

**PROCURADURÍA GENERAL DE LA
REPÚBLICA**

SUBDIRECCIÓN DE INFOTECNOLOGÍA

MANUAL DE PROCEDIMIENTOS

CÓDIGO
MP-SDIT-001

18 DE MAYO DE 2026

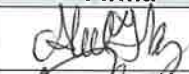
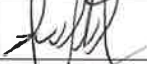
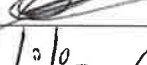
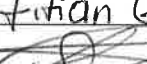
	PROCURADURÍA GENERAL DE LA REPÚBLICA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001	SUBDIRECCIÓN DE INFOTECNOLOGÍA	
MANUAL DE PROCEDIMIENTOS		UDEM
Versión 1.0	Fecha: 18 de mayo 2026	2 de 183

Responsables de los Cambios al Manual de Procedimientos

Elaboración del Documento

Elaborado por:	Cargo	Área de Trabajo	Fecha	Firma
Suyapa del Mar Andino Ordoñez	Jefa de Unidad	Unidad de Modernización	18 de mayo de 2026	

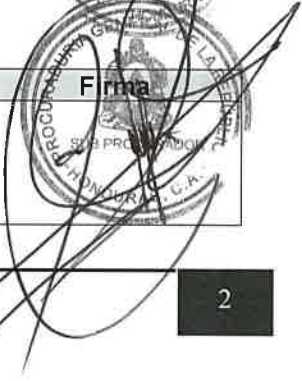
Revisión del Documento

Revisado por:	Cargo	Área de Trabajo	Fecha	Firma
Abel Fernando Perez Vargas	Auxiliar Técnico	Subdirección de Infotecnología	19 de mayo de 2026	
Ángel Gustavo Reyes Molina	Oficial Técnico	Subdirección de Infotecnología	19 de mayo de 2026	
Arnaldo Alcides García Alvarado	Oficial Técnico	Subdirección de Infotecnología	19 de mayo de 2026	
Cristian Alexander Martínez Ochoa	Oficial Técnico	Subdirección de Infotecnología	19 de mayo de 2026	
Daniel Isaac Membreño Anariba	Auxiliar Técnico	Subdirección de Infotecnología	19 de mayo de 2026	
Pablo Javier Padilla Avilés	Oficial Técnico	Subdirección de Infotecnología	19 de mayo de 2026	
Lilian Iveth Galo Andrade	Asistente Administrativo	Subdirección de Infotecnología	19 de mayo de 2026	
Lisandro Alfredo Suárez Salinas	Oficial Técnico	Subdirección de Infotecnología	19 de mayo de 2026	

Verificación del Documento

Verificado por:	Cargo	Área de Trabajo	Fecha	Firma
Jorge Efraín Salgado	Subdirector de Infotecnología	Subdirección de Infotecnología	20 de mayo de 2026	
Ingrid Karina López Fuentes	Directora	Dirección de Administración y Finanzas	20 de mayo de 2026	

Aprobación del Documento

Aprobado por:	Cargo	Área de Trabajo	Fecha	Firma
José Francisco Quiroz Mejía	Sub-Procurador General de la República	Despacho de la Sub-Procuraduría General de la República	22 de mayo de 2026	

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UEM 3 de 183

Tabla de Contenido

1. INTRODUCCIÓN.....	4
2. ANTECEDENTES	5
3. JUSTIFICACIÓN DEL MANUAL DE PROCEDIMIENTOS	8
4. ESTRUCTURA ORGANIZACIONAL.....	9
5. IDENTIFICACIÓN DE FUNCIONES SUSTANTIVAS	10
6. IDENTIFICACIÓN DE PROCEDIMIENTOS SUSTANTIVOS	11
7. FICHAS DE PROCESOS.....	12
8. DESCRIPCIÓN DE LOS PROCEDIMIENTOS.....	31

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UEM 4 de 183

1. INTRODUCCIÓN

El presente Manual de Procedimientos de la Subdirección de Infotecnología adscrita a la Dirección de Administración y Finanzas de la Procuraduría General de la República (PGR) constituye un instrumento técnico-administrativo orientado a documentar, ordenar y estandarizar los procedimientos desarrollados por dicha Subdirección en el marco de sus competencias institucionales. Su elaboración responde a la necesidad de contar con una herramienta formal que describa de manera clara, secuencial y verificable las actividades, responsables, insumos, productos, controles y flujos de trabajo vinculados a la gestión de los servicios tecnológicos, soporte informático, administración de sistemas, infraestructura tecnológica, seguridad de la información y demás funciones propias del área.

La Subdirección de Infotecnología cumple un rol estratégico de apoyo institucional, al facilitar el uso eficiente de las tecnologías de la información y comunicación en los procesos sustantivos, administrativos y de gestión de la PGR. En tal sentido, la documentación de sus procedimientos contribuye a fortalecer la continuidad operativa, la trazabilidad de las actividades, la seguridad de la información, la atención oportuna a los usuarios internos y la mejora continua de los servicios tecnológicos institucionales.

Este manual ha sido elaborado con base en el levantamiento, análisis y sistematización de la información relacionada con los procedimientos ejecutados por la Subdirección, considerando la normativa aplicable, la estructura organizacional vigente, las funciones asignadas, los riesgos asociados y los controles requeridos para asegurar una gestión eficiente, transparente y orientada a resultados. Su aplicación permitirá disponer de una referencia formal para la ejecución uniforme de las actividades, la supervisión del desempeño, la identificación de oportunidades de mejora y la actualización periódica de los procesos conforme a las necesidades institucionales.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 5 de 183

2. ANTECEDENTES

Marco Legal de Creación

- Decreto 131-1982, Constitución de la República de Honduras.
- Decreto No. 130-2017, Código Penal de Honduras vigente.
- Decreto 33-61, Ley Orgánica de la Procuraduría General de la República.
- Decreto 146-86, Ley de la Administración Pública.
- Decreto 152-87, Ley de Procedimiento Administrativo.
- Decreto No. 255-2002, Ley de Simplificación Administrativa.
- Decreto 170-2006, Ley de Transparencia y Acceso a la Información Pública.
- Decreto Ejecutivo PCM-047-2015, relacionado con la Dirección Nacional de Bienes del Estado
- Disposiciones Generales del Presupuesto General de Ingresos y Egresos de la República vigentes
- ISO 12207-018, Procesos del ciclo de vida del software.
- ISO 27000, Seguridad de la Información.
- ISO 27001-019, Sistema de Gestión de Seguridad de la Información.
- ISO 27701-020, Gestión de información de privacidad.
- ISO 27033-021, Seguridad de redes.
- ISO 22301-022, Sistema de Gestión de Continuidad del Negocio.
- ISO/IEC 20000-1, Sistema de Gestión de Servicios de Tecnologías de la Información.
- NIST Cybersecurity Framework.
- OWASP Application Security Verification Standard.
- Modelo OSI.
- Demás leyes de aplicación general

Misión

Representar y defender los intereses del Estado de Honduras en el marco del Estado democrático de derecho y el respeto irrestricto de la Constitución de la República mediante una procuración eficaz y eficiente.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UEM 6 de 183

Visión

Contribuir al 2030 en el fortalecimiento del Estado de Derecho y al Desarrollo de Honduras con objetividad y transparencia en el ejercicio de la representación y defensa de los intereses del Estado.

Objetivos Estratégicos

- Fortalecer la defensa de los intereses y derechos del Estado de Honduras.
- Mejorar la gestión y coordinación a lo interno de la PGR para ejercer oportunamente las funciones y atribuciones institucionales establecidas en la ley.

Valores

1. **Compromiso:** Calidad que se manifiesta en la dedicación y cumplimiento de una obligación aceptada y contraída.
2. **Efectividad:** combinación de eficiencia y eficacia. Eficiencia: cualidad que se manifiesta en la capacidad de disponer de alguien o de algo para conseguir un efecto determinado con el menor desperdicio o merma, es decir realizando una buena combinación en el uso de los recursos. Eficacia: cualidad que se manifiesta en la capacidad de lograr el efecto que se desea o se espera dentro de los límites de tiempo aceptables.
3. **Objetividad:** Capacidad que se refiere a expresar la realidad tal cual es, es decir a la emisión de un comentario que se encuentre sujeto en sí mismo al objeto o tema que se esté hablando, independientemente de la sensibilidad o afinidad que posea la persona que comente, esta debe limitarse a solamente indicar las características observables que posee dicho objeto.
4. **Probidad:** Honradez, rectitud de ánimo, integridad en el obrar.
5. **Responsabilidad:** Capacidad existente en todo sujeto para reconocer y aceptar las consecuencias de un hecho realizado libremente.
6. **Solidaridad:** Adhesión a las causas o compromisos de los demás miembros de la organización.
7. **Transparencia:** Calidad que identifica a la institución y sus miembros permitiendo que los demás entiendan claramente el mensaje que se está enviando con los planteamientos, acciones, y que además perciban un mensaje que exprese lo que realmente deseamos o sentimos. También incluye la obligación de dar cuenta a los ciudadanos de nuestros actos,

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UEM 7 de 183

especialmente acerca del cumplimiento de objetivos y del uso de los recursos públicos con el fin de prevenir la corrupción.

8. **Patriotismo:** sentimiento que tienen los seres humanos por la tierra natal o adoptiva a la que se siente ligado por unos determinados valores, afectos, cultura e historia.
9. **Equidad e Inclusión:** significa que cada persona tiene acceso a los recursos y oportunidades que necesita teniendo en cuenta los diferentes puntos de partida y las necesidades.

Alcance o Ámbito de Competencia

El presente manual será aplicable a los procedimientos ejecutados por la Subdirección de Infotecnología de la Procuraduría General de la República, en el ámbito de sus funciones técnicas, administrativas y de soporte institucional relacionadas con la gestión de tecnologías de la información y comunicación.

Su alcance comprende, de forma enunciativa y no limitativa, los procedimientos vinculados con la atención de solicitudes de soporte técnico, administración y mantenimiento de equipos informáticos, gestión de redes e infraestructura tecnológica, administración de sistemas, plataformas, usuarios y accesos, seguridad informática, protección de activos tecnológicos, registro y cierre de incidencias, así como la coordinación técnica para la adquisición, mantenimiento o mejora de bienes y servicios tecnológicos, cuando corresponda.

El manual aplica al personal de la Subdirección de Infotecnología y a las dependencias administrativas y sustantivas de la PGR que interactúan con esta dependencia. Su alcance inicia con la recepción, identificación o generación de una necesidad tecnológica, solicitud, incidencia o actividad programada, y finaliza con la entrega del servicio, solución técnica, informe, registro, actualización, cierre del caso o producto tecnológico correspondiente.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UEM 8 de 183

3. JUSTIFICACIÓN DEL MANUAL DE PROCEDIMIENTOS

La elaboración del Manual de Procedimientos de la Subdirección de Infotecnología adscrita a la Dirección de Administración y Finanzas, se justifica por la necesidad de contar con un instrumento técnico-administrativo que documente, ordene y estandarice las actividades vinculadas con la gestión de tecnologías de la información y comunicación. Al formalizar los procedimientos, se reducen criterios discrecionales, duplicidad de tareas, dependencia del conocimiento individual y riesgos derivados de la falta de trazabilidad, fortaleciendo así la continuidad operativa y la calidad de los servicios tecnológicos institucionales.

La Subdirección de Infotecnología cumple una función estratégica de apoyo para el funcionamiento de las áreas sustantivas y administrativas de la PGR, al brindar soporte técnico, administrar infraestructura tecnológica, gestionar sistemas, usuarios, accesos, redes, equipos y mecanismos de seguridad informática. Por ello, disponer de procedimientos claros permite delimitar responsabilidades, establecer puntos de control, mejorar los tiempos de respuesta, proteger los activos tecnológicos y asegurar que los servicios de IT se presten de forma eficiente, segura y alineada con las necesidades institucionales.

Este manual contribuye al fortalecimiento del control interno, la transparencia, la rendición de cuentas y la mejora continua, al facilitar la supervisión de las actividades, la identificación de riesgos, la conservación de evidencias y la evaluación del desempeño operativo. Asimismo, constituye una herramienta de consulta y gestión para el personal de la Subdirección, las dependencias usuarias, las autoridades institucionales y los órganos de control, promoviendo una administración tecnológica más ordenada, confiable y orientada al cumplimiento de los objetivos de la PGR.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 10 de 183

5. IDENTIFICACIÓN DE FUNCIONES SUSTANTIVAS

Las funciones sustantivas de la Subdirección de Infotecnología se orientan a garantizar la disponibilidad, continuidad, seguridad, eficiencia y mejora de los servicios tecnológicos que apoyan el cumplimiento de las competencias institucionales de la Procuraduría General de la República, en base a Constitución de la República, Ley de Transparencia y Acceso a la Información Pública, Código Penal vigente en materia de delitos informáticos, ISO/IEC 27001, ISO/IEC 27701, NIST CSF, OWASP ASVS se identificaron las siguientes funciones sustantivas:

- Gestionar el desarrollo, mantenimiento, actualización y mejora continua de los sistemas informáticos institucionales:**
Asegurando que respondan a las necesidades operativas de la PGR, cuenten con sistemas informáticos documentados, controles de seguridad, trazabilidad y criterios de calidad funcional.
- Administrar, operar y mantener la infraestructura tecnológica, redes, conectividad, servidores, comunicaciones y servicios tecnológicos institucionales:**
Garantizando disponibilidad, continuidad, desempeño y soporte a las operaciones de la PGR.
- Brindar soporte técnico oportuno a los usuarios internos de la PGR y Oficinas Regionales:**
Atendiendo, registrando, escalando y resolviendo incidentes, requerimientos y problemas relacionados con equipos, sistemas, accesos, redes, software y servicios tecnológicos.
- Gestionar el registro, asignación, control, custodia, mantenimiento, traslado, inventario y descargo de los activos tecnológicos institucionales:**
Asegurando su uso eficiente, trazabilidad patrimonial y resguardo conforme a la normativa aplicable sobre bienes del Estado.
- Administrar las bases de datos institucionales y los mecanismos de respaldo, recuperación, integridad, disponibilidad y resguardo de la información digital:**
Garantizando la continuidad de los servicios y la protección de la información institucional.
- Implementar y supervisar controles de seguridad tecnológica, gestión de usuarios, perfiles, permisos, accesos, autenticación y protección de activos de información:**
Reduciendo riesgos de acceso no autorizado, pérdida, alteración, divulgación indebida o uso inadecuado de la información institucional.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 11 de 183

6. IDENTIFICACIÓN DE PROCEDIMIENTOS SUSTANTIVOS

MATRIZ DE VALIDACIÓN DE FUNCIONES Y PROCEDIMIENTOS

Funciones Sustantivas	Procedimientos Por Incluir en el Manual
• Gestionar el desarrollo, mantenimiento, actualización y mejora continua de los sistemas informáticos institucionales:	• PR-SDIT-001-Gestión de Desarrollo y Mantenimiento de Sistemas, regula las actividades para el análisis, desarrollo, mantenimiento, actualización y mejora de los sistemas informáticos institucionales.
• Administrar, operar y mantener la infraestructura tecnológica, redes, conectividad, servidores, comunicaciones y servicios tecnológicos institucionales.	• PR-SDIT-002-Operación de Infraestructura Tecnológica y Redes, garantiza la disponibilidad, continuidad, desempeño y operación segura de los recursos tecnológicos institucionales.
• Brindar soporte técnico oportuno a los usuarios internos de la PGR y Oficinas Regionales.	• PR-SDIT-003- Soporte Técnico a Usuarios y PR-SDIT-007-Soporte Tecnológico a Oficinas Regionales, su propósito es brindar una atención oportuna y ordenada ante incidentes, requerimientos o fallas relacionadas con equipos y servicios tecnológicos.
• Gestionar el registro, asignación, control, custodia, mantenimiento, traslado, inventario y descargo de los activos tecnológicos institucionales.	• PR-SIT-004-Administración de Activos Tecnológicos, regula el registro, asignación, control, mantenimiento, traslado, custodia y seguimiento de los activos tecnológicos institucionales.
• Administrar las bases de datos institucionales y los mecanismos de respaldo, recuperación, integridad, disponibilidad y resguardo de la información digital.	• PR-SDIT-005-Administración de Bases de Datos y Respallos, su finalidad es proteger la disponibilidad, confidencialidad, integridad y continuidad de la información digital institucional.
• Implementar y supervisar controles de seguridad tecnológica, gestión de usuarios, perfiles, permisos, accesos, autenticación y protección de activos de información.	• PR-SDIT-006- Seguridad Tecnológica y Control de Acceso, define los controles para la gestión de usuarios, perfiles, permisos, accesos, autenticación y protección de los activos de información institucionales.

