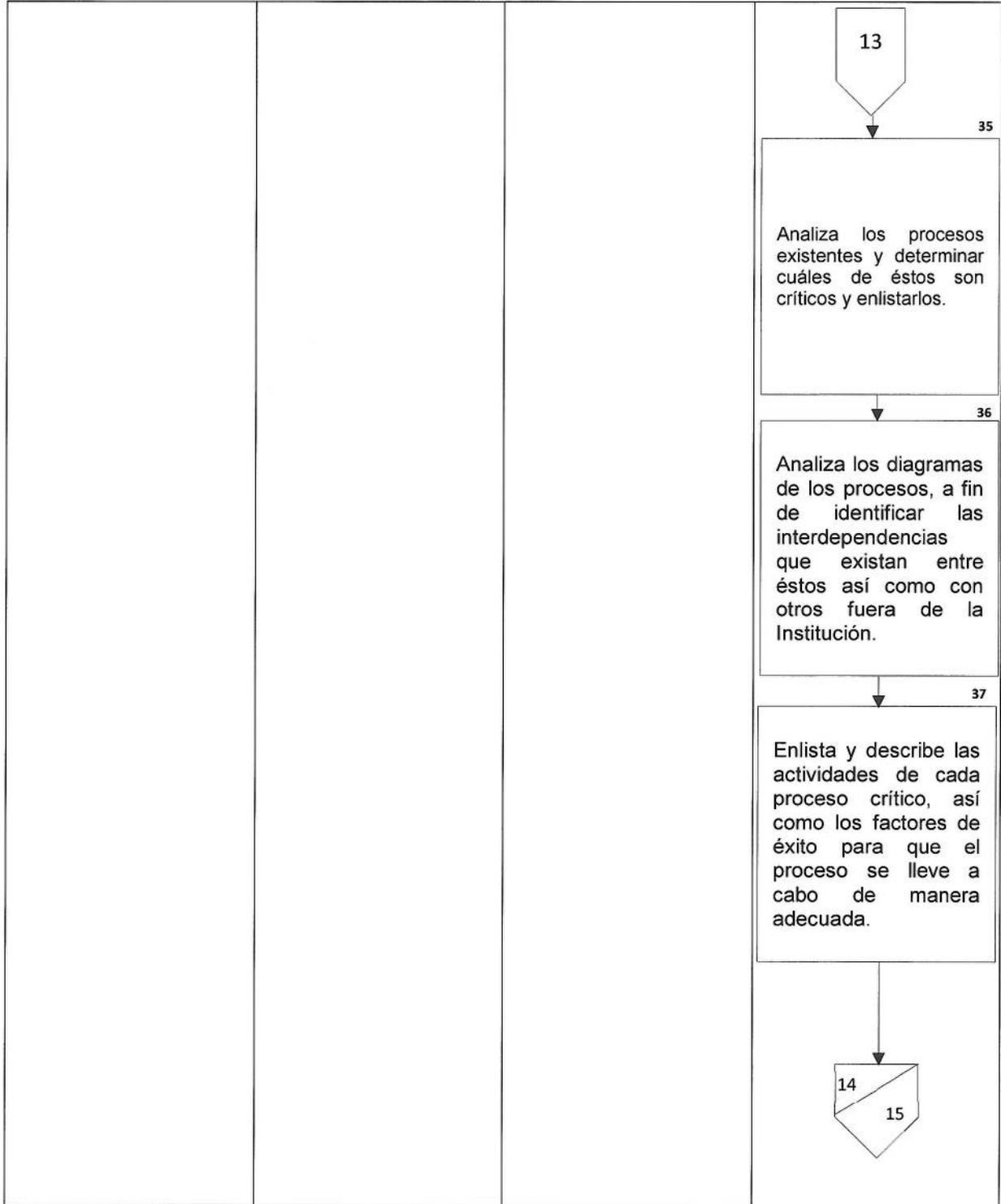


	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 35 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			

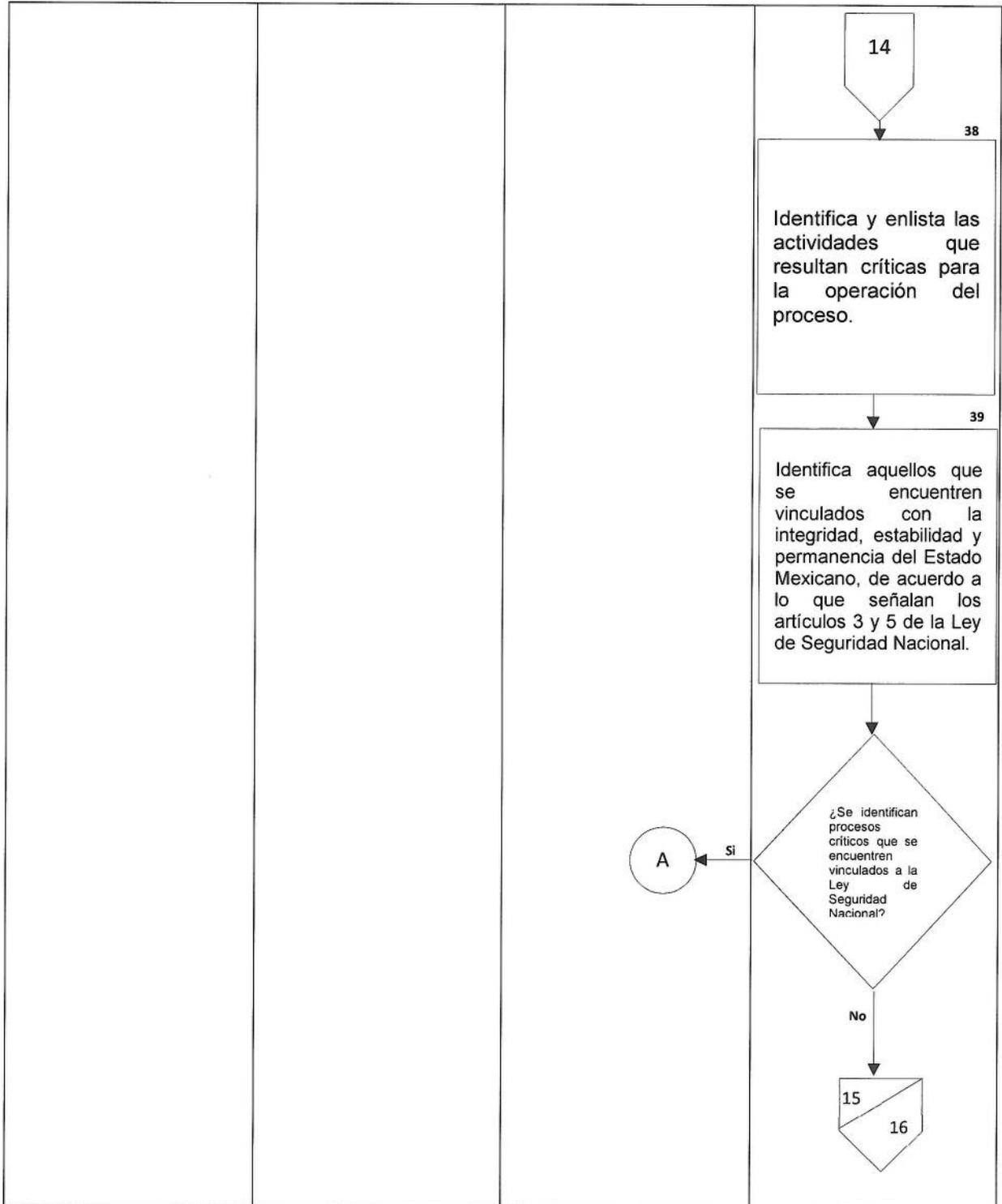




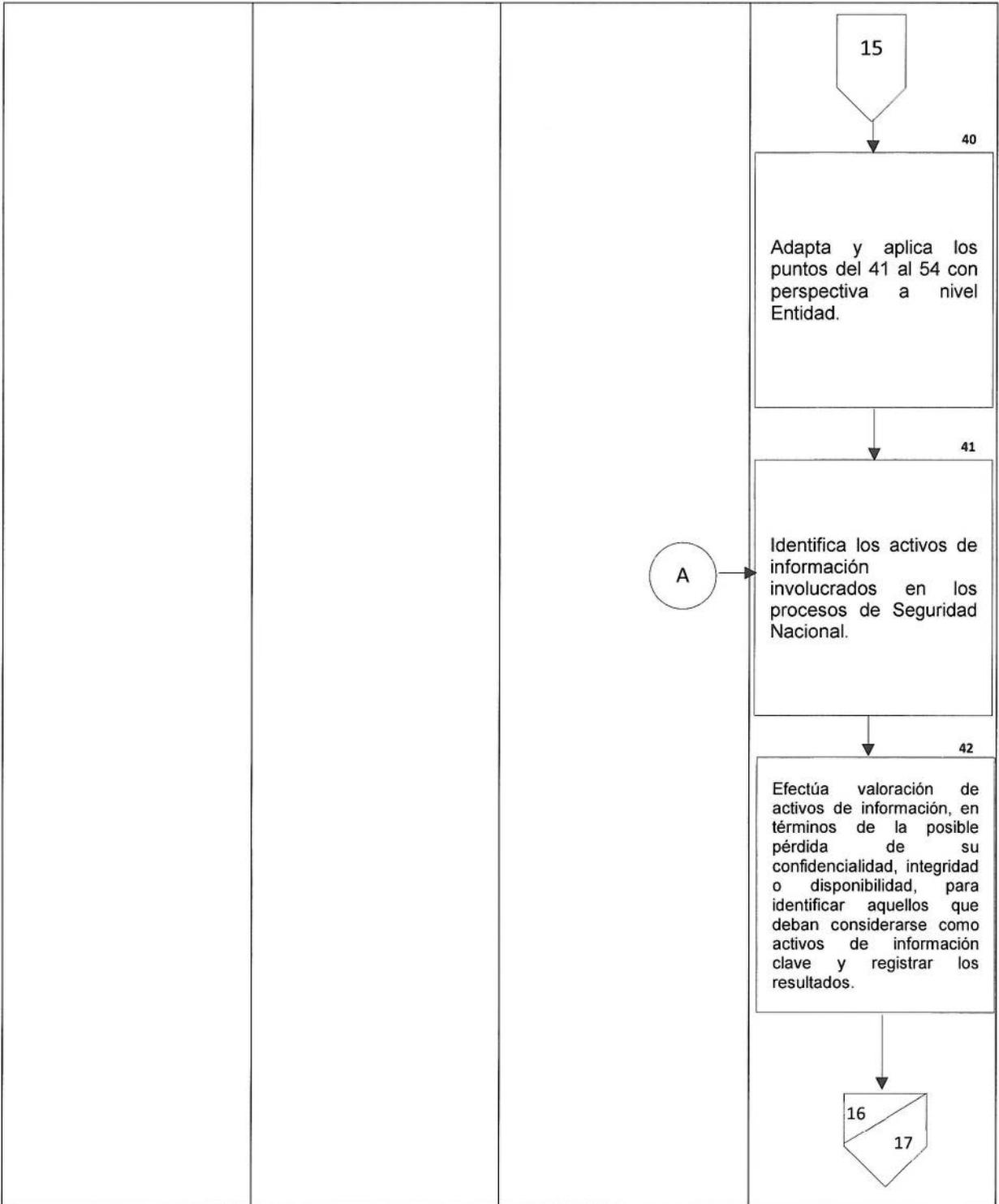
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		Hoja: 37 de 74



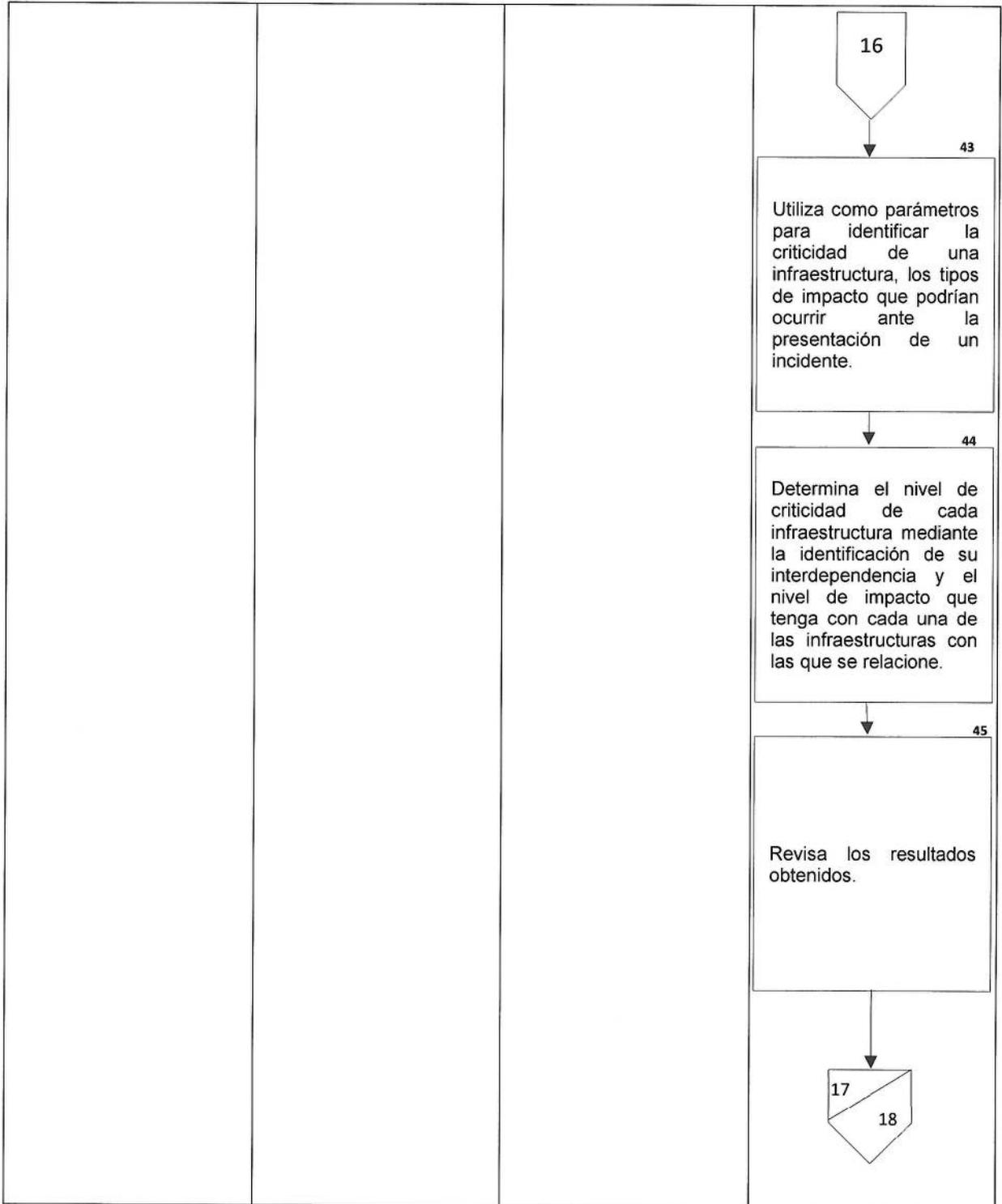
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 38 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



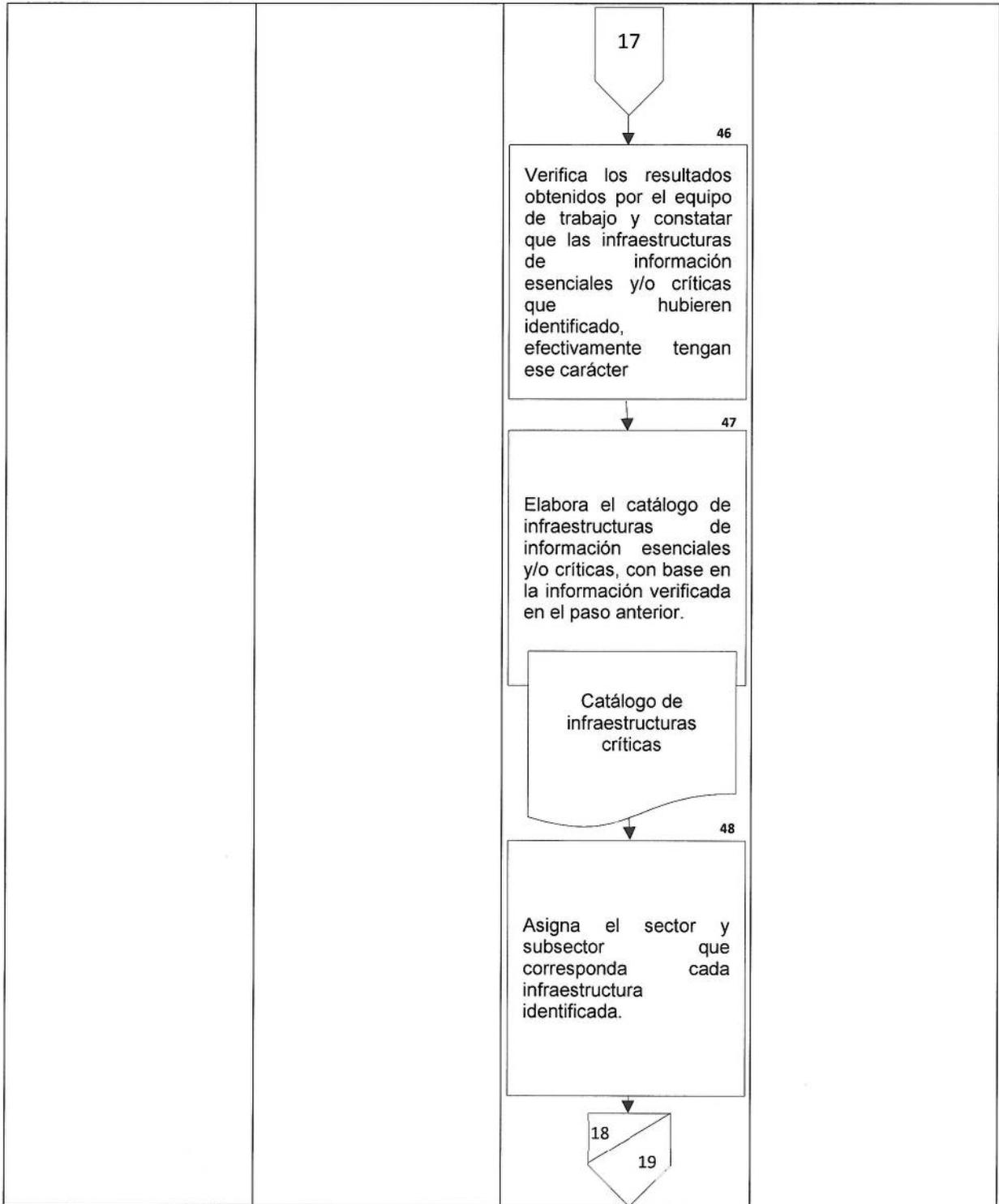
	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>BIRMEX</small> <small>INSTITUTO FEDERAL DE SEGURIDAD Y REACTIVOS MÉXICO</small> <small>S.A. DE C.V.</small>	Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 39 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



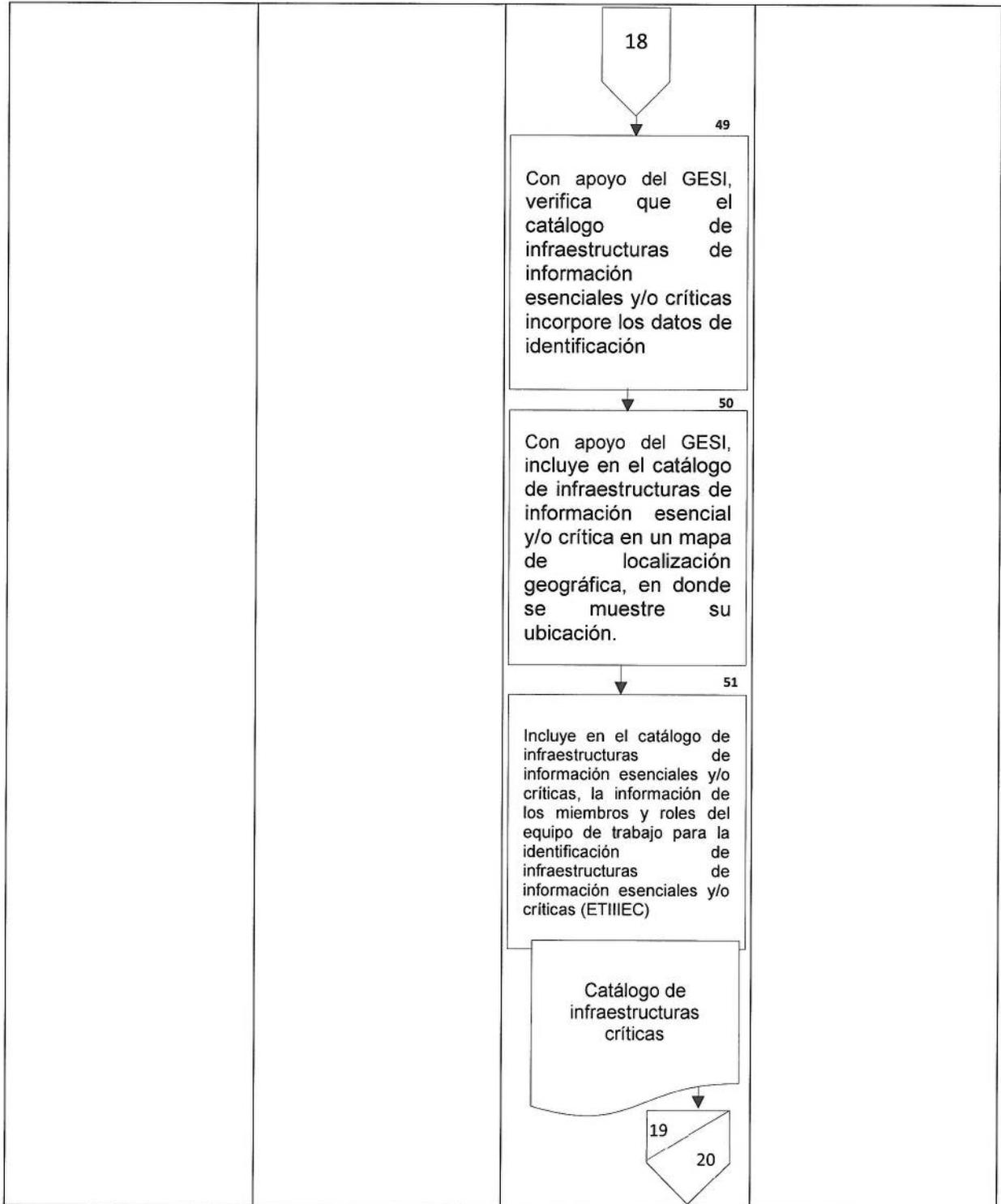
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 40 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			

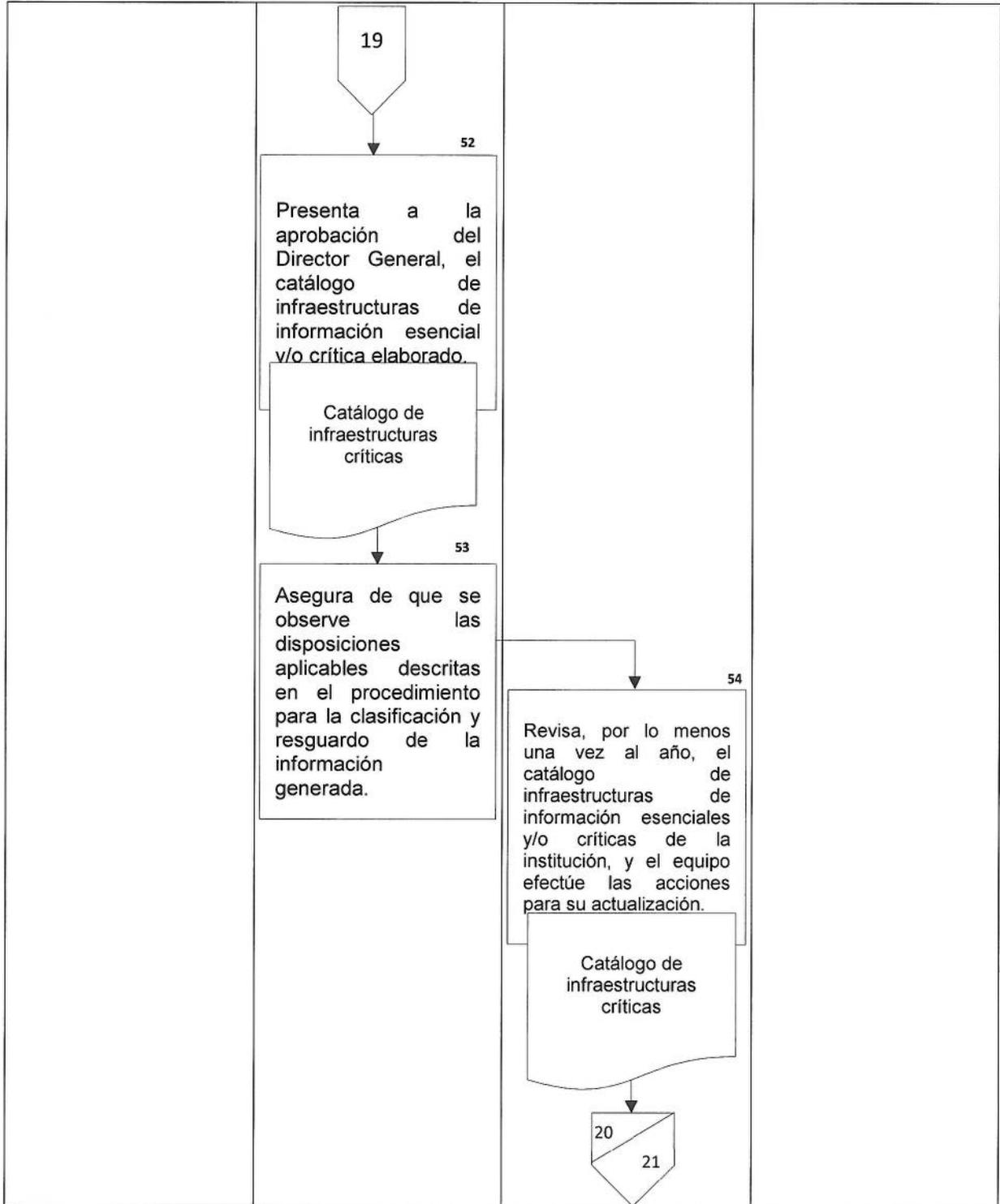


	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>UNIDAD ADMINISTRATIVA DE SEGURIDAD INFORMATICA Y REACTIVOS DEL MINISTERIO DE SALUD</small>	Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 41 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			

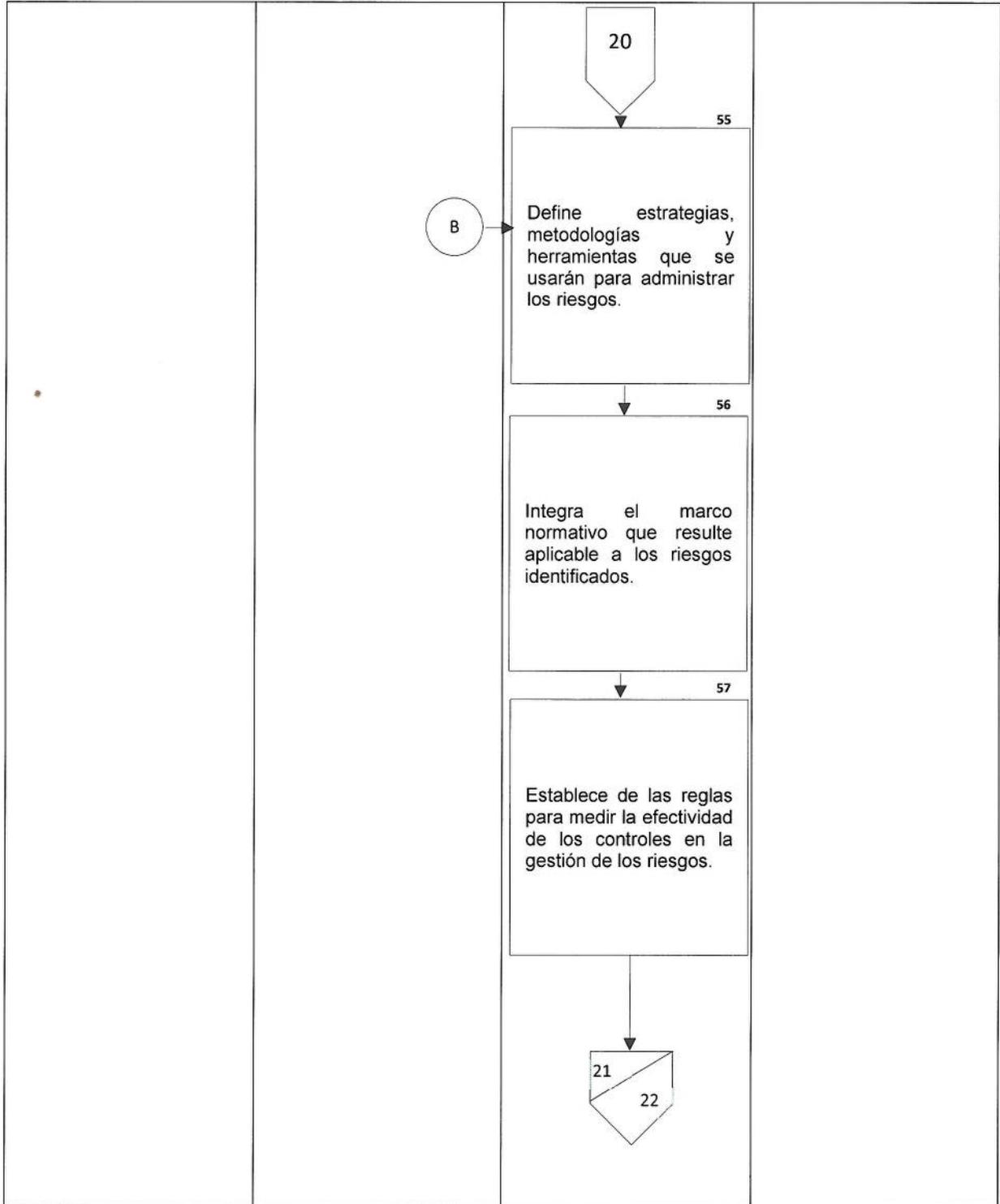


	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 42 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			

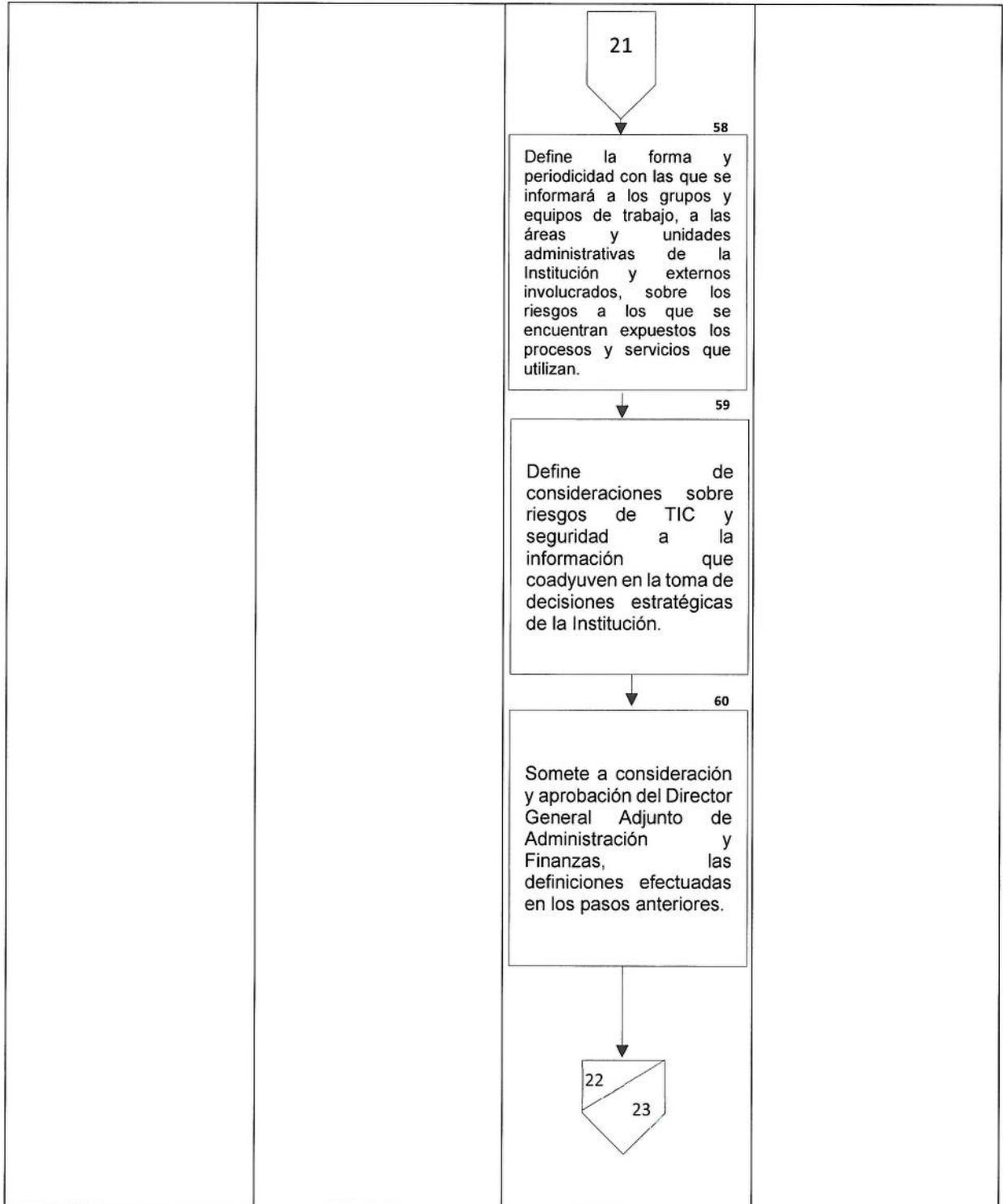




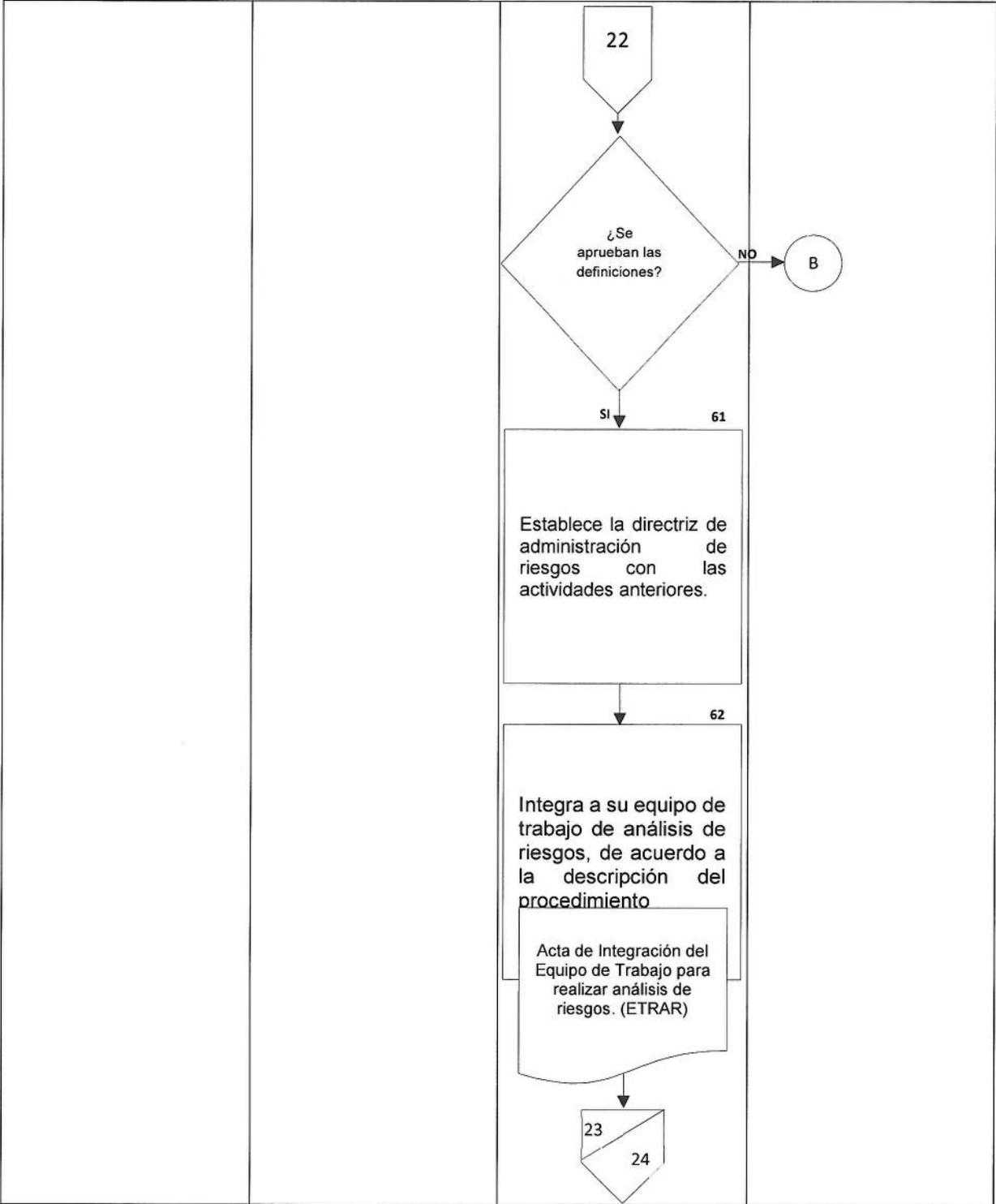
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 44 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