 PROCURADURÍA GENERAL DE LA REPÚBLICA	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	 UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 12 de 183

7. FICHAS DE PROCESOS

 PROCURADURÍA GENERAL DE LA REPÚBLICA		CÓDIGO DEL FORMULARIO NCI-TSC/141-00 NCI-TSC/142-00 03 PGR				
FICHA DE PROCESOS						
FECHA DE ELABORACION:	24 de abril de 2026					
PROCESO:	Gestión del Desarrollo, Implementación y Mantenimiento de Sistemas Informáticos					
SUBPROCESO:	Gestión del Desarrollo, Implementación y Mantenimiento de Sistemas Informáticos					
OBJETIVO:	Gestionar el desarrollo, implementación y mantenimiento de sistemas informáticos institucionales, mediante la planificación, análisis, diseño, construcción, despliegue y mejora continua de soluciones tecnológicas, asegurando su calidad, disponibilidad, seguridad y alineación con las necesidades institucionales y de la ciudadanía.					
ALCANCE:	El proceso inicia con la identificación y análisis de requerimientos de soluciones tecnológicas institucionales, y finaliza con la puesta en operación, mantenimiento, actualización y mejora continua de los sistemas informáticos, garantizando su funcionamiento, seguridad y disponibilidad.					
RESPONSABLE DEL PROCESO:	Oficial Técnico					
NORMATIVAS APLICABLES:	Constitución de la República de Honduras, Ley General de la Administración Pública, Ley Orgánica de PGR, Reglamento Interno PGR, Metodologías Ágiles para el Desarrollo de Sistemas, ISO 12207 Ciclo de Vida Sistemas e ISO: 27001					
ENTRADAS:	PROVEEDORES: Dependencias y Regionales PGR INSUMOS: Memorándum, ticket o correo electrónico de la necesidad, documentación soporte de las dependencias (formatos y tablas de Excel), Lenguajes de Programación [JavaScript, TypeScript, PHP, SQL, HTML5 y CSS3], Frameworks y Tecnologías de Desarrollo, Bases de Datos [MySQL y PostgreSQL], Herramientas de Desarrollo y Administración [Visual Studio Code, MySQL Workbench (Community Edition), Git / GitHub y Termius]					
SALIDAS:	#	PRODUCTOS: (Describir los documentos, informes y otros resultados que genera el proceso)	#	CLIENTES INTERNOS: (Detallar los procesos o unidades que recibirán los productos)	#	CLIENTES EXTERNOS: (Detallar los organismos, instituciones que recibirán los productos del proceso)
	1	Reporte de sistemas informáticos implementados y en producción	1	Dependencias y Regionales PGR	1	N/A
	2	Sistema Desarrollado	2	Dependencias y Regionales PGR	2	N/A
	3	Manual de usuario de las nuevas tecnologías	3	Dependencias y Regionales PGR	3	N/A
	4	Reporte de versiones de sistemas controlados y mantenimiento	4	Dependencias y Regionales PGR	4	N/A
	5	Reporte de usuarios con acceso a sistemas y capacitación básica en uso	5	Dependencias y Regionales PGR	5	N/A
PROCESOS RELACIONADOS: PR-SDI-002-Administración de infraestructura tecnológica, redes y conectividad, PR-SDI-005-Administración de Bases de Datos y Respaldo y PR-SDI-006-Seguridad Tecnológica y Control de Acceso.						
#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)	
1	Recibir solicitudes de desarrollo, mejora o mantenimiento de sistemas informáticos.	Oficial Técnico	1 día	Porcentaje de proyectos de desarrollo implementados en tiempo y forma	Reporte de sistemas informáticos implementados y en producción	
2	Analizar los requerimientos funcionales y técnicos de los usuarios.		3 días			

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 13 de 183

#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)
3	Validar los requerimientos con las unidades solicitantes.	Oficial Técnico	2 días	Porcentaje de proyectos de desarrollo implementados en tiempo y forma	Sistema Desarrollado
4	Priorizar los requerimientos conforme a criterios institucionales.		2 días		
5	Diseñar la arquitectura funcional y técnica del sistema informático.		3 días		
6	Definir especificaciones técnicas y funcionales del sistema.		2 días		
7	Planificar el desarrollo del sistema, estableciendo tiempos, recursos y entregables.		2 días		
8	Desarrollar el sistema informático conforme a los requerimientos definidos.		20 días		
9	Codificar los componentes del sistema utilizando estándares institucionales.		15 días		
10	Integrar los diferentes módulos del sistema.		5 días		
11	Ejecutar pruebas unitarias de los componentes desarrollados.		2 días		
12	Realizar pruebas integrales del sistema.		2 días		
13	Validar el cumplimiento de los requerimientos funcionales.		1 día		
14	Corregir errores identificados durante las pruebas.		5 días		
15	Preparar el ambiente de producción para la implementación del sistema.		2 días		
16	Desplegar el sistema en el ambiente productivo.		2 días		
17	Configurar el sistema para su operación institucional.		15 días		
18	Verificar el funcionamiento del sistema en producción.		2 días		
19	Monitorear el desempeño del sistema informático.		3 días		
20	Identificar fallas o necesidades de mejora en el sistema.		2 días		Reporte de versiones de sistemas controlados y mantenimiento
21	Corregir errores mediante mantenimiento correctivo.		5 días		
22	Actualizar el sistema conforme a cambios normativos o tecnológicos.		5 días		
23	Mejorar funcionalidades del sistema según requerimientos institucionales.		5 días		

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 14 de 183

N	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)
24	Controlar las versiones del sistema mediante herramientas de versionamiento.	Oficial Técnico	3 días	Porcentaje de proyectos de desarrollo implementados en tiempo y forma	Reporte de versiones de sistemas controlados y mantenimiento
25	Registrar los cambios realizados en el sistema.		3 días		
26	Registrar en los reportes todas las actividades de desarrollo, implementación y mantenimiento.		7 días		
27	Mantener actualizada la documentación técnica y funcional del sistema.		3 días		
28	Generar el manual de usuario del sistema.		4 días		Manual de usuario de las nuevas tecnologías
29	Capacitar a los usuarios en el uso del sistema (cuando aplique).	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	5 días		Reporte de usuarios con acceso a sistemas y capacitación básica en uso
30	Implementación del Sistema		5 días		

PLANES DE DIFUSIÓN: Página Web de la PGR, enviar una copia digital a los colaboradores(a) por medio del correo electrónico institucional y enviar una copia física, a la vez colgarlo en el Portal Único de Transparencia del IAP.

Elaborado por:	Revisado por:	Verificado por:	Aprobado por:
Suyapa del Mar Andino Ordóñez Jefa de la Unidad de Modernización	Lisandro Alfredo Suárez Salinas Oficial Técnico Cristian Alexander Martínez Ochoa Oficial Técnico	Jorge Efraín Salgado Subdirector de Infotecnología	Jorge Francisco Quiroz Mejía Sub-Procurador General de la República
Firma:  Fecha: 24 de abril de 2026	Firma:  Fecha: 24 de abril de 2026	Firma:  Fecha: 28 de abril de 2026	Firma:  Fecha: 29 de abril de 2026

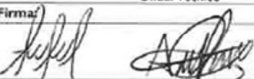
	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 15 de 183

		PROCURADURÍA GENERAL DE LA REPÚBLICA FICHA DE PROCESOS				CÓDIGO DEL FORMULARIO NCI-T5C/141-00 NCI-T5C/142-00 08 PGR	
FECHA DE ELABORACION:		29 de abril de 2026					
PROCESO:		Operación de Infraestructura Tecnológica y Redes.					
SUBPROCESO:		Operación de Infraestructura Tecnológica y Redes.					
OBJETIVO:		Garantizar la operación continua, segura, eficiente y disponible de la infraestructura tecnológica y de redes institucional, mediante la administración, monitoreo, mantenimiento y mejora de los recursos tecnológicos, asegurando el soporte a los procesos institucionales y la prestación oportuna de servicios a la ciudadanía.					
ALCANCE:		El proceso inicia con la identificación de requerimientos de operación, monitoreo o mantenimiento de los recursos tecnológicos institucionales, y finaliza con la garantía de disponibilidad, funcionamiento y soporte continuo de los servicios tecnológicos.					
RESPONSABLE DEL PROCESO:		Auxiliar Técnico y Oficial Técnico					
NORMATIVAS APLICABLES:		Constitución de la República de Honduras; Ley General de la Administración Pública; Ley orgánica de la Procuraduría General de la República, Reglamento Interno de Trabajo PGR, ISO: 27001, Iso: 27033, ISO:22301 e ISO:2000-1					
ENTRADAS:		PROVEEDORES: Dependencias PGR y proveedores tecnológicos autorizados.				INSUMOS: Memorándum, sistema de ticket o correo electrónico.	
SALIDAS:	#	PRODUCTOS: (Describir los documentos, informes y otros resultados que genera el proceso)	#	CLIENTES INTERNOS: (Detallar los procesos o unidades que recibirán los productos)	#	CLIENTES EXTERNOS: (Detallar los organismos, instituciones que recibirán los productos del proceso)	
	1	Reporte de consumo de ancho de banda.	1	Dependencias PGR	1	N/A	
	2	Reporte en sistema de tickets para los incidentes tecnológicos resueltos	2	Dependencias PGR	2	N/A	
PROCESOS RELACIONADOS:		PR-SDBN-002-Levantamiento de inventario, PR-SDCS-001-Compras Menores, PR-SDCS-003-Licitaciones, PR-SDCS-004-Compra Directa por Catálogo Electrónico, PR-SDIT-003-Soporte Técnico a Usuarios, PR-SDIT-004-Administración de Activos Tecnológicos, PR-SDIT-006-Seguridad Tecnológica y Control de Acceso y PR-SDIT-007-Soporte Tecnológico a Oficinas Regionales					
#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)		
1	Supervisar de forma continua el estado operativo de redes, servidores y sistemas, mediante herramientas de monitoreo, con el fin de detectar fallas, alertas o degradación del servicio.	Auxiliar Técnico y Oficial Técnico	1 día	Porcentaje de la disponibilidad en la infraestructura tecnológica y redes	Reporte del control de activos tecnológicos identificados		
2	Documentar cronológicamente todos los eventos relevantes de la operación tecnológica (incidentes, mantenimientos, caídas, accesos), garantizando trazabilidad y evidencia del proceso.	Auxiliar Técnico y Oficial Técnico	3 días		Reporte del control de activos tecnológicos identificados		
3	Identificar fallas o interrupciones en los servicios tecnológicos a través del monitoreo o reportes de usuarios.	Auxiliar Técnico y Oficial Técnico	1 día		Inventario actualizado		

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 16 de 183

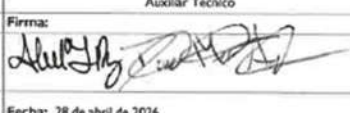
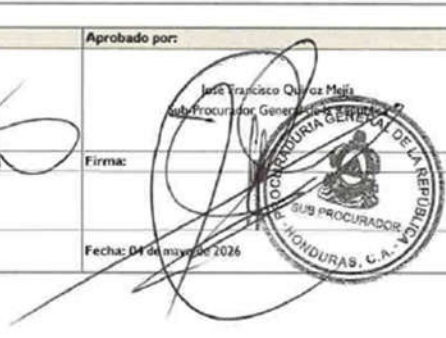
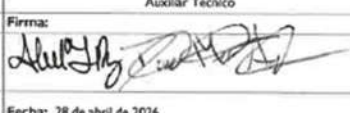
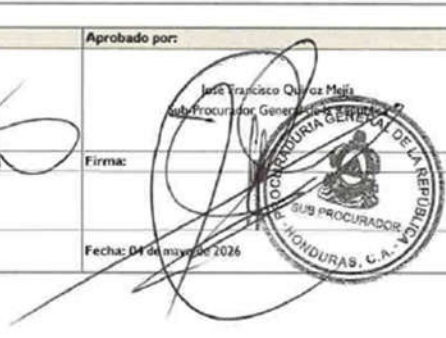
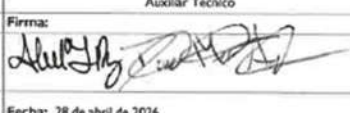
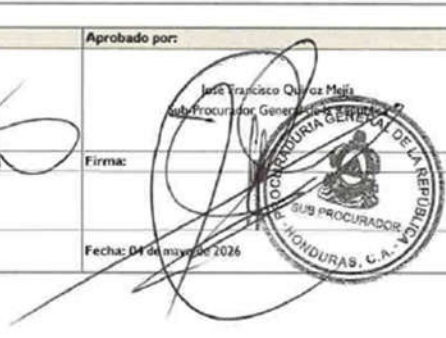
#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)
4	Categorizar los incidentes según su nivel de criticidad, impacto y urgencia para priorizar su atención.	Auxiliar Técnico y Oficial Técnico	15 min	Porcentaje de la disponibilidad en la infraestructura tecnológica y redes	Inventario actualizado
5	Analizar las causas de los incidentes mediante revisión técnica de equipos, sistemas y configuraciones.	Auxiliar Técnico y Oficial Técnico	1 hora		Actas de asignación préstamo de equipo Vale de préstamo y devolución
6	Aplicar soluciones técnicas para restablecer la operación normal de los servicios afectados.	Auxiliar Técnico y Oficial Técnico	4 horas		
7	Remitir los incidentes que no pueden ser resueltos en el primer nivel a instancias técnicas superiores o proveedores especializados.	Auxiliar Técnico y Oficial Técnico	3 días		
8	Finalizar formalmente la atención del incidente, verificando la solución e informando al usuario, dejando evidencia en el sistema de ticket.	Auxiliar Técnico y Oficial Técnico	10 min		
9	Brindar asistencia a usuarios internos en problemas relacionados con equipos, sistemas o conectividad.	Auxiliar Técnico y Oficial Técnico	1 hora		
10	Realizar acciones programadas para prevenir fallas en la infraestructura tecnológica (revisiones, limpieza, actualizaciones).	Auxiliar Técnico y Oficial Técnico	Semestral		Inventario actualizado
11	Intervenir equipos o sistemas que presentan fallas para restablecer su funcionamiento.	Auxiliar Técnico y Oficial Técnico	1 hora		
12	Reestablecer la conectividad de la red institucional, asegurando su disponibilidad y rendimiento en caso de ser fallas internas.	Auxiliar Técnico y Oficial Técnico	1 hora		
13	Asignar, modificar o revocar permisos de acceso a los recursos tecnológicos conforme a autorizaciones establecidas.	Auxiliar Técnico y Oficial Técnico	15 min		
14	Aplicar medidas de protección como antivirus, firewalls, parches de seguridad y control de accesos para proteger la infraestructura.	Auxiliar Técnico y Oficial Técnico	1 hora		Reportes de incidencias
15	Realizar copias de seguridad de configuración de los equipos de redes, garantizando la integridad y disponibilidad de los respaldos realizados.	Auxiliar Técnico y Oficial Técnico	1 hora		

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 17 de 183

#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)
15	Registrar y mantener actualizado el control de activos tecnológicos (equipos, servidores, dispositivos de red).	Auxiliar Técnico y Oficial Técnico	1 hora	Porcentaje de la disponibilidad en la infraestructura tecnológica y redes	Reportes de incidencias
PLANES DE DIFUSIÓN:		Página Web de la PGR, enviar una copia digital a los colaboradores(a) por medio del correo electrónico institucional y enviar una copia física, a la vez colgarlo en el Portal Único de Transparencia del IAIP.			
Elaborado por:		Revisado por:	Verificado por:	Aprobado por:	
Suyapa del Mar Andino Ordóñez Jefa de la Unidad de Modernización		Arnaldo Alcides García Alvarado Oficial Técnico Ángel Gustavo Reyes Molina Oficial Técnico		José Efraín Salgado Subdirector de Infotecología	
Firma: 		Firma: 		Firma: 	
Fecha: 29 de abril de 2026		Fecha: 29 de abril de 2026		Fecha: 30 de abril de 2026	
					
					

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 18 de 183

		PROCURADURÍA GENERAL DE LA REPÚBLICA FICHA DE PROCESOS		CÓDIGO DEL FORMULARIO NCI-TSC/141-00 NCI-TSC/142-00 03 PGR	
FECHA DE ELABORACION:		28 de abril de 2026			
PROCESO:		Soporte Técnico a Usuarios			
SUBPROCESO:		Soporte Técnico a Usuarios			
OBJETIVO:		Brindar ayuda a los usuarios para resolver problemas con equipos, sistemas o servicios tecnológicos, de forma rápida y eficiente, para que puedan realizar su trabajo sin interrupciones.			
ALCANCE:		Este proceso inicia cuando un usuario reporta un problema o solicita ayuda relacionada con equipos, sistemas o servicios tecnológicos, y finaliza cuando el problema ha sido resuelto, la solicitud ha sido atendida satisfactoriamente o con un dictamen técnico.			
RESPONSABLE DEL PROCESO:		Auxiliar Técnico y Asistente Administrativo			
NORMATIVAS APLICABLES:		Constitución de la República de Honduras, Ley General de la Administración Pública, Ley Orgánica de la Procuraduría General de la República, Reglamento Interno de Trabajo PGR, Modelo OSI e ISO 27000			
ENTRADAS:		PROVEEDORES: Dependencias PGR		INSUMOS: Memorándum, sistema de ticket o correo electrónico, herramientas de precisión, aspiradoras, aire comprimido, estación de calor, pasta térmica, taladros, herramientas para red y hacer diagnósticos, entre otros.	
SALIDAS:	# PRODUCTOS: (Describir los documentos, informes y otros resultados que genera el proceso)	# CLIENTES INTERNOS: (Detallar los procesos o unidades que recibirán los productos)	# CLIENTES EXTERNOS: (Detallar los organismos, instituciones que recibirán los productos del proceso)		
	1 Reportes de incidencias atendidas por medio de tickets	1 Dependencias PGR	1 Ciudadanía		
	2 Dictamen Técnico de Equipos Tecnológicos	2 Subdirección de Bienes Nacionales	2 Ciudadanía		
	3 Reporte de mantenimiento semestral	3 Dependencias PGR	3 Ciudadanía		
	4 Reportes periódicos de soporte trimestral	4 Dependencias PGR	4 Ciudadanía		
PROCESOS RELACIONADOS:		PR-SDIT-004-Administración de Activos Tecnológicos, PR-SDBN-002-Levantamiento de Inventario, PR-SDBN-003-Reasignación de Bienes, PR-SDBN-005-Descargo Definitivo de Bienes, PR-SDBN-005-Propiedad Estatal Perdida, PR-SDIT-007-Soporte Tecnológico a Oficinas Regionales, PR-RRPP-001-Gestión de la comunicación institucional interna y externa y el PR-RRPP-004-Gestión de protocolo y eventos institucionales.			
# ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)	
1 Recibir la solicitud o incidencia del usuario por orden de llegada (vía memorándum, sistema de tickets y correo electrónico).	Auxiliar Técnico	10 min	Porcentaje de solicitudes de soporte técnico atendidas dentro del tiempo establecido	Reportes de incidencias atendidas por medio de tickets	
2 Registrar la solicitud en el sistema de tickets.	Auxiliar Técnico	5 min			