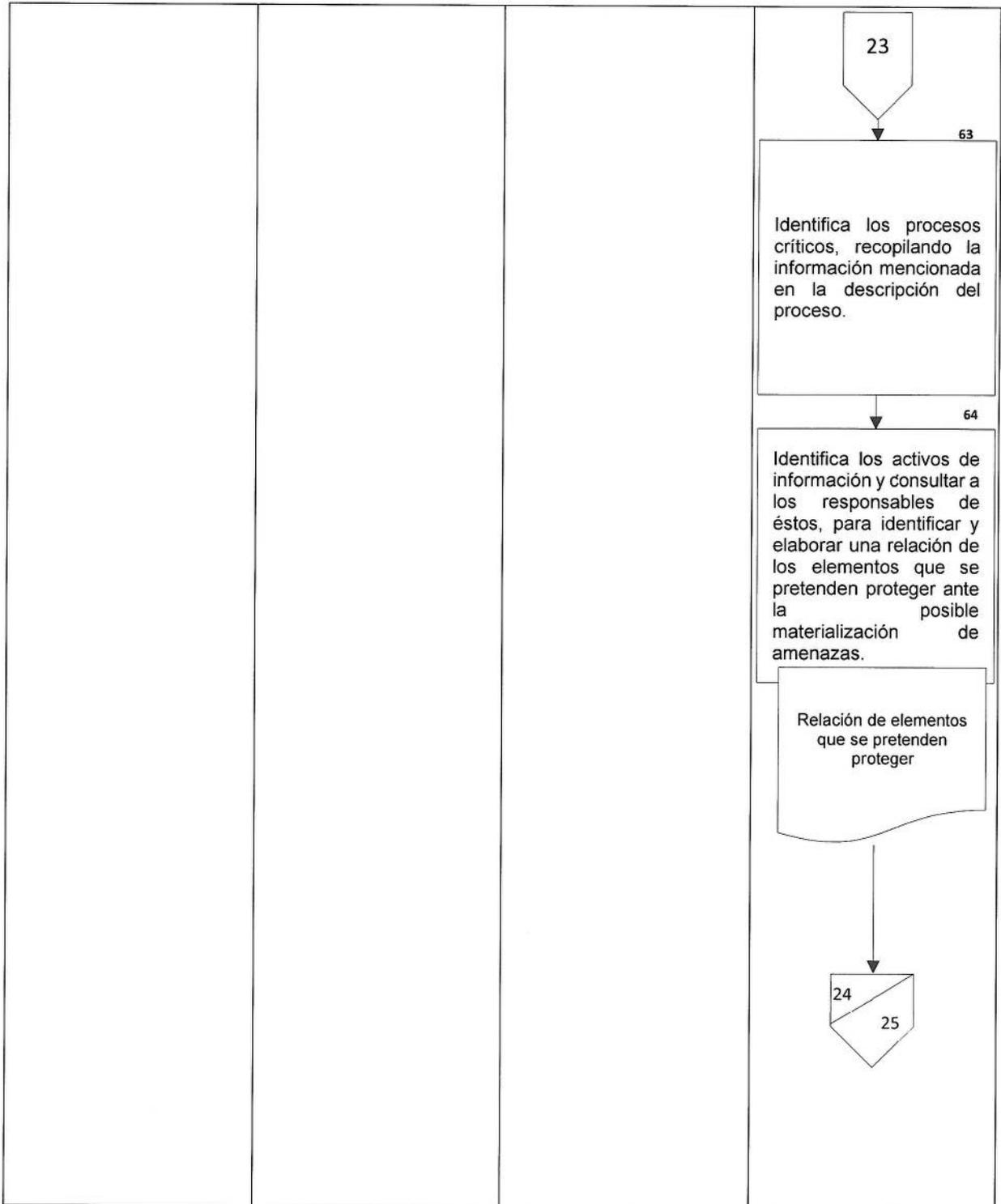
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 45 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



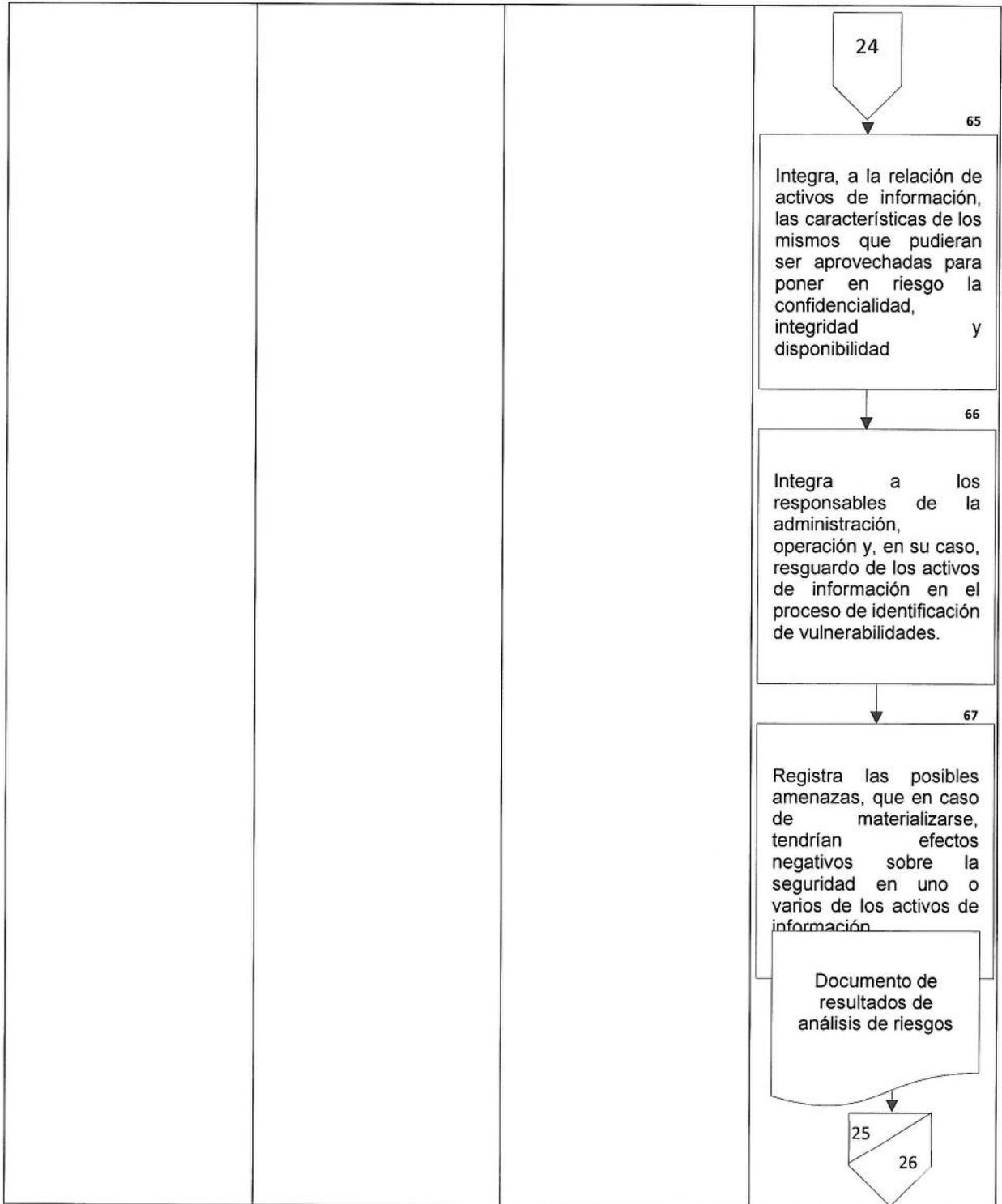
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 46 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



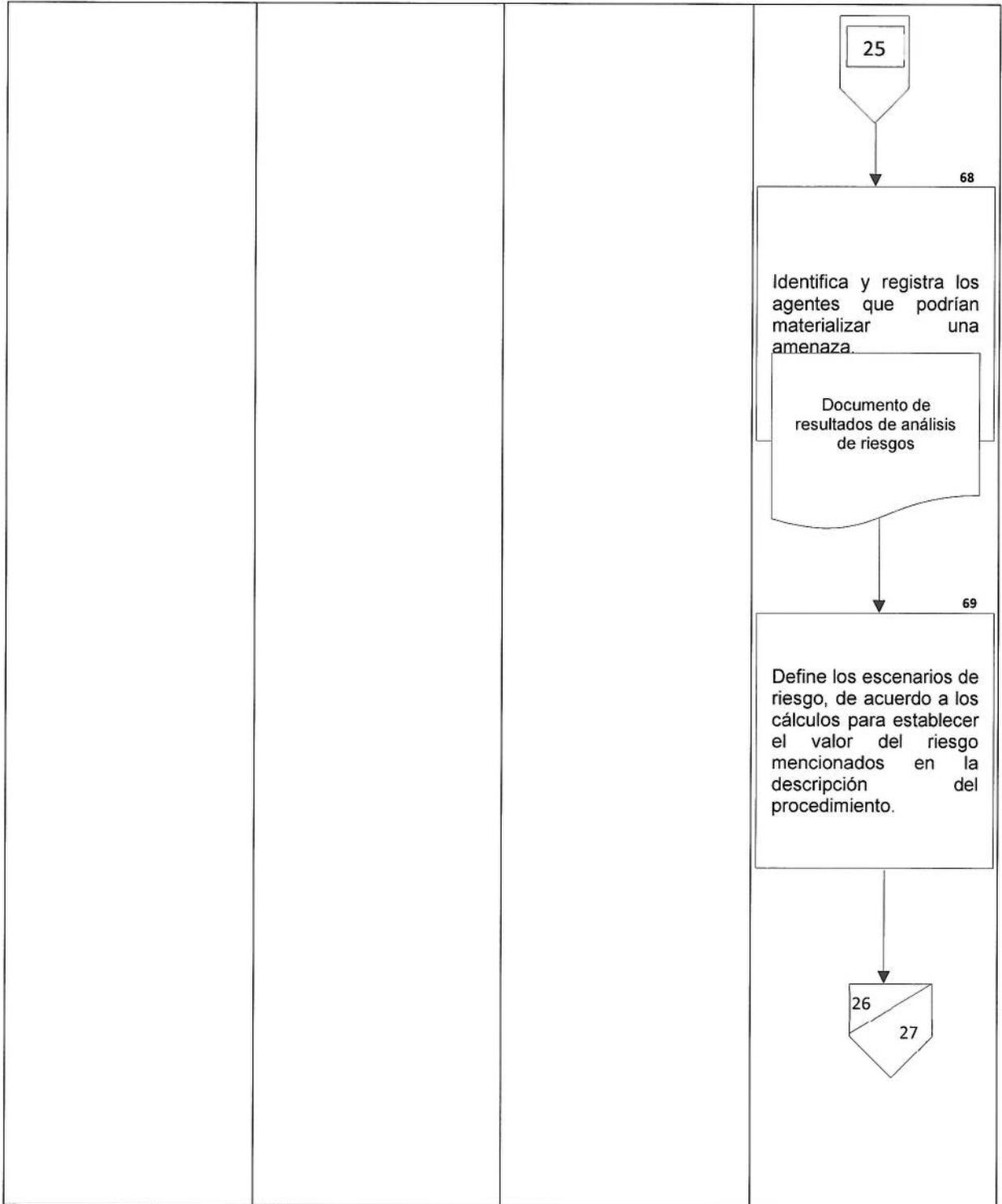
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		Hoja: 47 de 74



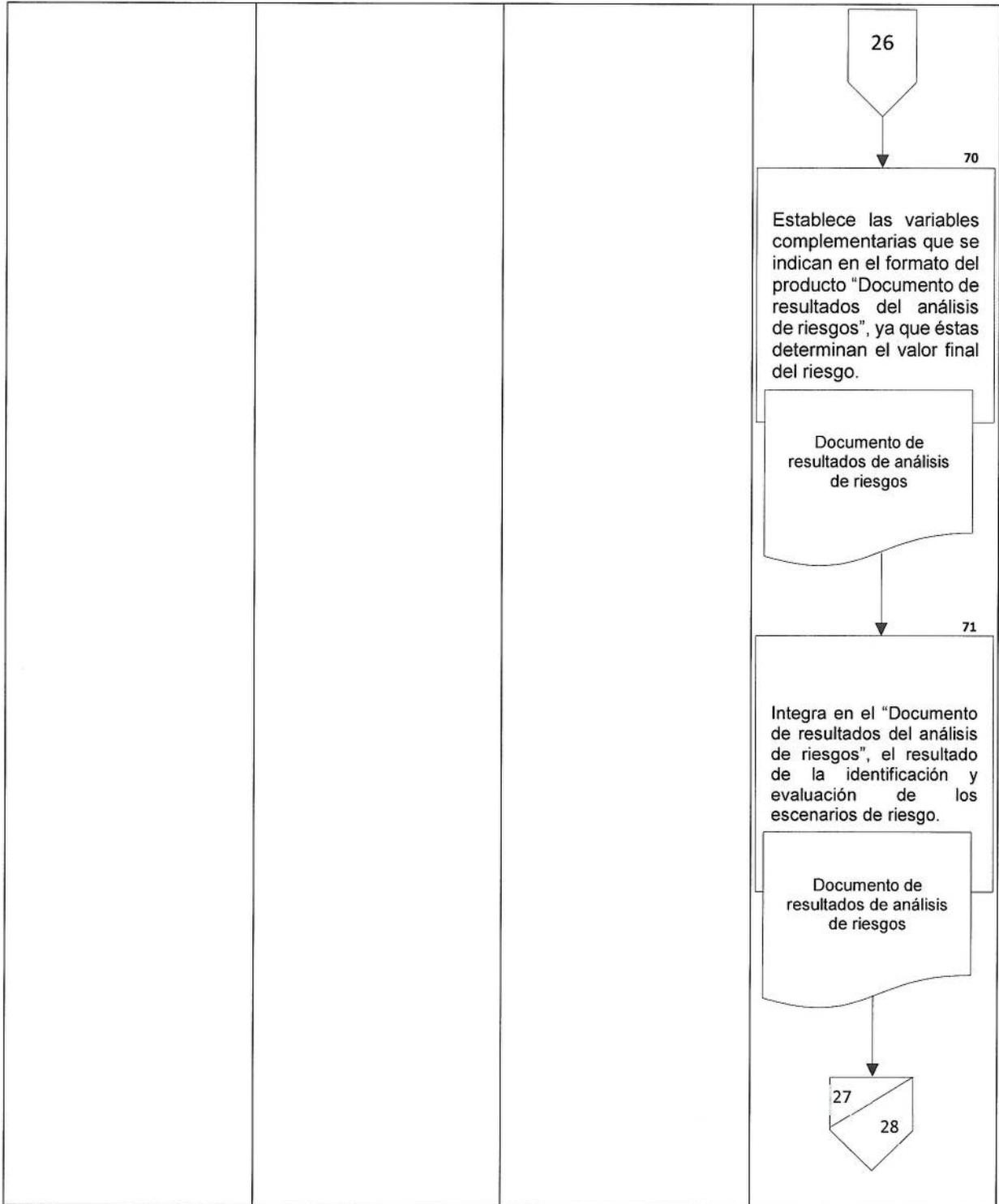
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: <b>48</b> de <b>74</b>
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		



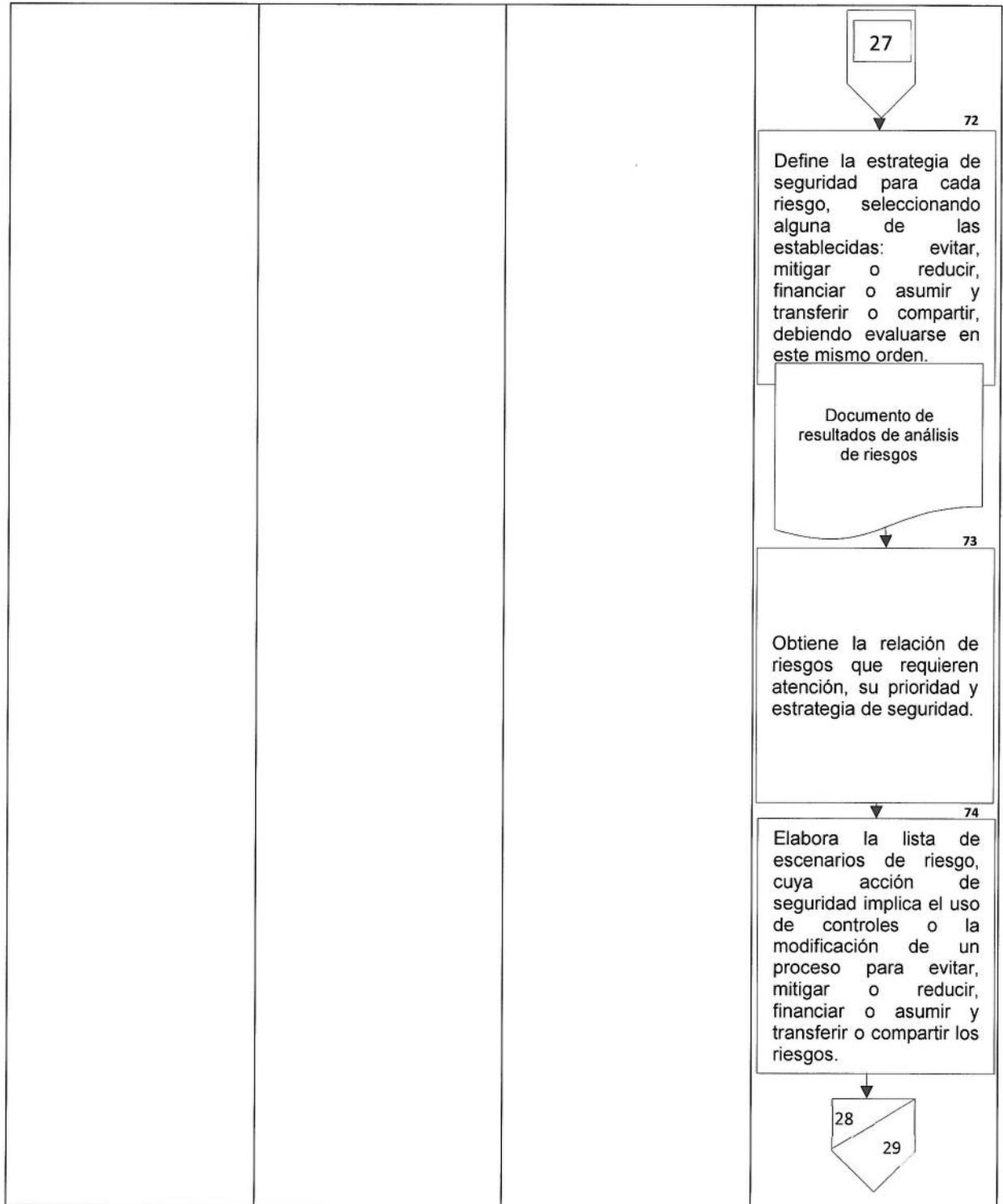
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 49 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



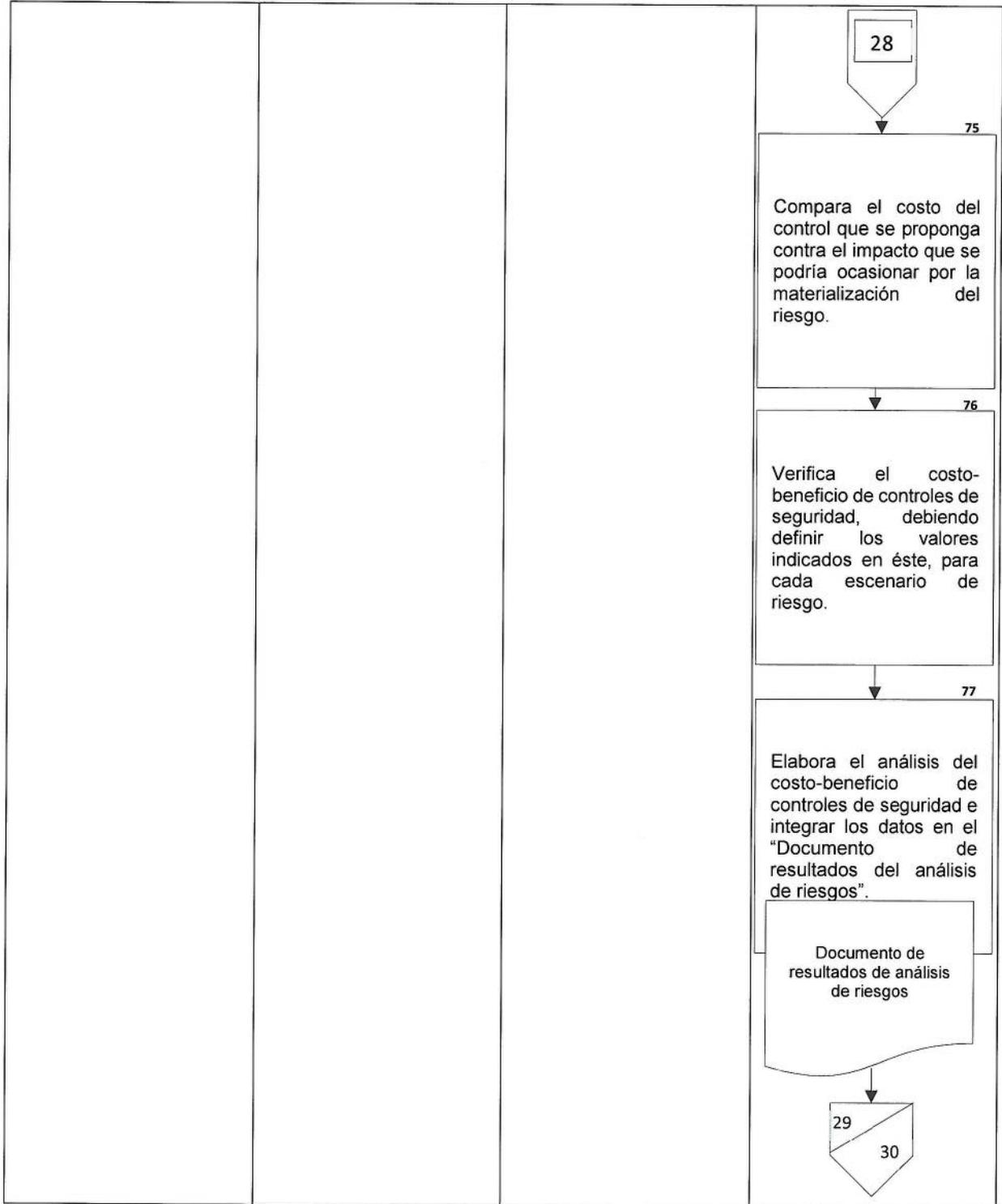
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 50 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



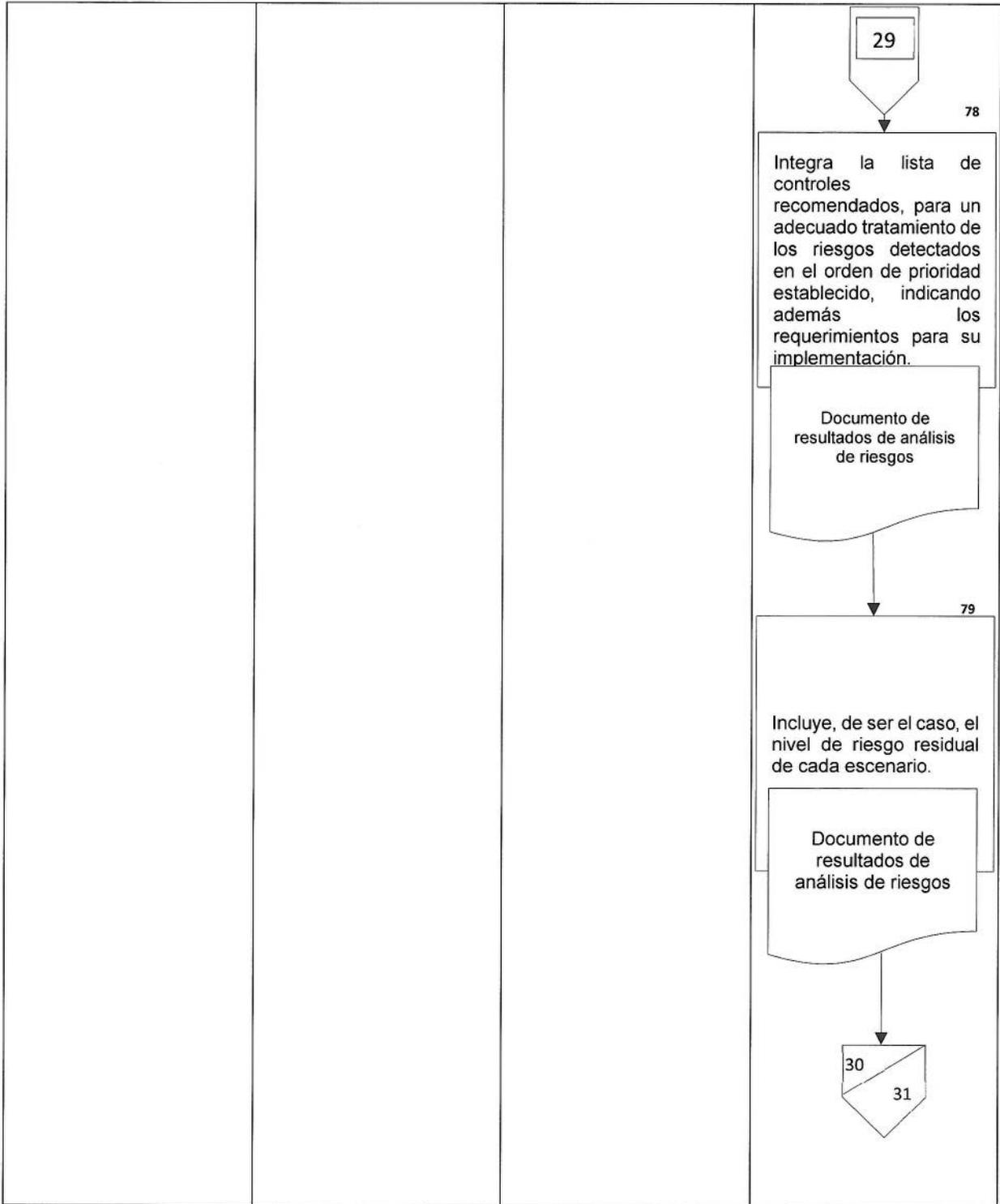
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 51 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



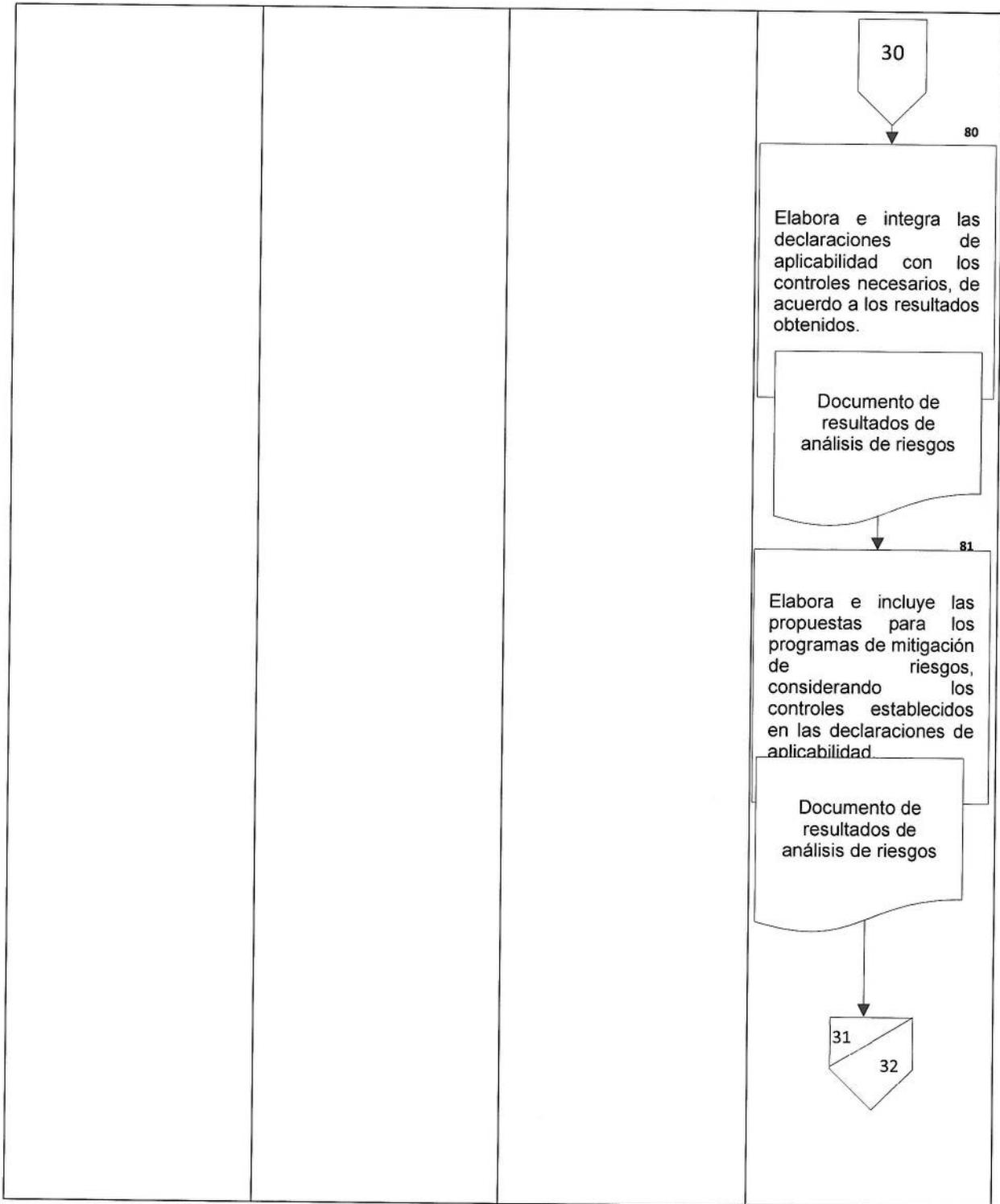
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 52 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



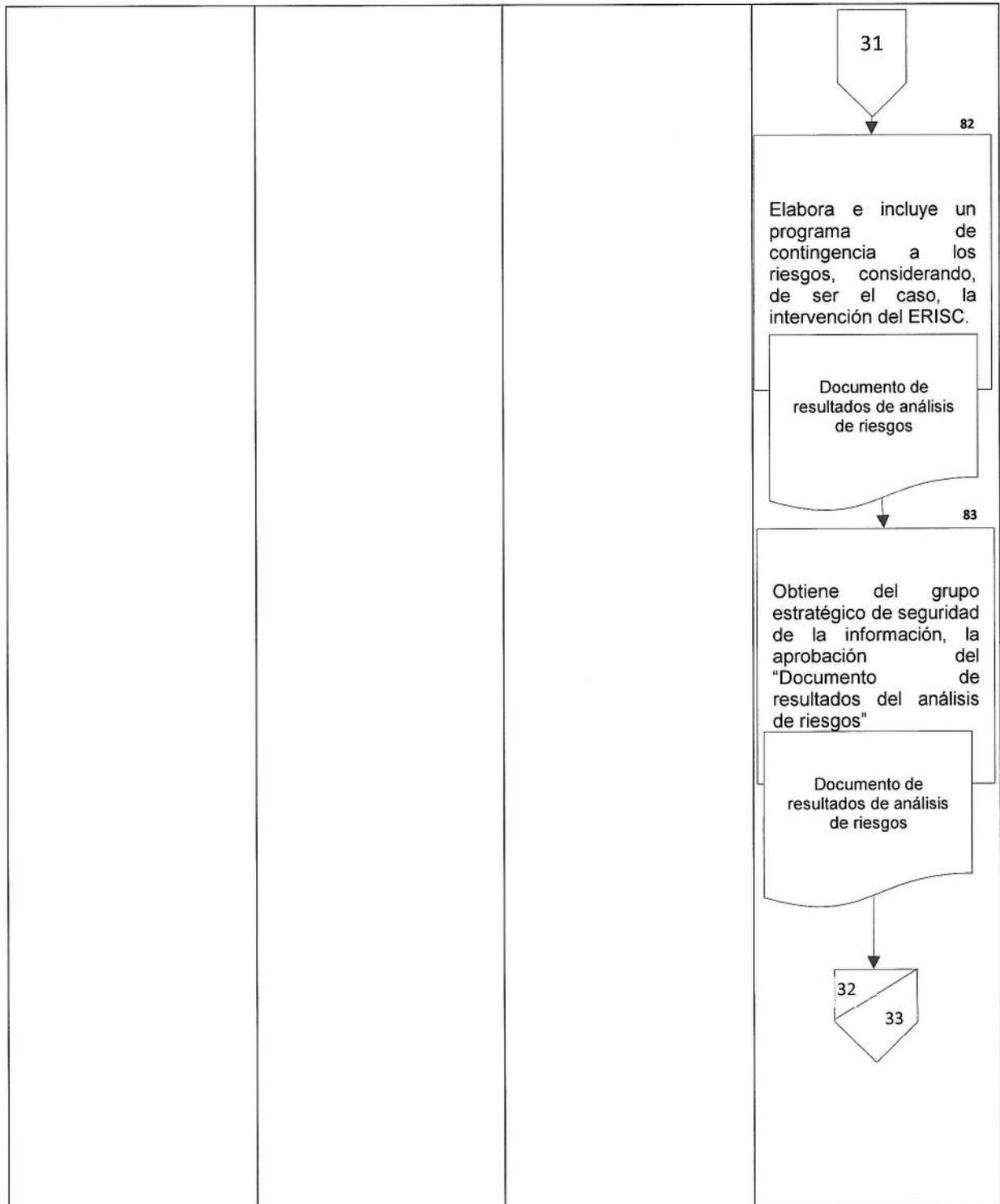
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		Hoja: 53 de 74