#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODO COMPLETADO: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)																
3	Clasificar la incidencia según tipo, prioridad y nivel de impacto.	Auxiliar Técnico	10 min	Porcentaje de solicitudes de soporte técnico atendidas dentro del tiempo establecido	Reportes de incidencias atendidas por medio de tickets Reportes periódicos de soporte trimestral																
4	Asignar el caso al personal técnico correspondiente.	Asistente Administrativo	10 min																		
5	Diagnosticar la causa del problema reportado.	Auxiliar Técnico	30 min																		
6	Determinar la solución técnica adecuada.	Auxiliar Técnico	1 día																		
7	Ejecutar la solución o intervención técnica (remota o presencial).	Auxiliar Técnico	1 día																		
8	Escalar el caso a un nivel superior o proveedor externo, cuando no pueda resolverse en primera instancia.	Auxiliar Técnico	1 día																		
9	Verificar el funcionamiento correcto del equipo, sistema o servicio intervenido.	Auxiliar Técnico	30 min																		
10	Confirmar con el usuario la solución del problema.	Auxiliar Técnico	5 min																		
11	Registrar las acciones realizadas y la solución aplicada en el sistema de tickets.	Auxiliar Técnico	10 min																		
12	Cerrar la solicitud o ticket de soporte técnico.	Auxiliar Técnico	5 min																		
13	Generar los Dictámenes Técnicos cuando corresponda.	Auxiliar Técnico	1 hora	Dictamen Técnico de Equipos Tecnológicos																	
14	Analizar las incidencias recurrentes para proponer mejoras preventivas.	Auxiliar Técnico	20 min	Reportes periódicos de soporte trimestral y Reporte de mantenimiento semestral																	
PLANES DE DIFUSIÓN: Página Web de la PGR, enviar una copia digital a los colaboradores(a) por medio del correo electrónico institucional y enviar una copia física, a la vez colgarlo en el Portal Único de Transparencia del IAIIP.																					
<table border="1"> <thead> <tr> <th>Elaborado por:</th> <th>Revisado por:</th> <th>Verificado por:</th> <th>Aprobado por:</th> </tr> </thead> <tbody> <tr> <td>Suyapa del Mar Andino Ordóñez Jefa de la Unidad de Modernización</td> <td>Abel Fernando Perez Vargas Auxiliar Técnico Daniel Isaac Membreño Anariba Auxiliar Técnico</td> <td>Jorge Brindley Subdirector de Modernización</td> <td>Jorge Francisco Quiroz Mejía Subprocurador General</td> </tr> <tr> <td>Firma: </td> <td>Firma: </td> <td>Firma: </td> <td>Firma: </td> </tr> <tr> <td>Fecha: 28 de abril de 2026</td> <td>Fecha: 28 de abril de 2026</td> <td>Fecha: 30 de abril de 2026</td> <td>Fecha: 04 de mayo de 2026</td> </tr> </tbody> </table>						Elaborado por:	Revisado por:	Verificado por:	Aprobado por:	Suyapa del Mar Andino Ordóñez Jefa de la Unidad de Modernización	Abel Fernando Perez Vargas Auxiliar Técnico Daniel Isaac Membreño Anariba Auxiliar Técnico	Jorge Brindley Subdirector de Modernización	Jorge Francisco Quiroz Mejía Subprocurador General	Firma: 	Firma: 	Firma: 	Firma: 	Fecha: 28 de abril de 2026	Fecha: 28 de abril de 2026	Fecha: 30 de abril de 2026	Fecha: 04 de mayo de 2026
Elaborado por:	Revisado por:	Verificado por:	Aprobado por:																		
Suyapa del Mar Andino Ordóñez Jefa de la Unidad de Modernización	Abel Fernando Perez Vargas Auxiliar Técnico Daniel Isaac Membreño Anariba Auxiliar Técnico	Jorge Brindley Subdirector de Modernización	Jorge Francisco Quiroz Mejía Subprocurador General																		
Firma: 	Firma: 	Firma: 	Firma: 																		
Fecha: 28 de abril de 2026	Fecha: 28 de abril de 2026	Fecha: 30 de abril de 2026	Fecha: 04 de mayo de 2026																		

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 20 de 183

		PROCURADURÍA GENERAL DE LA REPÚBLICA		CÓDIGO DEL FORMULARIO NCI-TSC/141-00 NCI-TSC/142-00 09 PGR		
FICHA DE PROCESOS						
FECHA DE ELABORACION:		09 de abril de 2026				
PROCESO:		Administración de activos tecnológicos				
SUBPROCESO:		Administración de activos tecnológicos				
OBJETIVO:		Administrar y controlar los activos tecnológicos institucionales durante su ciclo de vida, incluyendo su asignación y préstamo a otras dependencias, para garantizar su registro, custodia, seguimiento, mantenimiento, devolución y disposición final, conforme a la normativa vigente.				
ALCANCE:		El presente proceso comprende desde la recepción o incorporación de los activos tecnológicos a la institución, su verificación, registro e identificación en los controles correspondientes, así como su asignación, préstamo temporal a otras dependencias, traslado, mantenimiento preventivo y correctivo, seguimiento, devolución, reasignación, verificación física y control de custodios, hasta su baja, descarte o disposición final, conforme a la normativa administrativa, patrimonial y de control interno vigente.				
RESPONSABLE DEL PROCESO:		Asistente Administrativo, Auxiliar Técnico y Oficial Técnico				
NORMATIVAS APLICABLES:		Constitución de la República de Honduras; Ley General de la Administración Pública; Ley Orgánica de la Procuraduría General de la República; Reglamento de Organización y Funcionamiento de la Dirección Nacional de Bienes del Estado (DNBE); Disposiciones Generales del Presupuesto vigentes y demás leyes de aplicación general.				
ENTRADAS:		PROVEEDORES: Subdirección de Compras y Suministros, Subdirección de Bienes Nacionales, Otras dependencias y Regionales PGR		INSUMOS: Documentos de control, memorándum, sistema de tixect o correo electrónico.		
SALIDAS:	#	PRODUCTOS: (Describir los documentos, informes y otros resultados que genera el proceso)	#	CLIENTES INTERNOS: (Detallar los procesos o unidades que recibirán los productos)	#	CLIENTES EXTERNOS: (Detallar los organismos, instituciones que recibirán los productos del proceso)
	1	Reporte del control de activos tecnológicos identificados	1	Dirección de Administración y Finanzas	1	N/A
	2	Inventario actualizado	2	Subdirección de Bienes Nacionales	2	N/A
	3	Actas de asignación préstamo de equipo	3	Dependencias PGR	3	N/A
	4	Vale de préstamo y devolución	4	Dependencias PGR	4	N/A
	5	Reportes de incidencias	5	Dirección de Administración y Finanzas y Subdirección de Bienes Nacionales	5	N/A
	6	Conciliación de inventario	6	Subdirección de Bienes Nacionales	6	N/A
PROCESOS RELACIONADOS:		PR-SGBN-02-Levantamiento de Inventario, PR-SDBN-003-Reasignación de Bienes, PR-SDBN-004-Recepción y Asignación de Nuevos Bienes, PR-SDCS-001-Compras Menores, PR-SDCS-003-Licitaciones y PR-SDCS-004-Compras Directa por Catálogo Electrónico.				
#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)	
1	Recibir los activos tecnológicos adquiridos, donados, transferidos o reasignados.	Auxiliar Técnico y Oficial Técnico	2 días	Número de activos con registro completo	Reporte del control de activos tecnológicos identificados	

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 21 de 183

#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)
2	Verificar que los activos tecnológicos cumplan con las especificaciones técnicas, cantidad, estado físico y documentación soporte correspondiente.	Auxiliar Técnico y Oficial Técnico	2 días	Número de activos con registro completo	Reporte del control de activos tecnológicos identificados
3	Clasificar los activos tecnológicos según su tipo, estado, ubicación y responsable asignado.	Auxiliar Técnico y Oficial Técnico	2 días		Inventario actualizado
4	Asignar los activos tecnológicos al usuario de la dependencia correspondiente.	Auxiliar Técnico y Oficial Técnico	2 días		
5	Formalizar la entrega del activo tecnológico mediante acta, recibo, vale, formulario o documento de resguardo.	Auxiliar Técnico y Oficial Técnico	1 día		Actas de asignación préstamo de equipo Vale de préstamo y devolución
6	Recibir las solicitudes de préstamo temporal de activos tecnológicos de otras dependencias.	Asistente Administrativo	1 hora	Número de tickets resueltos dentro del plazo	
7	Verificar la disponibilidad del activo tecnológico solicitado para préstamo.	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	1 hora		
8	Autorizar el préstamo temporal del activo tecnológico, cuando corresponda.	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	1 hora	Número de activos de vueltos a tiempo	
9	Registrar el préstamo del activo tecnológico, indicando dependencia solicitante, responsable, fecha de entrega, plazo de uso y condiciones de devolución.	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	30 min		
10	Entregar el activo tecnológico en calidad de préstamo a la dependencia autorizada.	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	30 min		Reportes de incidencias
11	Actualizar los registros de ubicación, custodia y responsable del activo tecnológico prestado.	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	30 min		
12	Dar seguimiento a los activos tecnológicos prestados a otras dependencias.	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	30 min	Número de mantenimientos realizados	Inventario actualizado
13	Recibir los activos tecnológicos devueltos por las dependencias prestatarias.	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	30 min		Reportes de incidencias
14	Verificar el estado físico y funcional de los activos tecnológicos al momento de su devolución.	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	30 min		
15	Atender las solicitudes de traslado, devolución o reasignación de activos tecnológicos.	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	30 min	Número de activos conciliados	Conciliación de inventario
16	Registro del mantenimiento preventivo de los activos tecnológicos conforme a su uso, criticidad y vida útil.	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	1 día		
17	Conciliar la existencia física de los activos tecnológicos con los registros administrativos o patrimoniales.	Asistente Administrativo	5 días		

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 22 de 183

#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)
18	Identificar los activos tecnológicos en desuso, obsoletos, dañados o no reparables.	Asistente Administrativo	5 días	Número de activos registrados	Reportes de incidencias
19	Evaluar la procedencia de la baja, descarte, reposición o disposición final de los activos tecnológicos, conforme a la normativa aplicable.	Auxiliar Técnico y Oficial Técnico	1 día		
20	Archivar y resguardar la documentación soporte relacionada con la recepción, asignación, préstamo, traslado, devolución, mantenimiento y baja de los activos tecnológicos.	Asistente Administrativo	1 hora	Número de informes emitidos	Reporte del control de activos tecnológicos identificados
21	Emitir reportes periódicos sobre inventario, préstamos, asignaciones, estado, mantenimiento y movimiento de los activos tecnológicos.	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	Trimestral		
PLANES DE DIFUSIÓN:		Página Web de la PGR, enviar una copia digital a los colaboradores(a) por medio del correo electrónico institucional y enviar una copia física, a la vez colgarlo en el Portal Único de Transparencia del IAIP.			
Elaborado por:		Revisado por:		Verificado por:	
Suyapa del Mar Andino Ordóñez Jefe de la Unidad de Modernización		Lilia Iveth Galo Andrade Asistente Administrativo		José Eladio Salgado Subdirector de Tecnología	
Firma:		Firma:		Firma:	
Fecha: 09 de abril de 2026		Fecha: 10 de abril de 2026		Fecha: 16 de abril de 2026	

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 23 de 183

		PROCURADURÍA GENERAL DE LA REPÚBLICA FICHA DE PROCESOS		CÓDIGO DEL FORMULARIO NCI-TSC/141-00 NCI-TSC/142-00 00 PGR	
FECHA DE ELABORACION:		06 de mayo de 2026			
PROCESO:		Administración de Bases de Datos y Respaldos			
SUBPROCESO:		Administración de Bases de Datos y Respaldos			
OBJETIVO:		Garantizar la disponibilidad, integridad, confidencialidad y recuperación de la información institucional contenida en las bases de datos, mediante la administración eficiente, segura y controlada de los sistemas gestores de bases de datos, así como la ejecución, verificación y resguardo de los respaldos, asegurando la continuidad operativa de los servicios tecnológicos institucionales.			
ALCANCE:		El proceso inicia con la configuración, administración y monitoreo de las bases de datos institucionales, incluyendo la definición y ejecución de políticas de respaldo, y finaliza con la garantía de disponibilidad, seguridad, integridad y recuperación de la información institucional.			
RESPONSABLE DEL PROCESO:		Oficial Técnico			
NORMATIVAS APLICABLES:		Constitución de la República; Ley General de la Administración Pública; Ley Orgánica del Presupuesto; Reglamento Interno de Trabajo PGR, ISO 27001e ISO 27701			
ENTRADAS:		PROVEEDORES: Dependencias y Regionales PGR		INSUMOS: Sistemas gestores de bases de datos (DBMS) y Sistemas de Información	
SAIDAS:	PRODUCTOS: # (Describir los documentos, informes y otros resultados que genera el proceso)	CLIENTES INTERNOS: # (Detallar los procesos o unidades que recibirán los productos)	CLIENTES EXTERNOS: # (Detallar los organismos, instituciones que recibirán los productos del proceso)		
	1 Control de respaldos	1 Dependencias y Regionales PGR	1 Ciudadanía		
	2 Control de Permisos asignados o revocados	2 Dependencias y Regionales PGR			
PROCESOS RELACIONADOS:		PR-SDIT-001-Gestión de Desarrollo y Mantenimiento de Sistemas y PR-SDIT-006-Seguridad Tecnológica y Control de Acceso			
# ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)	
1 Administrar las bases de datos institucionales para garantizar su disponibilidad y correcto funcionamiento.	Oficial Técnico	Diario	Porcentaje de respaldos de bases de datos ejecutados exitosamente	Control de respaldos	
2 Configurar los sistemas gestores de bases de datos conforme a los requerimientos institucionales.		Mensual			
3 Monitorear el desempeño de las bases de datos para detectar problemas de rendimiento o capacidad.		Diario			
4 Optimizar las bases de datos mediante ajustes en estructuras, consultas e índices.		Mensual			
5 Gestionar los usuarios y permisos de acceso a las bases de datos conforme a autorizaciones establecidas.		Mensual		Control de Permisos asignados o revocados	

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 24 de 183

#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)
6	Implementar controles de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información.	Oficial Técnico	Mensual	Porcentaje de respaldos de bases de datos ejecutados exitosamente	Control de respaldos
7	Definir la programación de respaldos de acuerdo con las políticas institucionales.		Semanal		
8	Ejecutar respaldos de las bases de datos (completos, diferenciales o incrementales).		Semanal		
9	Verificar la correcta ejecución de los respaldos realizados.		Semanal		
10	Almacenar los respaldos en medios seguros conforme a los lineamientos establecidos.		15 días		
11	Realizar pruebas de restauración de respaldos para validar su integridad y disponibilidad.		Semestral		
12	Pruebas de restaurar bases de datos en caso de fallas, incidentes o pérdida de información		Semestral		
13	Diagnosticar las causas de fallas en bases de datos.		Trimestral		
14	Escalar incidentes complejos a los proveedores cuando corresponda.		Anual		
15	Registrar en control todas las operaciones realizadas sobre bases de datos y respaldos.		Semanal		
16	Evaluar el cumplimiento de políticas de respaldo y seguridad.		Semanal		
17	Implementar mejoras en la administración de bases de datos y gestión de respaldos.		Mensual		

PLANES DE DIFUSIÓN:

Página Web de la PGR, enviar una copia digital a los colaboradores(a) por medio del correo electrónico institucional y enviar una copia física, a la vez colgarlo en el Portal Único de Transparencia del IAIIP.