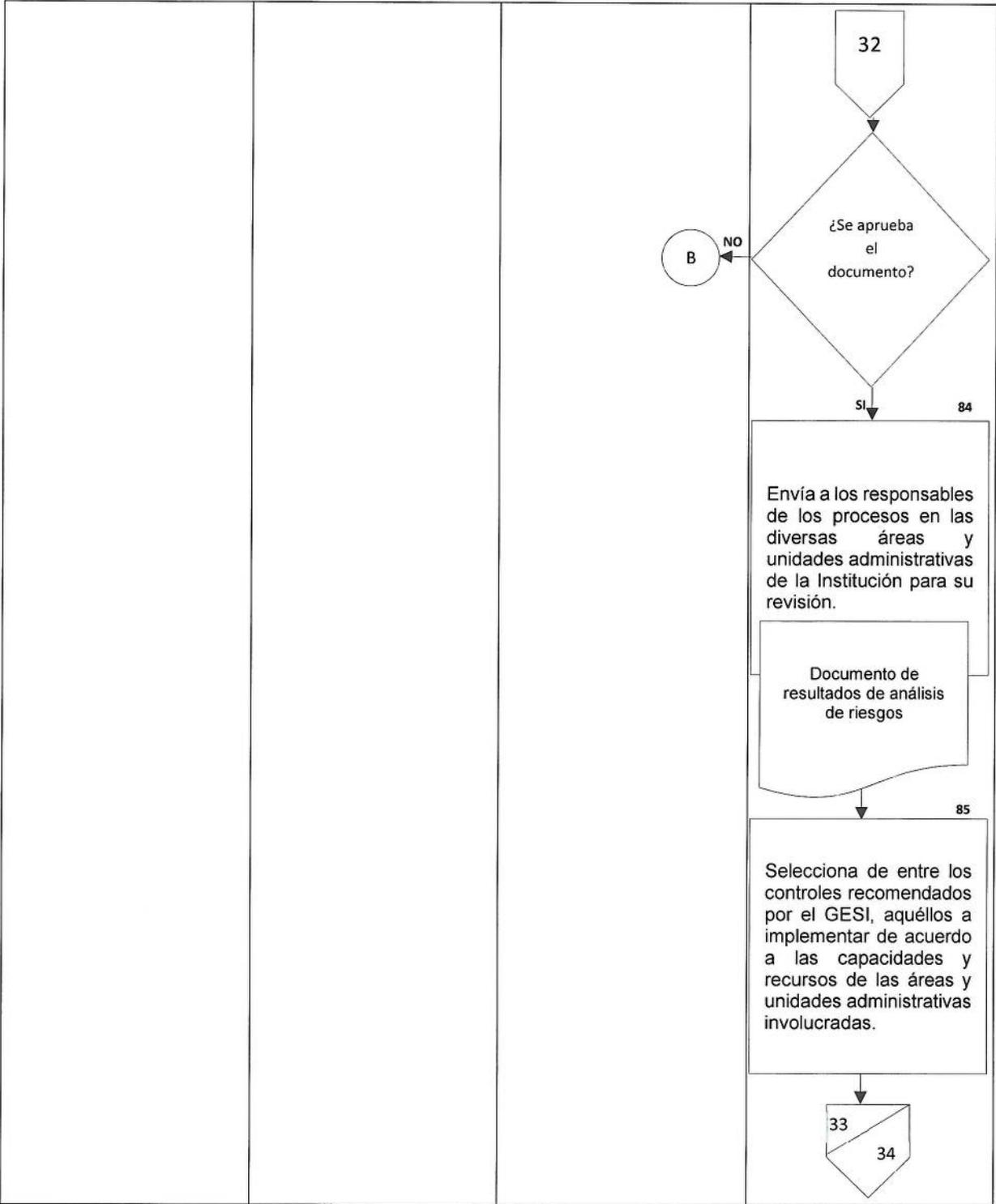


	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		Hoja: 54 de 74

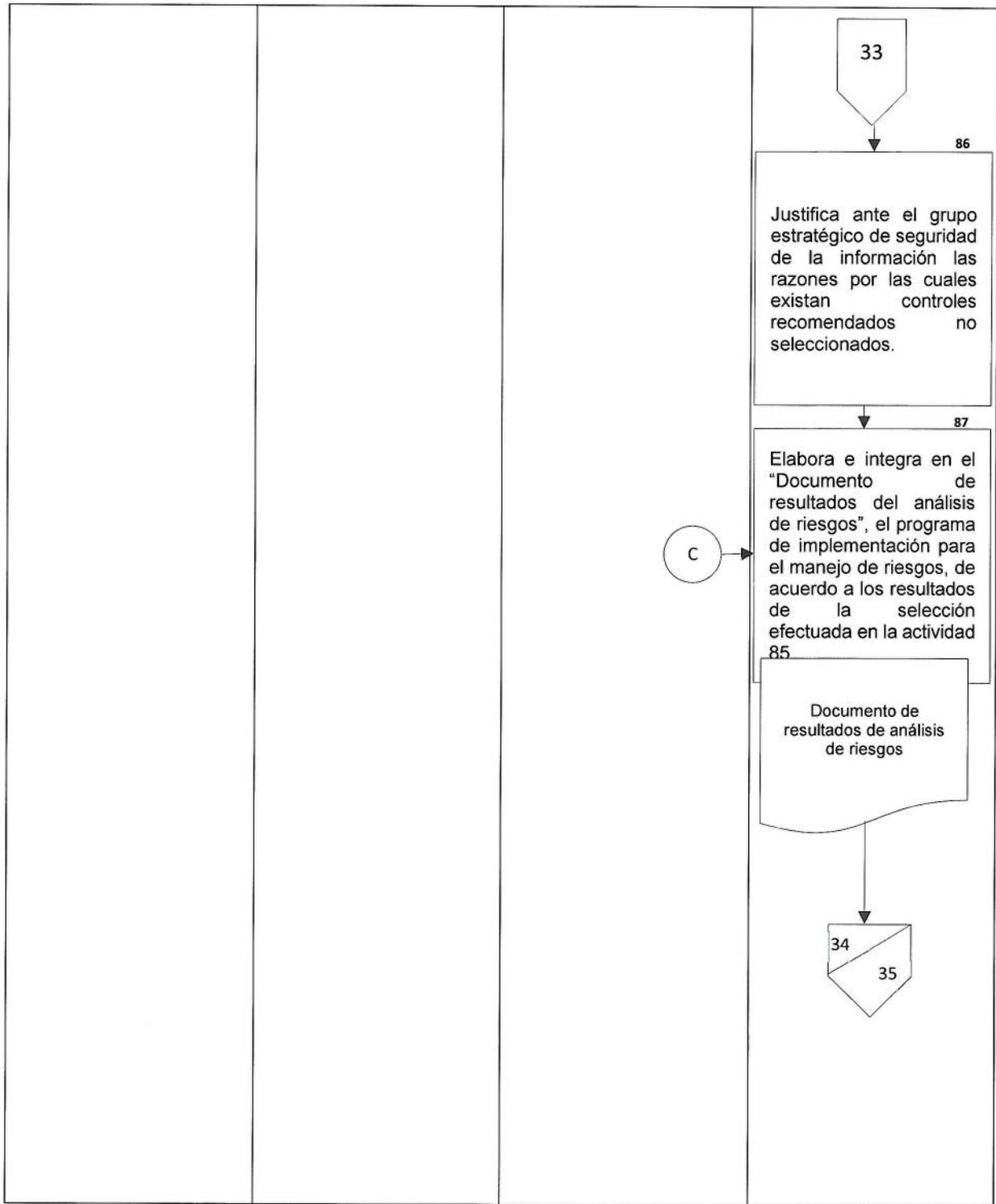


	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		Hoja: 55 de 74

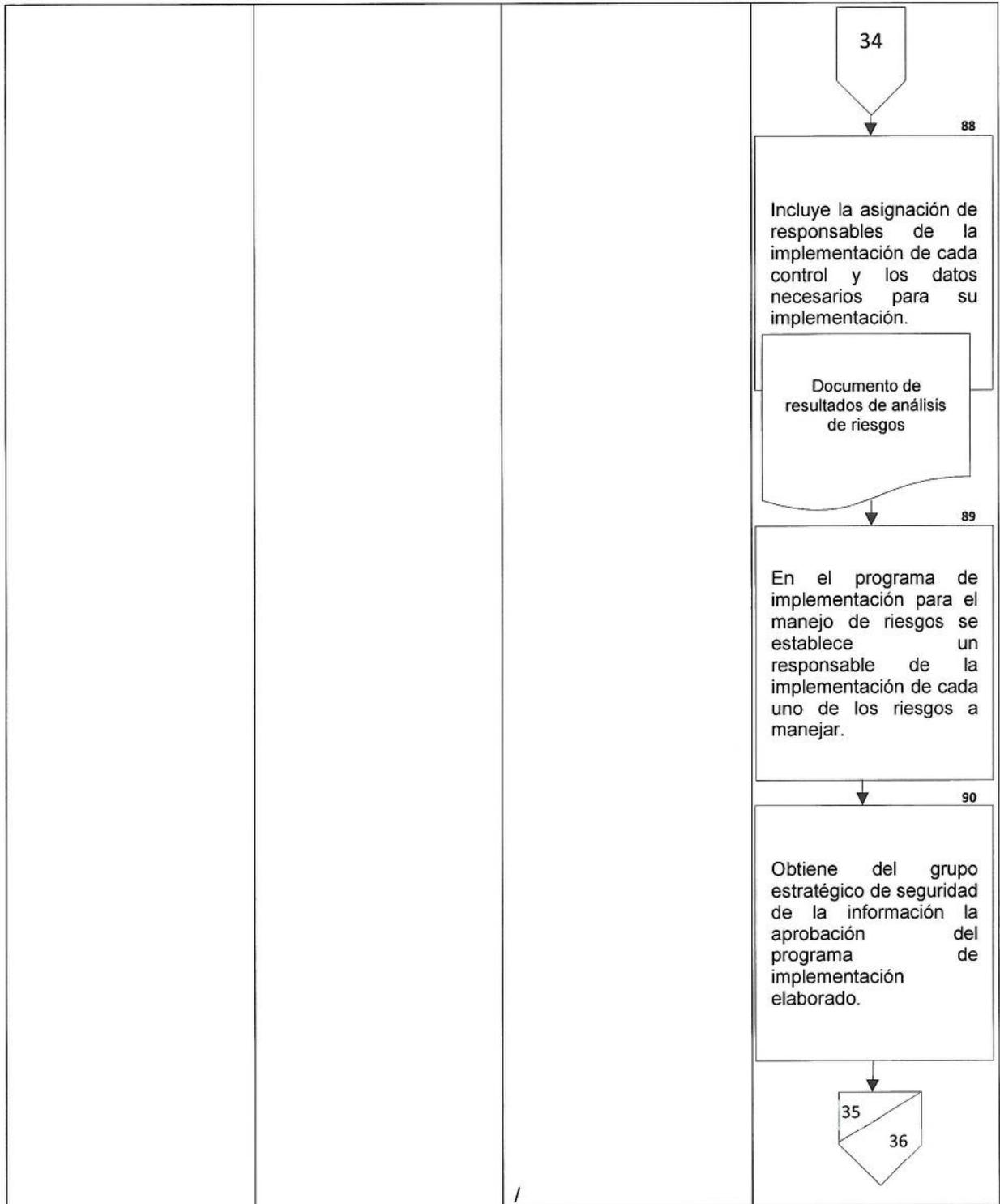




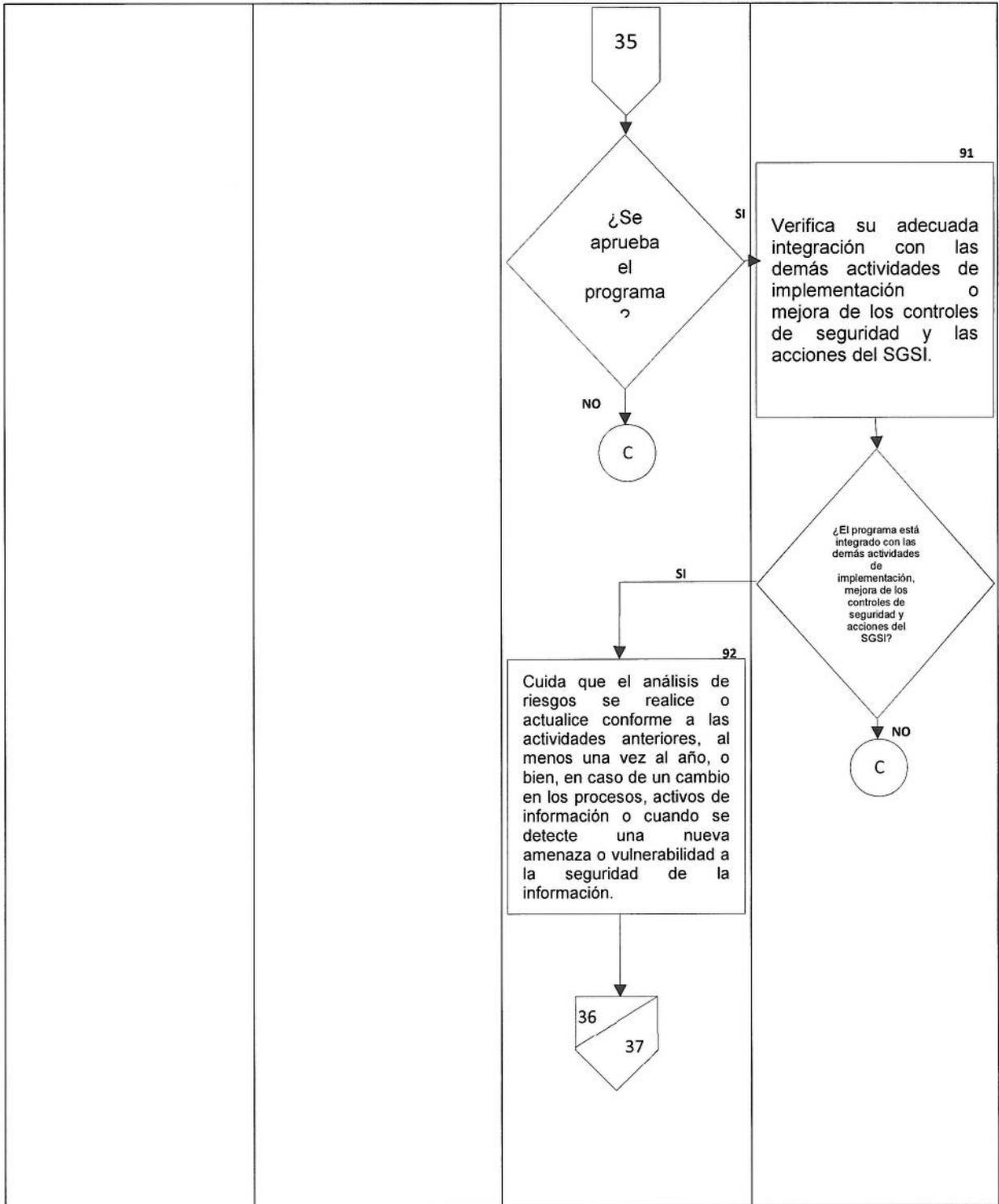
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 57 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



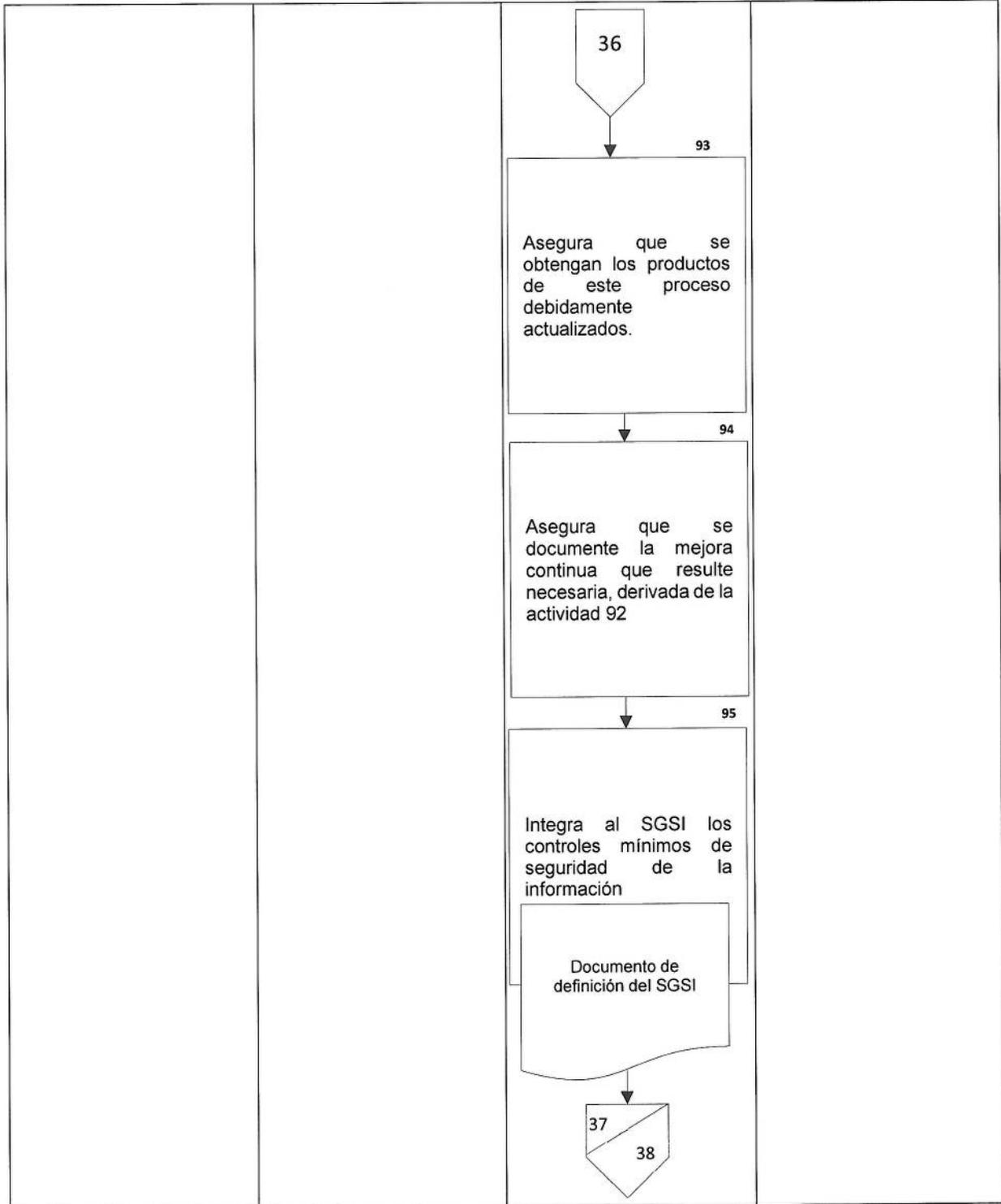
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 58 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



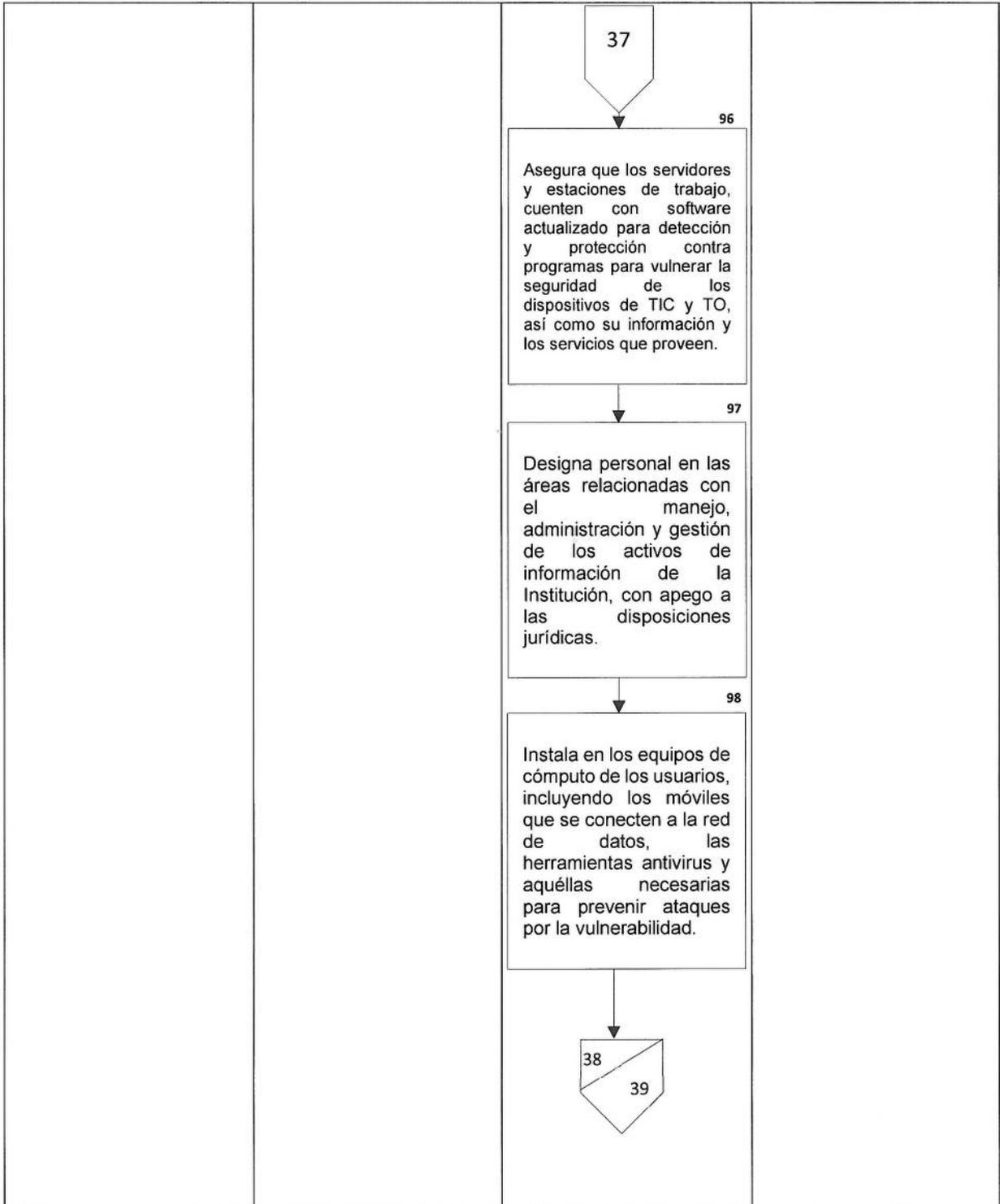
	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO</small> <small>SECRETARÍA DE SALUD</small>	Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 59 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



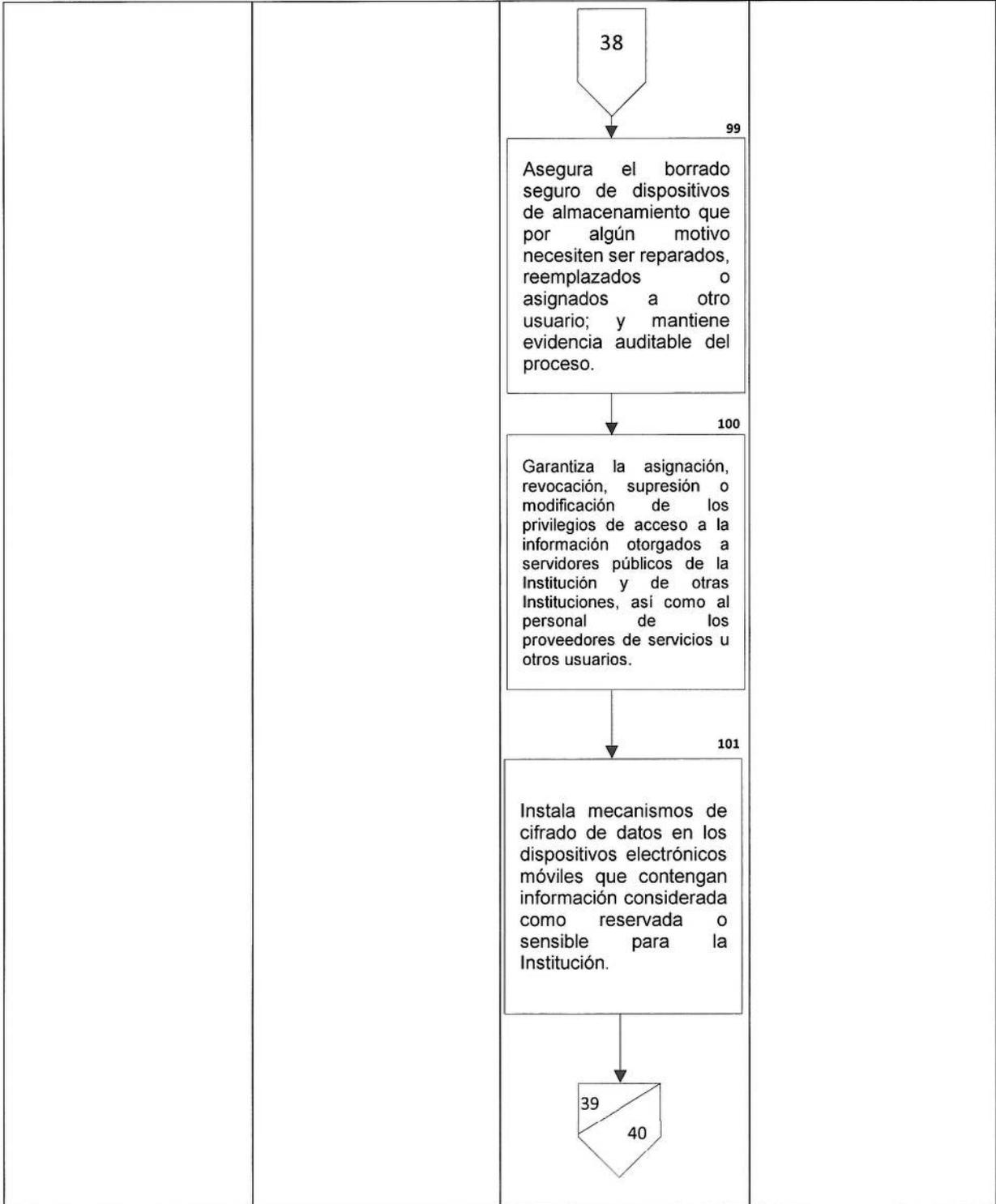
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 60 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



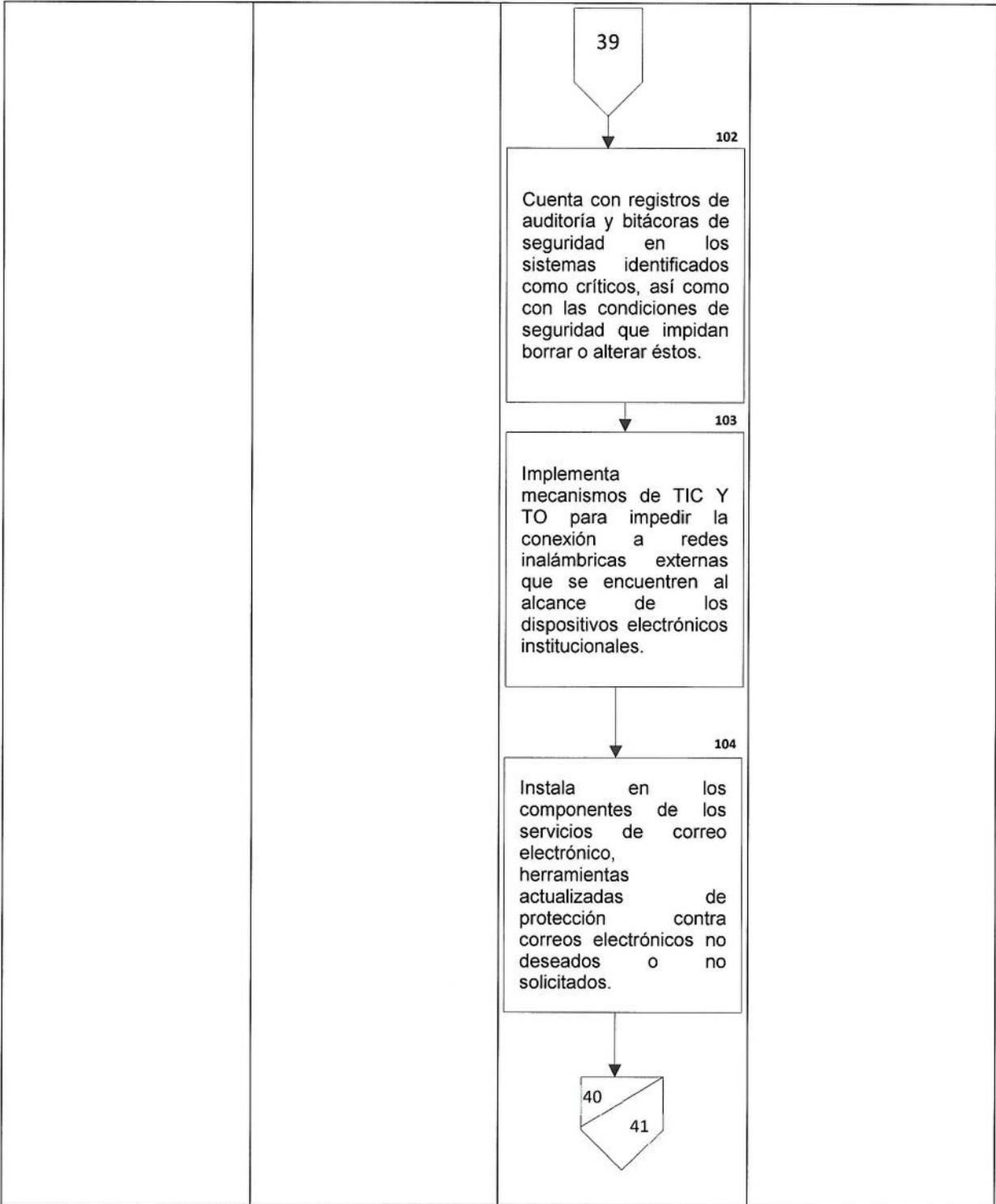
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 61 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



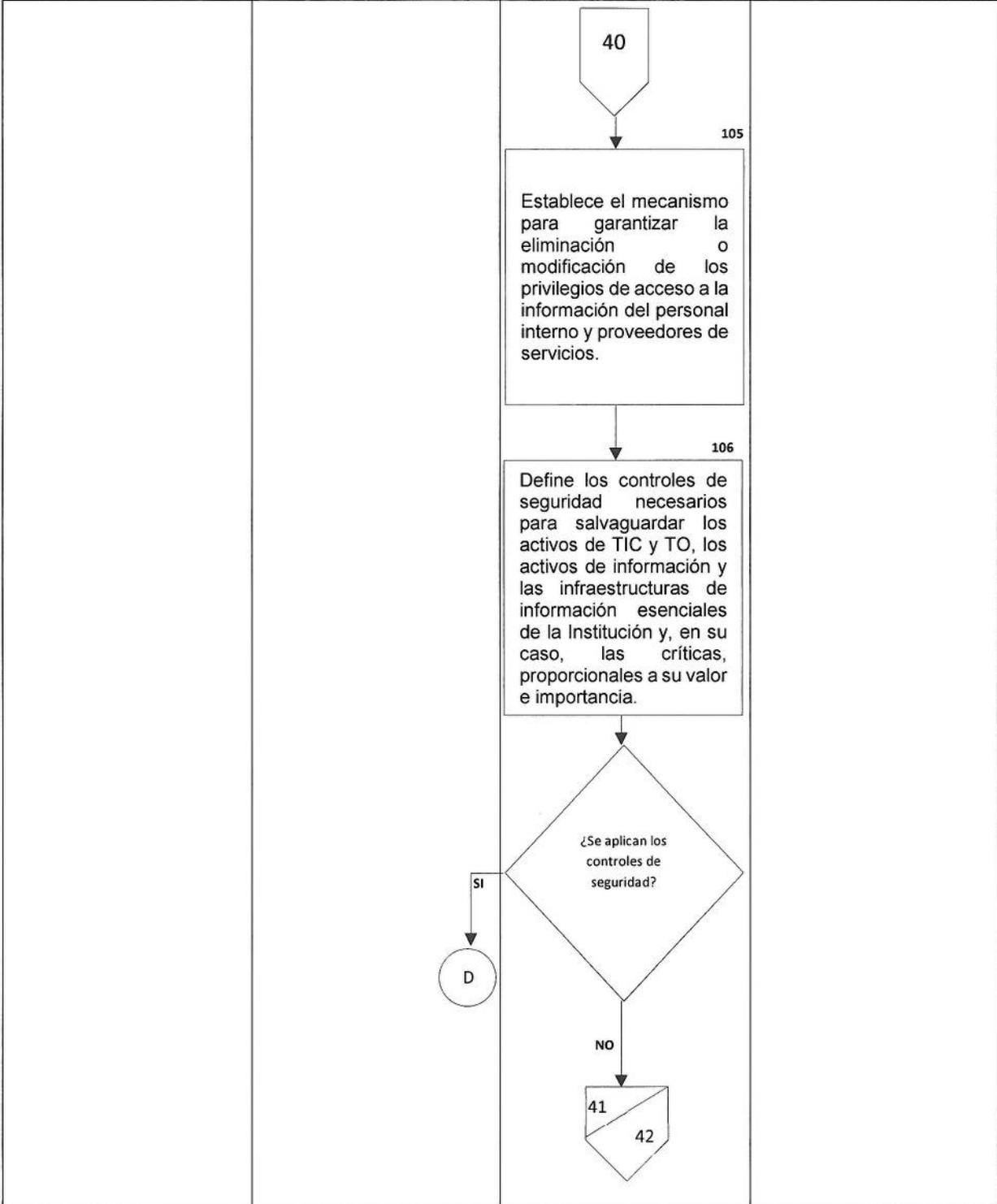
	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>BIRMEX</small> <small>INSTITUTO NACIONAL DE SALUD</small> <small>REACTIVOS DE DIAGNÓSTICO</small> <small>S.A. S.R.L.</small>	Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 62 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



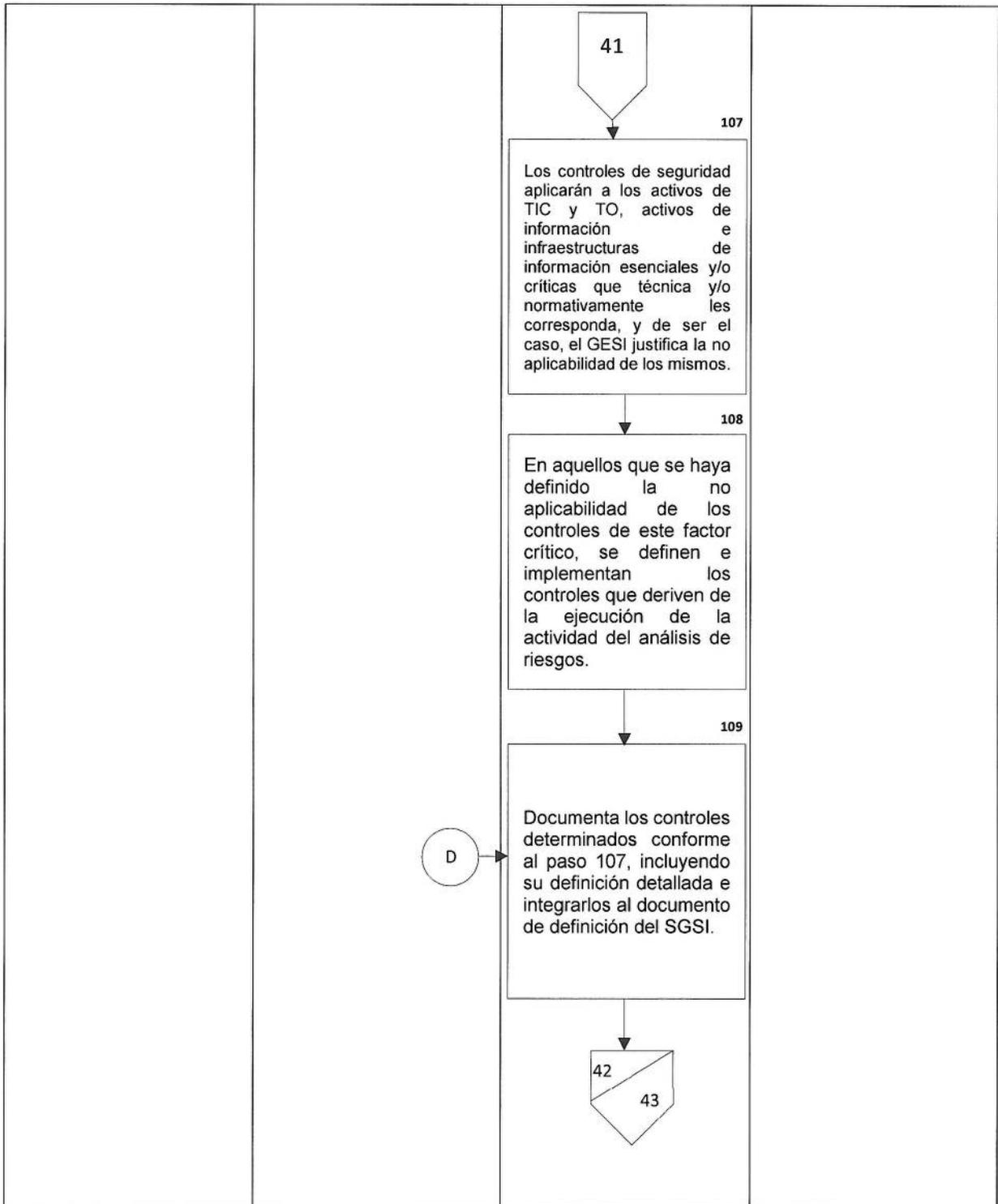
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 63 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		