Elaborado por:	Revisado por:	Verificado por:	Aprobado por:
Suyapa del Mar Andino Ordóñez Jefe de la Unidad de Modernización	Livandro Alfredo Suárez Salinas Oficial Técnico Pablo Javier Padilla Avilés Oficial Técnico Cristian Alexander Martínez Ochoa Oficial Técnico	 	José Francisco Quiroz Mejía Sub-Procurador General de la República
Firma: Fecha: 06 de mayo de 2026 	Firma: Fecha: 06 de mayo de 2026	Firma: Fecha: 07 de mayo de 2026	Firma: Fecha: 08 de mayo de 2026

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 25 de 183

		PROCURADURÍA GENERAL DE LA REPÚBLICA FICHA DE PROCESOS		CÓDIGO DEL FORMULARIO NCI-TSC/41-00 NCI-TSC/42-00 08 PGR	
FECHA DE ELABORACION:		20 de abril de 2026			
PROCESO:		Seguridad Tecnológica y Control de Acceso			
SUBPROCESO:		Seguridad Tecnológica y Control de Acceso			
OBJETIVO:		Proteger los sistemas, activos tecnológicos e información institucional mediante el control de accesos y la aplicación de medidas de seguridad tecnológica, para prevenir riesgos y fortalecer el control interno.			
ALCANCE:		El presente proceso comprende la administración de accesos a sistemas, plataformas, equipos y recursos tecnológicos institucionales, así como la ejecución de controles de seguridad tecnológica sobre usuarios, credenciales, dispositivos y servicios, incluyendo el registro, monitoreo, revisión, actualización y revocación de accesos, así como la atención y documentación de incidentes de seguridad, conforme a la normativa aplicable.			
RESPONSABLE DEL PROCESO:		Oficial Técnico de Infotecnología			
NORMATIVAS APLICABLES:		Constitución de la República, Ley General de la Administración Pública, Normativas y Marcos de Referencia de Ciberseguridad, NIST, OWASP ASVS e ISO 27001			
ENTRADAS:		PROVEEDORES: Dependencias PGR y Regionales		INSUMOS: Memorándum, correos, tickets, buscadores u OSINT	
SALIDAS:	# PRODUCTOS: (Describir los documentos, Informes y otros resultados que genera el proceso)	# CLIENTES INTERNOS: (Detallar los procesos o unidades que recibirán los productos)	# CLIENTES EXTERNOS: (Detallar los organismos, Instituciones que recibirán los productos del proceso)		
	1 Bitácoras y registros actualizados de accesos y cambios realizados.	1 Dependencias PGR y Regionales	1 N/A		
	2 Reportes de revisión periódica de usuarios, perfiles y privilegios.	2 Dependencias PGR y Regionales	2 N/A		
	3 Reportes periódicos de control de accesos y seguridad tecnológica.	3 Dependencias PGR y Regionales	3 N/A		
PROCESOS RELACIONADOS:		Gestión de Sistemas, Operación de Infraestructura Tecnológica y Redes, Administración de Bases de Datos y Respaldos			
# ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)	
1 Recibir solicitudes de creación, modificación, suspensión o cancelación de accesos a sistemas, plataformas, equipos o servicios tecnológicos.	Oficial Técnico de Infotecnología	5 min	Porcentaje de accesos tecnológicos autorizados y revisados conforme a la política institucional	Bitácoras y registros actualizados de accesos y cambios realizados.	
2 Verificar que la solicitud esté debidamente justificada, autorizada y respaldada por la dependencia competente.	Oficial Técnico de Infotecnología	5 min			
3 Validar el perfil, rol y nivel de acceso requerido conforme a las funciones del usuario solicitante.	Oficial Técnico de Infotecnología	10 min			
4 Determinar si el acceso solicitado procede de acuerdo con las políticas y controles institucionales.	Oficial Técnico de Infotecnología	5 min			

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 26 de 183

#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)
5	Crear usuarios y credenciales en los sistemas, plataformas o recursos tecnológicos autorizados.	Oficial Técnico de Infotecnología	5 min	Porcentaje de accesos tecnológicos autorizados y revisados conforme a la política institucional	Bitácoras y registros actualizados de accesos y cambios realizados.
6	Asignar perfiles, privilegios y permisos de acceso según el nivel autorizado.	Oficial Técnico de Infotecnología	15 min		Reportes de revisión periódica de usuarios, perfiles y privilegios.
7	Analizar la configuración, controles de seguridad sobre contraseñas, sesiones, autenticación y restricciones de acceso.	Oficial Técnico de Infotecnología	1 hora		
8	Entregar al usuario las credenciales o instrucciones de acceso bajo los mecanismos institucionales definidos.	Oficial Técnico de Infotecnología	5 min		
9	Restablecer contraseñas o accesos cuando exista solicitud debidamente autorizada.	Oficial Técnico de Infotecnología	5 min		
10	Modificar privilegios de acceso cuando exista cambio de puesto, funciones, dependencia o nivel de responsabilidad.	Oficial Técnico de Infotecnología	15 min		
11	Suspender o cancelar accesos de usuarios desvinculados, trasladados o con cambios de función.	Oficial Técnico de Infotecnología	5 min		Reportes periódicos de control de accesos y seguridad tecnológica.
12	Monitorear el uso de accesos y eventos de seguridad en sistemas, equipos o servicios tecnológicos.	Oficial Técnico de Infotecnología	30 min		
13	Identificar y analizar el acceso no autorizados, perfiles incompatibles, intentos fallidos o incidentes de seguridad.	Oficial Técnico de Infotecnología	1 hora		
14	Atender incidentes relacionados con accesos, credenciales o uso indebido de recursos tecnológicos.	Oficial Técnico de Infotecnología	15 min		
15	Aplicar medidas correctivas o preventivas ante hallazgos de seguridad o desviaciones de control.	Oficial Técnico de Infotecnología	1 hora		
16	Revisar periódicamente los permisos, perfiles y privilegios asignados a los usuarios.	Oficial Técnico de Infotecnología	1 hora		
17	Depurar usuarios inactivos, duplicados o con accesos improcedentes.	Oficial Técnico de Infotecnología	1 hora		
18	Documentar incidencias, revisiones, cambios de acceso y acciones correctivas ejecutadas.	Oficial Técnico de Infotecnología	2 horas		

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 27 de 183

ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)
Emitir reportes periódicos sobre accesos otorgados, modificados, cancelados e incidentes atendidos por sistemas. 19	Oficial Técnico de Infotecnología	1 hora	Porcentaje de accesos tecnológicos autorizados y revisados conforme a la política institucional	Bitácoras y registros actualizados de accesos y cambios realizados.
PLANES DE DIFUSIÓN:		Página Web de la PGR, enviar una copia digital a los colaboradores(a) por medio del correo electrónico institucional y enviar una copia física, a la vez colgarlo en el Portal Único de Transparencia del IAIP.		
Elaborado por:		Revisado por:		Verificado por:
Suyapa del Mar Andino Ordóñez Jefa de la Unidad de Modernización		Pablo Javier Padilla Avilés Oficial Técnico		Jorge Efraín Salgado Subdirector de Infotecnología
Firma:		Firma:		Firma:
Fecha: 20 de abril de 2026		Fecha: 20 de abril de 2026		Fecha: 22 de abril de 2026
Firma:		Firma:		Firma:
Fecha: 24 de abril de 2026		Fecha: 24 de abril de 2026		Fecha: 24 de abril de 2026

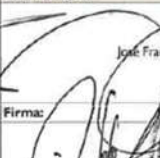
	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 28 de 183

		PROCURADURÍA GENERAL DE LA REPÚBLICA		CÓDIGO DEL FORMULARIO NCI-TSC/141-00 NCI-TSC/142-00 DE PGR	
FICHA DE PROCESOS					
FECHA DE ELABORACION:		27 de abril de 2026			
PROCESO:		Soporte Tecnológico a Oficinas Regionales			
SUBPROCESO:		Soporte Tecnológico a Oficinas Regionales			
OBJETIVO:		Brindar soporte tecnológico a las oficinas regionales para resolver problemas con equipos, sistemas y redes, de manera oportuna, asegurando que puedan operar de forma continua y eficiente.			
ALCANCE:		Este proceso inicia cuando una oficina regional solicita soporte técnico o reporta un problema tecnológico, y finaliza cuando el problema ha sido resuelto o la solicitud ha sido atendida satisfactoriamente o se realiza el dictamen técnico.			
RESPONSABLE DEL PROCESO:		Auxiliar Técnico			
NORMATIVAS APLICABLES:		Constitución de la República de Honduras; Ley General de la Administración Pública, Reglamento Interno de PGR, Modelo OSI e ISO 27000			
ENTRADAS:		PROVEEDORES: Regionales PGR		INSUMOS: Memorándum, sistema de ticket o correo electrónico, herramientas de precisión, aspiradoras, aire comprimido, estación de calor, pasta térmica, taladros, herramientas para red y hacer diagnósticos, entre otros.	
SALIDAS:	#	PRODUCTOS: (Describir los documentos, informes y otros resultados que genera el proceso)	#	CLIENTES INTERNOS: (Detallar los procesos o unidades que recibirán los productos)	# CLIENTES EXTERNOS: (Detallar los organismos, instituciones que recibirán los productos del proceso)
	1	Reporte de soporte técnico a regionales en el sistema de tickets o memorándum	1	Dependencias PGR	1 Ciudadanía
	2	Informe de incidencias atendidas a regionales	2	Dependencias PGR	2 Ciudadanía
	3	Dictámenes Técnico de Equipos Tecnológicos	3	Subdirección de Bienes Nacionales	3 Ciudadanía
	4	Reportes periódicos de soporte a regionales de mantenimiento.	4	Dependencias PGR	4 Ciudadanía
PROCESOS RELACIONADOS:		PR-SDIT-004 Administración de Activos Tecnológicos, PR-SDBN-003, PR-SDIT-Soporte Tecnológico a Oficinas Regionales, PR-RRPP-00X, PR-DDHH, PR-Dirección de Despacho			
#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)
1	Recibir la solicitud de soporte o requerimiento de la oficina regional.	Auxiliar Técnico	1 día	Porcentaje de solicitudes de soporte tecnológico a oficinas regionales atendidas dentro del plazo establecido	Reporte de soporte técnico a regionales en el sistema de tickets o memorándum
2	Registrar la solicitud en el sistema de tickets de soporte técnico.		5 min		
3	Clasificar la solicitud según tipo (incidencia, mantenimiento, instalación, levantamiento).		10 min		Reporte de soporte técnico a regionales en el sistema de tickets o memorándum
4	Priorizar la atención según criticidad e impacto operativo.		10 min		
5	Evaluar si la atención se realizará de forma remota o mediante visita técnica.		10 min		

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 29 de 183

#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permitan medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)
6	Programar la visita técnica cuando corresponda o el envío del equipo por correspondencia.	Auxiliar Técnico	30 min	Porcentaje de solicitudes de soporte tecnológico a oficinas regionales atendidas dentro del plazo establecido	Informe de incidencias atendidas a regionales
7	Diagnosticar el problema de forma remota.		15 min		
8	Brindar asistencia técnica al usuario.		4 horas		
9	Aplicar soluciones remotas a equipos, sistemas o redes.		2 horas		
10	Verificar el funcionamiento correcto posterior a la intervención.		30 min		
11	Escalar el caso a visita técnica si no se resuelve remotamente.		1 día		Reportes periódicos de soporte a regionales de mantenimiento.
12	Coordinar la visita con la oficina regional o el envío del equipo.		1 día		
13	Trasladar al personal técnico y los recursos necesarios.		5 días		
14	Realizar mantenimiento preventivo a equipos tecnológicos.		30 min		
15	Revisar el estado físico, lógico de equipos y redes.		2 horas		
16	Actualizar software y sistemas cuando corresponda.		3 horas		Informe de incidencias atendidas a regionales
17	Optimizar el rendimiento de los equipos y servicios.		2 horas		
18	Levantar información técnica de infraestructura tecnológica (redes, puntos, cámaras, etc.).		40 min		
19	Instalar puntos de red, equipos, cámaras u otros dispositivos.		2 horas		
20	Configurar equipos y servicios tecnológicos.		2 horas		
21	Probar el funcionamiento de las instalaciones realizadas.		1 hora		Dictamen Técnico de Equipos Tecnológicos
22	Diagnosticar fallas en sitio.		1 hora		

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 30 de 183

#	ACTIVIDADES:	RESPONSABLES: (Escribir los cargos de los responsables directos de cada actividad)	PERIODICIDAD: (Escribir el tiempo que se emplea para cada actividad)	INDICADORES: (Escribir los indicadores que permiten medir eficiencia, eficacia, costos y otros de cada actividad o grupo de actividades relacionadas)	PRODUCTOS: (Detallar los productos de los procesos)
23	Reparar equipos o componentes dañados.	Auxiliar Técnico	30 min	Porcentaje de solicitudes de soporte tecnológico a oficinas regionales atendidas dentro del plazo establecido	Informe de incidencias atendidas a regionales
24	Sustituir equipos o partes cuando sea necesario.		2 horas		
PLANES DE DIFUSIÓN:		Página Web de la PGR, enviar una copia digital a los colaboradores(a) por medio del correo electrónico institucional y enviar una copia física, a la vez colgarlo en el Portal Único de Transparencia del IAMP.			
Elaborado por:		Revisado por:	Verificado por:	Aprobado por:	
Suyapa del Mar Andino Ordóñez Jefa de la Unidad de Modernización		Abel Fernando Perez Vargas Auxiliar Técnico	 Jorge Fernando Sandoval Subdirector de la Procuraduría	 José Francisco Quiroz Mejía	
Firma: 		Daniel Isaac Membreno Anariba Auxiliar Técnico			
Fecha: 27 de abril de 2026		Fecha: 27 de abril de 2026	Fecha: 28 de abril de 2026	Fecha: 28 de abril de 2026	

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
MP-SDIT-001 Versión 1.0	MANUAL DE PROCEDIMIENTOS Fecha: 18 de mayo 2026	UDEM 31 de 183

8. DESCRIPCIÓN DE LOS PROCEDIMIENTOS



PGR
PROCURADURÍA GENERAL
DE LA REPÚBLICA



GOBIERNO DE LA
REPÚBLICA DE HONDURAS

PROCURADURÍA GENERAL DE LA REPÚBLICA

SUBDIRECCIÓN DE INFOTECNOLOGÍA

PROCEDIMIENTO GESTIÓN DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS

**CÓDIGO
PR-SDIT-001**

18 DE MAYO DE 2026

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UDEM 33 de 183

Responsables de los Cambios al Procedimiento

Elaboración del Documento

Elaborado por:	Cargo	Área de Trabajo	Fecha	Firma
Suyapa del Mar Andino Ordoñez	Jefa de Unidad	Unidad de Modernización	18 de mayo de 2026	

Revisión del Documento

Revisado por:	Cargo	Área de Trabajo	Fecha	Firma
Cristian Alexander Martínez Ochoa	Oficial Técnico	Subdirección de Infotecnología	19 de mayo de 2026	
Lisandro Alfredo Suárez Salinas	Oficial Técnico	Subdirección de Infotecnología	19 de mayo de 2026	

Verificación del Documento

Verificado por:	Cargo	Área de Trabajo	Fecha	Firma
Jorge Efrain Salgado	Subdirector de Infotecnología	Subdirección de Infotecnología	20 de mayo de 2026	
Ingrid Karina López Fuentes	Directora	Dirección de Administración y Finanzas	20 de mayo de 2026	

Aprobación del Documento

Aprobado por:	Cargo	Área de Trabajo	Fecha	Firma
José Francisco Quiroz Mejía	Sub-Procurador General de la República	Despacho de la Sub-Procuraduría General de la República	22 de mayo de 2026	

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UEM 34 de 183

Tabla de Contenido

1. Objetivo del Procedimiento	35
2. Alcance del Procedimiento.....	35
3. Marco Legal del Procedimiento	35
4. Políticas y Lineamientos del Procedimiento.....	35
5. Responsables del Procedimiento.....	36
6. Insumos del Procedimiento.....	37
7. Productos o Resultados del Procedimiento.....	37
8. Definición de Glosario de Términos, Siglas y Abreviaturas	37
9. Descripción del Procedimiento	40
10. Diagrama de Flujo del Procedimiento	44
11. Gestión del Riesgo	47
12. Elementos Transversales del Procedimiento	49
13. Bibliografía	50
14. Anexos.....	51
15. Control de Cambios al Procedimiento.....	55

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UDEM 35 de 183

1. Objetivo del Procedimiento

Gestionar el desarrollo, implementación y mantenimiento de sistemas informáticos institucionales, mediante la planificación, análisis, diseño, construcción, despliegue y mejora continua de soluciones tecnológicas, asegurando su calidad, disponibilidad, seguridad y alineación con las necesidades institucionales y de la ciudadanía.

2. Alcance del Procedimiento

El proceso inicia con la identificación y análisis de requerimientos de soluciones tecnológicas institucionales, y finaliza con la puesta en operación, mantenimiento, actualización y mejora continua de los sistemas informáticos, garantizando su funcionamiento, seguridad y disponibilidad.

3. Marco Legal del Procedimiento

No.	Código	Documento
1	Decreto 131-82	Constitución de la República
2	Decreto 74-61	Ley Orgánica de la Procuraduría General de la República
3	Decreto 146-86	Ley General de la Administración Pública
4	N/A	Reglamento Interno de PGR
5	N/A	Metodologías Ágiles para el Desarrollo de Sistemas,
6	ISO 12207-018	Procesos del ciclo de vida del software.
7	ISO 27001-019	Sistema de Gestión de Seguridad de la Información.

4. Políticas y Lineamientos del Procedimiento

- 4.1. Todo desarrollo o mantenimiento de sistemas deberá originarse a partir de una necesidad institucional debidamente identificada, documentada y validada por la autoridad competente.
- 4.2. Los requerimientos funcionales y técnicos deberán ser claros, completos y verificables antes de iniciar la fase de desarrollo o mantenimiento.
- 4.3. Los cambios a los requerimientos inicialmente aprobados deberán ser evaluados, documentados y autorizados formalmente por las partes involucradas.
- 4.4. El desarrollo de sistemas informáticos deberá realizarse utilizando metodologías, buenas prácticas y estándares que garanticen calidad, seguridad, escalabilidad y mantenibilidad.
- 4.5. Todo sistema desarrollado deberá contar con documentación técnica y funcional que respalde su operación, mantenimiento y mejora continua.
- 4.6. Antes de su implementación en ambiente productivo, los sistemas deberán someterse a pruebas funcionales, técnicas y de seguridad.
- 4.7. El mantenimiento de los sistemas informáticos podrá ser correctivo, preventivo o evolutivo, según la naturaleza de la necesidad identificada.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UDEM 36 de 183

- 4.8. Toda intervención de mantenimiento deberá quedar registrada como evidencia de control y trazabilidad.
- 4.9. Los sistemas informáticos deberán incorporar controles de seguridad que protejan la confidencialidad, integridad y disponibilidad de la información institucional.
- 4.10. El acceso a los sistemas y ambientes de desarrollo, prueba y producción deberá otorgarse conforme a perfiles y roles autorizados.
- 4.11. Las lecciones aprendidas derivadas de la ejecución del procedimiento deberán utilizarse para fortalecer la calidad de los sistemas informáticos institucionales.
- 4.12. Todo sistema informático institucional desarrollado, implementado o actualizado deberá contemplar actividades de capacitación dirigidas a los usuarios finales, previo o simultáneo a su puesta en operación.
- 4.13. Las actividades de capacitación podrán realizarse de forma presencial, virtual o mixta, según la naturaleza del sistema, disponibilidad institucional y cobertura requerida.
- 4.14. Todo sistema informático institucional deberá contar con al menos un Manual de Usuario, elaborado de forma clara, precisa y comprensible para los usuarios finales.
- 4.15. Los manuales de usuario deberán describir, como mínimo, las funcionalidades del sistema, los pasos operativos, los controles básicos de seguridad y las responsabilidades del usuario.

5. Responsables del Procedimiento

Área	Puesto de Trabajo	Responsabilidad
Subdirección de Infotecnología	Subdirector(a)	Es responsable de dirigir y supervisar el desarrollo, implementación y mantenimiento de los sistemas informáticos. Autoriza los requerimientos y cambios, verifica que el trabajo se realice conforme a la normativa vigente, y se asegura de que los sistemas funcionen correctamente, cuenten con documentación, capacitación a los usuarios y manuales de usuario actualizados.
Subdirección de Infotecnología	Oficial Técnico	Es responsable de realizar el trabajo técnico del sistema, como analizar las necesidades, desarrollar o modificar el sistema, hacer pruebas, corregir fallas y mantenerlo en funcionamiento. También apoya en la capacitación a los usuarios y en la elaboración o actualización de los manuales de usuario y documentación técnica.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001	Gestión de Desarrollo y Mantenimiento de Sistemas	UDEM
Versión 1.0	Fecha: 18 de mayo 2023	37 de 183

6. Insumos del Procedimiento

Código	Insumos	Lugar de Guarda	Tiempo de Guarda
M-PGR-SDIT-XXX-202X	Memorándum	Subdirección de Infotecnología	5 años
N/A	Sistemas de tikect o correo electrónico	Subdirección de Infotecnología	5 años
N/A	Documentación soporte de las dependencias (formatos y tablas de Excel)	Subdirección de Infotecnología	5 años

7. Productos o Resultados del Procedimiento

Código	Productos	Lugar de Guarda	Tiempo de Guarda
F-SDIT-001	Reporte de sistemas informáticos implementados y en producción	Subdirección de Infotecnología	5 años
N/A	Sistema Desarrollado	Subdirección de Infotecnología	5 años
INF-SDIT-001	Manual de usuario de las nuevas tecnologías	Subdirección de Infotecnología	5 años
N/A	Reporte de versiones de sistemas controlados y mantenimiento	Subdirección de Infotecnología	5 años
F-SDIT-003	Reporte de usuarios con acceso a sistemas y Capacitación básica en uso	Subdirección de Infotecnología	5 años

8. Definición de Glosario de Términos, Siglas y Abreviaturas

8.1. Términos

Ambiente de desarrollo: Entorno destinado a la programación, configuración y construcción del sistema antes de su validación formal. (Perssman, 2020).

Ambiente de producción: Entorno operativo real donde el sistema es utilizado por los usuarios finales. (Sommerville, 2011)

Ambiente de prueba: Entorno controlado donde se valida el funcionamiento del sistema antes de su paso a producción. (IEEE, 2013).

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001	Gestión de Desarrollo y Mantenimiento de Sistemas	UEM
Versión 1.0	Fecha: 18 de mayo 2023	38 de 183

Análisis de requerimientos: Proceso de identificar, documentar, validar y organizar las necesidades funcionales y no funcionales de un sistema antes de su desarrollo. (Sommerville, 2011).

Calidad del software: Grado en que un producto de software satisface requisitos establecidos y necesidades implícitas. (ISO/IEC, 2011)

Confidencialidad: Propiedad de la información de no ponerse a disposición o revelarse a individuos, entidades o procesos no autorizados. (ISO, 2022).

Control de cambios: Proceso formal para registrar, evaluar, aprobar e implementar modificaciones a requerimientos, componentes o versiones del sistema. (Project Management Institute, 2021)

Desarrollo de software: Conjunto de actividades para diseñar, construir, probar, desplegar y mantener aplicaciones informáticas. (Perssman, 2020).

Despliegue: Proceso de liberar e instalar una nueva versión del sistema en un entorno determinado. (Sommerville, 2011).

Documentación técnica: Conjunto de documentos que describen arquitectura, configuración, componentes, procesos y mantenimiento del sistema. (IEEE, 2018).

Escalabilidad: Capacidad de un sistema para mantener o mejorar su desempeño cuando aumenta la carga de trabajo o el número de usuarios. (Bass, 2021).

Integridad: Propiedad de exactitud y completitud de la información y de los métodos de procesamiento. (ISO, 2022).

Manual de usuario: Documento que explica de forma clara el uso operativo del sistema para los usuarios finales. (IEEE, 2018).

Mantenibilidad: Facilidad con la que un sistema puede ser modificado para corregir defectos, mejorar el rendimiento o adaptarse a cambios. (ISO/IEC, 2011).

Mantenimiento evolutivo: Adaptación o ampliación del sistema para incorporar nuevas funciones o responder a cambios institucionales. (ISO/IEC/IEEE, 2017).

Mantenimiento preventivo: Cambios efectuados para prevenir fallas futuras y mejorar la estabilidad o mantenibilidad del sistema. (IEEE, 2014).

Pruebas funcionales: Verificaciones orientadas a comprobar que el sistema cumple con los requerimientos especificados y produce los resultados esperados. (IEEE, 2013).

Pruebas de seguridad: Proceso de identificación de vulnerabilidades y validación de controles de protección en una aplicación. (OWASP Foundation, 2023)

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UEM 39 de 183

Pruebas técnicas: Evaluaciones del comportamiento técnico del sistema, incluyendo rendimiento, compatibilidad, estabilidad o integridad operativa. (Perssman, 2020).

Requerimiento funcional: Especificación de una función o servicio que el sistema debe proporcionar para satisfacer una necesidad del usuario o del negocio. (Sommerville, 2011).

Requerimiento técnico: Condición o característica técnica que debe cumplir un sistema para operar adecuadamente, como compatibilidad, rendimiento, arquitectura o seguridad. (Perssman, 2020).

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO, 2022).

Trazabilidad: Capacidad de seguir la relación entre requerimientos, cambios, pruebas, versiones y resultados a lo largo del ciclo de vida del sistema. (IEEE, 2018).

Memorándum: Comunicación escrita breve utilizada en el ámbito institucional o empresarial para informar, recordar o instruir sobre asuntos específicos. (Real Academia Española, 2023)

Normativa: Conjunto de normas jurídicas que regulan una materia específica dentro de un ordenamiento legal. (Carbonell, 2019)

Oficio: Documento formal mediante el cual una autoridad comunica decisiones, solicitudes o información a otra autoridad o entidad. (De la Torre, Técnicas de redacción jurídica, 2018)

8.2. Siglas

ISO: International Organization for Standardization

NIST: National Institute of Standards and Technology

PGR: Procuraduría General de la República.

SDIT: Subdirección de Infotecnología.

TIC: Tecnologías de la Información y la Comunicación.

UEM: Unidad de Modernización.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UEM 40 de 183

9. Descripción del Procedimiento

Oficial Técnico

- 9.1. Recibir solicitudes de desarrollo, mejora o mantenimiento de sistemas informáticos. Consiste en recibir formalmente las solicitudes enviadas por las distintas dependencias de la institución, deben indicar de forma clara la necesidad o problema que se desea resolver. Esta actividad permite iniciar el proceso y dejar constancia de la petición recibida.
- 9.2. Analizar los requerimientos funcionales y técnicos de los usuarios; se revisa la información proporcionada por el usuario para entender qué necesita el sistema y cómo debe funcionar, se identifican las funciones principales y los aspectos técnicos requeridos. Este análisis permite definir correctamente el alcance del trabajo a realizar.
- 9.3. Validar los requerimientos con las dependencias solicitantes, se confirma que los requerimientos identificados reflejan su necesidad real, a la vez se aclaran dudas y se realizan ajustes si es necesario; esta validación evita errores o malentendidos durante el desarrollo del sistema.
- 9.4. Priorizar los requerimientos conforme a criterios institucionales. Los requerimientos se ordenan según su importancia, urgencia y disponibilidad de recursos, esto permite atender primero las necesidades más relevantes.
- 9.5. Diseñar la arquitectura funcional y técnica del sistema informático, en esta actividad se define cómo estará estructurado el sistema y cómo interactuarán sus componentes. Incluye la forma en que los usuarios utilizarán el sistema y cómo se procesará la información, sirve como base para el desarrollo del sistema.
- 9.6. Definir especificaciones técnicas y funcionales del sistema. Se detallan las funciones que tendrá el sistema y los requisitos técnicos necesarios, sirven como guía para el desarrollo y las pruebas.
- 9.7. Planificar el desarrollo del sistema, estableciendo tiempos, recursos y entregables, en esta actividad se elabora un plan de trabajo que define fechas, responsables y productos esperados, permite dar seguimiento ordenado al avance del sistema.
- 9.8. Desarrollar el sistema informático conforme a los requerimientos definidos, se construye el sistema siguiendo las especificaciones aprobadas y se desarrollan las funcionalidades acordadas con el usuario. Esta actividad materializa la solución informática solicitada.
- 9.9. Codificar los componentes del sistema utilizando estándares institucionales, se escribe el código del sistema siguiendo normas y buenas prácticas establecidas. Esto asegura que el sistema sea ordenado y fácil de mantener facilitando las futuras mejoras o correcciones.
- 9.10. Integrar los diferentes módulos del sistema, unen las distintas partes del sistema para que funcionen como un todo. Se verifica que los módulos se comuniquen correctamente entre sí; esta integración permite evaluar el funcionamiento completo del sistema.
- 9.11. Ejecutar pruebas unitarias de los componentes desarrollados. Se prueban individualmente las partes del sistema para verificar su correcto funcionamiento. Estas pruebas permiten detectar errores de manera temprana y ayudan a asegurar la calidad del desarrollo.
- 9.12. Realizar pruebas integrales del sistema, se evalúa el sistema completo en conjunto y verifica que todas las funciones operen correctamente. Estas pruebas simulan el uso real del sistema.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UEM 41 de 183

- 9.13. Validar el cumplimiento de los requerimientos funcionales, se confirma que el sistema cumple con lo solicitado por el usuario. La validación se realiza con base en los requerimientos aprobados, asegurando que el sistema satisface la necesidad institucional.
- 9.14. Corregir errores identificados durante las pruebas. Se atienden las fallas detectadas en las pruebas y realizan los ajustes necesarios para corregir errores. Esto mejora la estabilidad y confiabilidad del sistema.
- 9.15. Preparar el ambiente de producción para la implementación del sistema, en esta actividad se acondiciona el entorno donde operará el sistema oficialmente. Incluye configuraciones técnicas necesarias para su funcionamiento. Esta preparación evita problemas al momento de su uso.
- 9.16. Desplegar el sistema en el ambiente productivo, se instala el sistema en el entorno donde será utilizado por los usuarios, verificando que el despliegue se realice correctamente. Esta actividad marca el paso previo al uso institucional.
- 9.17. Configurar el sistema para su operación institucional, se ajustan parámetros del sistema según las necesidades de la institución, a la vez crear usuarios, permisos y configuraciones básicas. Esto permite que el sistema sea utilizado correctamente.
- 9.18. Verificar el funcionamiento del sistema en producción, comprobando que el sistema opere correctamente una vez instalado, revisar que las funciones principales estén disponibles. Esta verificación asegura la correcta implementación.
- 9.19. Monitorear el desempeño del sistema informático, dando seguimiento al funcionamiento del sistema durante su uso. Se observa su estabilidad, velocidad y disponibilidad, permitiendo detectar posibles problemas oportunamente.
- 9.20. Identificar fallas o necesidades de mejora en el sistema, recopilando incidencias reportadas por los usuarios para identificar oportunidades de mejora. Esto contribuye a la mejora continua del sistema.
- 9.21. Corregir errores mediante mantenimiento correctivo, solucionar fallas detectadas durante la operación del sistema. El objetivo es restablecer su funcionamiento normal. Este mantenimiento asegura la continuidad del servicio.
- 9.22. Actualizar el sistema conforme a cambios normativos o tecnológicos, se realizan ajustes para cumplir nuevas disposiciones legales o técnicas. Las actualizaciones mantienen el sistema vigente y funcional para evitar riesgos por desactualización.
- 9.23. Mejorar funcionalidades del sistema según requerimientos institucionales, se incorporan nuevas funciones solicitadas por la institución. Estas mejoras optimizan el uso del sistema y permiten adaptarlo a nuevas necesidades.
- 9.24. Controlar las versiones del sistema mediante herramientas de versionamiento, registrando los cambios realizados en cada versión del sistema. Esto permite identificar qué modificaciones se han hecho y cuándo, a la vez facilita la gestión y recuperación de versiones anteriores.
- 9.25. Registrar los cambios realizados en el sistema, se documentan todas las modificaciones efectuadas. Este registro sirve como evidencia y control, apoyando la trazabilidad del procedimiento.
- 9.26. Registrar en los reportes todas las actividades de desarrollo, implementación y mantenimiento. Se elaboran reportes que reflejan el trabajo realizado, permiten seguimiento y control, sirven como respaldo administrativo y técnico.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001	Gestión de Desarrollo y Mantenimiento de Sistemas	UEM
Versión 1.0	Fecha: 18 de mayo 2023	43 de 183



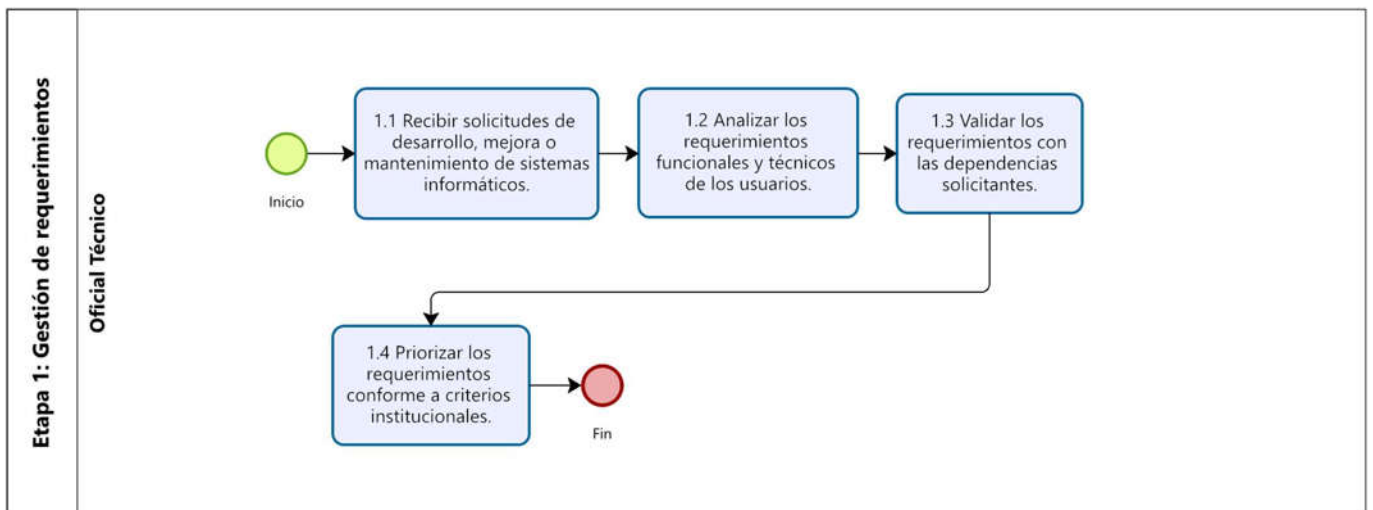
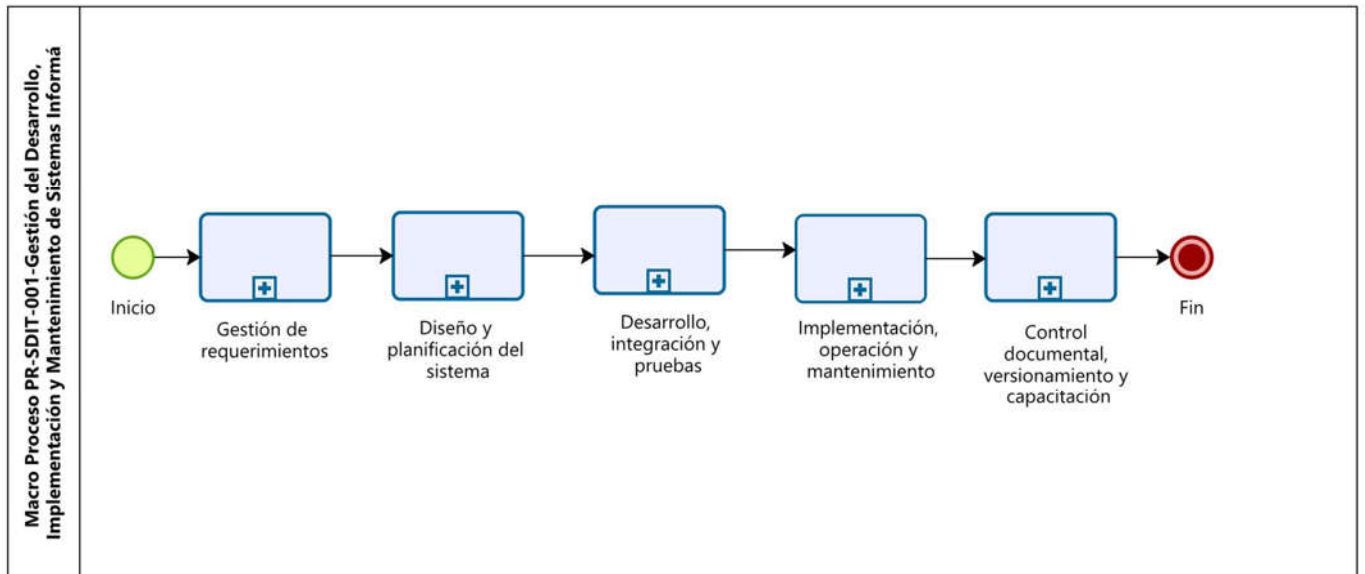
Matriz de Actividades, Responsables y Formularios
Manual de Procedimientos de la Subdirección de Infotecnología
Proceso de Gestión del Desarrollo, Implementación y Mantenimiento de Sistemas Informáticos