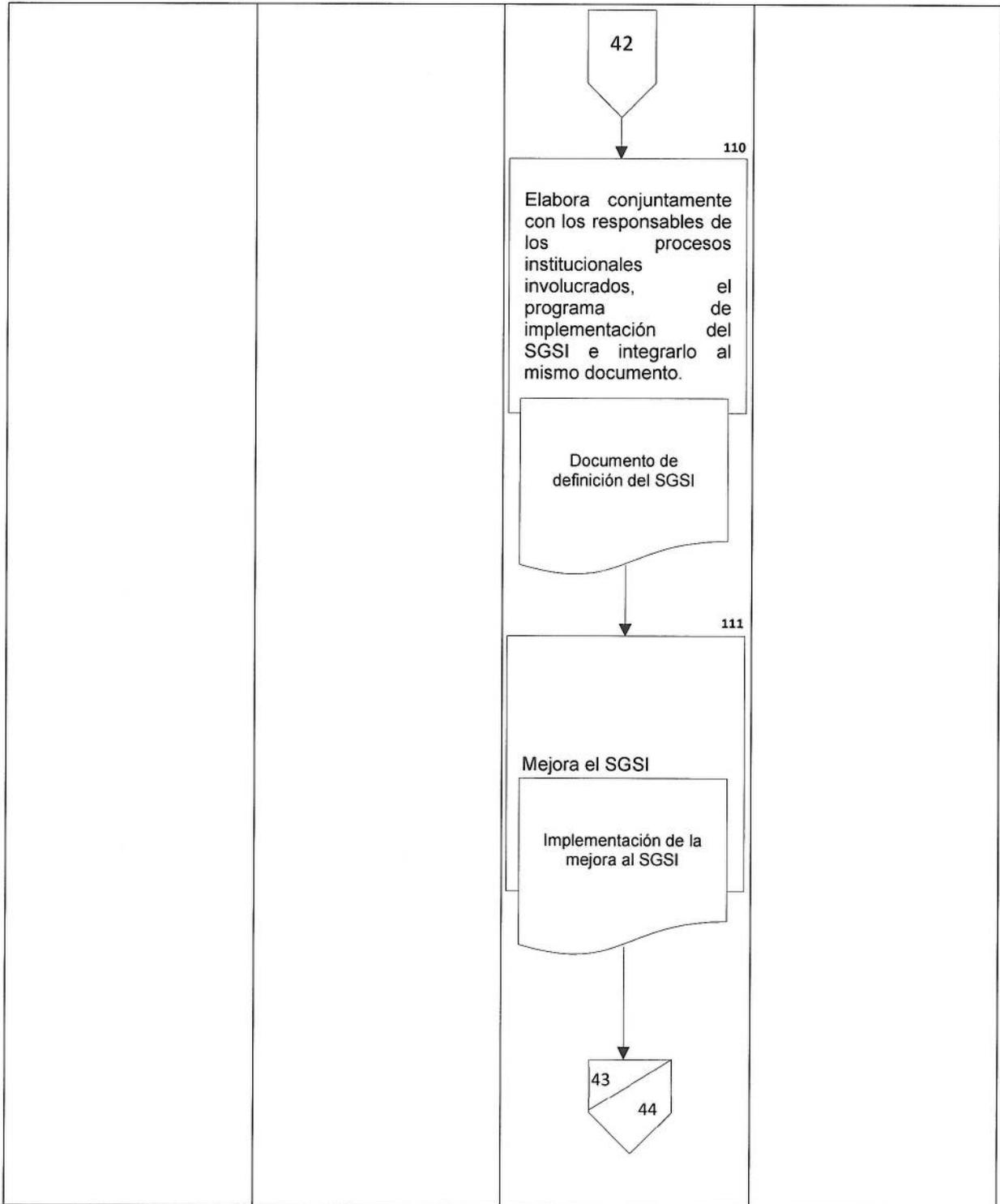
	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>MINISTERIO DE SALUD Y  REACTIVACIÓN MÉXICO  S.A. DE C.V.</small>	Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 64 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



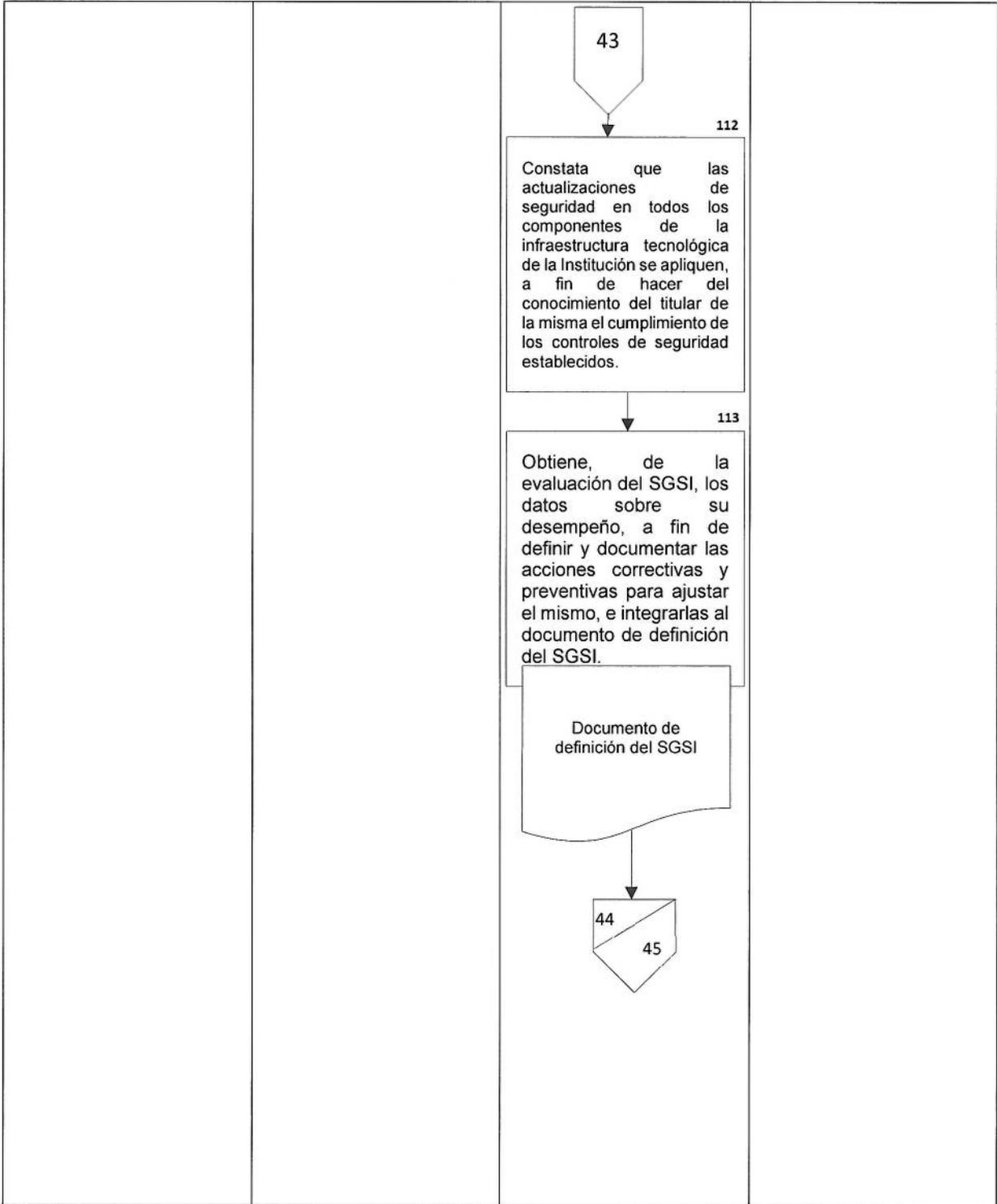
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 65 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



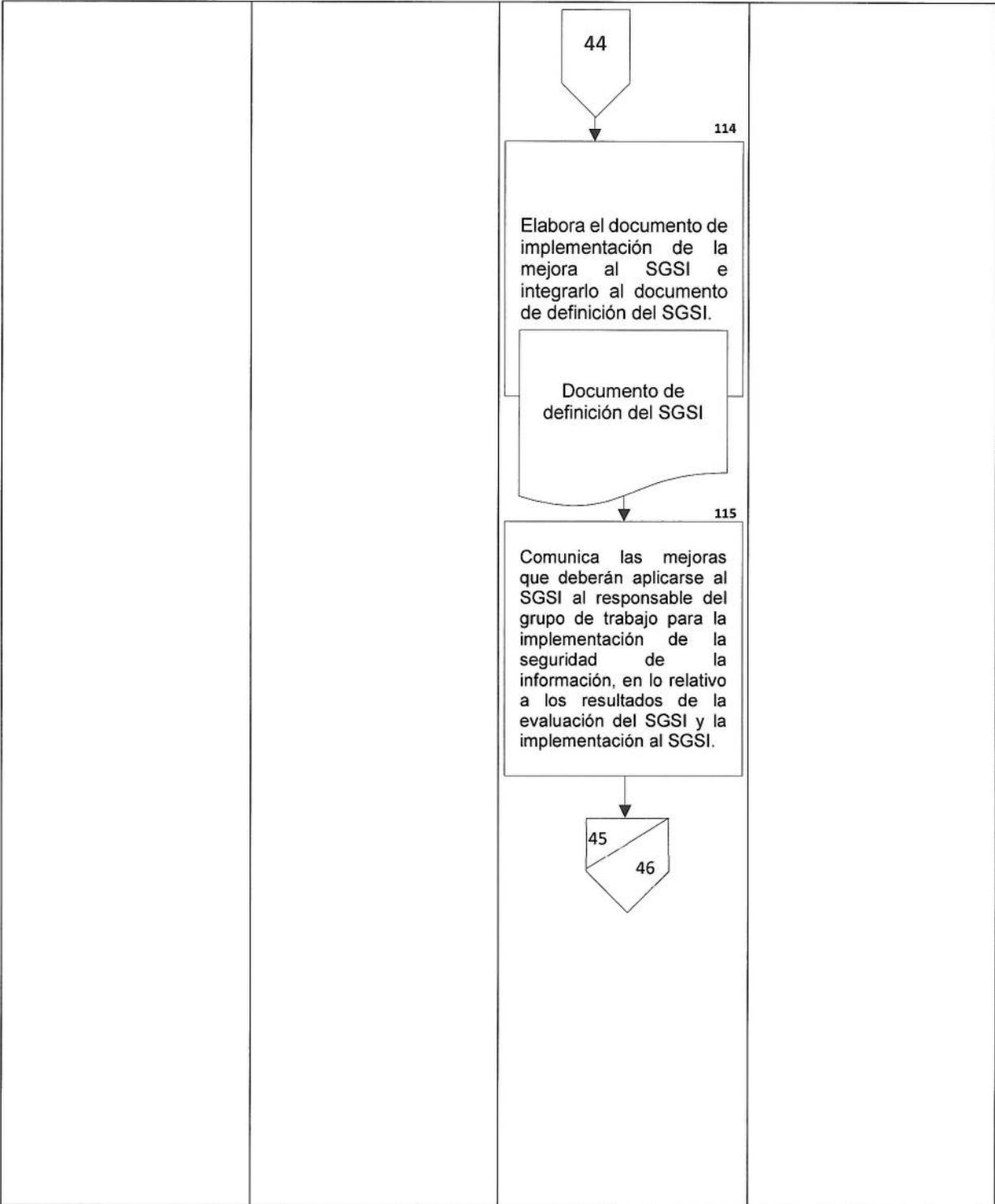
	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>INSTITUTO MEXICANO DE SEGURIDAD Y SALUD SECRETARÍA DE SALUD</small>	Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 66 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



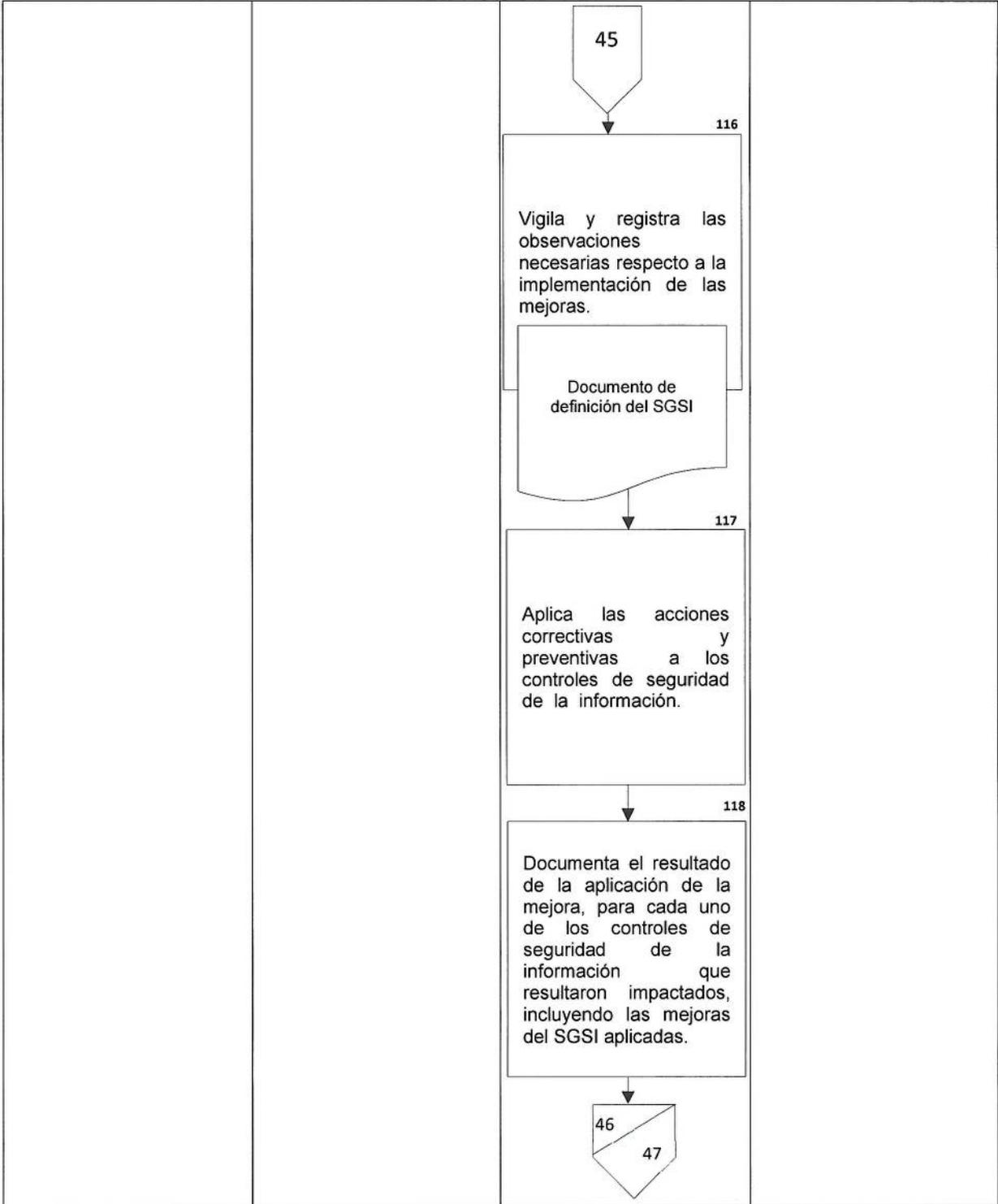
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 67 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



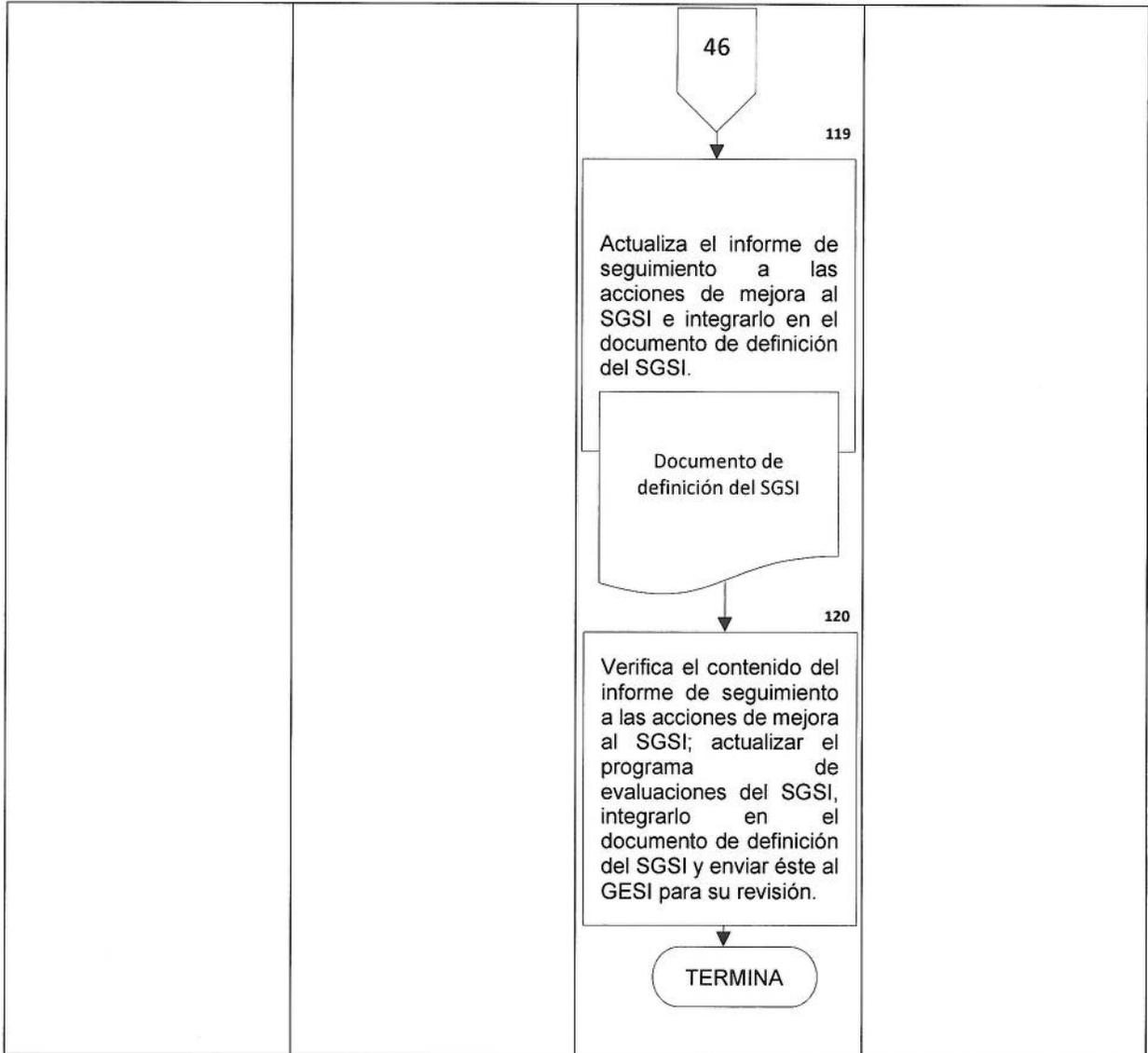
	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>BIRMEX</small> <small>INSTITUTO VENEZOLANO DE SEGURIDAD E INFORMACIÓN</small> <small>S.A. DE C.V.</small>	Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 68 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>BIRMEX</small> <small>COMISIÓN NACIONAL DE SEGURIDAD DE LA INFORMACIÓN</small> <small>SECRETARÍA DE SALUD</small>	Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 69 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 70 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			



	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 71 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

## 6. DOCUMENTOS DE REFERENCIA

Nombre del documento	Código (cuando aplique)
6.1 Ley de la Seguridad Nacional	No aplica
6.2 Reglamento para coordinación de Acciones ejecutivas en materia de Seguridad Nacional	No aplica
6.3 Plan Nacional de desarrollo 2013-2018	No aplica
6.4 Lineamientos para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión.	No aplica
6.5 Documento Técnico de Interoperabilidad de los Sistemas Automatizados de Control de Gestión (DTISACG).	No aplica
6.6 Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.	No aplica

## 7. REGISTROS

Registros	Tiempo de conservación	Responsable de conservarlo	Código de registro o identificación única
Documento de Integración y operación del grupo estratégico e seguridad de la información	1 año	Responsable de la Seguridad de la Información en la Institución	No aplica
Catálogo de infraestructuras críticas	6 meses	El grupo estratégico de Seguridad de la Información (GESI)	No aplica
Documento de resultados de análisis de riesgos	6 meses	Equipo de trabajo de análisis de riesgos con apoyo de las unidades administrativas involucradas	No aplica
Documento de definición del SGSI	6 meses	El grupo estratégico de Seguridad de la Información (GESI)	No aplica
Propuesta Capacitación, conceptos e importancia de la Seguridad de la Información	6 meses	Responsable de la seguridad de la información en la institución	No aplica
Intento de violaciones e incidentes de seguridad	6 meses	Responsable de la supervisión de la implementación de los controles de seguridad de la información y manejo de riesgos.	No aplica
Relación de elementos que se pretenden proteger	6 meses	Equipo de trabajo de análisis de riesgos con apoyo de las unidades administrativas involucradas	No aplica

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 72 de 74
<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>			

## 8. GLOSARIO DEL PROCEDIMIENTO

- 8.1 Activos de TIC:** los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos;
- 8.2 ACNF:** proceso de administración de la configuración;
- 8.3 ADP:** proceso de administración de proyectos;
- 8.4 ADS:** proceso de administración de servicios;
- 8.5 APCT:** proceso de administración del presupuesto y las contrataciones;
- 8.6 Aplicativo de Cómputo:** el software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo a requerimientos previamente definidos;
- 8.7 APRO:** proceso de administración de proveedores;
- 8.8 Arquitectura Empresarial:** la información del estado actual y futuro de una Institución, a partir del análisis con perspectiva estratégica; considerando modelos de negocio, procesos, aplicativos y tecnologías de la información y comunicaciones;
- 8.9 Arquitectura Orientada a Servicios:** la metodología y marco de trabajo, para construir componentes de software reutilizables para la interoperabilidad de aplicativos de cómputo;
- 8.10 AOP:** proceso de administración de la operación;
- 8.11 ASI:** proceso de administración de la seguridad de la Información.
- 8.12 Borrado Seguro:** el proceso mediante el cual se elimina de manera permanente y de forma irre recuperable la información contenida en medios de almacenamiento digital;
- 8.13 Cartera Ejecutiva de Proyectos de TIC:** Conjunto total de proyectos de TIC que la institución propondrá a la Unidad para su seguimiento;
- 8.14 Cartera Operativa de Proyectos de TIC:** Conjunto total de proyectos que soportan la operación diaria de la DTI y no son considerados como estratégicos;
- 8.15 Centro de Datos:** el lugar físico en los que se ubiquen los activos de TIC y desde el que se proveen servicios de TIC;
- 8.16 Cómputo en la Nube:** al modelo de prestación de servicios digitales que permite a las Instituciones acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios;
- 8.17 CMDB:** Base de Datos de la Gestión de la Configuración.
- 8.18 Dependencias:** las Secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como a la Oficina de la Presidencia de la República y la Procuraduría General de la República; así como los Órganos Reguladores Coordinados en Materia Energética;
- 8.19 Dominio Tecnológico:** las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo;
- 8.20 EDN:** la Estrategia Digital Nacional contenida en el Objetivo número 5 del Programa;
- 8.21 EIDA:** el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, establecido mediante Acuerdo publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011;
- 8.22 Entidades:** los organismos descentralizados, empresas de participación estatal mayoritaria, instituciones nacionales de crédito, organizaciones auxiliares nacionales de crédito e instituciones nacionales de seguros y de fianzas, y fideicomisos públicos que en términos de la Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales, sean considerados entidades de la Administración Pública Federal Paraestatal;
- 8.23 ERISC:** equipo de respuesta a incidentes de seguridad en TIC en la Institución;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b> <b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		Hoja: 73 de 74

- 8.24 Estándar abierto:** a las especificaciones cuya utilización esté disponible de manera gratuita o que no suponga una dificultad de acceso, y que su uso y aplicación no esté condicionada al pago de un derecho de propiedad
- 8.25 Herramienta de Gestión de la Política TIC:** sistema web usado para llevar a cabo la comunicación de actividades de reporte establecidas en el Acuerdo, considerando el reporte de PETIC, la obtención del dictamen técnico que emite la Unidad, autorización por parte de la UPCP, la arquitectura empresarial, el MAAGTICSI, entre otros;
- 8.26 Infraestructuras Críticas de Información:** Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia.
- 8.27 Infraestructuras de Información esenciales:** Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de información, TIC y TO, cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación de las Instituciones.
- 8.28 Infraestructura de TIC:** el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC;
- 8.29 Infraestructura Pasiva:** elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de las dependencias o entidades, que sean necesarios para la instalación y operación de las redes, así como para la prestación de servicios de procesamiento de datos, de telecomunicaciones y radiodifusión;
- 8.30 Instancias de Seguridad Nacional:** las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquellas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional;
- 8.31 Institución:** las dependencias y entidades de la Administración Pública Federal, tal y como se definen en este Acuerdo;
- 8.32 Lineamientos:** los Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicados en el Diario Oficial de la Federación el 30 de enero de 2013;
- 8.33 MAAGMAASSP:** el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público;
- 8.34 MAAGTICSI:** el Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información. Anexo Único del presente Acuerdo;
- 8.35 Niveles de servicio:** el establecimiento en un lenguaje no técnico del servicio brindado, incluyendo al menos la definición, disponibilidad, calidad, tiempos de respuesta y solución.
- 8.36 OPEC:** proceso de operación de los controles de seguridad de la información y del erisc;
- 8.37 PE:** proceso de planeación estratégica;
- 8.38 PETIC:** el conjunto de proyectos que elaboran las Instituciones, conformado por un máximo de 7 proyectos estratégicos, en los términos establecidos en el presente Acuerdo;
- 8.39 Portafolio de proyectos de TIC:** es el total de los proyectos de TIC agrupados según su clasificación en Cartera Ejecutiva de Proyectos de TIC y Cartera Operativa de Proyectos de TIC que la Institución planea desarrollar, en los términos establecidos por el MAAGTICSI;
- 8.40 Programa:** el Programa para un Gobierno Cercano y Moderno 2013-2018, aprobado mediante Decreto publicado en el Diario Oficial de la Federación el 30 de agosto de 2013;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 74 de 74
	<b>5. Procedimiento para la Administración de la Seguridad de la Información.</b>		

- 8.41 Proyectos de TIC:** el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC y que cuenta con presupuesto para su ejecución; considerando 2 tipos: proyectos operativos que soportan las actividades diarias de la DTI y proyectos estratégicos en los términos señalados en el presente Acuerdo;
- 8.42 Retos Públicos:** el modelo que fomenta la democratización del gasto público y la innovación, invitando a los emprendedores del país a plantear soluciones a retos de gobierno mediante el desarrollo de aplicativos tecnológicos web y móviles;
- 8.43 SEGOB:** la Secretaría de Gobernación;
- 8.44 Seguridad de la información:** la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma;
- 8.45 Seguridad Nacional:** las acciones a las que se refiere el artículo 3 de la Ley de Seguridad Nacional;
- 8.46 SGSI:** El sistema de gestión de seguridad de la información que, por medio del análisis de riesgos y de la definición de controles, define las guías para la implementación, operación, monitoreo, revisión y mejora de la seguridad de la información;
- 8.47 SFP:** la Secretaría de la Función Pública;
- 8.48 SHCP:** la Secretaría de Hacienda y Crédito Público;
- 8.49 Tecnologías Verdes:** el conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las tecnologías de la información y comunicaciones, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías;
- 8.50 TIC:** las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video;
- 8.51 Unidad:** la Unidad de Gobierno Digital de la SFP;
- 8.52 DTIC:** la Dirección de Tecnologías de Información y Comunicaciones o área responsables de las TIC en la Institución

## 9. CAMBIOS DE VERSIÓN DEL PROCEDIMIENTO

Numero de revisión	Fecha de actualización	Descripción del cambio
0	No aplica	No aplica

## 10. ANEXOS DEL PROCEDIMIENTO

No aplica

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 1 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

## 1. PROPÓSITO

Establecer la funcionalidad del proceso de Administración de Proyectos, derivado del Manual Administrativo de Aplicación General en Materias de Tecnología de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), mediante la asignación de los roles identificados en el proceso y sus subprocesos, formalizando la asignación del rol a los responsables que participan en la ejecución de cada una de las tareas del proceso, con el fin de obtener la información, evidencias y entregables que generen las actividades ejecutadas durante el proceso.

## 2. ALCANCE

- 2.1 Obtener el mapa del proceso y de las actividades de los subprocesos involucrados, que permitan identificar la funcionalidad del proceso ADP.
- 2.2 Identificar los roles o los actores que se requieren para que el proceso genere las evidencias y entregables que demuestren la funcionalidad del proceso.
- 2.3 Identificar a las áreas o personas que se harán responsables de los diferentes roles que requiere el proceso.
- 2.4 Formalizar las asignaciones de responsables de roles y actividades.
- 2.5 Establecer si es necesario entre las áreas identificadas que participarán con alguna responsabilidad en el proceso un OLA, acuerdo de operación, en el cual se especifiquen los servicios que se aportarán y los tiempos en los que se atenderán y los entregables comprometidos que requiere el proceso.
- 2.6 Identificar las capacitaciones que se requieran en las diferentes áreas o personas que asuman el rol asignado, para que se consideren en un programa de capacitación.
- 2.7 Identificar los indicadores de desempeño del proceso y registrarlos periódicamente para su evaluación posterior.
- 2.8 Identificar los indicadores de los servicios considerados y sus métricas.

## 3. POLÍTICAS DE OPERACIÓN, NORMAS Y LINEAMIENTOS

- 3.1 El responsable de este proceso es el administrador de la Cartera Operativa de Proyectos de TIC.
- 3.2 El administrador de la Cartera Operativa de Proyectos de TIC designará, para cada proyecto que se autorice, al administrador de proyecto o responsable, solicitando para ello autorización al titular de la DTI.
- 3.3 Los administradores del proyecto deberán asegurarse de que todos los proyectos que administren cuenten al menos con su documento de planeación del proyecto, así como los documentos de planeación subsidiarios, desde su inicio hasta su cierre, y de que éste se actualice en tiempo y forma de acuerdo a los avances de los proyectos hasta su cierre.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b> <b>6. Procedimiento para la Administración de Proyectos.</b>		Hoja: 2 de 20

3.4 Los administradores de proyecto deben asegurarse que cualquier cambio a un proyecto que administren se realice mediante una solicitud de cambio autorizada por los involucrados.

3.5 Los responsables de proyecto deberán asegurarse que las metodologías y/o mejores prácticas que se adopten para los diversos tipos de proyectos, se documenten para cada uno de los proyectos que desarrollen en la DTI.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 3 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

#### 4. DESCRIPCIÓN DEL PROCEDIMIENTO

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director de Tecnologías de la Información (Grupo de trabajo para la dirección de TIC)	1	Autoriza la fijación de prioridades de la Cartera Operativa de Proyectos de TIC.	
	2	Confirma la asignación de presupuesto estimado para cada uno de los proyectos que integran la Cartera.	
	3	Verifica la alineación de las inversiones en proyectos de TIC con las necesidades, objetivos de la Institución y elementos de Arquitectura Empresarial que apliquen.	
	4	Autoriza la suspensión, cambios, cierre o cancelación de proyectos de TIC o la reasignación de recursos entre proyectos pertenecientes a la Cartera Operativa de Proyectos de TIC.	
	5	Toma acuerdos respecto a la gobernabilidad del portafolio de proyectos de TIC que sea presentado al titular de la DTI	
Departamento de Informática (Soporte Administrativo DTI)	6	Integra la Cartera Operativa de Proyectos de TIC, definiendo los proyectos de TIC que contendrán e identificar los proyectos que se administrarán individualmente.	Cartera Operativa de Proyectos TIC
	7	Prioriza y equilibrar la Cartera Operativa de Proyectos de TIC, a efecto de optimizar el uso de los recursos.	
	8	Da seguimiento a la Cartera Operativa de Proyectos de TIC y difundirla, a fin de prever riesgos y desviaciones.	
Director de Tecnologías de la Información	9	Presenta la Cartera Operativa de Proyectos de TIC al grupo de trabajo para la dirección de TIC, para su aprobación y autorizaciones procedentes.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 4 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Departamento de Informática (Soporte Administrativo DTI)	10	<p>Evalua los proyectos e iniciativas pertenecientes a la Cartera Operativa de Proyectos de TIC que serán propuestas al grupo de trabajo para la dirección de TIC para su priorización y, en su caso, autorización. Para llevar a cabo la evaluación deberá considerar, cuando menos, los análisis relativos a:</p> <p>a) Las funciones sustantivas que sustentan la iniciativa o proyecto de TIC.</p> <p>b) La capacidad de recursos humanos.</p> <p>c) La capacidad financiera y/o presupuestaria.</p> <p>d) La capacidad de activos e infraestructura de TIC.</p>	Cartera Operativa de Proyectos TIC
	11	Establece y mantiene actualizada la Cartera Operativa de Proyectos de TIC.	
	12	Mantiene el equilibrio de los recursos, mediante la revisión a los informes de rendimiento de las Cartera Operativa de Proyectos de TIC y de ser el caso, sugerir al grupo de trabajo para la dirección de TIC, un cambio de prioridad o la continuación, suspensión o cancelación de iniciativas, o de proyectos de TIC	
	13	Somete a la autorización del grupo de trabajo para la dirección de TIC, los ajustes la Cartera Operativa de Proyectos de TIC y preparar las justificaciones de cada ajuste.	
	14	Designa responsables para cada iniciativa, o proyecto operativo de TIC, autorizado.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 5 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

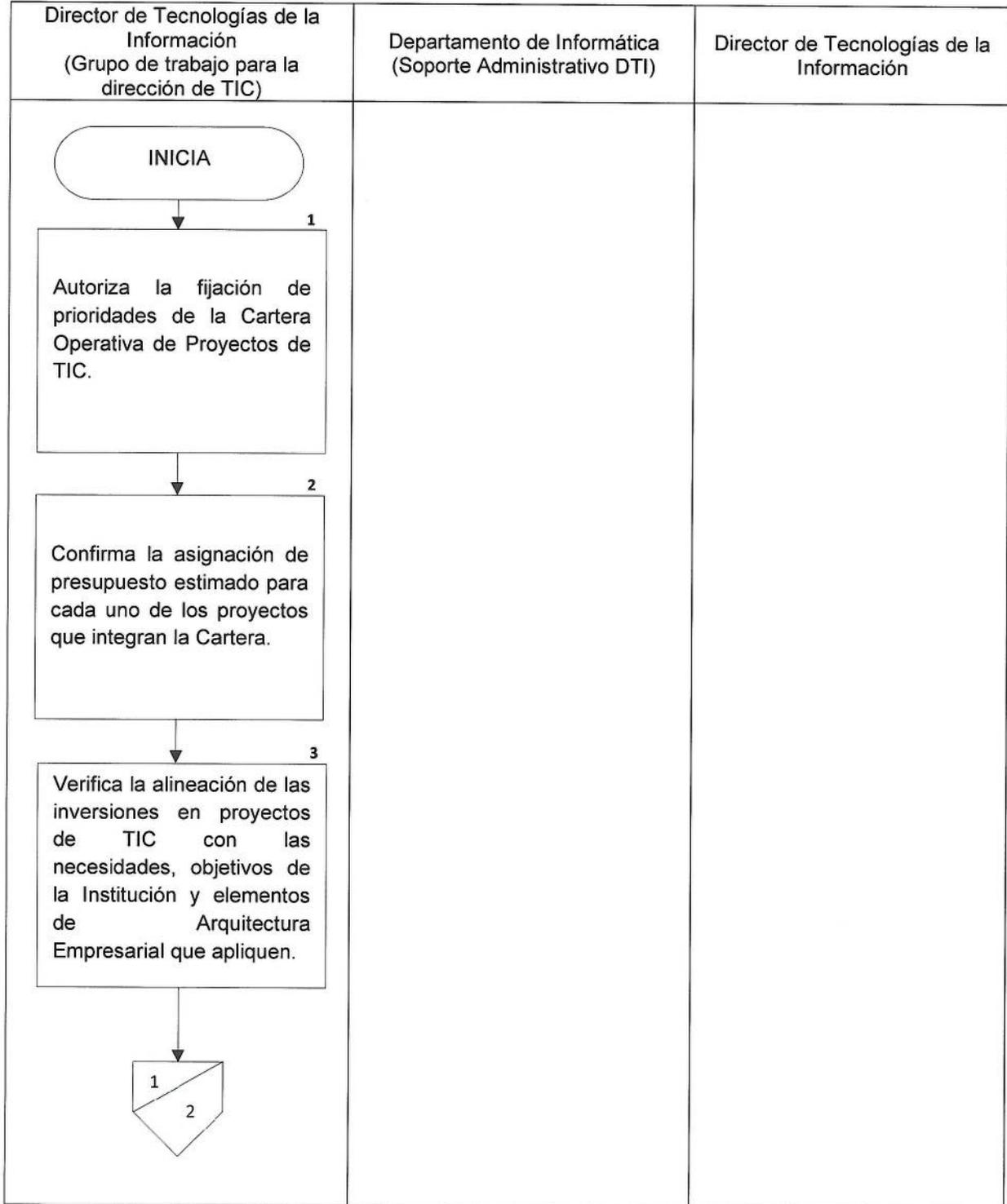
Responsable	No. Act.	Descripción de actividades	Documento o anexo
Departamento de Informática (Soporte Administrativo DTI)	15	Genera con la información recopilada de las actividades de este proceso el documento de planeación y acta de constitución del proyecto para su registro.	Acta de Constitución del Proyecto  Acta de Aceptación de Entregables
	16	Actualiza el tablero de control de proyectos de TIC y difundirlo.	Tablero de Control de Proyectos
	17	Determina los proyectos que integrarán la Cartera de Operativa de Proyectos de TIC y elaborar su justificación.	
	18	Elabora un cronograma ejecutivo para la Cartera de TIC, que muestre la duración y las fechas de inicio y fin de cada proyecto, e incluya hitos de control y riesgos potenciales.	Cronograma Ejecutivo para la Cartera de TIC
	19	Se asegura de que se cuente con las asignaciones y autorizaciones necesarias para el inicio de un programa de proyectos de TIC y sus proyectos.	
	20	Da seguimiento a la Cartera de Operativa de Proyectos de TIC, desde su inicio y hasta su conclusión, cambios controlados, incidentes o riesgos que se materialicen.	
	21	Elabora el análisis comparativo entre el avance real y el planeado.	Cronograma Ejecutivo para la Cartera de TIC
	22	Actualiza el tablero de control de proyectos, de manera que permita identificar niveles críticos y apoyar la definición de acciones correctivas a la estrategia del programa de proyectos.	Tablero de Control de Proyectos