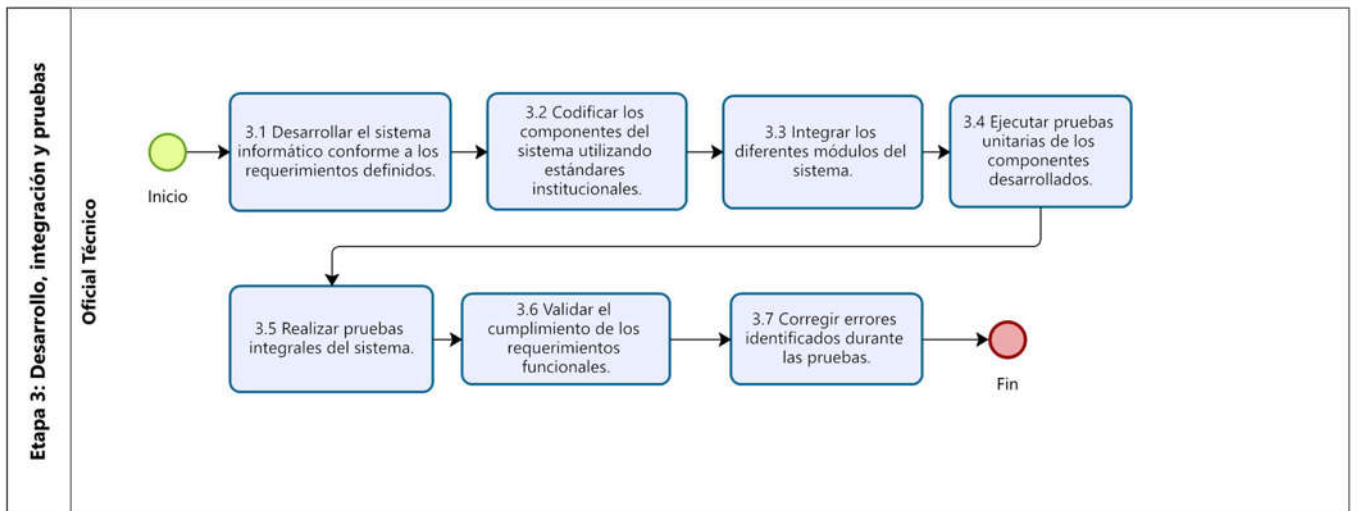
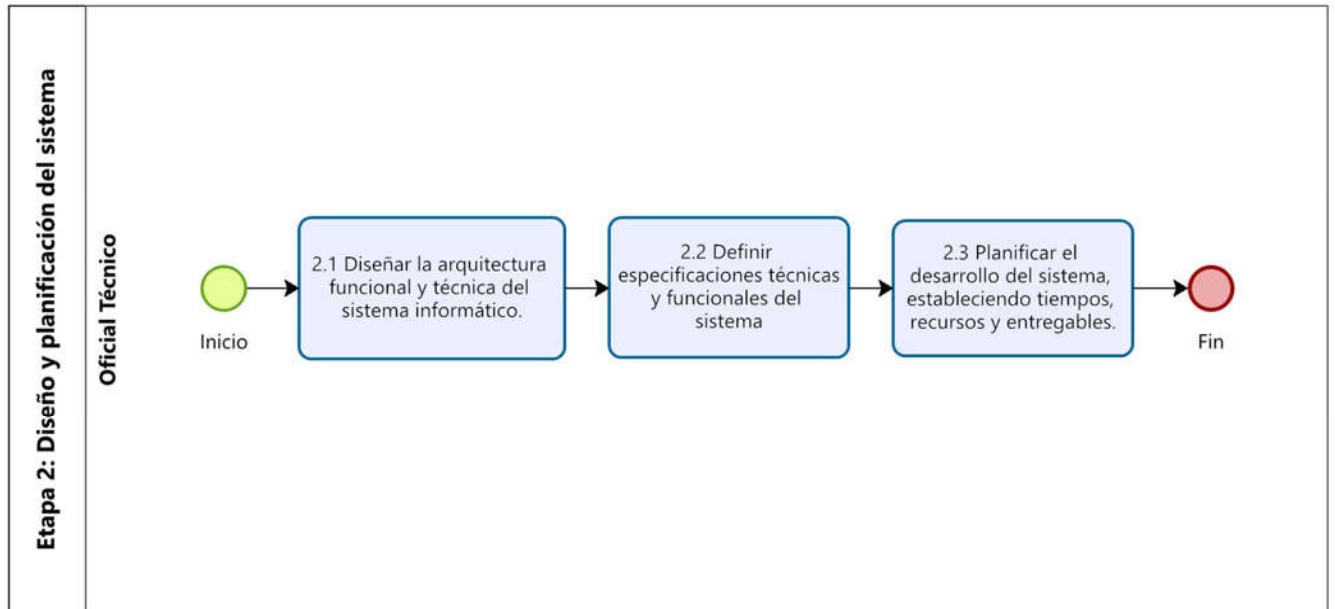
No.	Etapas del Proceso	Objetivo de la Etapa	Insumo	Actividad	Tiempo	Responsable	Producto	Envío a:
4	Implementación, operación y mantenimiento	Preparar, desplegar, configurar e implementar el sistema en producción, verificando su funcionamiento, monitoreando su desempeño y realizando mantenimiento, actualizaciones y mejoras.	Tecnologías de Desarrollo, Bases de Datos (MySQL y PostgreSQL), Herramientas de Desarrollo y Administración (Visual Studio Code, MySQL Workbench (Community Edition), Git / GitHub y Termius)	4.4 Verificar el funcionamiento del sistema en producción.	2 días	Oficial Técnico	Reporte de versiones de sistemas controlados y mantenimiento	Dependencias PGR
				4.5 Monitorear el desempeño del sistema informático.	3 días			
				4.6 Identificar fallas o necesidades de mejora en el sistema.	2 días			
				4.7 Corregir errores mediante mantenimiento correctivo.	5 días			
				4.8 Actualizar el sistema conforme a cambios normativos o tecnológicos.	5 días			
				4.9 Mejorar funcionalidades del sistema según requerimientos institucionales.	5 días			
				5.1 Controlar las versiones del sistema mediante herramientas de versionamiento.	3 días		Reporte de versiones de sistemas controlados y mantenimiento	Oficial Técnico
				5.2 Registrar los cambios realizados en el sistema.	3 días			
				5.3 Registrar en los reportes todas las actividades de desarrollo, implementación y mantenimiento.	7 días			
5	Control documental, versionamiento y capacitación	Registrar cambios, controlar versiones, documentar las actividades realizadas, mantener actualizada la documentación técnica y funcional, elaborar manuales y capacitar usuarios cuando corresponda.		5.4 Mantener actualizada la documentación técnica y funcional del sistema.	3 días	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	Manual de usuario de las nuevas tecnologías	Dependencias PGR
				5.5 Generar el manual de usuario del sistema.	4 días		Reporte de usuarios con acceso a sistemas y capacitación básica en uso	
				5.6 Capacitar a los usuarios en el uso del sistema (cuando aplique).	5 días			
				5.7 Implementación del Sistema	5 días			

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UDEM 44 de 183

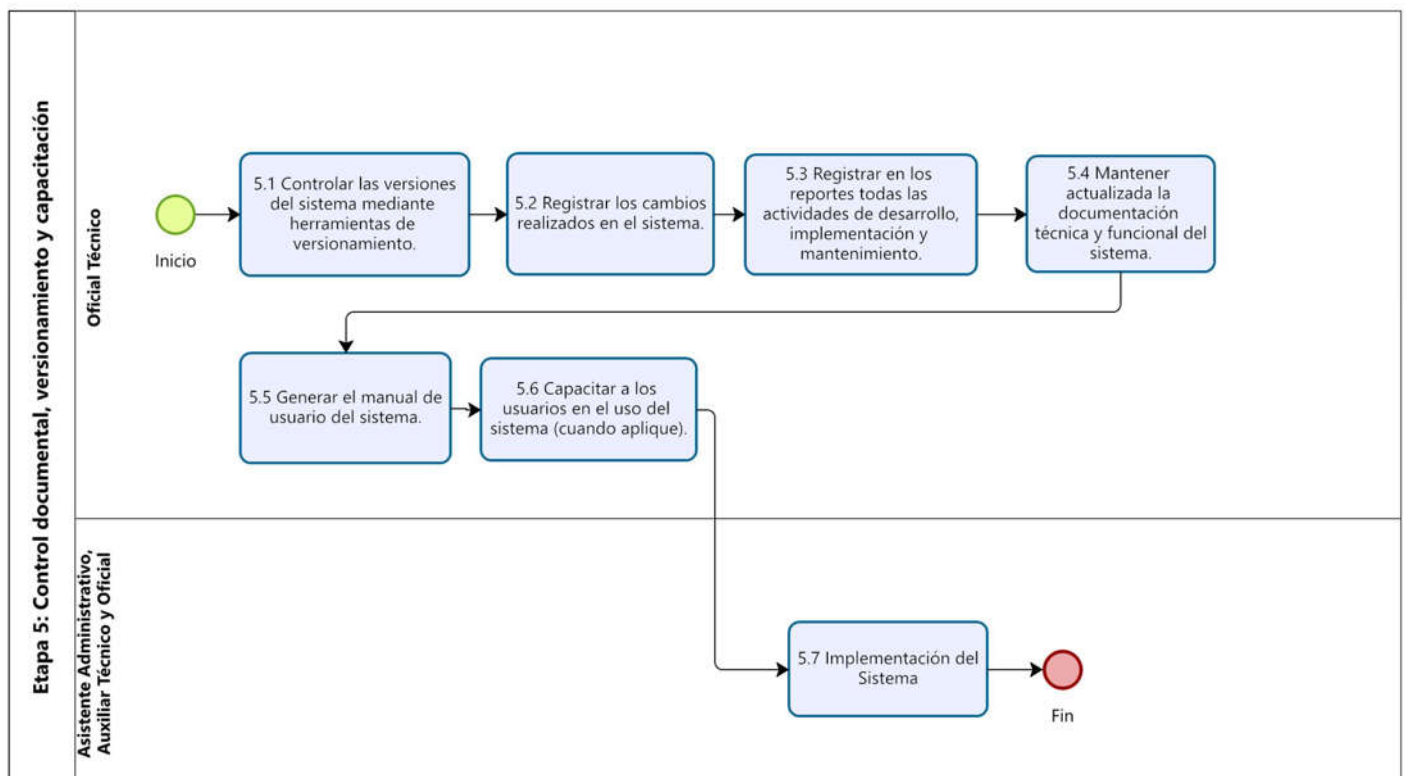
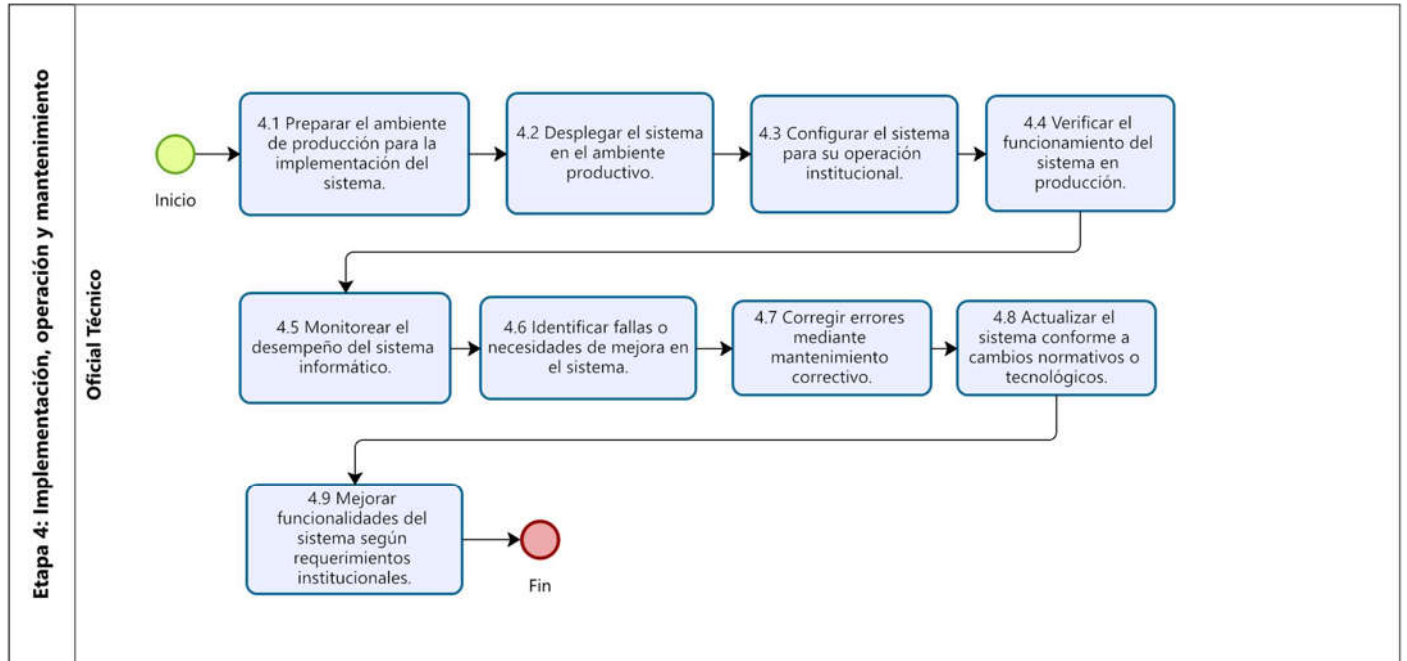
10. Diagrama de Flujo del Procedimiento



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UDEM 45 de 183

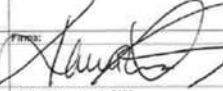


	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UDEM 46 de 183



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UDEM 47 de 183

11. Gestión del Riesgo

PGR		PROCURADURÍA GENERAL DE LA REPÚBLICA										NCI-TSC/223-00; NCI-TSC/223-00; NCI-TSC/224-00	
		MATRIZ PARA LA EVALUACIÓN, ANÁLISIS Y RESPUESTA A LOS RIESGOS										Formulario 27 PGR	
PROCESO:		Gestión del Desarrollo, Implementación y Mantenimiento de Sistemas Informáticos											
NOMBRE DEL SUBPROCESO:		Gestión del Desarrollo, Implementación y Mantenimiento de Sistemas Informáticos											
OBJETIVO:		Gestionar el desarrollo, implementación y mantenimiento de sistemas informáticos institucionales, mediante la planificación, análisis, diseño, construcción, despliegue y mejora continua de soluciones tecnológicas, asegurando su calidad, disponibilidad, seguridad y alineación con las necesidades institucionales y de la ciudadanía.											
(1) No.	(2) Etapa del proceso	(3) Descripción del Riesgo	Riesgo Inherente		(6) Zona de Riesgo Preliminar	(7) Controles obligatorios para mitigar los riesgos	(8) Controles que existen en la entidad	(9) Controles pendientes por establecer para mitigar los riesgos	Riesgo Residual		(12) Zona de Riesgo Final	(13) Respuesta a los Riesgos	
			(4) P	(5) I					(10) P	(11) I			
1	Gestión de requerimientos	1.1 Los requerimientos formulados por las dependencias de la PGR carecen, en algunas casos, de la claridad y precisión necesarias, lo que puede provocar el desarrollo de funcionalidades que no responden de manera efectiva a las necesidades reales de los usuarios institucionales.	2	2	B	Realizar reuniones de validación con la dependencia solicitante. Elaborar acta, correo o constancia de conformidad de requerimientos. No iniciar desarrollo sin requerimientos validados y aprobados.	Realizar reuniones de validación con la dependencia solicitante. Elaborar acta, correo o constancia de conformidad de requerimientos. No iniciar desarrollo sin requerimientos validados y aprobados.		1	1	B	Aceptar	
2	Diseño y planificación del sistema	2.1 La planificación del desarrollo del sistema puede ser deficiente por estimaciones incorrectas de tiempo.	2	2	B	Elaborar plan de trabajo con cronograma, responsables y entregables. Revisar la planificación por la Subdirección de Infotecnología. Verificar compatibilidad con infraestructura, bases de datos, estándares institucionales y disponibilidad del personal técnico.	Elaborar plan de trabajo con cronograma, responsables y entregables. Revisar la planificación por la Subdirección de Infotecnología. Verificar compatibilidad con infraestructura, bases de datos, estándares institucionales y disponibilidad del personal técnico.		1	1	B	Aceptar	
3	Desarrollo, integración y pruebas	3.1 Durante el desarrollo del sistema pueden presentarse errores de programación o fallos de integración entre módulos.	3	2	M	Realizar revisión de código por pares o responsable técnico. Usar ambiente de desarrollo separado. Comparar avances contra matriz de requerimientos aprobada. Registrar incidencias y correcciones realizadas.	Realizar revisión de código por pares o responsable técnico. Usar ambiente de desarrollo separado. Comparar avances contra matriz de requerimientos aprobada. Registrar incidencias y correcciones realizadas.		2	2	B	Aceptar	
4	Implementación, operación y mantenimiento	4.1 Durante la implementación, operación o mantenimiento del sistema puede ocurrir incompatibilidad de instalación con los equipos.	2	2	B	Ejecutar respaldos periódicos y respaldos previos a cambios críticos. Restringir modificaciones directas en bases de datos. Mantener bitácoras de operación. Probar restauración de respaldos. Definir responsables de custodia de la información.	Ejecutar respaldos periódicos y respaldos previos a cambios críticos. Restringir modificaciones directas en bases de datos. Mantener bitácoras de operación. Probar restauración de respaldos. Definir responsables de custodia de la información.		1	1	B	Aceptar	
5	Control documental, versionamiento y capacitación	5.1 La documentación del proceso puede ser incompleta, estar dispersa o no existir, afectando la trazabilidad de solicitudes, aprobaciones, pruebas, cambios, mantenimientos e implementación del sistema.	2	2	B	Establecer estructura documental mínima. Registrar solicitudes, actas, aprobaciones, reportes, pruebas y constancias. Aplicar codificación y control de versiones documentales.	Establecer estructura documental mínima. Registrar solicitudes, actas, aprobaciones, reportes, pruebas y constancias. Aplicar codificación y control de versiones documentales.		1	1	B	Aceptar	
Elaborado por:						Revisado por:						Aprobado por:	
Lisandro Alfredo Suárez Salinas Oficial Técnico Cristian Alexander Martínez Ochoa Oficial Técnico Suyapa del Mar Andino Ordóñez Jefa de la Unidad de Modernización						Ingrid Karina López Fuentes Directora de Administración y Finanzas Jorge Elías Salgado Subdirector de Infotecnología						Jessa Francisco Quintanilla Subprocurador General de la República Procuraduría General de la República	
Firma:  Fecha: 19 de mayo de 2023						Firma:  Fecha: 20 de mayo de 2023						Firma:  Fecha: 20 de mayo de 2023	
													