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 6 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

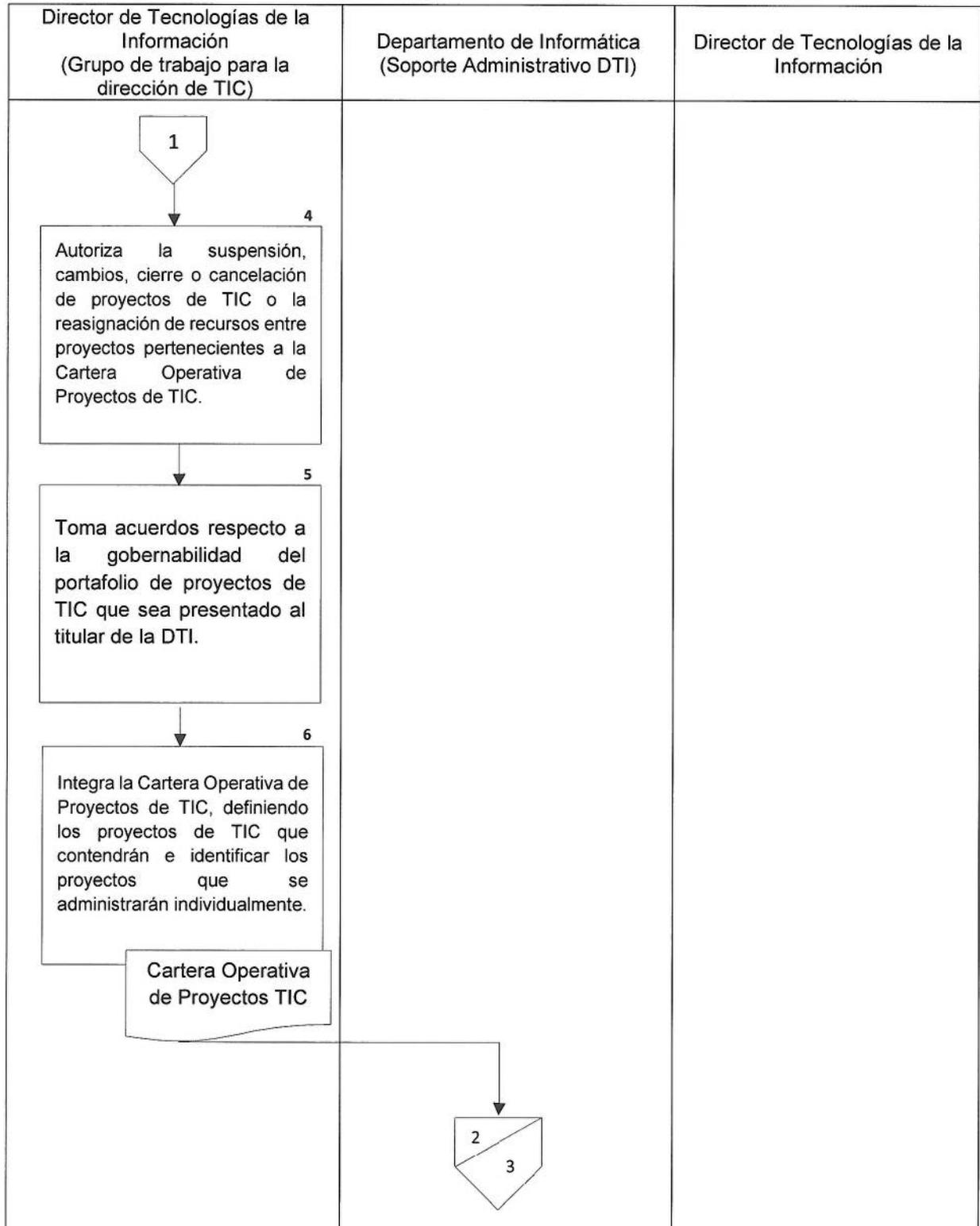
Responsable	No. Act.	Descripción de actividades	Documento o anexo
Departamento de Informática (Soporte Administrativo DTI)	23	Verifica y evalúa de manera continua el estado que guarda cada uno de los proyectos de TIC, de acuerdo a sus hitos y puntos de control, para determinar su contribución al Portafolio de proyectos de TIC y actualizar el tablero de control de proyectos.	Tablero de Control de Proyectos
	24	Mantiene permanentemente informado al grupo de trabajo para la dirección de TIC, por medio del tablero de control de proyectos de TIC, el cual deberá contener, al menos, la información sintetizada del avance de la Cartera Operativa de Proyectos de TIC, el resultado de los indicadores del desempeño de la Cartera Operativa de Proyectos y, en su caso, de las eventualidades o riesgos que se hayan presentado.	
	25	Revisa los resultados y la documentación de los programas de proyectos y de los proyectos de TIC asociados a la iniciativa de TIC que se pretenda cerrar.	Acta de Cierre de Proyecto
	26	Preserva y mantiene disponible la información del desarrollo de cada proyecto perteneciente a la Cartera Operativa de proyectos de TIC.	
	27	Concluye las iniciativas y proyectos de TIC, mediante la elaboración y presentación de un informe final que contenga la evaluación de los resultados y los beneficios obtenidos.	Informe final de evaluación de resultados y beneficios obtenidos
		TERMINA	

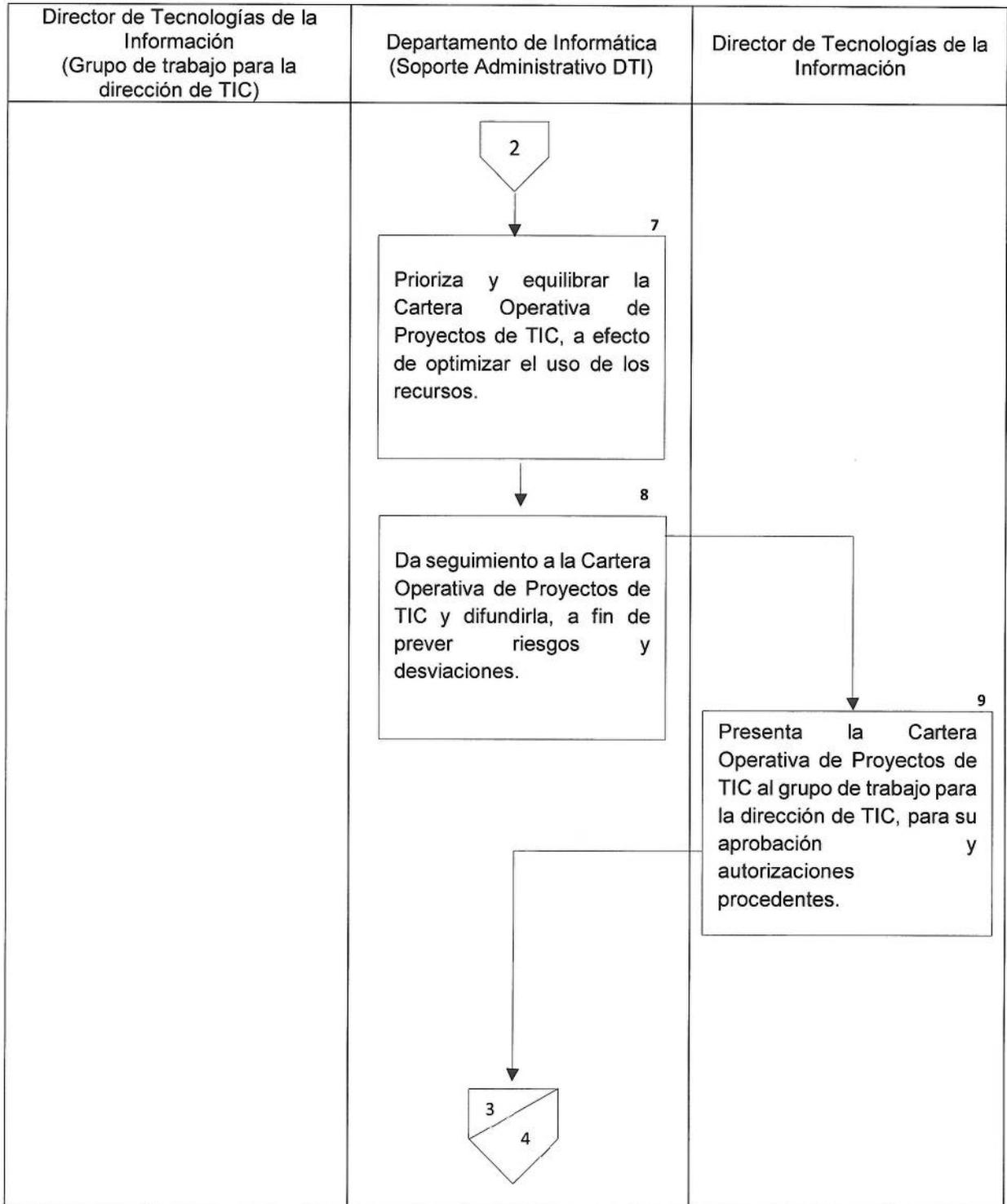
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 7 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

## 5. DIAGRAMA DE FLUJO

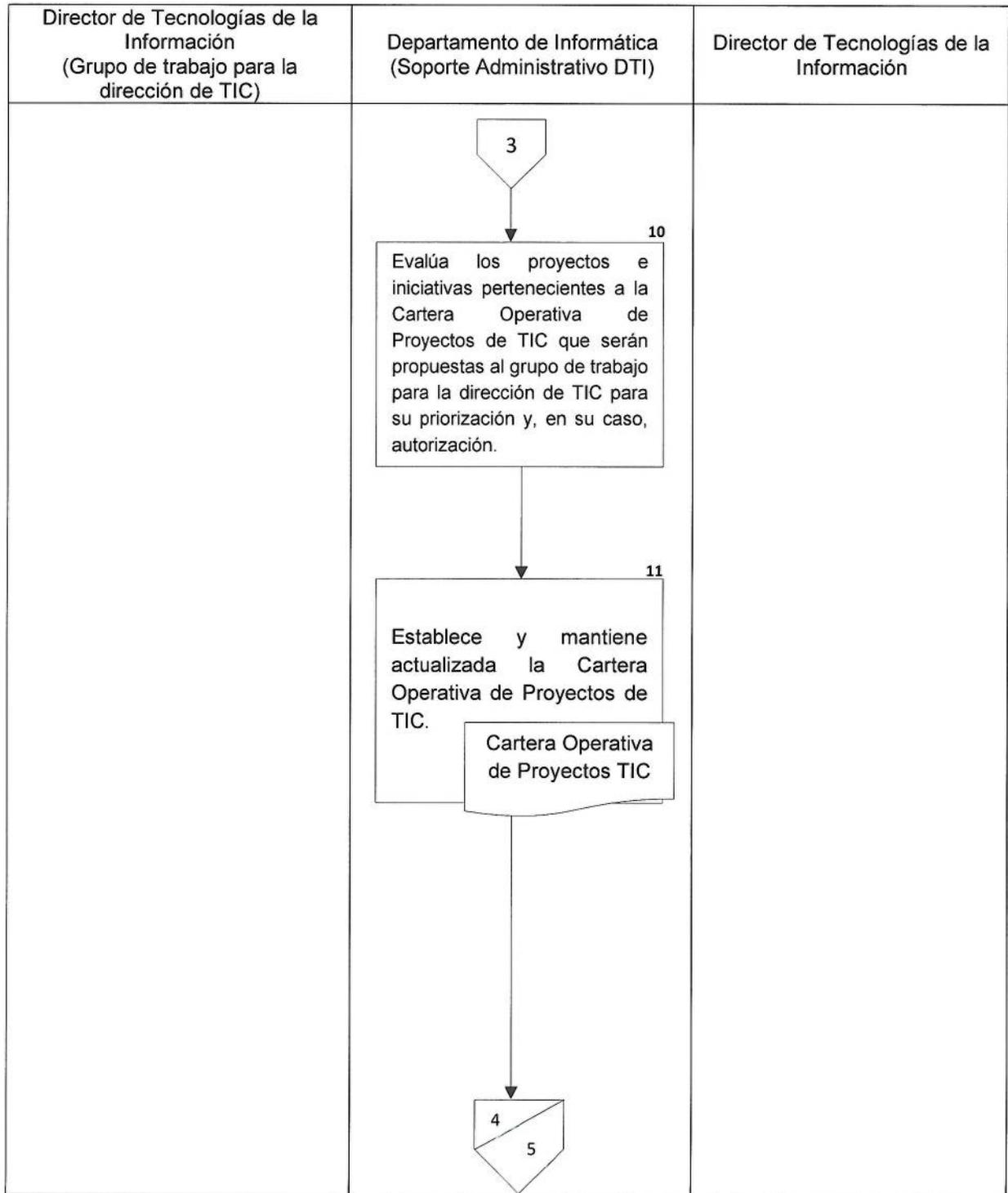


	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 8 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

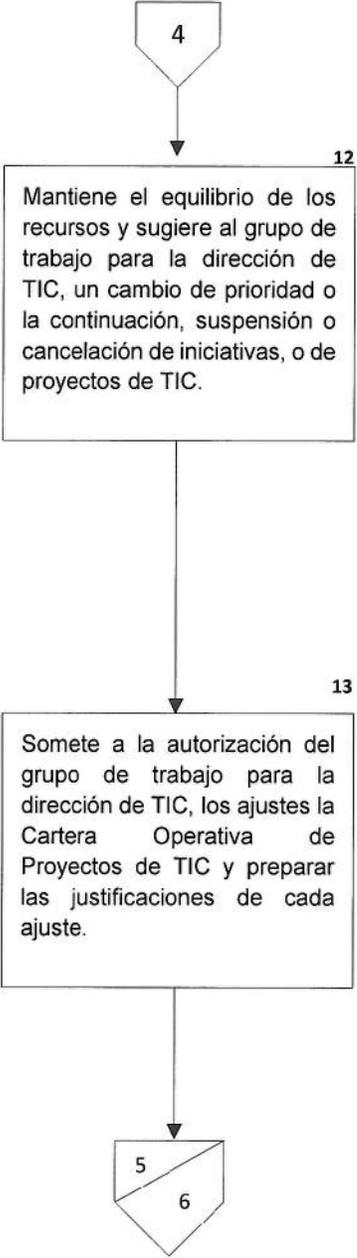




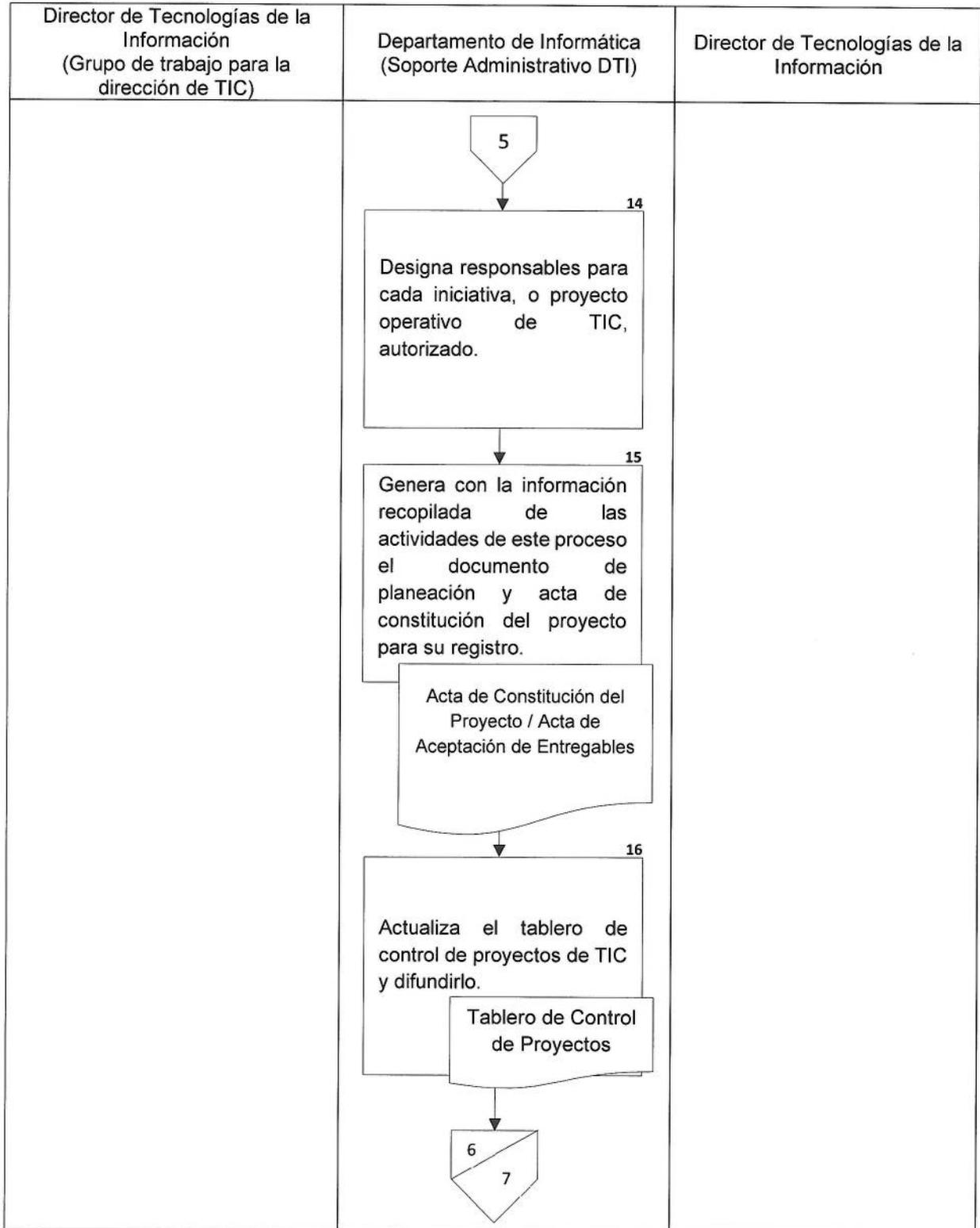
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 10 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		



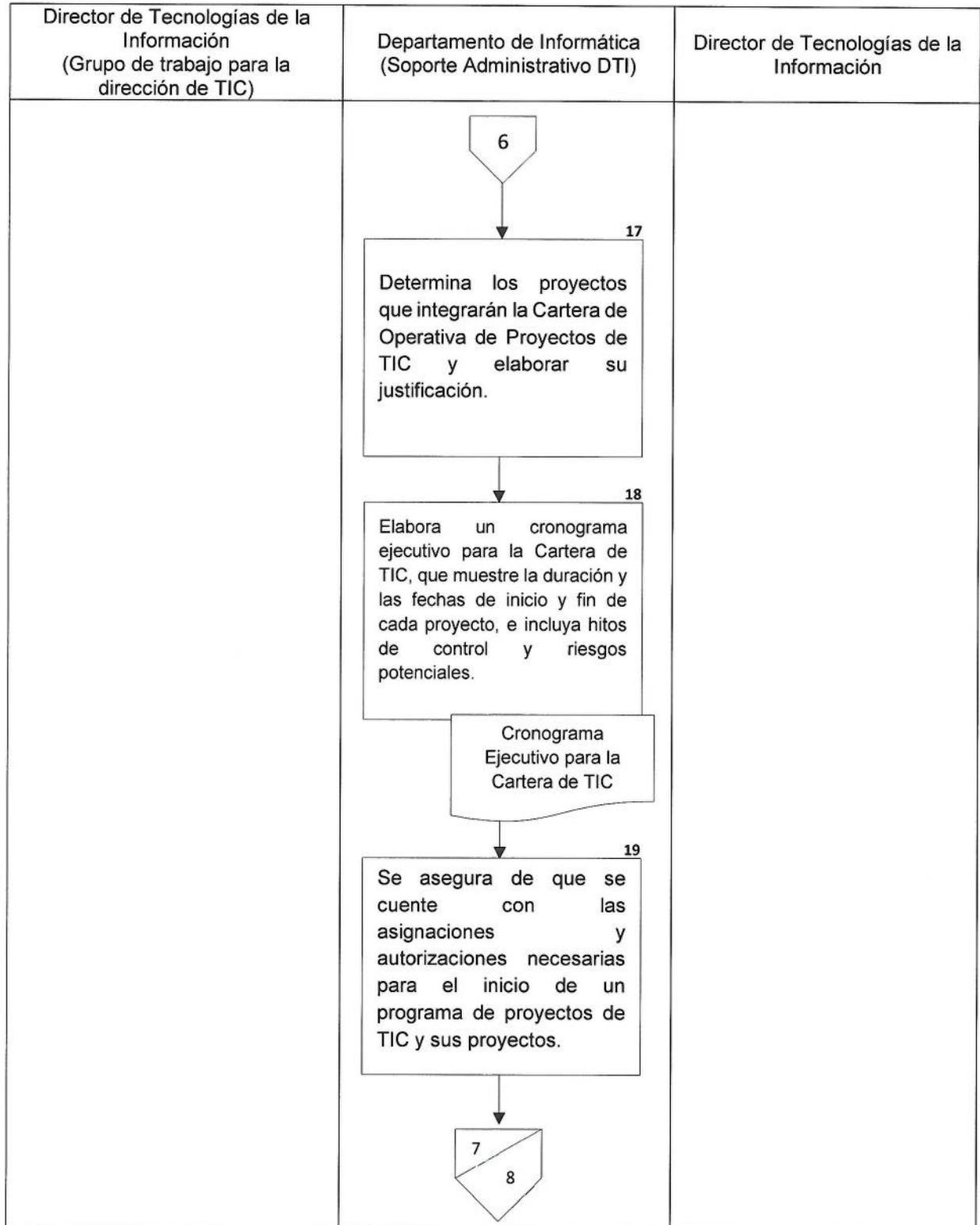
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 11 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

Director de Tecnologías de la Información (Grupo de trabajo para la dirección de TIC)	Departamento de Informática (Soporte Administrativo DTI)	Director de Tecnologías de la Información
	 <pre> graph TD     4{{4}} --&gt; 12[12 Mantiene el equilibrio de los recursos y sugiere al grupo de trabajo para la dirección de TIC, un cambio de prioridad o la continuación, suspensión o cancelación de iniciativas, o de proyectos de TIC.]     12 --&gt; 13[13 Somete a la autorización del grupo de trabajo para la dirección de TIC, los ajustes la Cartera Operativa de Proyectos de TIC y preparar las justificaciones de cada ajuste.]     13 --&gt; 5_6{{5/6}}           </pre>	

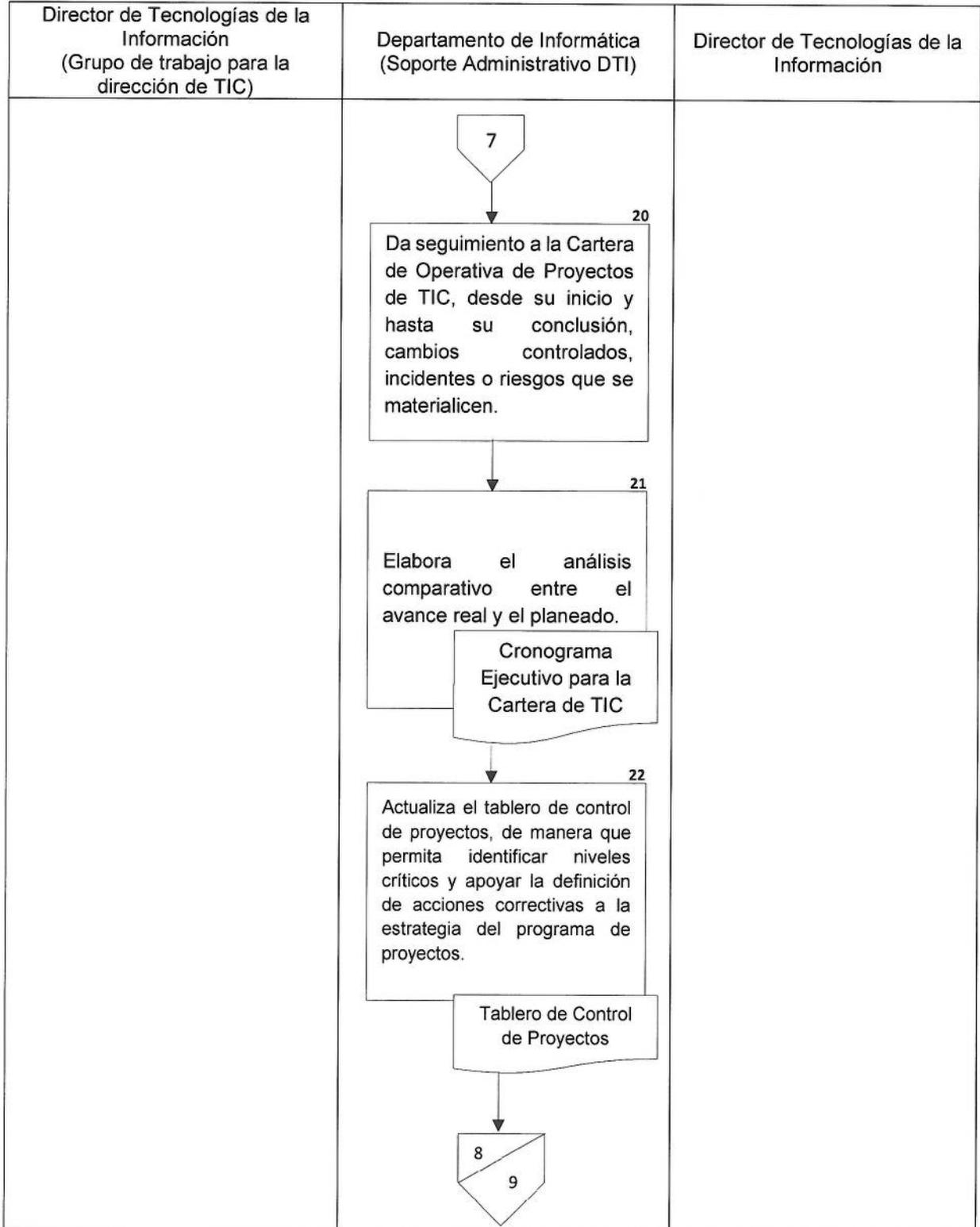
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 12 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

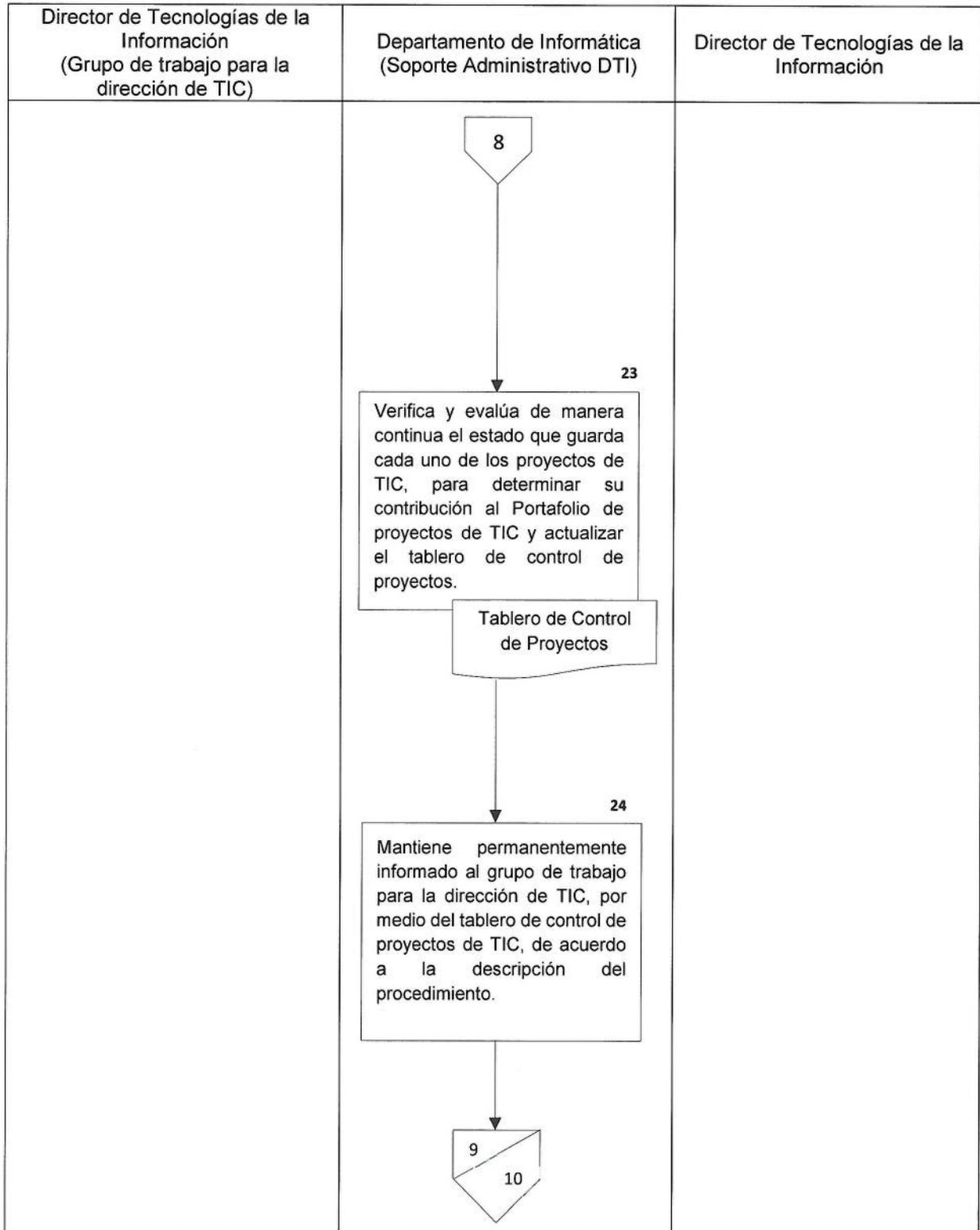


	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b> <b>6. Procedimiento para la Administración de Proyectos.</b>		Hoja: 13 de 20

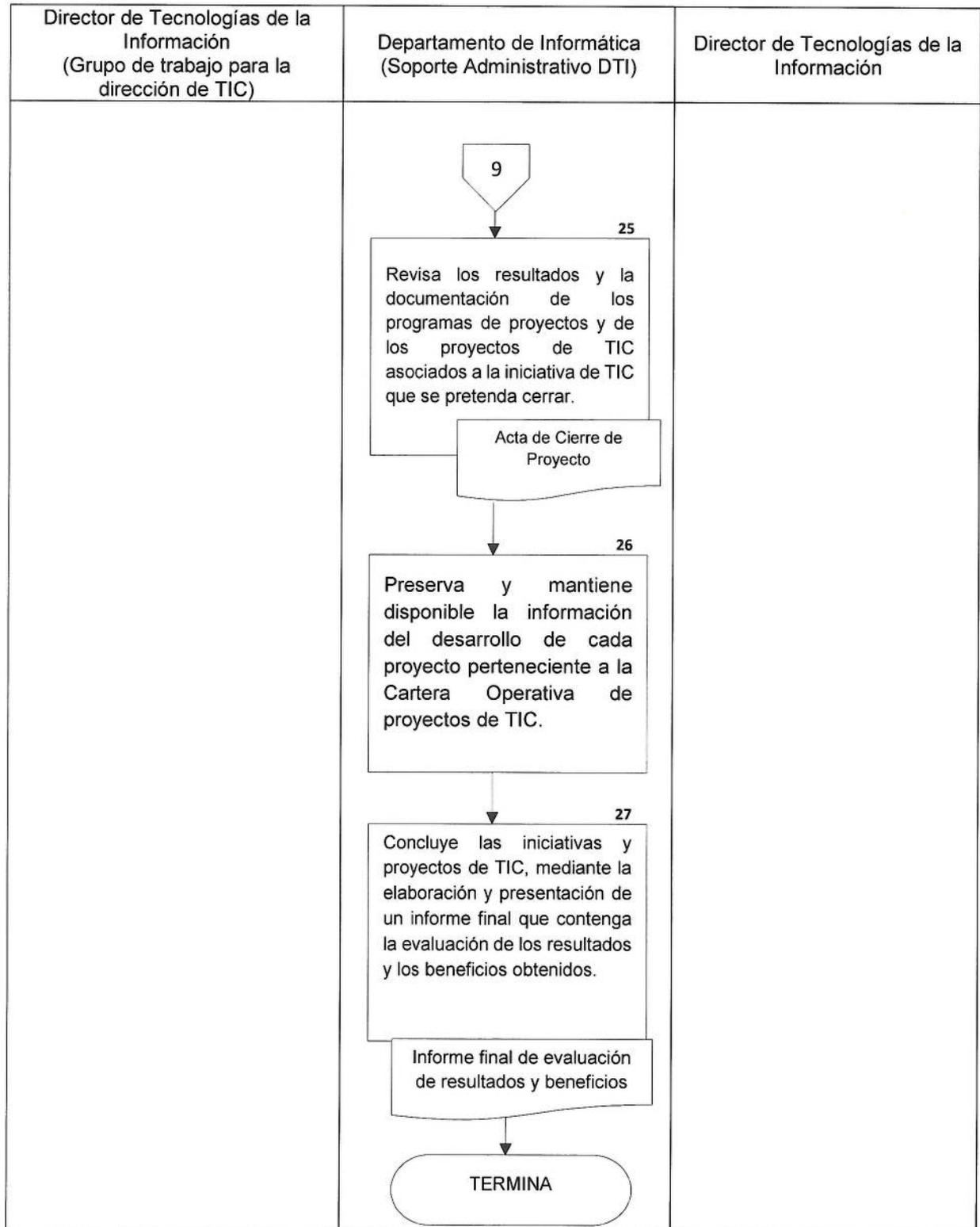


	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 14 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		





	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b> <b>6. Procedimiento para la Administración de Proyectos.</b>		Hoja: 16 de 20



	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 17 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

## 6. DOCUMENTOS DE REFERENCIA

Nombre del documento	Código (cuando aplique)
6.1 Cartera Operativa de Proyectos (PE)	No aplica

## 7. REGISTROS

Registros	Tiempo de conservación	Responsable de conservarlo	Código de registro o identificación única
Cartera Operativa de Proyectos TIC	6 meses	Administrador del Proceso	No aplica
Acta de Constitución del Proyecto	6 meses	Administrador del Proceso	No aplica
Acta de Aceptación de Entregables	6 meses	Administrador del Proceso	No aplica
Tablero de Control de Proyectos	6 meses	Administrador del Proceso	No aplica
Cronograma Ejecutivo para la Cartera de TIC	6 meses	Administrador del Proceso	No aplica
Acta de Cierre de Proyecto	6 meses	Administrador del Proceso	No aplica
Informe final de evaluación de resultados y beneficios obtenidos	6 meses	Administrador del Proceso	No aplica

## 8. GLOSARIO DEL PROCEDIMIENTO

- 8.1 Activos de TIC:** los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos;
- 8.2 ACNF:** proceso de administración de la configuración;
- 8.3 ADP:** proceso de administración de proyectos;
- 8.4 ADS:** proceso de administración de servicios;
- 8.5 APCT:** proceso de administración del presupuesto y las contrataciones;
- 8.6 Aplicativo de Cómputo:** el software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo a requerimientos previamente definidos;
- 8.7 APRO:** proceso de administración de proveedores;
- 8.8 Arquitectura Empresarial:** la información del estado actual y futuro de una Institución, a partir del análisis con perspectiva estratégica; considerando modelos de negocio, procesos, aplicativos y tecnologías de la información y comunicaciones;
- 8.9 Arquitectura Orientada a Servicios:** la metodología y marco de trabajo, para construir componentes de software reutilizables para la interoperabilidad de aplicativos de cómputo;
- 8.10 AOP:** proceso de administración de la operación;
- 8.11 ASI:** proceso de administración de la seguridad de la Información.
- 8.12 Borrado Seguro:** el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: <b>18</b> de <b>20</b>
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

- 8.13 Cartera Ejecutiva de Proyectos de TIC:** Conjunto total de proyectos de TIC que la institución propondrá a la Unidad para su seguimiento;
- 8.14 Cartera Operativa de Proyectos de TIC:** Conjunto total de proyectos que soportan la operación diaria de la DTI y no son considerados como estratégicos;
- 8.15 Centro de Datos:** el lugar físico en los que se ubiquen los activos de TIC y desde el que se proveen servicios de TIC;
- 8.16 Cómputo en la Nube:** al modelo de prestación de servicios digitales que permite a las Instituciones acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios;
- 8.17 Dependencias:** las Secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como a la Oficina de la Presidencia de la República y la Procuraduría General de la República; así como los Órganos Reguladores Coordinados en Materia Energética;
- 8.18 Dominio Tecnológico:** las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo;
- 8.19 EDN:** la Estrategia Digital Nacional contenida en el Objetivo número 5 del Programa;
- 8.20 EIDA:** el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, establecido mediante Acuerdo publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011;
- 8.21 Entidades:** los organismos descentralizados, empresas de participación estatal mayoritaria, instituciones nacionales de crédito, organizaciones auxiliares nacionales de crédito e instituciones nacionales de seguros y de fianzas, y fideicomisos públicos que en términos de la Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales, sean considerados entidades de la Administración Pública Federal Paraestatal;
- 8.22 ERISC:** equipo de respuesta a incidentes de seguridad en TIC en la Institución;
- 8.23 Estándar abierto:** a las especificaciones cuya utilización esté disponible de manera gratuita o que no suponga una dificultad de acceso, y que su uso y aplicación no esté condicionada al pago de un derecho de propiedad
- 8.24 Herramienta de Gestión de la Política TIC:** sistema web usado para llevar a cabo la comunicación de actividades de reporte establecidas en el Acuerdo, considerando el reporte de PETIC, la obtención del dictamen técnico que emite la Unidad, autorización por parte de la UPCP, la arquitectura empresarial, el MAAGTICSI, entre otros;
- 8.25 Infraestructuras Críticas de Información:** Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia.
- 8.26 Infraestructuras de Información esenciales:** Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de información, TIC y TO, cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación de las Instituciones.
- 8.27 Infraestructura de TIC:** el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC;
- 8.28 Infraestructura Pasiva:** elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones,

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 19 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de las dependencias o entidades, que sean necesarios para la instalación y operación de las redes, así como para la prestación de servicios de procesamiento de datos, de telecomunicaciones y radiodifusión;

- 8.29 Instancias de Seguridad Nacional:** las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquellas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional;
- 8.30 Institución:** las dependencias y entidades de la Administración Pública Federal, tal y como se definen en este Acuerdo;
- 8.31 Lineamientos:** los Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicados en el Diario Oficial de la Federación el 30 de enero de 2013;
- 8.32 MAAGMAASSP:** el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público;
- 8.33 MAAGTICSI:** el Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información. Anexo Único del presente Acuerdo;
- 8.34 Niveles de servicio:** el establecimiento en un lenguaje no técnico del servicio brindado, incluyendo al menos la definición, disponibilidad, calidad, tiempos de respuesta y solución.
- 8.35 OPEC:** proceso de operación de los controles de seguridad de la información y del erisc;
- 8.36 PE:** proceso de planeación estratégica;
- 8.37 PETIC:** el conjunto de proyectos que elaboran las Instituciones, conformado por un máximo de 7 proyectos estratégicos, en los términos establecidos en el presente Acuerdo;
- 8.38 Portafolio de proyectos de TIC:** es el total de los proyectos de TIC agrupados según su clasificación en Cartera Ejecutiva de Proyectos de TIC y Cartera Operativa de Proyectos de TIC que la Institución planea desarrollar, en los términos establecidos por el MAAGTICSI;
- 8.39 Programa:** el Programa para un Gobierno Cercano y Moderno 2013-2018, aprobado mediante Decreto publicado en el Diario Oficial de la Federación el 30 de agosto de 2013;
- 8.40 Proyectos de TIC:** el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC y que cuenta con presupuesto para su ejecución; considerando 2 tipos: proyectos operativos que soportan las actividades diarias de la DTI y proyectos estratégicos en los términos señalados en el presente Acuerdo;
- 8.41 Retos Públicos:** el modelo que fomenta la democratización del gasto público y la innovación, invitando a los emprendedores del país a plantear soluciones a retos de gobierno mediante el desarrollo de aplicativos tecnológicos web y móviles;
- 8.42 SEGOB:** la Secretaría de Gobernación;
- 8.43 Seguridad de la información:** la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma;
- 8.44 Seguridad Nacional:** las acciones a las que se refiere el artículo 3 de la Ley de Seguridad Nacional;
- 8.45 SFP:** la Secretaría de la Función Pública;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 20 de 20
	<b>6. Procedimiento para la Administración de Proyectos.</b>		

**8.46 SHCP:** la Secretaría de Hacienda y Crédito Público;

**8.47 Tecnologías Verdes:** el conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las tecnologías de la información y comunicaciones, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías;

**8.48 TIC:** las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video;

**8.49 Unidad:** la Unidad de Gobierno Digital de la SFP;

**8.50 DTIC:** la Dirección de Tecnologías de Información y Comunicaciones o área responsables de las TIC en la Institución.

## 9. CAMBIOS DE VERSIÓN DEL PROCEDIMIENTO

Numero de revisión	Fecha de actualización	Descripción del cambio
0	N/A	N/A

## 10. ANEXOS DEL PROCEDIMIENTO

No aplica

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 1 de 12
	<b>7. Procedimiento para la Administración de Proveedores.</b>		

## 1. PROPÓSITO

Establecer la funcionalidad del proceso de Administración de Proveedores, derivado del Manual Administrativo de Aplicación General en Materias de Tecnología de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), mediante la asignación de los roles identificados en el proceso y sus subprocesos, formalizando la asignación del rol a los responsables que participan en la ejecución de cada una de las tareas del proceso, con el fin de obtener la información, evidencias y entregables que generen las actividades ejecutadas durante el proceso.

## 2. ALCANCE

- 2.1 Obtener el mapa del proceso y de las actividades de los subprocesos involucrados, que permitan identificar la funcionalidad del proceso APRO.
- 2.2 Identificar los roles o los actores que se requieren para que el proceso genere las evidencias y entregables que demuestren la funcionalidad del proceso.
- 2.3 Identificar a las áreas o personas que se harán responsables de los diferentes roles que requiere el proceso.
- 2.4 Formalizar las asignaciones de responsables de roles y actividades.
- 2.5 Establecer si es necesario entre las áreas identificadas que participarán con alguna responsabilidad en el proceso un OLA, acuerdo de operación, en el cual se especifiquen los servicios que se aportarán y los tiempos en los que se atenderán y los entregables comprometidos que requiere el proceso.
- 2.6 Identificar las capacitaciones que se requieran en las diferentes áreas o personas que asuman el rol asignado, para que se consideren en un programa de capacitación.
- 2.7 Identificar los indicadores de desempeño del proceso y registrarlos periódicamente para su evaluación posterior.
- 2.8 Identificar los indicadores de los servicios considerados y sus métricas.

## 3. POLÍTICAS DE OPERACIÓN, NORMAS Y LINEAMIENTOS

- 3.1 El responsable de este proceso deberá ser asignado por el titular de la DTI.
- 3.2 Este proceso deberá ejecutarse con apego a las disposiciones que en materia de adquisiciones y arrendamientos de bienes muebles y contratación de servicios resulten aplicables, así como al Acuerdo por el que se expide el MAAGMAASSP.
- 3.3 El responsable de este proceso designará a los administradores de contratos de bienes y servicios de TIC y solicitará para ello el visto bueno del titular de la DTI.
- 3.4 Este proceso deberá ejecutarse con apego, en lo que respecta a la administración de contratos, a lo que dispongan las políticas, bases y lineamientos en materia de adquisiciones, arrendamientos y servicios de cada Institución.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 2 de 12
<b>7. Procedimiento para la Administración de Proveedores.</b>			

#### 4. DESCRIPCIÓN DEL PROCEDIMIENTO

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Departamento de Informática (Soporte Administrativo DTI)	1	Apoya técnicamente a los administradores de contratos de bienes y servicios de TIC en el seguimiento a las obligaciones adquiridas mediante los contratos celebrados por la DTI.	Lista de verificación de obligaciones
	2	Elabora, de conformidad con el contrato de que se trate, una lista de apoyo para la verificación y seguimiento de las obligaciones contractuales, la cual deberá contener al menos, lo siguiente: a) La totalidad de las obligaciones asumidas por el proveedor y la Institución. b) Los supuestos en que se aplicarán penalizaciones al proveedor. c) Las fechas de entrega de los bienes o de prestación de los servicios contratados y en su caso, el calendario de entrega de los productos o entregables. d) Los datos del enlace o de los enlaces o responsables, designados por el proveedor. ¿Participan diversos proveedores en un contrato?  No: Continuar en actividad 4 Si: Continuar en actividad 3	
	3	Identifica qué obligaciones corresponden a cada proveedor.	
	4	Solicita a cada uno de los administradores de contrato el cumplimiento de las obligaciones asumidas por el proveedor en el contrato.	
	5	Solicita a cada uno de los administradores de contrato los avances del proveedor y el desempeño al que éste se encuentre obligado.	

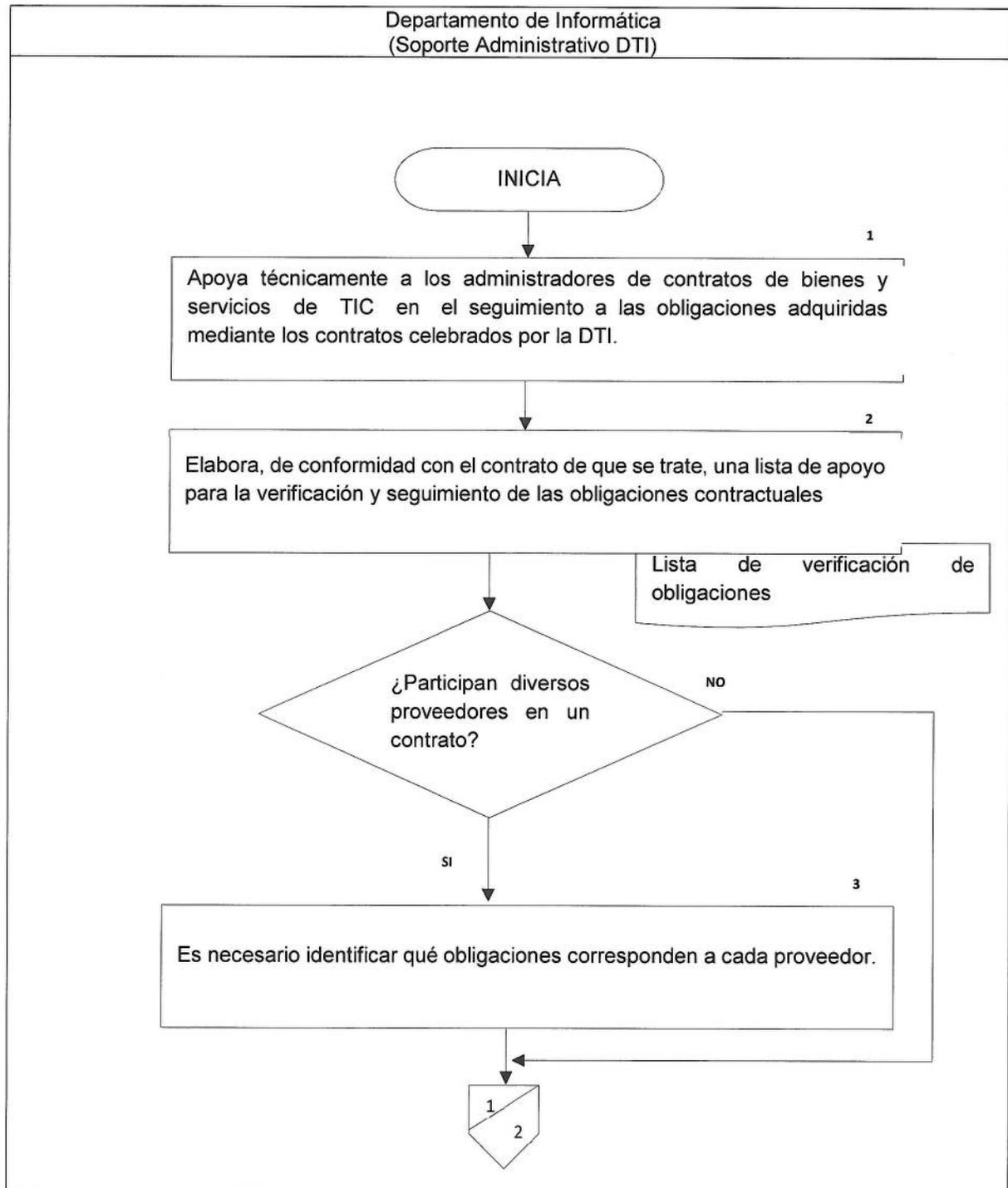
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 3 de 12
	<b>7. Procedimiento para la Administración de Proveedores.</b>		

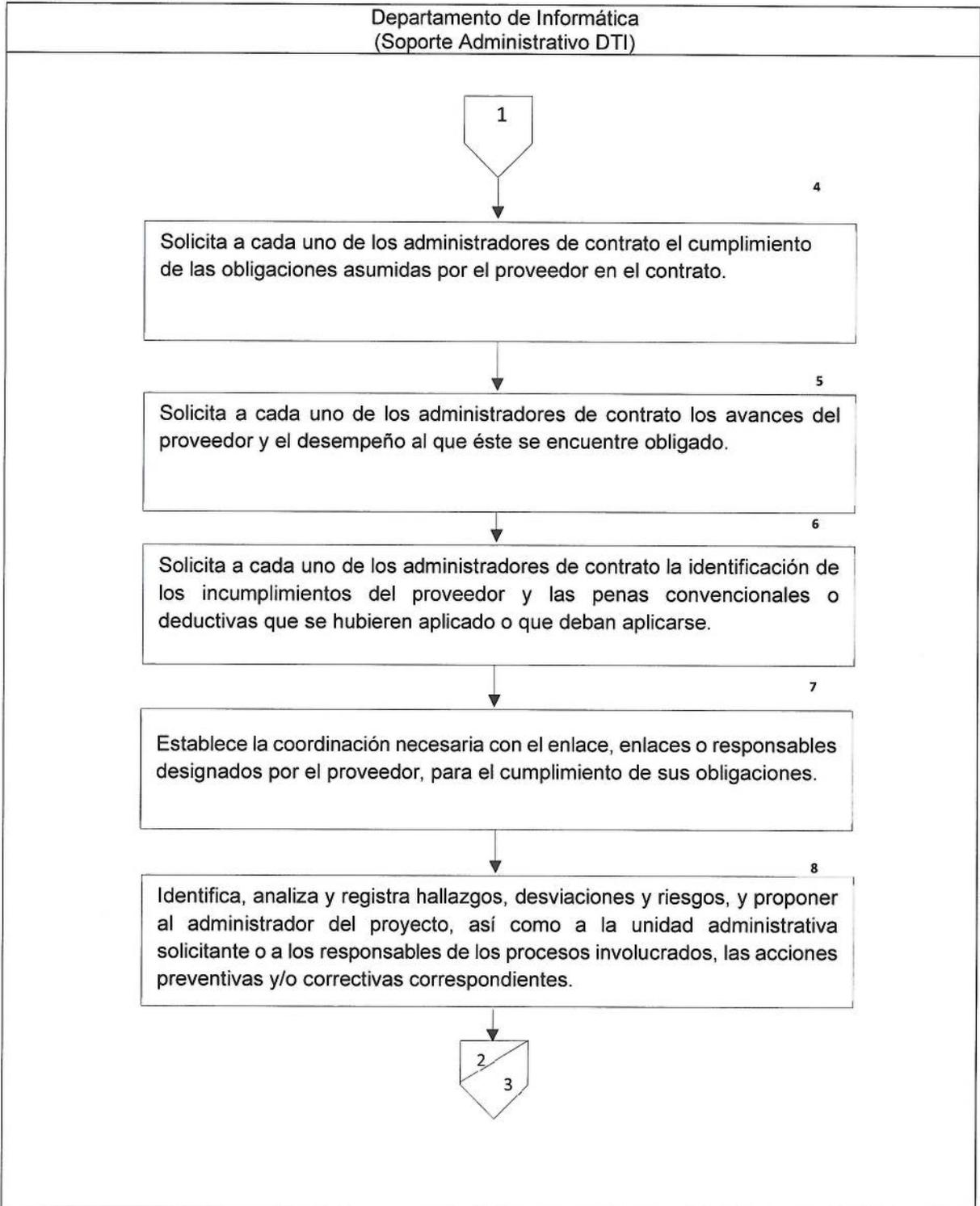
Responsable	No. Act.	Descripción de actividades	Documento o anexo
Departamento de Informática (Soporte Administrativo DTI)	6	Solicita a cada uno de los administradores de contrato la identificación de los incumplimientos del proveedor y las penas convencionales o deductivas que se hubieren aplicado o que deban aplicarse.	
	7	Establece la coordinación necesaria con el enlace, enlaces o responsables designados por el proveedor, para el cumplimiento de sus obligaciones.	
	8	Identifica, analiza y registra hallazgos, desviaciones y riesgos, y proponer al administrador del proyecto, así como a la unidad administrativa solicitante o a los responsables de los procesos involucrados, las acciones preventivas y/o correctivas correspondientes.	
	9	Da seguimiento a las acciones preventivas y/o correctivas que se determinen hasta su cierre.	
	10	Elabora un reporte de avance sobre el cumplimiento de obligaciones	Reporte de avance sobre el cumplimiento de obligaciones
	11	Apoya en la revisión del cumplimiento de las obligaciones contractuales del proveedor, principalmente para la aceptación de los bienes o servicios objeto de la contratación.	
	12	Confirma, cuando proceda, que los accesos a los activos o servicios de TIC proporcionados al proveedor, para el cumplimiento del contrato, han sido retirados al darse por finiquitado el mismo.	
	13	Actualiza el reporte de avance sobre el cumplimiento de obligaciones con la información final	Reporte de avance sobre el cumplimiento de obligaciones

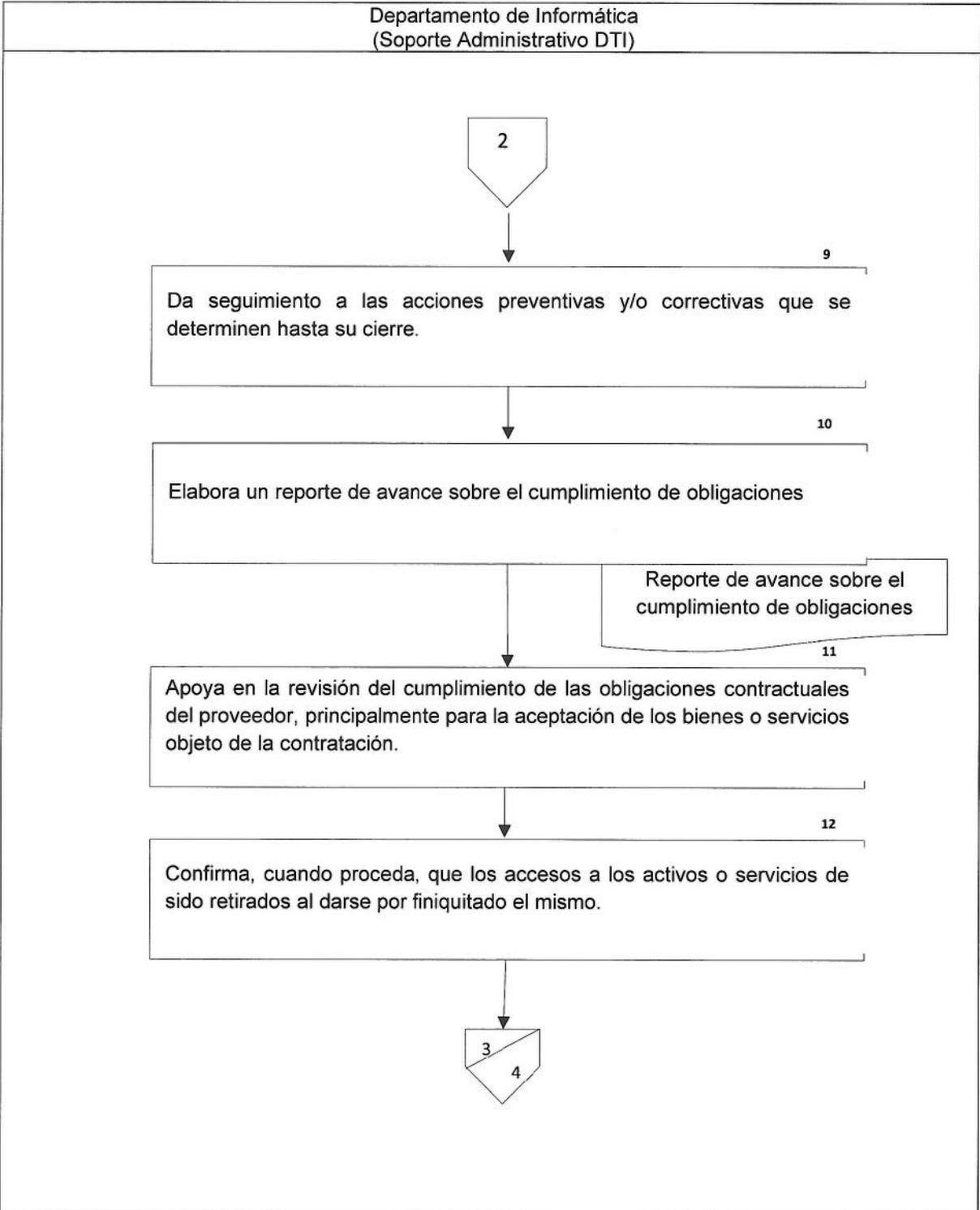
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		
	<b>7. Procedimiento para la Administración de Proveedores.</b>		

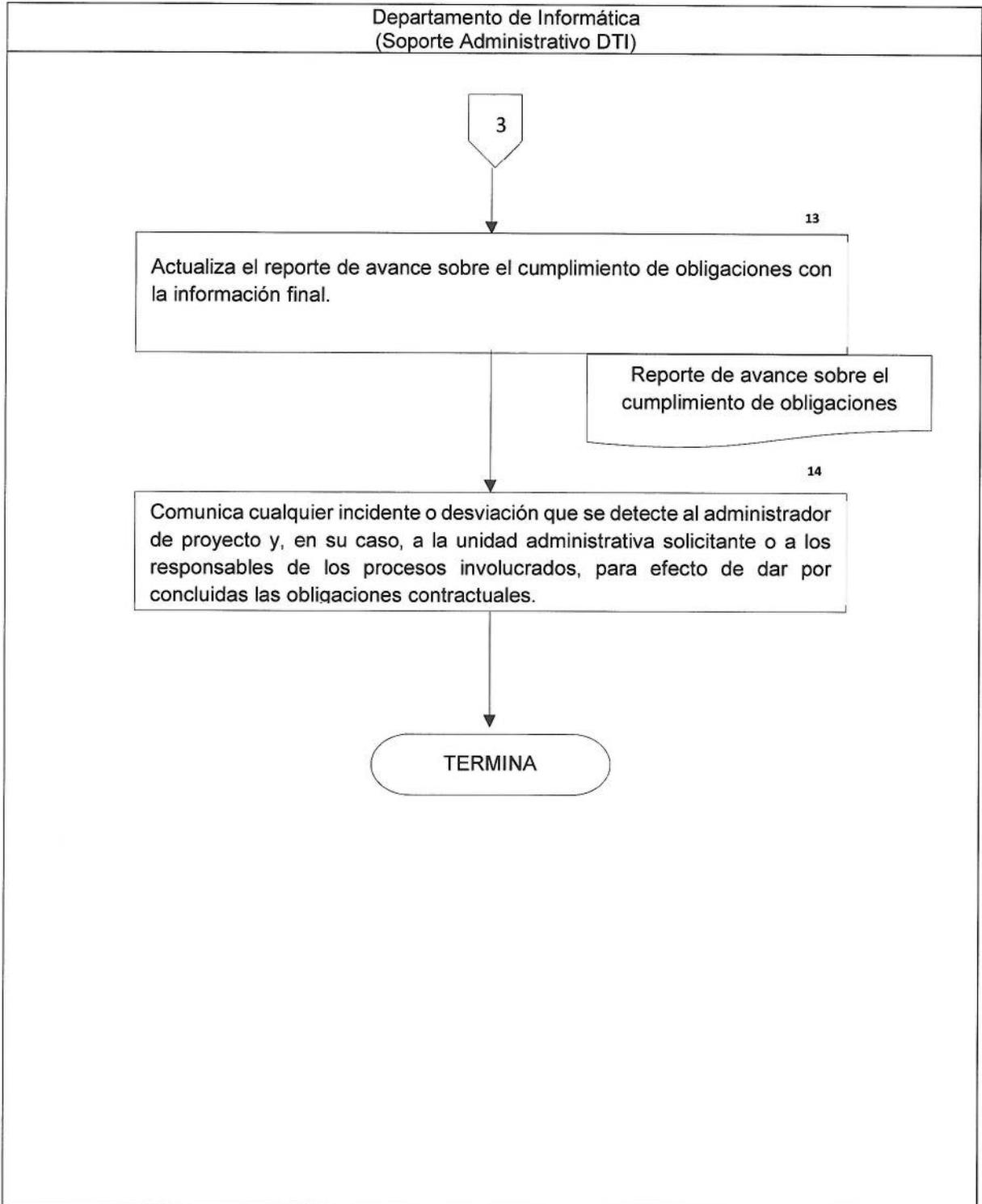
Responsable	No. Act.	Descripción de actividades	Documento o anexo
	14	<p>Comunica cualquier incidente o desviación que se detecte al administrador de proyecto y, en su caso, a la unidad administrativa solicitante o a los responsables de los procesos involucrados, así como a la unidad administrativa facultada en la Institución para efecto de dar por concluidas las obligaciones contractuales, en términos de las disposiciones aplicables.</p> <p>TERMINA</p>	

## 5. DIAGRAMA DE FLUJO









	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 9 de 12
	<b>7. Procedimiento para la Administración de Proveedores.</b>		

## 6. DOCUMENTOS DE REFERENCIA

Nombre del documento	Código (cuando aplique)
6.1 MAAGMAASSP, Manual Administrativo de Aplicación General en Mater de Adquisiciones, Arrendamientos y Servicios del Sector Público	No aplica

## 7. REGISTROS

Registros	Tiempo de conservación	Responsable de conservarlo	Código de registro o identificación única
Lista de verificación de obligaciones	6 meses	El responsable de proceso APRO	No aplica
Reporte de avance sobre el cumplimiento de obligaciones	6 meses	El responsable de proceso APRO	No aplica

## 8. GLOSARIO DEL PROCEDIMIENTO

- 8.1 Activos de TIC:** los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos;
- 8.2 ACNF:** proceso de administración de la configuración;
- 8.3 ADP:** proceso de administración de proyectos;
- 8.4 ADS:** proceso de administración de servicios;
- 8.5 APCT:** proceso de administración del presupuesto y las contrataciones;
- 8.6 Aplicativo de Cómputo:** el software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo a requerimientos previamente definidos;
- 8.7 APRO:** proceso de administración de proveedores;
- 8.8 Arquitectura Empresarial:** la información del estado actual y futuro de una Institución, a partir del análisis con perspectiva estratégica; considerando modelos de negocio, procesos, aplicativos y tecnologías de la información y comunicaciones;
- 8.9 Arquitectura Orientada a Servicios:** la metodología y marco de trabajo, para construir componentes de software reutilizables para la interoperabilidad de aplicativos de cómputo;
- 8.10 AOP:** proceso de administración de la operación;
- 8.11 ASI:** proceso de administración de la seguridad de la Información.
- 8.12 Borrado Seguro:** el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital;
- 8.13 Cartera Ejecutiva de Proyectos de TIC:** Conjunto total de proyectos de TIC que la institución propondrá a la Unidad para su seguimiento;
- 8.14 Cartera Operativa de Proyectos de TIC:** Conjunto total de proyectos que soportan la operación diaria de la DTI y no son considerados como estratégicos;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 10 de 12
	<b>7. Procedimiento para la Administración de Proveedores.</b>		

- 8.15 Centro de Datos:** el lugar físico en los que se ubiquen los activos de TIC y desde el que se proveen servicios de TIC;
- 8.16 Cómputo en la Nube:** al modelo de prestación de servicios digitales que permite a las Instituciones acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios;
- 8.17 Dependencias:** las Secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como a la Oficina de la Presidencia de la República y la Procuraduría General de la República; así como los Órganos Reguladores Coordinados en Materia Energética;
- 8.18 Dominio Tecnológico:** las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo;
- 8.19 EDN:** la Estrategia Digital Nacional contenida en el Objetivo número 5 del Programa;
- 8.20 EIDA:** el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, establecido mediante Acuerdo publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011;
- 8.21 Entidades:** los organismos descentralizados, empresas de participación estatal mayoritaria, instituciones nacionales de crédito, organizaciones auxiliares nacionales de crédito e instituciones nacionales de seguros y de fianzas, y fideicomisos públicos que en términos de la Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales, sean considerados entidades de la Administración Pública Federal Paraestatal;
- 8.22 ERISC:** equipo de respuesta a incidentes de seguridad en TIC en la Institución;
- 8.23 Estándar abierto:** a las especificaciones cuya utilización esté disponible de manera gratuita o que no suponga una dificultad de acceso, y que su uso y aplicación no esté condicionada al pago de un derecho de propiedad
- 8.24 Herramienta de Gestión de la Política TIC:** sistema web usado para llevar a cabo la comunicación de actividades de reporte establecidas en el Acuerdo, considerando el reporte de PETIC, la obtención del dictamen técnico que emite la Unidad, autorización por parte de la UPCP, la arquitectura empresarial, el MAAGTICSI, entre otros;
- 8.25 Infraestructuras Críticas de Información:** Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia.
- 8.26 Infraestructuras de Información esenciales:** Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de información, TIC y TO, cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación de las Instituciones.
- 8.27 Infraestructura de TIC:** el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC;
- 8.28 Infraestructura Pasiva:** elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de las dependencias o entidades, que sean necesarios para la instalación y operación de las redes, así como para la prestación de servicios de procesamiento de datos, de telecomunicaciones y radiodifusión;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 11 de 12
	<b>7. Procedimiento para la Administración de Proveedores.</b>		

- 8.29 Instancias de Seguridad Nacional:** las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquellas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional;
- 8.30 Institución:** las dependencias y entidades de la Administración Pública Federal, tal y como se definen en este Acuerdo;
- 8.31 Lineamientos:** los Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicados en el Diario Oficial de la Federación el 30 de enero de 2013;
- 8.32 MAAGMAASSP:** el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público;
- 8.33 MAAGTICSI:** el Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información. Anexo Único del presente Acuerdo;
- 8.34 Niveles de servicio:** el establecimiento en un lenguaje no técnico del servicio brindado, incluyendo al menos la definición, disponibilidad, calidad, tiempos de respuesta y solución.
- 8.35 OPEC:** proceso de operación de los controles de seguridad de la información y del erisc;
- 8.36 PE:** proceso de planeación estratégica;
- 8.37 PETIC:** el conjunto de proyectos que elaboran las Instituciones, conformado por un máximo de 7 proyectos estratégicos, en los términos establecidos en el presente Acuerdo;
- 8.38 Portafolio de proyectos de TIC:** es el total de los proyectos de TIC agrupados según su clasificación en Cartera Ejecutiva de Proyectos de TIC y Cartera Operativa de Proyectos de TIC que la Institución planea desarrollar, en los términos establecidos por el MAAGTICSI;
- 8.39 Programa:** el Programa para un Gobierno Cercano y Moderno 2013-2018, aprobado mediante Decreto publicado en el Diario Oficial de la Federación el 30 de agosto de 2013;
- 8.40 Proyectos de TIC:** el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC y que cuenta con presupuesto para su ejecución; considerando 2 tipos: proyectos operativos que soportan las actividades diarias de la DTI y proyectos estratégicos en los términos señalados en el presente Acuerdo;
- 8.41 Retos Públicos:** el modelo que fomenta la democratización del gasto público y la innovación, invitando a los emprendedores del país a plantear soluciones a retos de gobierno mediante el desarrollo de aplicativos tecnológicos web y móviles;
- 8.42 SEGOB:** la Secretaría de Gobernación;
- 8.43 Seguridad de la información:** la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma;
- 8.44 Seguridad Nacional:** las acciones a las que se refiere el artículo 3 de la Ley de Seguridad Nacional;
- 8.45 SFP:** la Secretaría de la Función Pública;
- 8.46 SHCP:** la Secretaría de Hacienda y Crédito Público;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 12 de 12
	<b>7. Procedimiento para la Administración de Proveedores.</b>		

**8.47 Tecnologías Verdes:** el conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las tecnologías de la información y comunicaciones, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías;

**8.48 TIC:** las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video;

**8.49 Unidad:** la Unidad de Gobierno Digital de la SFP;

**8.50 DTIC:** la Dirección de Tecnologías de Información y Comunicaciones o área responsables de las TIC en la Institución.

## 9. CAMBIOS DE VERSIÓN DEL PROCEDIMIENTO

Numero de revisión	Fecha de actualización	Descripción del cambio
0	No aplica	No aplica

## 10. ANEXOS DEL PROCEDIMIENTO

No aplica

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 1 de 20
	<b>8. Procedimiento para la Administración de la Operación.</b>		

## 1. PROPÓSITO

Establecer la funcionalidad del proceso de Administración de la Operación, derivado del Manual Administrativo de Aplicación General en Materias de Tecnología de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), mediante la asignación de los roles identificados en el proceso y sus subprocesos, formalizando la asignación del rol a los responsables que participan en la ejecución de cada una de las tareas del proceso, con el fin de obtener la información, evidencias y entregables que generen las actividades ejecutadas durante el proceso.

## 2. ALCANCE

- 2.1 Obtener el mapa del proceso y de las actividades de los subprocesos involucrados, que permitan identificar la funcionalidad del proceso AOP.
- 2.2 Identificar los roles o los actores que se requieren para que el proceso genere las evidencias y entregables que demuestren la funcionalidad del proceso.
- 2.3 Identificar a las áreas o personas que se harán responsables de los diferentes roles que requiere el proceso.
- 2.4 Formalizar las asignaciones de responsables de roles y actividades.
- 2.5 Establecer si es necesario entre las áreas identificadas que participarán con alguna responsabilidad en el proceso un OLA, acuerdo de operación, en el cual se especifiquen los servicios que se aportarán y los tiempos en los que se atenderán y los entregables comprometidos que requiere el proceso.
- 2.6 Identificar las capacitaciones que se requieran en las diferentes áreas o personas que asuman el rol asignado, para que se consideren en un programa de capacitación.
- 2.7 Identificar los indicadores de desempeño del proceso y registrarlos periódicamente para su evaluación posterior.
- 2.8 Identificar los indicadores de los servicios considerados y sus métricas.