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UDEM 48 de 183

	PROCURADURÍA GENERAL DE LA REPÚBLICA		NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00		
	MAPA PARA LA VALORACIÓN PRELIMINAR Y FINAL DE LOS RIESGOS		Formulario 28 PGR		
PROPÓSITO:	Facilitar la valoración y determinación de la zona de riesgos, de acuerdo con la explicación que consta en el Anexo 22 Instructivo para la gestión de riesgos				
PROBABILIDAD					
Muy Alta (5)	A	A	E	E	E
Alta (4)	M	A	A	E	E
Moderada (3)	B	3.1 M	A	E	E
Baja (2)	B	1.1 2.1 4.1 5.1 y 5.2 B	M	A	E
Muy Baja (1)	B	B	M	A	A
	Muy Bajo (1)	Bajo (2)	Moderado (3)	Alto (4)	Muy Alto(5)
IMPACTOS					
ZONA DE RIESGO:					
B: Zona de Riesgo Baja: Respuesta, Aceptar el riesgo					
M: Zona de Riesgo Moderada: Respuestas, Aceptar el riesgo o reducir el riesgo. Costo Beneficio					
A: Zona de Riesgos Alta: Respuestas, Reducir el riesgo, o evitar, o compartir, o transferir					
E: Zona de Riesgo Extrema: Respuestas, Reducir el riesgo (costo beneficio), o evitar, o compartir o transferir					

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UEM 49 de 183

12. Elementos Transversales del Procedimiento



Matriz de Verificación
Inclusión de Elementos Transversales Estratégicos
Manual de Procedimientos de la Subdirección de Infotecnología



Denominación del Proceso: Gestión del Desarrollo, Implementación y Mantenimiento de Sistemas Informáticos			
Preguntas de Verificación	Si	No	Respuestas de Verificación
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Control Interno y anticorrupción</u> ?	X		El proceso cuenta con controles de autorización, segregación de funciones, uso de bitácoras, gestión de accesos, ejecución de pruebas, respaldos de información y trazabilidad de cambios. Estas medidas permiten reducir riesgos como la manipulación indebida de la información, la discrecionalidad, la pérdida de datos y el uso no autorizado de los sistemas.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Descentralización</u> ?		X	No se identifican actividades descentralizadas hacia las oficinas regionales. El desarrollo, implementación y mantenimiento de los sistemas informáticos se concentra en la Subdirección de Infotecnología. En ese sentido, se recomienda evaluar la implementación de mecanismos de coordinación o enlaces regionales. Las demás dependencias participan en la identificación de necesidades, definición de requerimientos, validación de pruebas y reporte de incidencias.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Participación Ciudadana</u> ?		X	No se contempla consulta directa a la ciudadanía durante el desarrollo de los sistemas informáticos.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Transparencia y Acceso a la Información Pública</u> ?	X		El proceso garantiza que los sistemas generen información íntegra, trazable y disponible para la elaboración de reportes, la rendición de cuentas y la atención de solicitudes de información pública. Asimismo, contempla controles para la protección de datos clasificados como reservados, confidenciales o sensibles.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Archivo Documental</u> ?	X		Se conservan expedientes físicos o digitales que incluyen solicitudes, especificaciones, aprobaciones, resultados de pruebas, manuales, bitácoras, informes y actas de cierre. Esta documentación debe mantenerse debidamente codificada, versionada y bajo la responsabilidad de funcionarios claramente definidos.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al cumplimiento de los indicadores de <u>PEI Institucional</u> ?	X		El proceso se vincula con metas de modernización, eficiencia, transformación digital, disponibilidad de sistemas y atención de incidencias. Cada desarrollo o mantenimiento debe relacionarse con objetivos estratégicos, POA, productos institucionales y responsables de seguimiento.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UEM 50 de 183

13. Bibliografía

- Project Management Institute. (2021). A guide to the project management body of knowledge (PMBOK® guide) (7th ed.). PMBOK® guide.
- Bass, L. C. (2021). *Software architecture in practice (4th ed.)*. Addison-Wesley.
- Bobbio, N. (2000). *Estado, gobierno y sociedad: Por una teoría general de la política*. Fondo de Cultura Económica.
- *Enciclopedia Concepto*. (2013). Obtenido de <https://concepto.de/analisis-3/>
- García de Enterría, E. &. (2017). *Curso de Derecho Administrativo (Vol. I)*. Civitas.
- González, M. (2020). *Manual de Asesoría Jurídica Preventiva*. Jurídica Continental.
- Heller, H. (2003). *Teoría del Estado*. Fondo de Cultura Económica.
- IEEE. (2013). *Standard of system and software verification and validation*. IEEE.
- IEEE. (2014). *IEEE Standard for Software Maintenance*. IEEE.
- IEEE. (2018). *IEEE Std 1063-2001: Standard for Software User Documentation*. IEEE.
- ISO. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.
- ISO/IEC. (2011). *ISO/IEC 25010:2011 Systems and software engineering—Systems and software Quality Requirements and Evaluation (SQuaRE)—System and software quality models*. ISO.
- ISO/IEC/IEEE. (2017). *ISO/IEC/IEEE 14764:2017 Systems and software engineering—Software life cycle processes—Software maintenance*. ISO.
- OWASP Foundation. (2023). *OWASP Application Security Verification Standard 4.0.3*. Obtenido de <https://owasp.org>
- Perssman, R. &. (2020). *Ingeniería de Software: Un enfoque práctico 9na edición*. McGraw-Hill.
- *Real Academia Española*. (2023). Obtenido de Diccionario de la lengua española (23.ª ed.): <https://dle.rae.es>
- Sommerville. (2011). *Ingeniería de software (9.ª ed.)*. Pearson.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UDEM 51 de 183

14. Anexos

14.1. F-SDIT-001-Reporte de sistemas informáticos implementados y en producción

PROCURADURÍA GENERAL DE LA REPÚBLICA				
	SUBDIRECCIÓN DE INFOTECNOLOGÍA			F-SDIT-001
	REPORTE DE SISTEMAS INFORMÁTICOS IMPLEMENTADOS Y EN PRODUCCIÓN V 1.0 Fecha: 20 de mayo de 2026			
REPORTE TRIMESTRAL (DESARROLLO)				
	ACCIÓN	OBSERVACIÓN	OBJETIVO POA	MEDIO DE VERIFICACIÓN
SEMANA 1				
SEMANA 2				
SEMANA 3				
SEMANA 4				

 PGR PROCURADURÍA GENERAL DE LA REPÚBLICA	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	 UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UDEM 52 de 183

14.2. INF-SDIT-001-Manual de usuario de las nuevas tecnologías

 PGR PROCURADURÍA GENERAL DE LA REPÚBLICA	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCION DE INFOTECNOLOGIA	
INF-SDIT-001 Versión 1.0	MANUAL DE USUARIO SISTEMA XXXXXXXX Fecha: 27 de junio 2026	SDIT 2 de 3

1. Introducción

Breve descripción del sistema y finalidad del manual

2. Objetivo del Análisis

Qué busca facilitar el manual al usuario

3. Acceso al Sistema

Dirección de acceso, usuarios (usuario general, operador, supervisor, administrador, usuario de consulta), contraseña e ingreso

4. Pantalla Principal

Menú y principales opciones disponibles

5. Uso del Sistema

Instrucciones paso a paso de cada función

6. Estados y seguimiento

Estados que puede tener una gestión o solicitud

7. Seguridad y contraseña

Cambio de contraseña, protección de credenciales y cierre de sesión

8. Problemas frecuentes

Problema, posible causa y solución

9. Soporte Técnico

Unidad o canal al que debe acudir el usuario

10. Control de cambios

Versión	Fecha	Descripción de modificaciones	Firma de aprobación
Elaborado por			
Revisado por			
Aprobado por			

 PGR PROCURADURÍA GENERAL DE LA REPÚBLICA	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCION DE INFOTECNOLOGIA	
INF-SDIT-001 Versión 1.0	MANUAL DE USUARIO SISTEMA XXXXXXXX Fecha: 27 de junio 2026	SDIT 3 de 3

11. Responsables

Responsabilidad	Nombre y Cargo	Firma	Fecha
Elaborado por			
Revisado por			
Aprobado por			

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UDEM 53 de 183

14.3. Reporte de versiones de sistemas controlados y mantenimiento


PGR-Honduras

[Overview](#)
[Repositories 23](#)
[Projects](#)
[Packages](#)
[Teams](#)
[People](#)
[Insights](#)
[Settings](#)



Procuraduría General de la Republica - Honduras
[Follow](#)

2 followers
Honduras

Type
Language
Sort
New

Memo-Frontend Private

TypeScript
0 stars
0 forks
0 issues
Updated yesterday

Memo-Backend Private

JavaScript
0 stars
0 forks
0 issues
Updated yesterday

requisiciones-pgr Private

Sistema de Requisiciones para la PGR
PHP
0 stars
0 forks
0 issues
Updated yesterday

SIP-Frontend Private

Frontend del Sistema para ingresos y pagos
TypeScript
0 stars
0 forks
0 issues
Updated last week

SIP-Backend Private

Sistema para ingresos y pagos de la PGR
JavaScript
0 stars
0 forks
0 issues
Updated last week

PDF-backend Private

Backend para la creación de pdf's
JavaScript
0 stars
0 forks
0 issues
Updated last week

smit-pgr Private

Sistema de mantenimiento IT
PHP
0 stars
0 forks
0 issues
Updated 2 weeks ago

Solvencias-Proyecto Private

TypeScript
0 stars
0 forks
0 issues
Updated 2 weeks ago

SSS-Admin-SU Private

En este repositorio se hará la creación de las paginas correspondientes a la vista del administrador SU.
TypeScript
1 star
0 forks
0 issues
Updated 2 weeks ago

SSS-Admin Private

Aplicación para los administradores del Sistema de Solicitud de Solvencias de la PGR
HTML
1 star
0 forks
0 issues
Updated 2 weeks ago

[View all repositories](#)



THURSDAY, JUNE 18

GitHub Product Roadmap – Q2 2026

- What's new and what's coming next
- How to secure and govern AI at scale
- Rise of connected, agent workflows

[Register for the webinar](#)

View as: Public

You are viewing the README and pinned repositories as a public user.
You can create a README file visible to anyone.
Get started with tasks that most successful organizations complete.

Discussions

Set up discussions to engage with your community!
[Turn on discussions](#)

People

[Invite someone](#)

Top languages

JavaScript
TypeScript
PHP
HTML


© 2026 GitHub, Inc.
[Terms](#)
[Privacy](#)
[Security](#)
[Status](#)
[Community](#)
[Docs](#)
[Contact](#)
[Manage cookies](#)
Do not share my personal information

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-001 Versión 1.0	Gestión de Desarrollo y Mantenimiento de Sistemas Fecha: 18 de mayo 2023	UEM 55 de 183

15. Control de Cambios al Procedimiento

Historial de Cambios al Procedimiento

Fecha	Versión	Autor		Descripción del cambio	Cambio Autorizado por:	
		Cargo	Área		Cargo	Firma

PROCURADURÍA GENERAL DE LA REPÚBLICA

SUBDIRECCIÓN DE INFOTECNOLOGÍA

PROCEDIMIENTO OPERACIÓN DE INFRAESTRUCTURA TECNOLÓGICA Y REDES

**CÓDIGO
PR-SDIT-002**

20 DE MAYO DE 2026

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 57 de 183

Responsables de los Cambios al Procedimiento

Elaboración del Documento

Elaborado por:	Cargo	Área de Trabajo	Fecha	Firma
Suyapa del Mar Andino Ordoñez	Jefa de Unidad	Unidad de Modernización	20 de mayo de 2026	



Revisión del Documento

Revisado por:	Cargo	Área de Trabajo	Fecha	Firma
Arnaldo Alcides García Alvarado	Oficial Técnico	Subdirección de Infotecnología	21 de mayo de 2026	
Cristian Alexander Martínez Ochoa	Oficial Técnico	Subdirección de Infotecnología	21 de mayo de 2026	

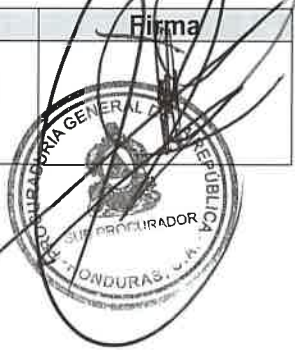
Verificación del Documento

Verificado por:	Cargo	Área de Trabajo	Fecha	Firma
Jorge Efraín Salgado	Subdirector de Infotecnología	Subdirección de Infotecnología	22 de mayo de 2026	
Ingrid Karina López Fuentes	Directora	Dirección de Administración y Finanzas	22 de mayo de 2026	



Aprobación del Documento

Aprobado por:	Cargo	Área de Trabajo	Fecha	Firma
José Francisco Quiroz Mejía	Sub-Procurador General de la República	Despacho de la Sub-Procuraduría General de la República	26 de mayo de 2026	



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UEM 58 de 183

Tabla de Contenido

1. Objetivo del Procedimiento	59
2. Alcance del Procedimiento.....	59
3. Marco Legal del Procedimiento	59
4. Políticas y Lineamientos del Procedimiento.....	59
5. Responsables del Procedimiento.....	60
6. Insumos del Procedimiento.....	61
7. Productos o Resultados del Procedimiento.....	61
8. Definición de Glosario de Términos, Siglas y Abreviaturas	61
9. Descripción del Procedimiento	63
10. Diagrama de Flujo del Procedimiento	66
11. Gestión del Riesgo	69
12. Elementos Transversales del Procedimiento	71
13. Bibliografía	72
14. Anexos.....	73
15. Control de Cambios al Procedimiento.....	76

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 59 de 183

1. Objetivo del Procedimiento

Garantizar la operación continua, segura, eficiente y disponible de la infraestructura tecnológica y de redes institucional, mediante la administración, monitoreo, mantenimiento y mejora de los recursos tecnológicos, asegurando el soporte a los procesos institucionales y la prestación oportuna de servicios a la ciudadanía.

2. Alcance del Procedimiento

El proceso inicia con la identificación de requerimientos de operación, monitoreo o mantenimiento de los recursos tecnológicos institucionales, y finaliza con la garantía de disponibilidad, funcionamiento y soporte continuo de los servicios tecnológicos.

3. Marco Legal del Procedimiento

No.	Código	Documento
1	Decreto 131-82	Constitución de la República
2	Decreto 74-61	Ley Orgánica de la Procuraduría General de la República
3	Decreto 146-86	Ley General de la Administración Pública
4	N/A	Reglamento Interno de Trabajo PGR
5	ISO: 27001-020	Sistema de Gestión de Seguridad de la Información
6	ISO: 27033-021	Seguridad de redes.
7	ISO:22301-022	Sistema de Gestión de Continuidad del Negocio
8	ISO:2000-1	Sistema de Gestión de Servicios de Tecnologías de la Información

4. Políticas y Lineamientos del Procedimiento

4.1. Cumplimiento normativo

La operación de la infraestructura tecnológica y redes deberá ejecutarse conforme al marco legal vigente, las normas técnicas aplicables y las disposiciones institucionales emitidas por la autoridad competente.

4.2. Responsabilidad y segregación de funciones

Las actividades de administración, operación, monitoreo y control de la infraestructura tecnológica y redes deberán realizarse por personal autorizado, con funciones claramente definidas y debidamente segregadas, conforme a la estructura organizacional aprobada.

4.3. Disponibilidad y continuidad operativa

La operación de la infraestructura tecnológica y redes deberá orientarse a garantizar la continuidad, estabilidad y disponibilidad de los servicios tecnológicos institucionales, priorizando la atención de los servicios críticos.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 60 de 183

4.4. Seguridad de la información y accesos

El acceso a la infraestructura tecnológica y redes deberá restringirse exclusivamente a personal autorizado, mediante controles de seguridad lógica y física que protejan la confidencialidad, integridad y disponibilidad de la información institucional.

4.5. Gestión y control de cambios

Toda modificación a la infraestructura tecnológica o a la configuración de redes deberá ser previamente solicitada, evaluada, autorizada y documentada, asegurando la trazabilidad y minimizando el impacto en la operación institucional.

4.6. Atención y registro de incidencias

Las incidencias que afecten la infraestructura tecnológica y redes deberán ser registradas, atendidas y cerradas conforme a los niveles de prioridad establecidos, dejando evidencia de las acciones correctivas aplicadas.

4.7. Documentación y trazabilidad

Todas las actividades realizadas en el marco del procedimiento deberán documentarse mediante registros, bitácoras e informes, los cuales deberán mantenerse actualizados, codificados, versionados y bajo la responsabilidad de los funcionarios designados.

4.8. Mejora continua

El procedimiento de operación de infraestructura tecnológica y redes deberá revisarse y actualizarse periódicamente, considerando cambios normativos, tecnológicos, resultados de evaluaciones y análisis de riesgos.