## 3. POLÍTICAS DE OPERACIÓN, NORMAS Y LINEAMIENTOS

- 3.1 El responsable de este proceso estará a cargo de la operación del centro de cómputo y comunicaciones, o bien, del enlace con los responsables de los servicios de cómputo y comunicaciones que se encuentren contratados.
- 3.2 El responsable de este proceso deberá revisar y en su caso, aprobar los cambios a los elementos o componentes del ambiente operativo.
- 3.3 El responsable de este proceso, en coordinación con cada responsable de dominio tecnológico, se asegurará de que los servidores de cómputo de la red institucional, así como los componentes del ambiente operativo que manejen fecha y hora en sus sistemas operativos, se encuentren sincronizados a la hora oficial para los Estados Unidos Mexicanos generada por el Centro Nacional de Metrología, en los husos horarios establecidos en la Ley del Sistema de Horario en los Estados Unidos Mexicanos, para lo cual hará uso del servicio que dicho centro proporciona de manera gratuita.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b> <b>8. Procedimiento para la Administración de la Operación.</b>		Hoja: 2 de 20

- 3.4 El responsable de este proceso se deberá asegurar que se realicen oportunamente las evaluaciones, para determinar la efectividad de los controles de seguridad implementados.
- 3.5 El responsable de este proceso deberá verificar que se siguen en todo momento los controles de seguridad establecidos en el SGSI.
- 3.6 El titular de la DTI deberá asignar al Responsable del mantenimiento de la infraestructura.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: <b>3</b> de <b>20</b>
	<b>8. Procedimiento para la Administración de la Operación.</b>		

#### 4. DESCRIPCIÓN DEL PROCEDIMIENTO

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Departamento de Informática (Soporte Administrativo DTI)	1	Mantiene un mecanismo de operación de TIC para los sistemas, aplicaciones y servicios de TIC, que contemple las acciones a seguir para la programación, ejecución y seguimiento de las tareas de la operación, mantenimiento y respaldo formalizándolas a través del Mecanismo de operación y mantenimiento de TIC.	Mecanismo de Operación y Mantenimiento de TIC
	2	Define e implementa, en la medida de lo posible y conforme a las necesidades y recursos de la DTI, herramientas tecnológicas para notificar y rectificar fallas críticas en las tareas de la operación, así como para monitorear el estado y operación de los dispositivos dentro de los límites aceptables, con la finalidad de prevenir fallas en la operación.	
Departamento de Informática (Soporte Administrativo DTI), en coordinación con el Director de Tecnologías de la Información	3	Integra en el documento Mecanismo de operación y mantenimiento de TIC las acciones de carácter preventivo para evitar fallas a los componentes de dicha infraestructura.	Mecanismo de Operación y Mantenimiento de TIC
	4	Difunde el documento de Mecanismo de Operación y Mantenimiento de TIC a los responsables de los procesos de la DTI que estén involucrados.	
	5	Aplica los controles de mitigación de riesgos establecidos en el Proceso de Administración de la Seguridad de la Información (ASI), relativos a componentes de infraestructura.	
	6	Efectúa el respaldo y protección de los datos almacenados en la infraestructura tecnológica, así como del software que se encuentre instalado.	
	7	Verifica que el ambiente de desarrollo y pruebas sea el adecuado para efectuar las tareas de instalación o de mantenimiento a la infraestructura tecnológica.	
Director de Tecnología de la Información (Personal Operativo DTI)			

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 4 de 20
	<b>8. Procedimiento para la Administración de la Operación.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director de Tecnología de la Información (Personal Operativo DTI)	8	Verifica que el ambiente de desarrollo y pruebas esté separado del ambiente productivo.	
	9	Modifica, en los componentes instalados, las contraseñas originales, configuraciones y parámetros que puedan afectar la seguridad y suprimir los accesos temporales utilizados en la instalación.	
	10	Implementa, en la realización de las tareas de instalación y mantenimiento de la infraestructura tecnológica, los controles de seguridad del SGSI.	
	11	Evalúa la efectividad de los controles de seguridad aplicados en la instalación de los componentes y en las tareas de mantenimiento.	
	12	Registra y da seguimiento a los incidentes de mantenimiento, con el propósito de analizar y eliminar las vulnerabilidades dentro de la infraestructura tecnológica.	
	13	Informa de los incidentes de mantenimiento a los responsables de los dominios tecnológico involucrados.	
	14	Registra el resultado de las pruebas realizadas y mantenerlas disponibles como información de conocimiento.	
Departamento de Informática (Soporte Administrativo DTI)	15	Mantiene un control en la ejecución de tareas para la operación de TIC, que incluya de manera detallada la calendarización, tareas y responsables de estas, así como los elementos de la configuración que se verán afectados.	
	16	Da seguimiento a las tareas de mantenimiento calendarizadas.	
Departamento de Informática (Soporte Administrativo DTI)	17	Valida que el personal a su cargo ejecute las tareas contenidas en el programa de ejecución de tareas para la operación de TIC que les	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 5 de 20
	<b>8. Procedimiento para la Administración de la Operación.</b>		

Responsable	No. Act.	Descripción de actividades	Documento o anexo
		corresponda desarrollar y documentarlas en una bitácora de operación.	
	18	Valida que el personal a su cargo registre y dé trámite a las solicitudes de cambio que deriven de la ejecución de las tareas de operación y efectuar tales cambios de manera administrada, estableciendo controles de seguridad en cada caso.	
	19	Valida que el personal a su cargo registre y dé el trámite que corresponda a cualquier solicitud de servicio con motivo de incidentes de operación que deriven de la ejecución de las tareas de operación, y efectuar el seguimiento de la solicitud de manera administrada, estableciendo controles de seguridad en cada caso.	
	20	Revisa las bitácoras de operación, para constatar que las tareas ejecutadas coinciden con las tareas programadas.	Bitácoras de Operación
	21	Revisa que se registre cualquier tarea ejecutada como parte de la operación, a efecto de contar con registros que permitan identificar la causa raíz de incidentes, así como confirmar la ejecución satisfactoria de las tareas de la operación.	
	22	Identifica los eventos que se presenten en la operación de la infraestructura y de los servicios de TIC	
	23	Da seguimiento a los eventos e incidentes que se presenten en la operación y registrar aquellos que aporten experiencia y conocimiento, con el propósito de apoyar el análisis para la solución de problemas o la prevención de incidentes, así como la mejora de las tareas de operación en la Institución y estar en posibilidad de transmitirlos a otras Instituciones.	

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b> <b>8. Procedimiento para la Administración de la Operación.</b>		Hoja: 6 de 20

Responsable	No. Act.	Descripción de actividades	Documento o anexo
Departamento de Informática (Soporte Administrativo DTI) en coordinación con el Director de Tecnologías de la Información	24	Incorpora los controles de seguridad para los riesgos de seguridad física identificados en el Proceso de Administración de la Seguridad de la Información (ASI).	
	25	Incorpora controles de seguridad para limitar el acceso a la información sensible del centro de datos.	
	26	Incorpora controles de seguridad para efectuar el retiro, transporte y almacenamiento de activos de TIC, de forma segura.	
	27	Incorpora controles de seguridad para el borrado seguro de la información de los dispositivos de almacenamiento fijos, removibles y externos, retirados por daño o reemplazo.	
	28	Incorpora controles de seguridad para el registro de incidentes sobre la seguridad del ambiente físico, mediante la solicitud de servicio respectiva.	
	29	Mantiene y actualiza sistema de seguridad física en el centro de datos, de acuerdo con el SGSI.	
	30	Integra al sistema de seguridad física en el centro de datos los controles de seguridad que de acuerdo con el SGSI se requieran para el acceso físico a las áreas reservadas de la DTI.	
	31	Integra al sistema de seguridad física en el centro de datos, los controles de seguridad que de acuerdo con el SGSI sean necesarios para hacer frente a los riesgos ambientales.	
	32	Difunde al interior de la DTI los controles de seguridad implementados y verificar su cumplimiento.	
		33	Registra los incidentes del ambiente físico que se presenten y administrarlos hasta su solución.

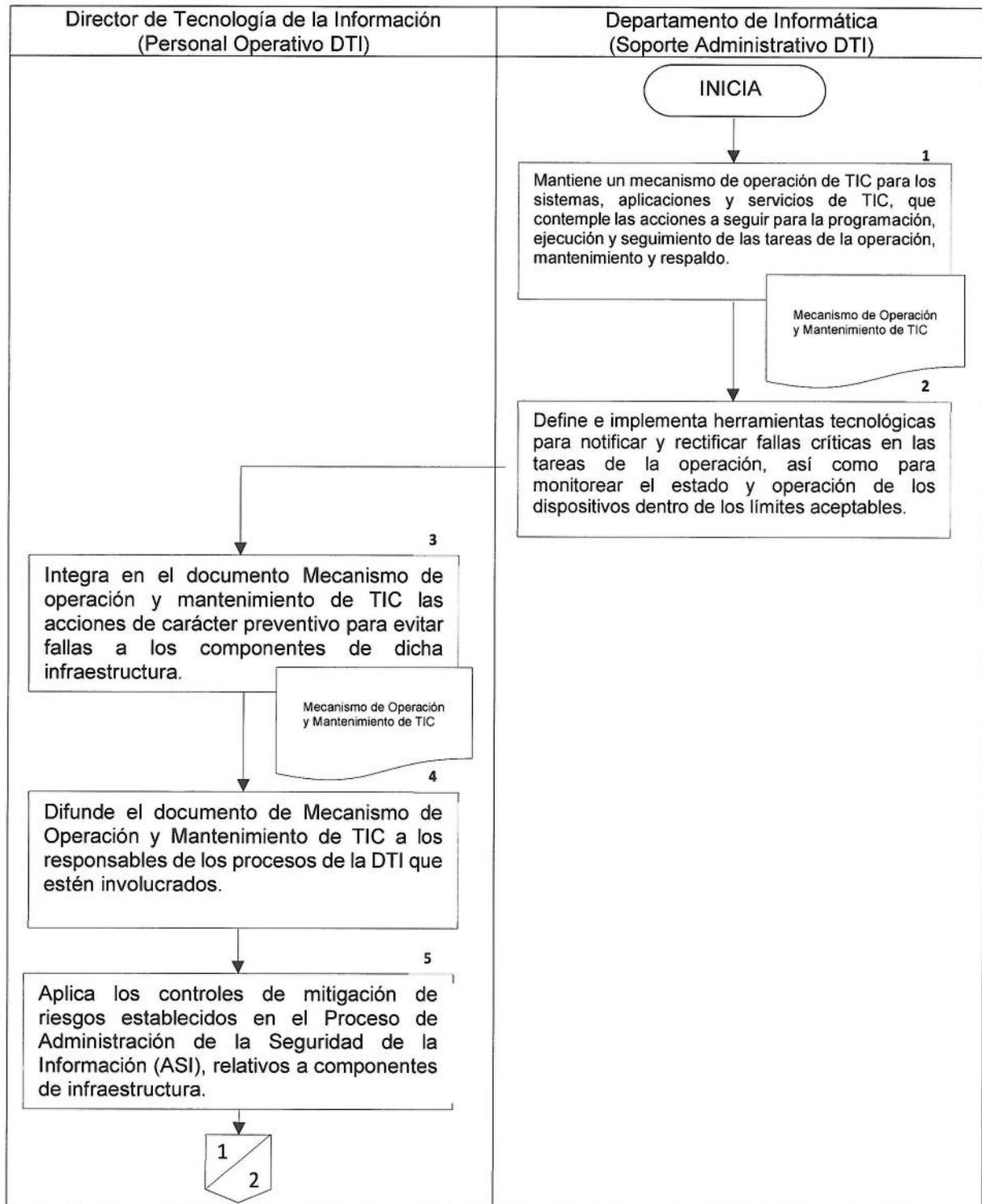
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 7 de 20
	<b>8. Procedimiento para la Administración de la Operación.</b>		

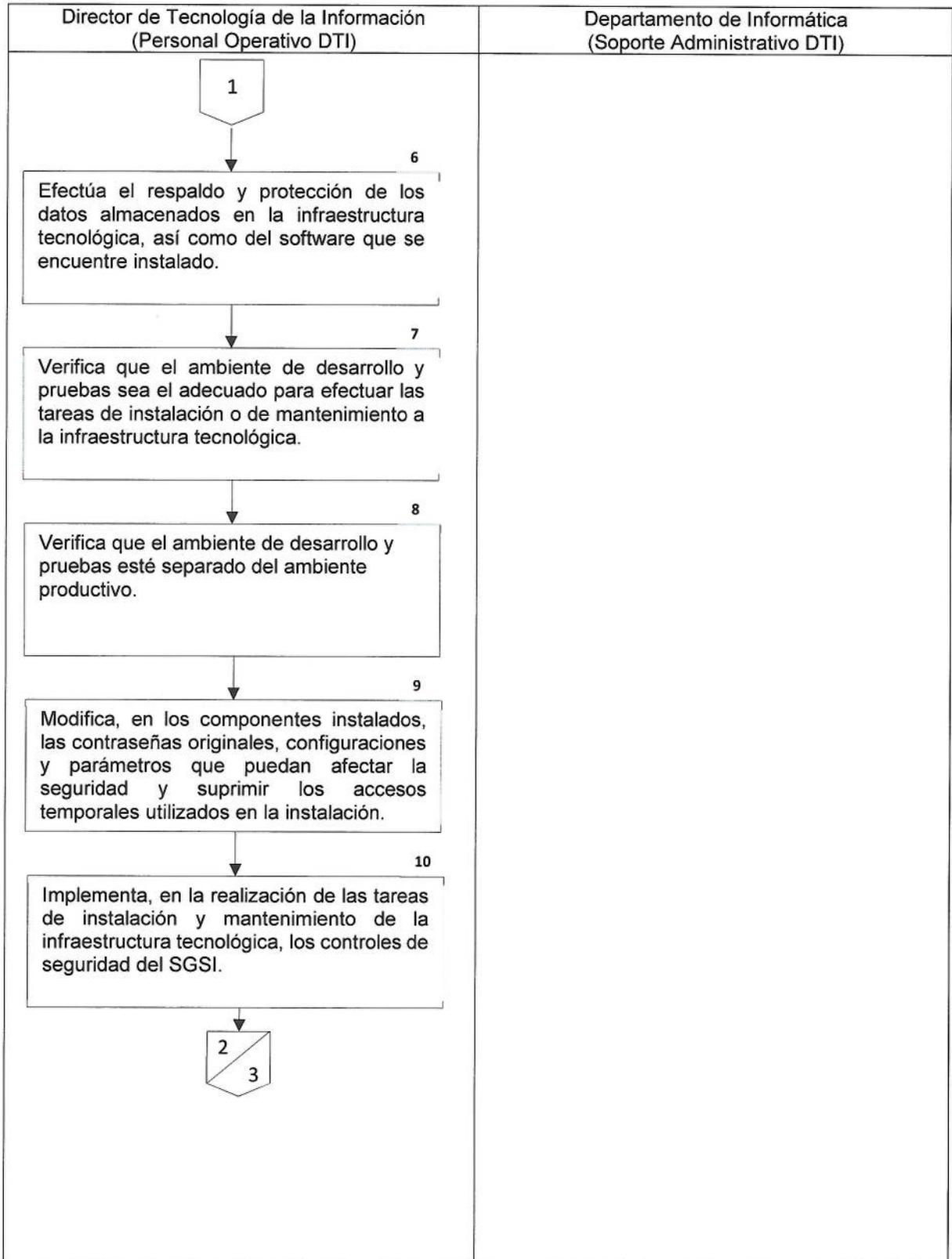
Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director de Tecnología de la Información (Personal Operativo DTI)	34	Elabora un programa de aprovisionamiento de la infraestructura tecnológica, el cual contendrá al menos: a) Los componentes que requiere y la justificación de los mismos, con base en el programa de tecnología y los servicios de TIC que soportará o complementará. b) La estimación de costos, beneficios, vida útil, disponibilidad de soporte técnico y/o mantenimiento, periodo de permanencia en el mercado, y apego a estándares tecnológicos. c) La fecha estimada en que se requerirá contar con cada componente.	Programa de mantenimiento de la infraestructura tecnológica
	35	Obtiene del grupo de trabajo para la dirección de TIC la aprobación del programa de aprovisionamiento de la infraestructura tecnológica. ¿Se aprueba programa de aprovisionamiento de infraestructura tecnológica?  No: Continuar en actividad 34 Si: Continuar en actividad 36	
Director de Tecnologías de la Información	36	Envía el programa de aprovisionamiento de la infraestructura tecnológica al responsable del proceso APCT para su trámite.	
Director de Tecnología de la Información (Personal Operativo DTI)	37	Da seguimiento al avance del programa de aprovisionamiento de la infraestructura tecnológica.	
	38	Efectúa revisiones periódicas a la infraestructura tecnológica e identificar las posibles actualizaciones o mejoras a la misma, para efectos de que sean incluidas al programa de aprovisionamiento de la infraestructura tecnológica.	Programa de aprovisionamiento de la infraestructura tecnológica

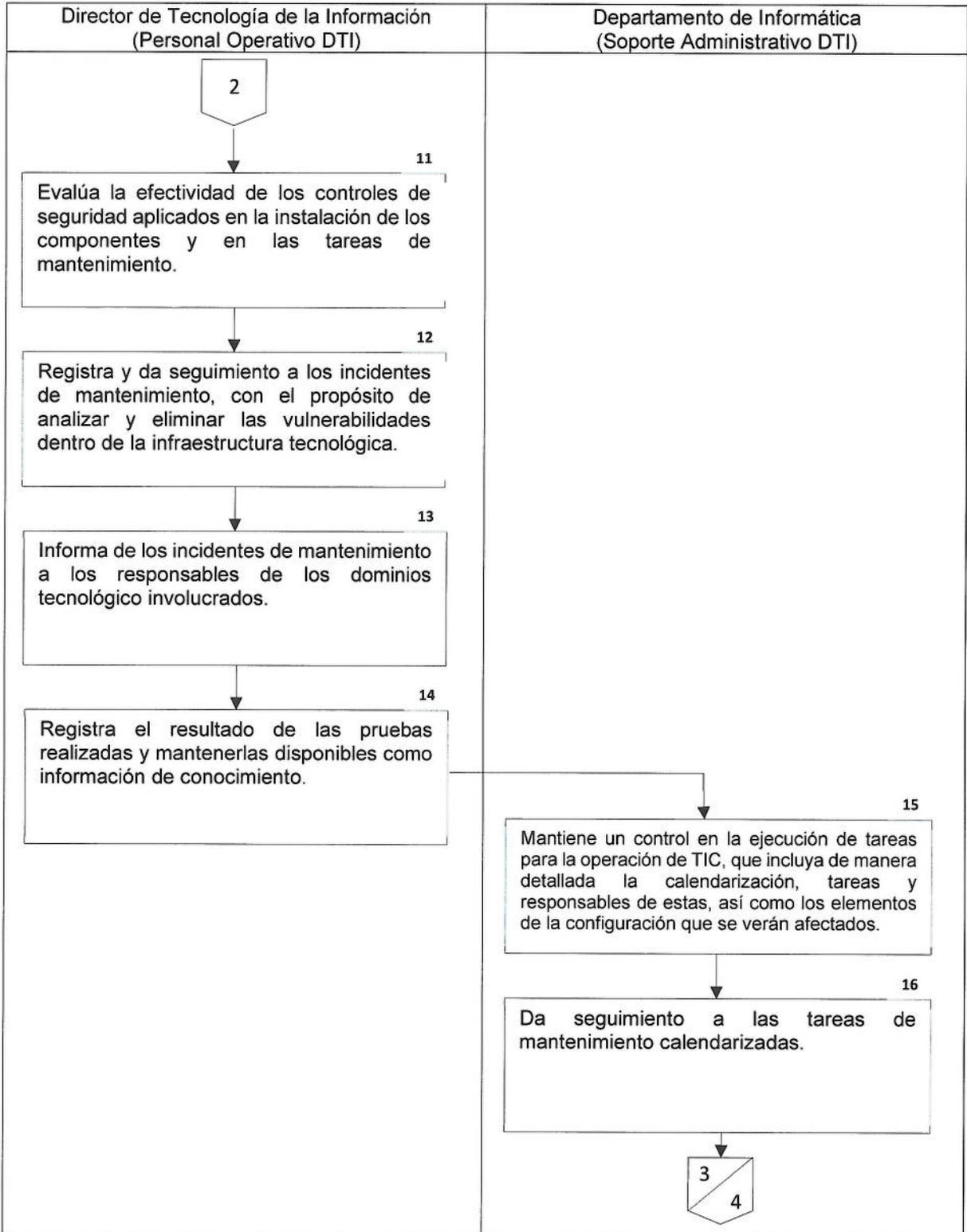
	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 8 de 20
<b>8. Procedimiento para la Administración de la Operación.</b>			

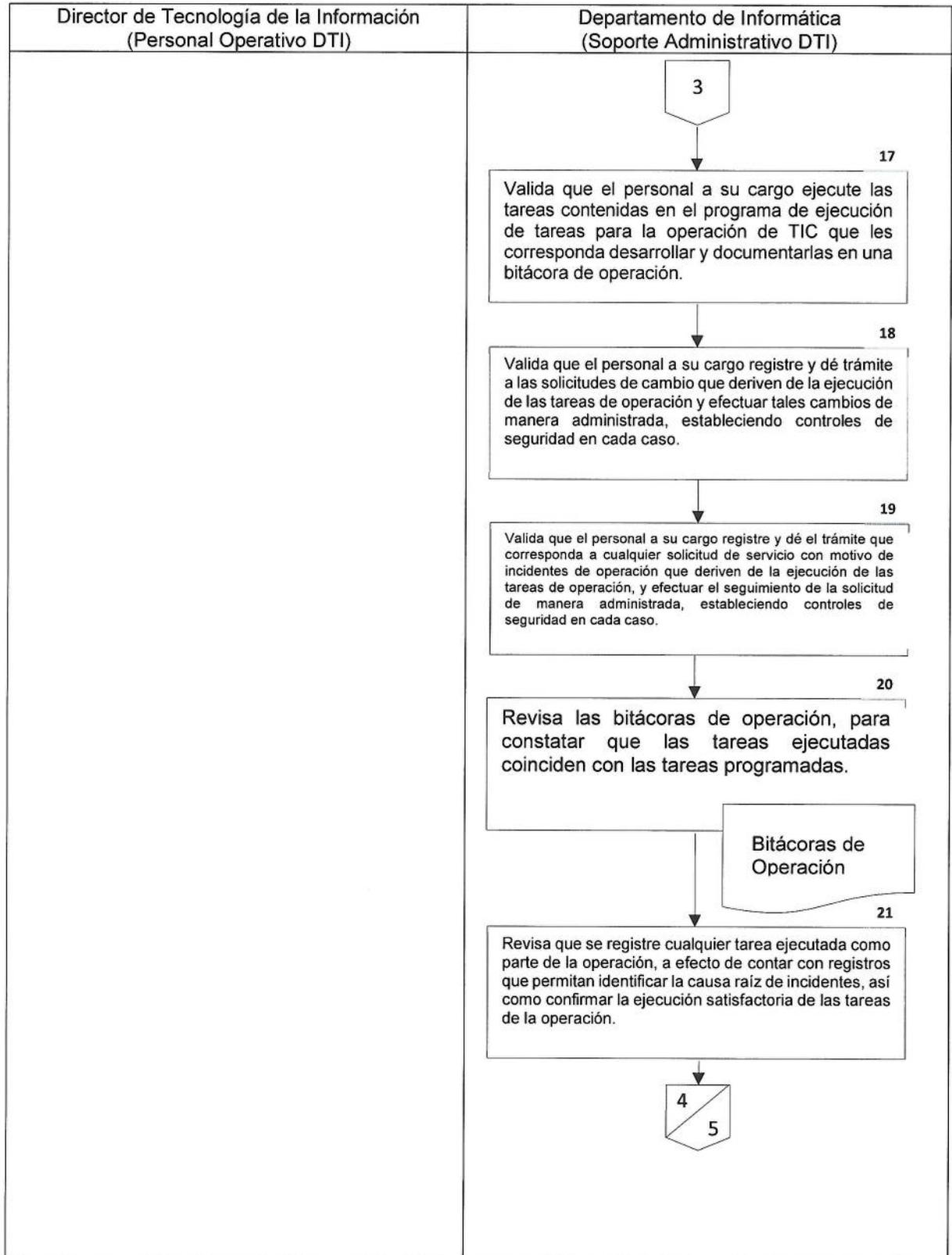
Responsable	No. Act.	Descripción de actividades	Documento o anexo
	39	Evalúa la eficiencia de los resultados del programa de aprovisionamiento de la infraestructura tecnológica e integrar la evaluación al propio programa.  TERMINA	Programa de aprovisionamiento de la infraestructura tecnológica

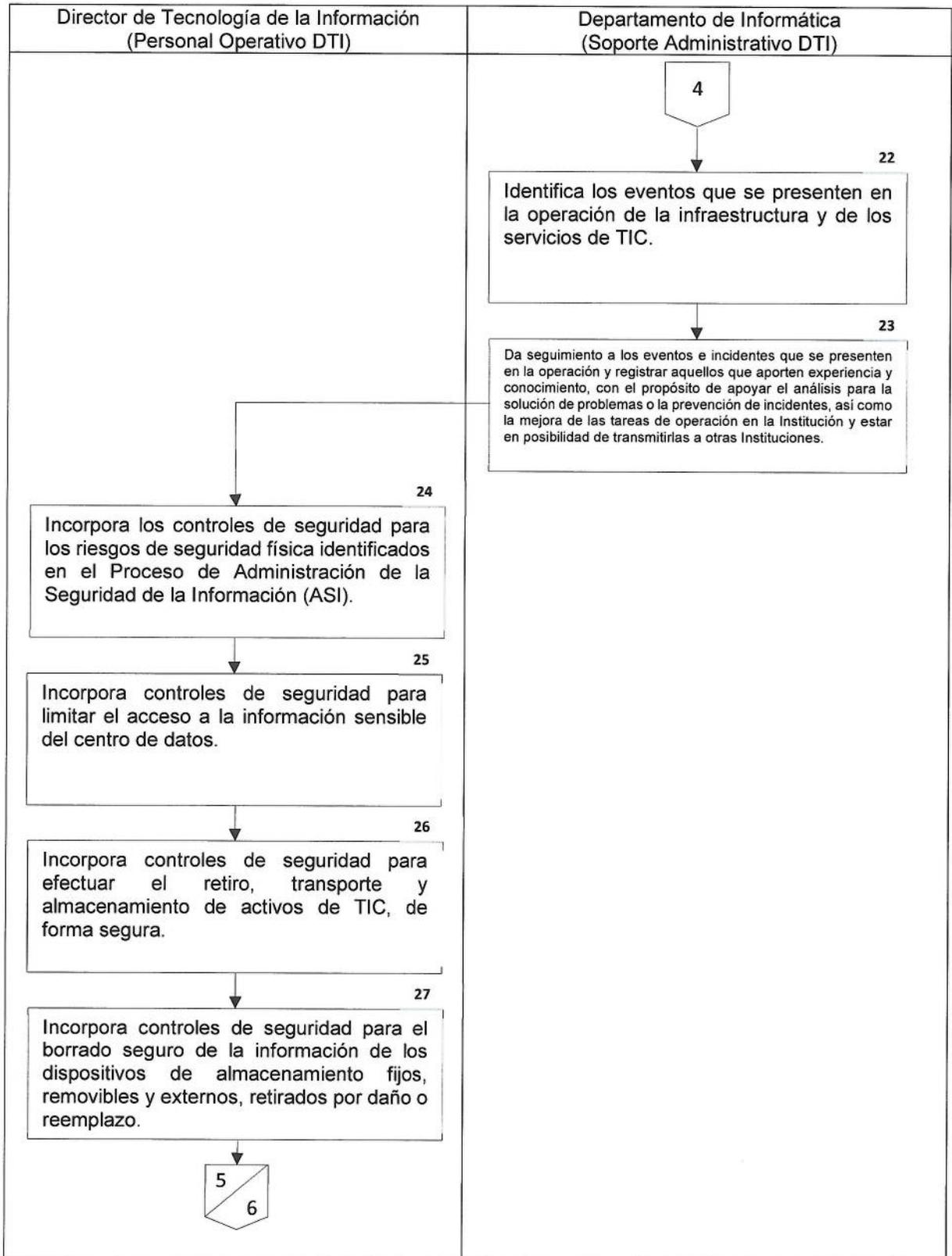
## 5. DIAGRAMA DE FLUJO

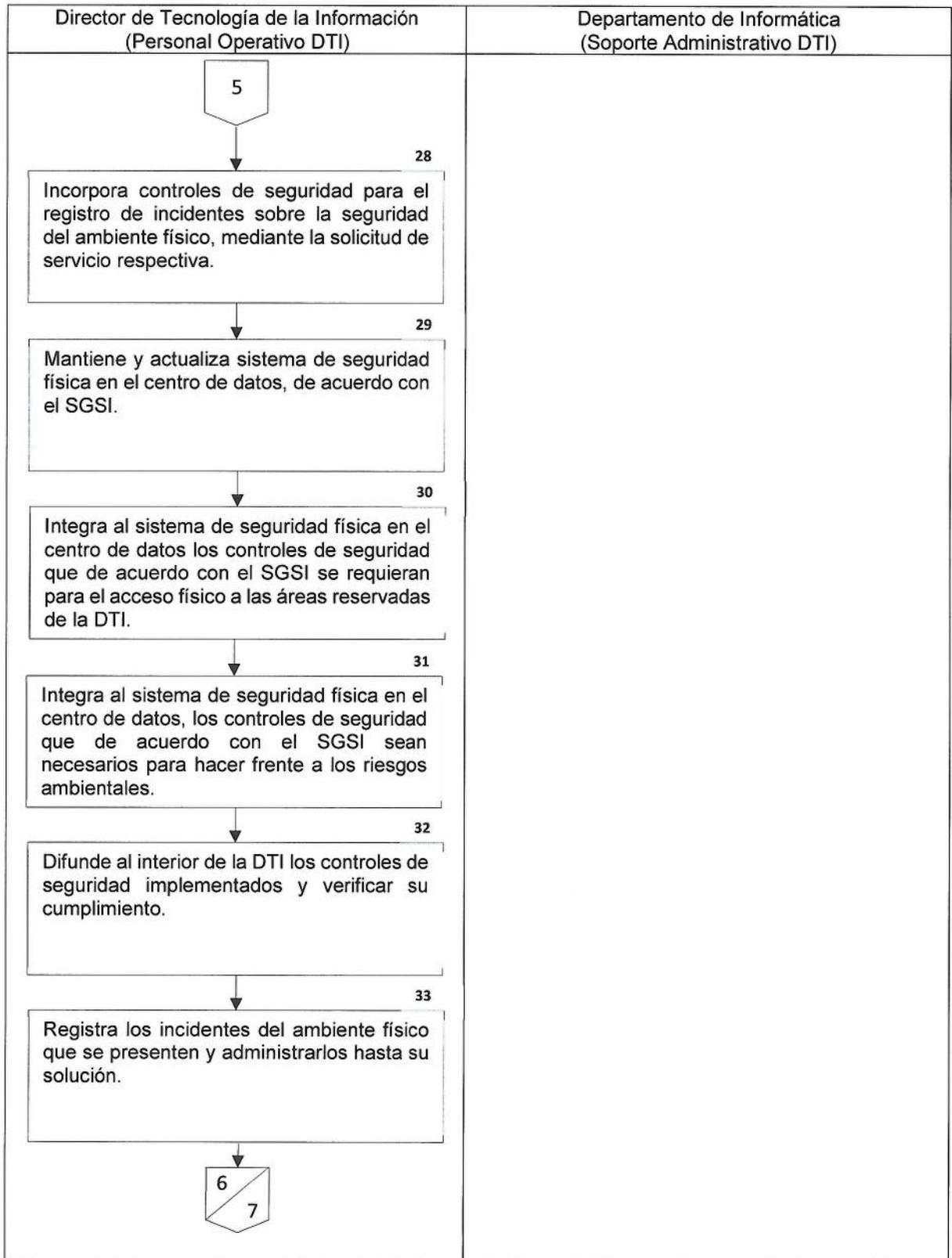


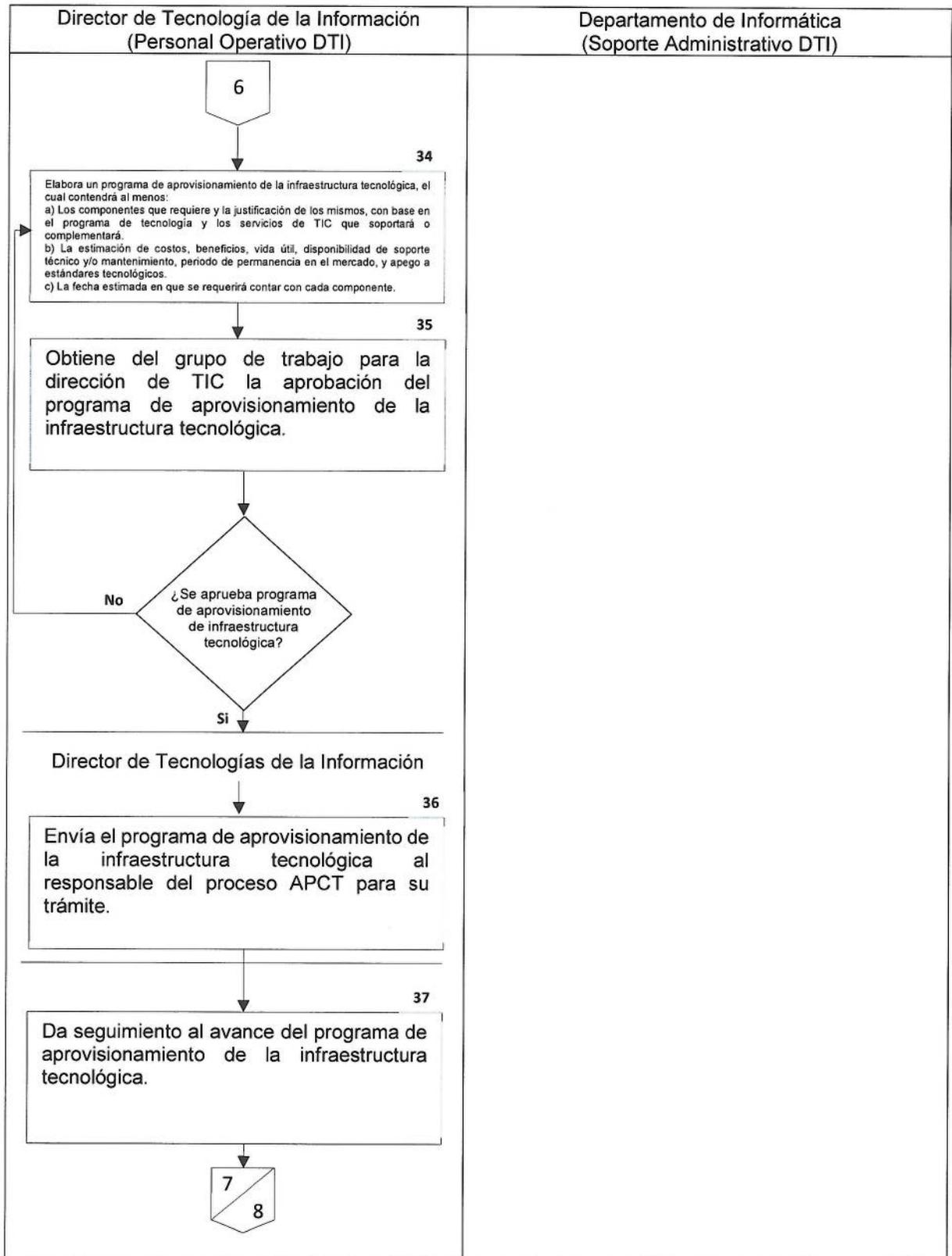




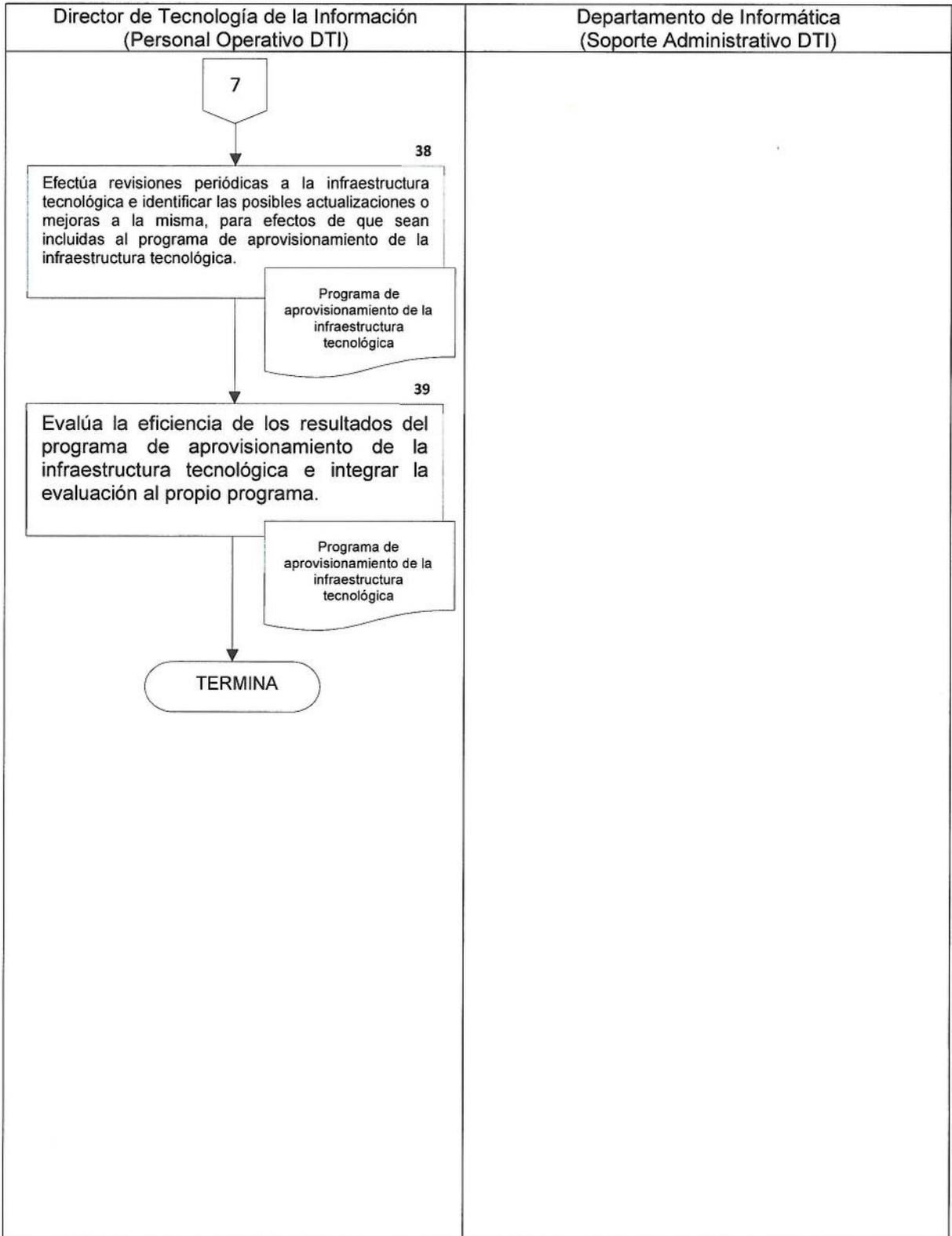








	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b> <b>8. Procedimiento para la Administración de la Operación.</b>		Hoja: 16 de 20



	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 17 de 20
	<b>8. Procedimiento para la Administración de la Operación.</b>		

## 6. DOCUMENTOS DE REFERENCIA

Nombre del documento	Código (cuando aplique)
6.1 Documento de análisis de riesgos (ASI)	No aplica
6.2 El sistema de gestión de seguridad de la información que, por medio del análisis de riesgos y de la definición de controles, define las guías para la implementación, operación, monitoreo, revisión y mejora de la seguridad de la información (SGSI /ASI)	No aplica

## 7. REGISTROS

Registros	Tiempo de conservación	Responsable de conservarlo	Código de registro o identificación única
Documento de resultados de análisis de riesgos	6 meses	Equipo de trabajo de análisis de riesgos con apoyo de las unidades administrativas involucradas	No aplica
Documento de definición del SGSI	6 meses	El grupo estratégico de Seguridad de la Información (GESI)	No aplica
Programa de aprovisionamiento de la infraestructura tecnológica	6 meses	Responsable del mantenimiento de la infraestructura	No aplica
Programa de mantenimiento de la infraestructura tecnológica	6 meses	Responsable del mantenimiento de la infraestructura	No aplica
Mecanismo de Operación y Mantenimiento de TIC	6 meses	Responsable del proceso AOP	No aplica
Bitácoras de Operación	6 meses	Responsable del proceso AOP	No aplica
Incidentes de mantenimiento	6 meses	Responsable del mantenimiento de la infraestructura	No aplica

## 8. GLOSARIO DEL PROCEDIMIENTO

- 8.1 Activos de TIC:** los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos;
- 8.2 ACNF:** proceso de administración de la configuración;
- 8.3 ADP:** proceso de administración de proyectos;
- 8.4 ADS:** proceso de administración de servicios;
- 8.5 APCT:** proceso de administración del presupuesto y las contrataciones;
- 8.6 Aplicativo de Cómputo:** el software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo a requerimientos previamente definidos;
- 8.7 APRO:** proceso de administración de proveedores;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 18 de 20
	<b>8. Procedimiento para la Administración de la Operación.</b>		

- 8.8 Arquitectura Empresarial:** la información del estado actual y futuro de una Institución, a partir del análisis con perspectiva estratégica; considerando modelos de negocio, procesos, aplicativos y tecnologías de la información y comunicaciones;
- 8.9 Arquitectura Orientada a Servicios:** la metodología y marco de trabajo, para construir componentes de software reutilizables para la interoperabilidad de aplicativos de cómputo;
- 8.10 AOP:** proceso de administración de la operación;
- 8.11 ASI:** proceso de administración de la seguridad de la Información.
- 8.12 Borrado Seguro:** el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital;
- 8.13 Cartera Ejecutiva de Proyectos de TIC:** Conjunto total de proyectos de TIC que la institución propondrá a la Unidad para su seguimiento;
- 8.14 Cartera Operativa de Proyectos de TIC:** Conjunto total de proyectos que soportan la operación diaria de la DTI y no son considerados como estratégicos;
- 8.15 Centro de Datos:** el lugar físico en los que se ubiquen los activos de TIC y desde el que se proveen servicios de TIC;
- 8.16 Cómputo en la Nube:** al modelo de prestación de servicios digitales que permite a las Instituciones acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios;
- 8.17 Dependencias:** las Secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como a la Oficina de la Presidencia de la República y la Procuraduría General de la República; así como los Órganos Reguladores Coordinados en Materia Energética;
- 8.18 Dominio Tecnológico:** las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo;
- 8.19 CMDB:** Base de Datos de la Gestión de la Configuración.
- 8.20 EDN:** la Estrategia Digital Nacional contenida en el Objetivo número 5 del Programa;
- 8.21 EIDA:** el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, establecido mediante Acuerdo publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011;
- 8.22 Entidades:** los organismos descentralizados, empresas de participación estatal mayoritaria, instituciones nacionales de crédito, organizaciones auxiliares nacionales de crédito e instituciones nacionales de seguros y de fianzas, y fideicomisos públicos que en términos de la Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales, sean considerados entidades de la Administración Pública Federal Paraestatal;
- 8.23 ERISC:** equipo de respuesta a incidentes de seguridad en TIC en la Institución;
- 8.24 Estándar abierto:** a las especificaciones cuya utilización esté disponible de manera gratuita o que no suponga una dificultad de acceso, y que su uso y aplicación no esté condicionada al pago de un derecho de propiedad
- 8.25 Herramienta de Gestión de la Política TIC:** sistema web usado para llevar a cabo la comunicación de actividades de reporte establecidas en el Acuerdo, considerando el reporte de PETIC, la obtención del dictamen técnico que emite la Unidad, autorización por parte de la UPCP, la arquitectura empresarial, el MAAGTICSI, entre otros;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 19 de 20
	<b>8. Procedimiento para la Administración de la Operación.</b>		

- 8.26 Infraestructuras Críticas de Información:** Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia.
- 8.27 Infraestructuras de Información esenciales:** Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de información, TIC y TO, cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación de las Instituciones.
- 8.28 Infraestructura de TIC:** el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC;
- 8.29 Infraestructura Pasiva:** elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de las dependencias o entidades, que sean necesarios para la instalación y operación de las redes, así como para la prestación de servicios de procesamiento de datos, de telecomunicaciones y radiodifusión;
- 8.30 Instancias de Seguridad Nacional:** las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquellas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional;
- 8.31 Institución:** las dependencias y entidades de la Administración Pública Federal, tal y como se definen en este Acuerdo;
- 8.32 Lineamientos:** los Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicados en el Diario Oficial de la Federación el 30 de enero de 2013;
- 8.33 MAAGMAASSP:** el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público;
- 8.34 MAAGTICSI:** el Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información. Anexo Único del presente Acuerdo;
- 8.35 Niveles de servicio:** el establecimiento en un lenguaje no técnico del servicio brindado, incluyendo al menos la definición, disponibilidad, calidad, tiempos de respuesta y solución.
- 8.36 OPEC:** proceso de operación de los controles de seguridad de la información y del erisc;
- 8.37 PE:** proceso de planeación estratégica;
- 8.38 PETIC:** el conjunto de proyectos que elaboran las Instituciones, conformado por un máximo de 7 proyectos estratégicos, en los términos establecidos en el presente Acuerdo;
- 8.39 Portafolio de proyectos de TIC:** es el total de los proyectos de TIC agrupados según su clasificación en Cartera Ejecutiva de Proyectos de TIC y Cartera Operativa de Proyectos de TIC que la Institución planea desarrollar, en los términos establecidos por el MAAGTICSI;
- 8.40 Programa:** el Programa para un Gobierno Cercano y Moderno 2013-2018, aprobado mediante Decreto publicado en el Diario Oficial de la Federación el 30 de agosto de 2013;
- 8.41 Proyectos de TIC:** el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC y que cuenta con presupuesto para su ejecución; considerando 2 tipos: proyectos operativos que soportan las actividades diarias de la DTI y proyectos estratégicos en los términos señalados en el presente Acuerdo;

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 20 de 20
	<b>8. Procedimiento para la Administración de la Operación.</b>		

**8.42 Retos Públicos:** el modelo que fomenta la democratización del gasto público y la innovación, invitando a los emprendedores del país a plantear soluciones a retos de gobierno mediante el desarrollo de aplicativos tecnológicos web y móviles;

**8.43 SEGOB:** la Secretaría de Gobernación;

**8.44 Seguridad de la información:** la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma;

**8.45 Seguridad Nacional:** las acciones a las que se refiere el artículo 3 de la Ley de Seguridad Nacional;

**8.46 SGSI:** El sistema de gestión de seguridad de la información que, por medio del análisis de riesgos y de la definición de controles, define las guías para la implementación, operación, monitoreo, revisión y mejora de la seguridad de la información;

**8.47 SFP:** la Secretaría de la Función Pública;

**8.48 SHCP:** la Secretaría de Hacienda y Crédito Público;

**8.49 Tecnologías Verdes:** el conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las tecnologías de la información y comunicaciones, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías;

**8.50 TIC:** las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video;

**8.51 Unidad:** la Unidad de Gobierno Digital de la SFP;

**8.52 DTIC:** la Dirección de Tecnologías de Información y Comunicaciones o área responsables de las TIC en la Institución.

## 9. CAMBIOS DE VERSIÓN DEL PROCEDIMIENTO

Numero de revisión	Fecha de actualización	Descripción del cambio
0	No aplica	No aplica

## 10. ANEXOS DEL PROCEDIMIENTO

No aplica

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 1 de 10
	<b>9. Operación de los Controles de Seguridad de la Información y del Equipo de Respuesta a Incidentes de Seguridad en TIC en la Institución.</b>		

## 1. PROPÓSITO

Establecer la funcionalidad del proceso de Operación de los Controles de Seguridad de la Información y del Equipo de Respuesta a Incidentes de Seguridad en TIC en la Institución (ERISC), derivado del Manual Administrativo de Aplicación General en Materias de Tecnología de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), mediante la asignación de los roles identificados en el proceso y sus subprocesos, formalizando la asignación del rol a los responsables que participan en la ejecución de cada una de las tareas del proceso, con el fin de obtener la información, evidencias y entregables que generen las actividades ejecutadas durante el proceso.

## 2. ALCANCE

- 2.1 Obtener el mapa del proceso y de las actividades de los subprocesos involucrados, que permitan identificar la funcionalidad del proceso OPEC.
- 2.2 Identificar los roles o los actores que se requieren para que el proceso genere las evidencias y entregables que demuestren la funcionalidad del proceso.
- 2.3 Identificar a las áreas o personas que se harán responsables de los diferentes roles que requiere el proceso.
- 2.4 Formalizar las asignaciones de responsables de roles y actividades.
- 2.5 Establecer si es necesario entre las áreas identificadas que participarán con alguna responsabilidad en el proceso un OLA, acuerdo de operación, en el cual se especifiquen los servicios que se aportarán y los tiempos en los que se atenderán y los entregables comprometidos que requiere el proceso.
- 2.6 Identificar las capacitaciones que se requieran en las diferentes áreas o personas que asuman el rol asignado, para que se consideren en un programa de capacitación.
- 2.7 Identificar los indicadores de desempeño del proceso y registrarlos periódicamente para su evaluación posterior.
- 2.8 Identificar los indicadores de los servicios considerados y sus métricas.

## 3. POLÍTICAS DE OPERACIÓN, NORMAS Y LINEAMIENTOS

- 3.1 El responsable de este proceso estará a cargo de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 2 de 10
	<b>9. Operación de los Controles de Seguridad de la Información y del Equipo de Respuesta a Incidentes de Seguridad en TIC en la Institución.</b>		

#### 4. DESCRIPCIÓN DEL PROCEDIMIENTO

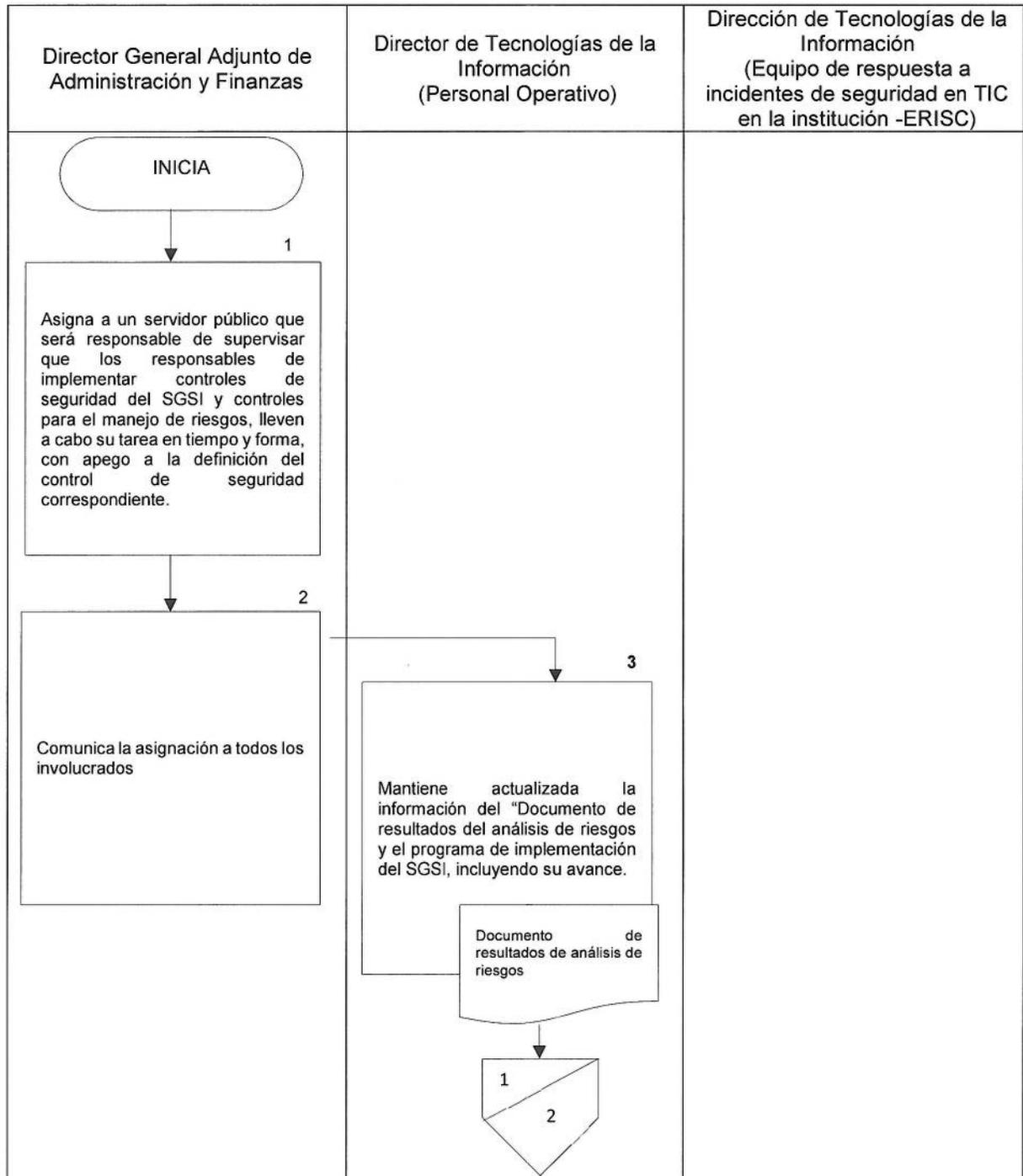
Responsable	No. Act.	Descripción de actividades	Documento o anexo
Director General Adjunto de Administración y Finanzas	1	Asigna a un servidor público que será responsable de supervisar que los responsables de implementar controles de seguridad del SGSI y controles para el manejo de riesgos, lleven a cabo su tarea en tiempo y forma, con apego a la definición del control de seguridad correspondiente.	
	2	Comunica la asignación a todos los involucrados	
Director de Tecnologías de la Información (Personal Operativo)	3	Mantiene actualizada la información del "Documento de resultados del análisis de riesgos y el programa de implementación del SGSI, incluyendo su avance.	Documento de resultados de análisis de riesgos
Director General Adjunto de Administración y Finanzas	4	Establece las reglas de operación del ERISC, en las que se preverán los mecanismos de coordinación del ERISC al interior de la Institución o con otros ERISC u organizaciones externas, en concordancia con la directriz rectora de respuesta a incidentes, incluyendo al menos, los relativos a: a) Los canales de comunicación, que deberán ser seguros. b) Los relativos a la diseminación de datos de los incidentes.	
Dirección de Tecnologías de la Información (Equipo de respuesta a incidentes de seguridad en TIC en la institución - ERISC)	5	Elabora, de acuerdo a lo establecido en la directriz rectora de respuesta a incidentes, la guía técnica de atención a incidentes, de acuerdo a la criticidad de los activos de TIC afectados, considerando en su elaboración al menos los siguientes apartados: a) Detección y registro de los incidentes. b) Priorización de los incidentes. c) Investigación técnica de los incidentes. d) Criterios técnicos de contención de los incidentes, de acuerdo a la criticidad de los activos de TIC. e) Obtención, preservación y destino de los indicios de los incidentes. f) Erradicación de los incidentes. g) Recuperación de la operación. h) Documentación de las lecciones aprendidas.	Guía Técnica de atención a incidentes

 	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>LABORATORIO DE BIOMÉTRICA Y REACTIVOS QUÍMICOS S. S. DE C. S.</small>	Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 3 de 10
	<b>9. Operación de los Controles de Seguridad de la Información y del Equipo de Respuesta a Incidentes de Seguridad en TIC en la Institución.</b>		

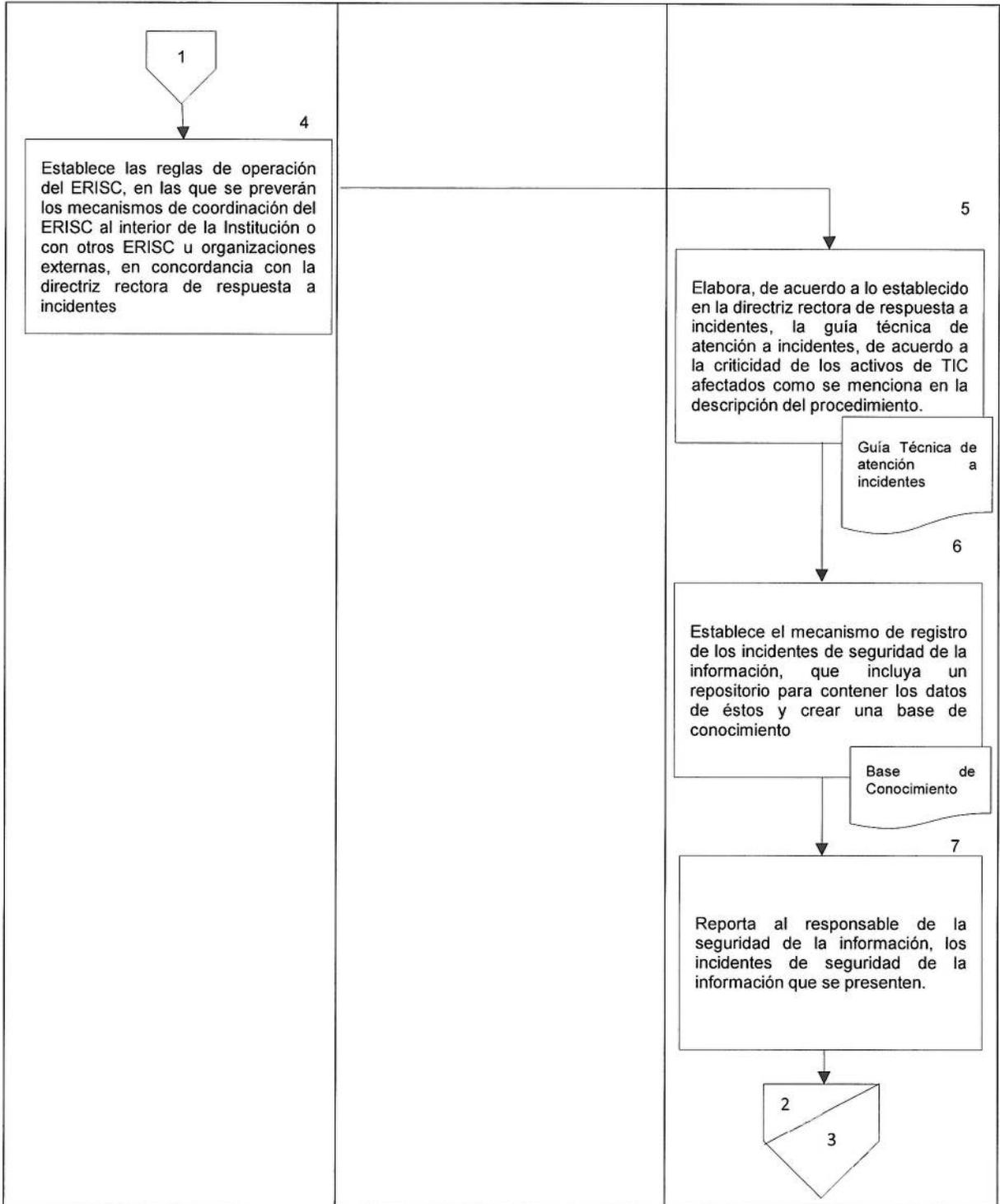
Responsable	No. Act.	Descripción de actividades	Documento o anexo
Dirección de Tecnologías de la Información (Equipo de respuesta a incidentes de seguridad en TIC en la institución - ERISC)	6	Establece el mecanismo de registro de los incidentes de seguridad de la información, que incluya un repositorio para contener los datos de éstos y crear una base de conocimiento	Base de Conocimiento
	7	Reporta al responsable de la seguridad de la información, los incidentes de seguridad de la información que se presenten	
	8	Define las acciones de atención a los incidentes con apoyo de la guía técnica de atención de incidentes, respecto del incidente que se haya presentado.	
	9	Asegura que los responsables de la implementación de los controles de seguridad de la información y de manejo de riesgos, ejecuten las acciones siguientes: a) Apliquen la solución necesaria. b) Registren los datos del incidente y su solución. c) Comuniquen el incidente y su solución al grupo estratégico de seguridad de la información y a los responsables de los dominios tecnológicos involucrados, así como a los usuarios afectados.	
	10	Integra los datos del incidente y su solución a los repositorios con los que cuenta la DTI y en su caso, a los repositorios de la Institución que determine el grupo estratégico de seguridad de la información.  TERMINA	Base de Conocimiento

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 4 de 10
	<b>9. Operación de los Controles de Seguridad de la Información y del Equipo de Respuesta a Incidentes de Seguridad en TIC en la Institución.</b>		

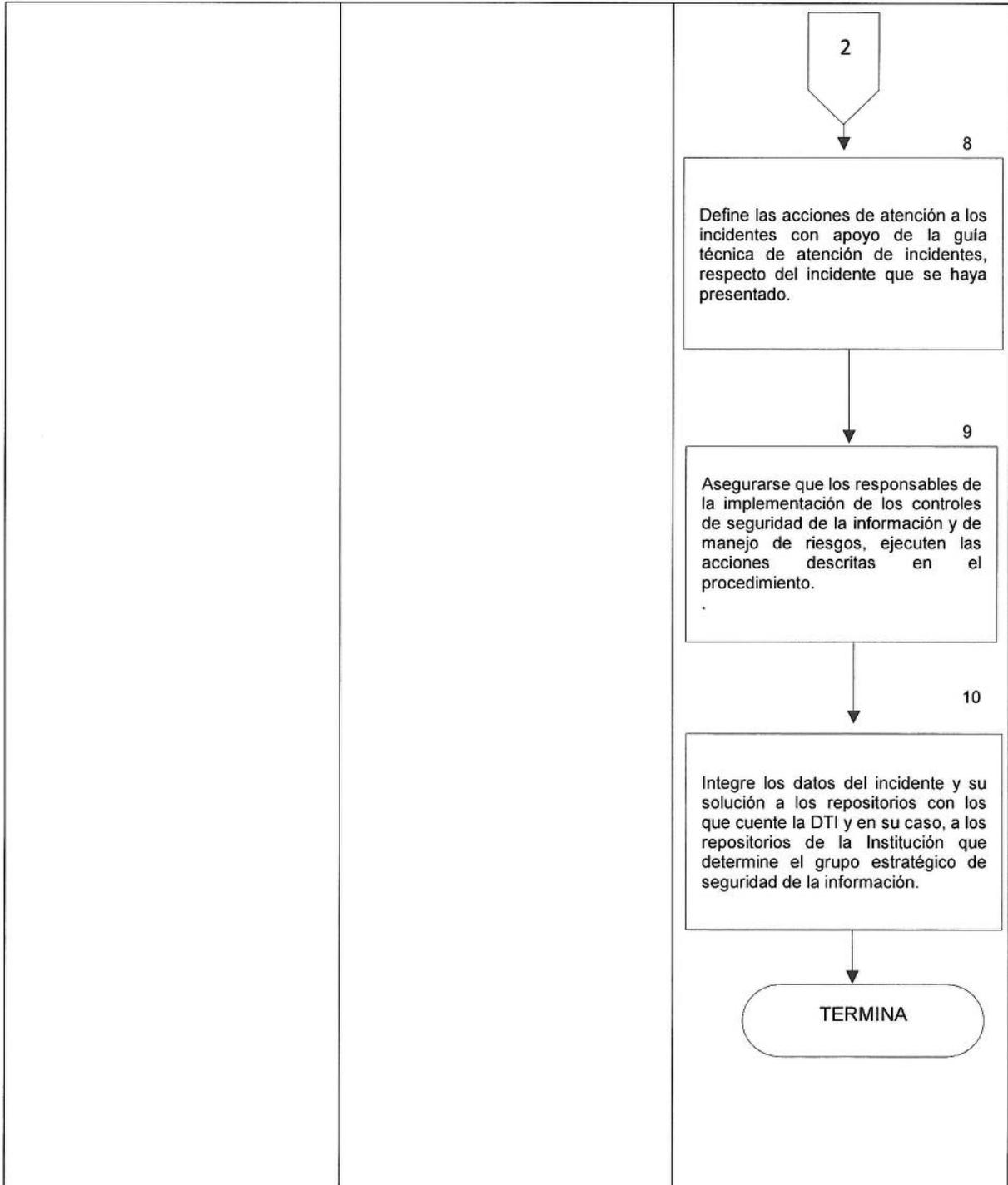
## 5. DIAGRAMA DE FLUJO



	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 5 de 10
	<b>9. Operación de los Controles de Seguridad de la Información y del Equipo de Respuesta a Incidentes de Seguridad en TIC en la Institución.</b>		



	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	Dirección de Tecnologías de la Información		Hoja: 6 de 10
	<b>9. Operación de los Controles de Seguridad de la Información y del Equipo de Respuesta a Incidentes de Seguridad en TIC en la Institución.</b>		



	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 7 de 10
	<b>9. Operación de los Controles de Seguridad de la Información y del Equipo de Respuesta a Incidentes de Seguridad en TIC en la Institución.</b>		

## 6. DOCUMENTOS DE REFERENCIA

Nombre del documento	Código (cuando aplique)
6.1 Documento de análisis de riesgos (ASI)	No aplica
6.2 El sistema de gestión de seguridad de la información que, por medio del análisis de riesgos y de la definición de controles, define las guías para la implementación, operación, monitoreo, revisión y mejora de la seguridad de la información (SGSI /ASI)	No aplica

## 7. REGISTROS

Registros	Tiempo de conservación	Responsable de conservarlo	Código de registro o identificación única
Guía Técnica de Atención a Incidentes	1 año	Equipo de respuesta a incidentes de seguridad en TIC en la institución (ERISC)	No aplica
Documento de resultados de análisis de riesgos	1 año	Responsable del proceso ASI	No aplica
Documento de definición del SGSI	1 año	Responsable del proceso ASI	No aplica

## 8. GLOSARIO DEL PROCEDIMIENTO

- 8.1 Activos de TIC:** los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos;
- 8.2 ACNF:** proceso de administración de la configuración;
- 8.3 ADP:** proceso de administración de proyectos;
- 8.4 ADS:** proceso de administración de servicios;
- 8.5 APCT:** proceso de administración del presupuesto y las contrataciones;
- 8.6 Aplicativo de Cómputo:** el software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas contruidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo a requerimientos previamente definidos;
- 8.7 APRO:** proceso de administración de proveedores;
- 8.8 Arquitectura Empresarial:** la información del estado actual y futuro de una Institución, a partir del análisis con perspectiva estratégica; considerando modelos de negocio, procesos, aplicativos y tecnologías de la información y comunicaciones;
- 8.9 Arquitectura Orientada a Servicios:** la metodología y marco de trabajo, para construir componentes de software reutilizables para la interoperabilidad de aplicativos de cómputo;
- 8.10 AOP:** proceso de administración de la operación;
- 8.11 ASI:** proceso de administración de la seguridad de la Información.

	<b>MANUAL DE PROCEDIMIENTOS</b>	 <small>COMITÉ INTERSECTORIAL DE SEGURIDAD EN BIRMEX</small> <small>SECRETARÍA DE SALUD</small>	Revisión: A
	<b>Dirección de Tecnologías de la Información</b>		Hoja: 8 de 10
	<b>9. Operación de los Controles de Seguridad de la Información y del Equipo de Respuesta a Incidentes de Seguridad en TIC en la Institución.</b>		

- 8.12 Borrado Seguro:** el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital;
- 8.13 Cartera Ejecutiva de Proyectos de TIC:** Conjunto total de proyectos de TIC que la institución propondrá a la Unidad para su seguimiento;
- 8.14 Cartera Operativa de Proyectos de TIC:** Conjunto total de proyectos que soportan la operación diaria de la DTI y no son considerados como estratégicos;
- 8.15 Centro de Datos:** el lugar físico en los que se ubiquen los activos de TIC y desde el que se proveen servicios de TIC;
- 8.16 Cómputo en la Nube:** al modelo de prestación de servicios digitales que permite a las Instituciones acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios;
- 8.17 Dependencias:** las Secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como a la Oficina de la Presidencia de la República y la Procuraduría General de la República; así como los Órganos Reguladores Coordinados en Materia Energética;
- 8.18 Dominio Tecnológico:** las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo;
- 8.19 EDN:** la Estrategia Digital Nacional contenida en el Objetivo número 5 del Programa;
- 8.20 EIDA:** el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, establecido mediante Acuerdo publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011;
- 8.21 Entidades:** los organismos descentralizados, empresas de participación estatal mayoritaria, instituciones nacionales de crédito, organizaciones auxiliares nacionales de crédito e instituciones nacionales de seguros y de fianzas, y fideicomisos públicos que en términos de la Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales, sean considerados entidades de la Administración Pública Federal Paraestatal;
- 8.22 ERISC:** equipo de respuesta a incidentes de seguridad en TIC en la Institución;
- 8.23 Estándar abierto:** a las especificaciones cuya utilización esté disponible de manera gratuita o que no suponga una dificultad de acceso, y que su uso y aplicación no esté condicionada al pago de un derecho de propiedad
- 8.24 Herramienta de Gestión de la Política TIC:** sistema web usado para llevar a cabo la comunicación de actividades de reporte establecidas en el Acuerdo, considerando el reporte de PETIC, la obtención del dictamen técnico que emite la Unidad, autorización por parte de la UPCP, la arquitectura empresarial, el MAAGTICSI, entre otros;
- 8.25 Infraestructuras Críticas de Información:** Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia.

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b> <b>9. Operación de los Controles de Seguridad de la Información y del Equipo de Respuesta a Incidentes de Seguridad en TIC en la Institución.</b>		Hoja: 9 de 10

- 8.26 Infraestructuras de Información esenciales:** Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de información, TIC y TO, cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación de las Instituciones.
- 8.27 Infraestructura de TIC:** el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC;
- 8.28 Infraestructura Pasiva:** elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de las dependencias o entidades, que sean necesarios para la instalación y operación de las redes, así como para la prestación de servicios de procesamiento de datos, de telecomunicaciones y radiodifusión;
- 8.29 Instancias de Seguridad Nacional:** las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquellas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional;
- 8.30 Institución:** las dependencias y entidades de la Administración Pública Federal, tal y como se definen en este Acuerdo;
- 8.31 Lineamientos:** los Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicados en el Diario Oficial de la Federación el 30 de enero de 2013;
- 8.32 MAAGMAASSP:** el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público;
- 8.33 MAAGTICSI:** el Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información. Anexo Único del presente Acuerdo;
- 8.34 Niveles de servicio:** el establecimiento en un lenguaje no técnico del servicio brindado, incluyendo al menos la definición, disponibilidad, calidad, tiempos de respuesta y solución.
- 8.35 OPEC:** proceso de operación de los controles de seguridad de la información y del erisc;
- 8.36 PE:** proceso de planeación estratégica;
- 8.37 PETIC:** el conjunto de proyectos que elaboran las Instituciones, conformado por un máximo de 7 proyectos estratégicos, en los términos establecidos en el presente Acuerdo;
- 8.38 Portafolio de proyectos de TIC:** es el total de los proyectos de TIC agrupados según su clasificación en Cartera Ejecutiva de Proyectos de TIC y Cartera Operativa de Proyectos de TIC que la Institución planea desarrollar, en los términos establecidos por el MAAGTICSI;
- 8.39 Programa:** el Programa para un Gobierno Cercano y Moderno 2013-2018, aprobado mediante Decreto publicado en el Diario Oficial de la Federación el 30 de agosto de 2013;
- 8.40 Proyectos de TIC:** el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC y que cuenta con presupuesto para su ejecución; considerando 2 tipos:

	<b>MANUAL DE PROCEDIMIENTOS</b>		Revisión: A
	<b>Dirección de Tecnologías de la Información</b> <b>9. Operación de los Controles de Seguridad de la Información y del Equipo de Respuesta a Incidentes de Seguridad en TIC en la Institución.</b>		Hoja: 10 de 10

proyectos operativos que soportan las actividades diarias de la DTI y proyectos estratégicos en los términos señalados en el presente Acuerdo;

**8.41 Retos Públicos:** el modelo que fomenta la democratización del gasto público y la innovación, invitando a los emprendedores del país a plantear soluciones a retos de gobierno mediante el desarrollo de aplicativos tecnológicos web y móviles;

**8.42 SEGOB:** la Secretaría de Gobernación;

**8.43 Seguridad de la información:** la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma;

**8.44 Seguridad Nacional:** las acciones a las que se refiere el artículo 3 de la Ley de Seguridad Nacional;

**8.45 SFP:** la Secretaría de la Función Pública;

**8.46 SHCP:** la Secretaría de Hacienda y Crédito Público;

**8.47 Tecnologías Verdes:** el conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las tecnologías de la información y comunicaciones, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías;

**8.48 TIC:** las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video;

**8.49 Unidad:** la Unidad de Gobierno Digital de la SFP;

**8.50 DTIC:** la Dirección de Tecnologías de Información y Comunicaciones o área responsables de las TIC en la Institución.

## 9. CAMBIOS DE VERSIÓN DEL PROCEDIMIENTO

Numero de revisión	Fecha de actualización	Descripción del cambio
0	No aplica	No aplica

## 10. ANEXOS DEL PROCEDIMIENTO

No aplica