5. Responsables del Procedimiento

Área	Puesto de Trabajo	Responsabilidad
Subdirección de Infotecnología	Subdirector(a)	Dirigir, supervisar y aprobar la operación de la infraestructura tecnológica y redes institucionales. Autorizar cambios relevantes, priorizar la atención de incidencias críticas y asegurar el cumplimiento del marco normativo, las políticas institucionales y los objetivos estratégicos.
Subdirección de Infotecnología	Oficial Técnico	Ejecutar y dar seguimiento a la operación diaria de la infraestructura tecnológica y redes. Administrar configuraciones, monitorear el funcionamiento de los servicios, atender incidencias, implementar cambios autorizados y mantener actualizada la documentación técnica correspondiente.
Subdirección de Infotecnología	Auxiliar Técnico	Apoyar en las actividades operativas y de mantenimiento de la infraestructura tecnológica y redes. Registrar incidencias, realizar verificaciones básicas, colaborar en tareas de

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 61 de 183

		soporte técnico y mantener actualizados los registros y bitácoras bajo la supervisión del Oficial Técnico.
--	--	--

6. Insumos del Procedimiento

Código	Insumos	Lugar de Guarda	Tiempo de Guarda
M-PGR-SDIT-XXX-202X	Memorándum	Subdirección de Infotecnología	5 años
N/A	Sistemas de tikect o correo electrónico	Subdirección de Infotecnología	5 años

7. Productos o Resultados del Procedimiento

Código	Productos	Lugar de Guarda	Tiempo de Guarda
F-SDIT-002	Reporte de consumo de ancho de banda	Subdirección de Infotecnología	1 año
N/A	Reporte en sistema de tickets para los incidentes tecnológicos resueltos	Subdirección de Infotecnología	1 año

8. Definición de Glosario de Términos, Siglas y Abreviaturas

8.1. Términos

Acceso: Proceso mediante el cual se autoriza o deniega a personas o sistemas el uso de recursos tecnológicos, información o instalaciones, de acuerdo con políticas y reglas previamente establecidas. (National Institute of Standards and Technology, 2020)

Bitácora: Registro físico o digital en el que se documentan de forma cronológica las actividades, eventos, incidencias, cambios y acciones realizadas sobre la infraestructura tecnológica y las redes. (Standardization, 2015)

Disponibilidad: Propiedad de la información, los sistemas o los servicios de estar accesibles y utilizables cuando un usuario autorizado los requiere. (International Organization for Standardization, 2018)

Gestión de Cambios: Proceso mediante el cual se solicitan, evalúan, autorizan, implementan y documentan las modificaciones realizadas a la infraestructura tecnológica o a la configuración de redes, con el fin de minimizar impactos en la operación. (Office of Government Commerce., 2019)

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UEM 62 de 183

Incidencia: Evento no planificado que interrumpe, reduce la calidad o afecta el funcionamiento normal de un servicio, sistema o componente de la infraestructura tecnológica.

Infraestructura Tecnológica: Conjunto de recursos físicos y lógicos que soportan los servicios informáticos institucionales, incluyendo servidores, equipos de red, sistemas operativos, plataformas y servicios asociados. (International Organization for Standardization, 2018).

Red de Datos: Conjunto de dispositivos interconectados que permiten la transmisión y el intercambio de información entre sistemas informáticos, mediante protocolos y estándares de comunicación establecidos. (Cisco Systems., 2024)

Respaldo (Copia de Seguridad): Copia de la información, software o sistemas, almacenada en un medio seguro, que permite la recuperación de datos ante fallos, pérdidas, incidentes de seguridad o interrupciones del servicio.

Seguridad de la Información: Conjunto de políticas, procedimientos y controles destinados a proteger la confidencialidad, integridad y disponibilidad de la información institucional frente a amenazas internas o externas. (International Organization for Standardization, 2018)

Trazabilidad: Capacidad de identificar, rastrear y reconstruir el historial de cambios, eventos o actividades realizadas sobre un sistema, componente o información, mediante registros y evidencias documentadas. (Standardization, 2015)

Memorándum: Comunicación escrita breve utilizada en el ámbito institucional o empresarial para informar, recordar o instruir sobre asuntos específicos. (Real Academia Española, 2023)

Normativa: Conjunto de normas jurídicas que regulan una materia específica dentro de un ordenamiento legal. (Carbonell, 2019)

Oficio: Documento formal mediante el cual una autoridad comunica decisiones, solicitudes o información a otra autoridad o entidad. (De la Torre, Técnicas de redacción jurídica, 2018)

8.2. Siglas

ISO: International Organization for Standardization

NIST: National Institute of Standards and Technology

PGR: Procuraduría General de la República.

SDIT: Subdirección de Infotecnología.

TIC: Tecnologías de la Información y la Comunicación.

UEM: Unidad de Modernización.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UEM 63 de 183

9. Descripción del Procedimiento

Auxiliar Técnico y Oficial Técnico

- 9.1. Supervisar de forma continua el estado operativo de redes, servidores y sistemas, mediante herramientas de monitoreo, con el fin de detectar fallas, alertas o degradación del servicio. Esta actividad permite conocer en tiempo real el funcionamiento de la infraestructura tecnológica, se realiza utilizando herramientas de monitoreo que generan alertas ante comportamientos anómalos, como resultado se pueden atender fallas antes de que afecten a los usuarios.
- 9.2. Documentar cronológicamente todos los eventos relevantes de la operación tecnológica (incidentes, mantenimientos, caídas, accesos), garantizando trazabilidad y evidencia del proceso, permite llevar un control ordenado de lo ocurrido durante la operación diaria. Esta información sirve como evidencia para auditorías, seguimiento y mejora del servicio.
- 9.3. Identificar fallas o interrupciones en los servicios tecnológicos a través del monitoreo o reportes de usuarios. Las fallas pueden detectarse automáticamente o ser reportadas por los usuarios internos, permite reconocer oportunamente problemas que afectan la operación institucional; su correcta identificación facilita una atención más rápida y efectiva.
- 9.4. Categorizar los incidentes según su nivel de criticidad, impacto y urgencia para priorizar su atención. Los incidentes se clasifican de acuerdo con el nivel de afectación al servicio y a los usuarios, esta priorización permite atender primero los problemas más críticos.
- 9.5. Analizar las causas de los incidentes mediante revisión técnica de equipos, sistemas y configuraciones. Se revisan los componentes tecnológicos involucrados para identificar el origen del problema, este análisis técnico permite comprender qué provocó la falla y ayuda a evitar que el incidente vuelva a presentarse.
- 9.6. Aplicar soluciones técnicas para restablecer la operación normal de los servicios afectados. Se ejecutan acciones correctivas conforme a procedimientos técnicos establecidos, con el propósito de restablecer el servicio en el menor tiempo posible. Una vez aplicada la solución, se verifica que el sistema funcione correctamente.
- 9.7. Remitir los incidentes que no pueden ser resueltos en el primer nivel a instancias técnicas superiores o proveedores especializados. Cuando la solución supera las capacidades del nivel técnico operativo, el incidente se escala formalmente, esta remisión se realiza con la información y evidencias necesarias a los proveedores para garantizar una atención especializada y documentada.
- 9.8. Finalizar formalmente la atención del incidente, verificando la solución e informando al usuario, dejando evidencia en el sistema de ticket. Se confirma que el problema fue resuelto de manera satisfactoria este registro final permite dejar constancia del trabajo realizado y del resultado obtenido.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UEM 64 de 183

- 9.9. Brindar asistencia a usuarios internos en problemas relacionados con equipos, sistemas o conectividad, busca apoyar a los usuarios en el uso correcto de los recursos tecnológicos atendiendo consultas, fallas menores o dificultades operativas.
- 9.10. Realizar acciones programadas para prevenir fallas en la infraestructura tecnológica (revisiones, limpieza, actualizaciones). Su finalidad es reducir la probabilidad de fallas o interrupciones, ayudan a prolongar la vida útil de los equipos y sistemas.
- 9.11. Intervenir equipos o sistemas que presentan fallas para restablecer su funcionamiento. Se realizan revisiones y ajustes técnicos sobre los equipos afectados puede incluir reparaciones, configuraciones o reemplazos, se espera la recuperación del funcionamiento normal.
- 9.12. Reestablecer la conectividad de la red institucional, asegurando su disponibilidad y rendimiento en caso de ser fallas internas. Se analizan y corrigen los problemas que afectan la red interna, garantiza que los usuarios puedan acceder a los sistemas y servicios. La conectividad estable es clave para la operación institucional.
- 9.13. Asignar, modificar o revocar permisos de acceso a los recursos tecnológicos conforme a autorizaciones establecidas. Los accesos se gestionan según solicitudes y autorizaciones formales. Con ello se protege la información y los sistemas institucionales.
- 9.14. Aplicar medidas de protección como antivirus, firewalls, parches de seguridad y control de accesos para proteger la infraestructura. Se implementan controles de seguridad para prevenir amenazas internas y externas, estas medidas reducen riesgos de ataques o pérdida de información contribuyendo a la seguridad institucional.
- 9.15. Realizar copias de seguridad de configuración de los equipos de redes, garantizando la integridad y disponibilidad de los respaldos realizados. Permiten recuperar configuraciones en caso de fallas o incidentes esta actividad es clave para la continuidad del servicio tecnológico.
- 9.16. Registrar y mantener actualizado el control de activos tecnológicos (equipos, servidores, dispositivos de red). Se lleva un inventario actualizado de los recursos tecnológicos institucionales. Este registro facilita la gestión, mantenimiento y control de los activos.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 65 de 183



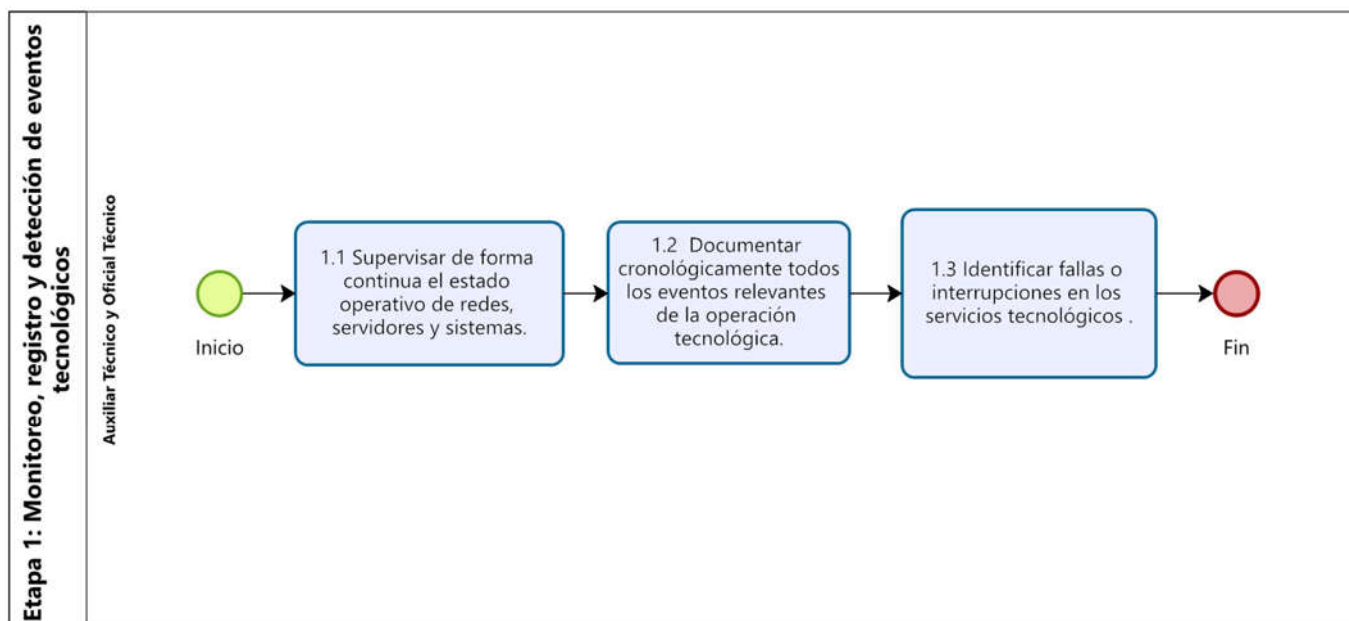
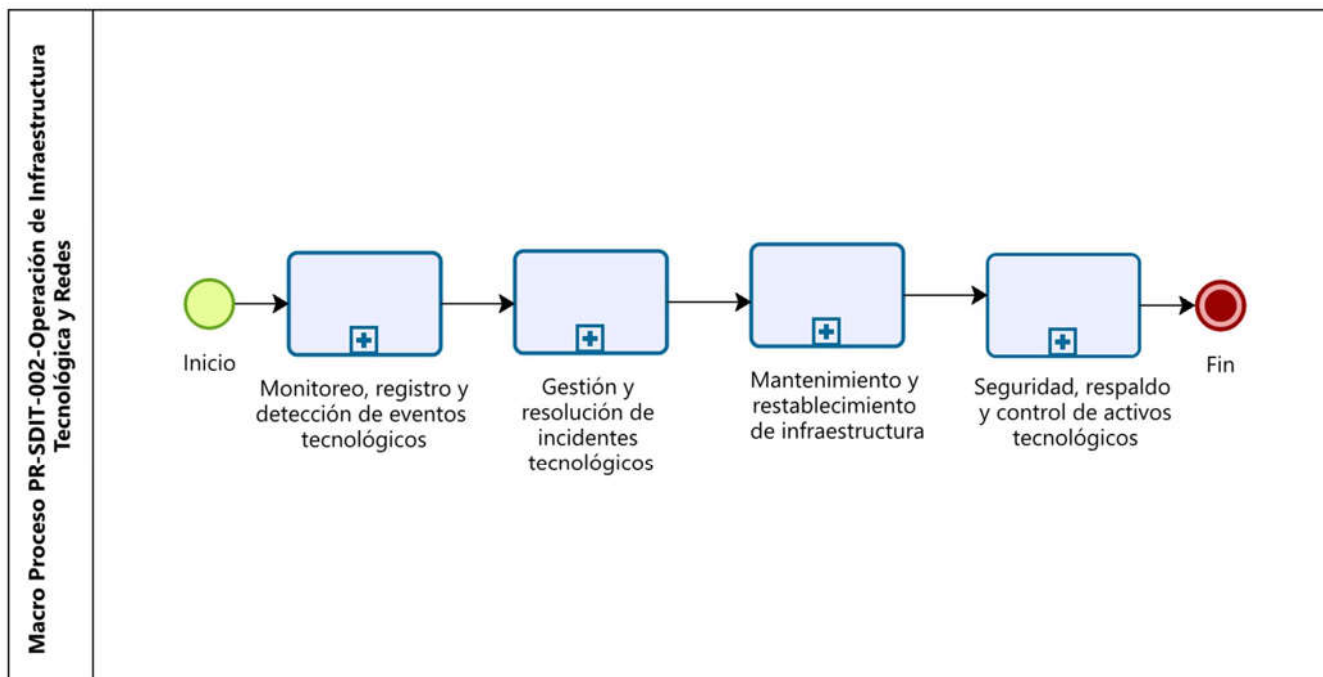
Matriz de Actividades, Responsables y Formularios
Manual de Procedimientos de la Subdirección de Infotecnología
Proceso de Operación de Infraestructura Tecnológica y Redes



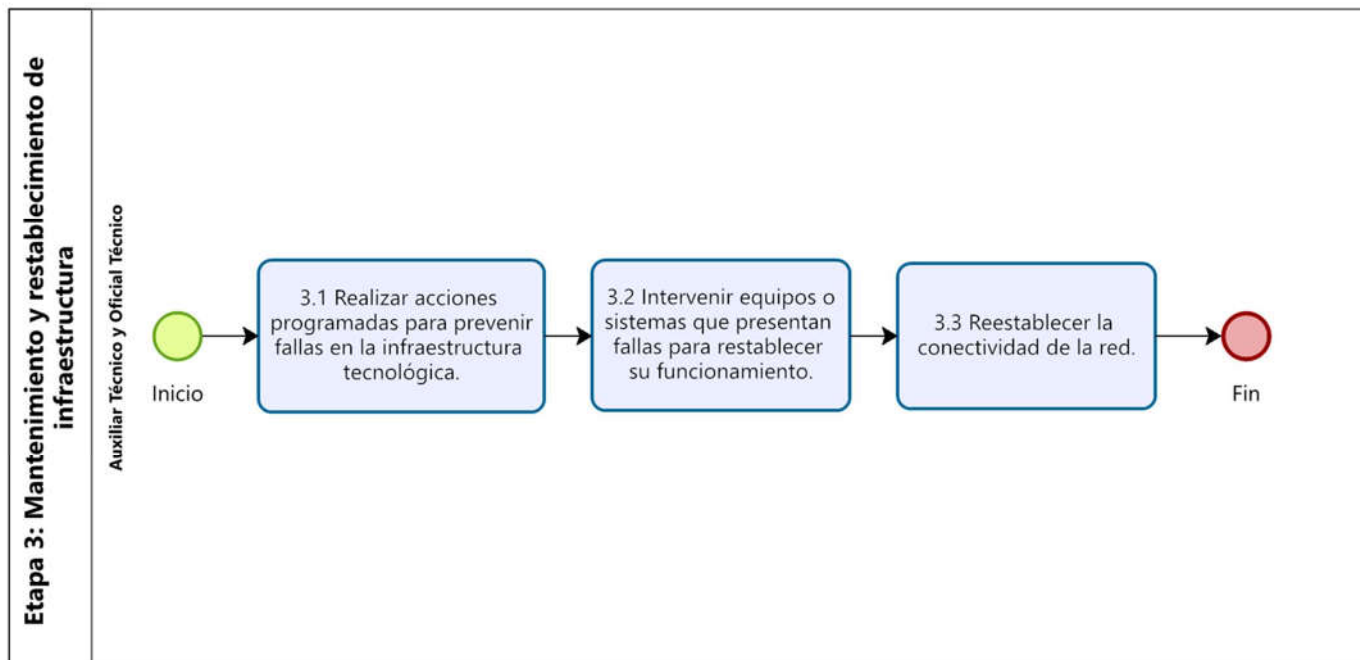
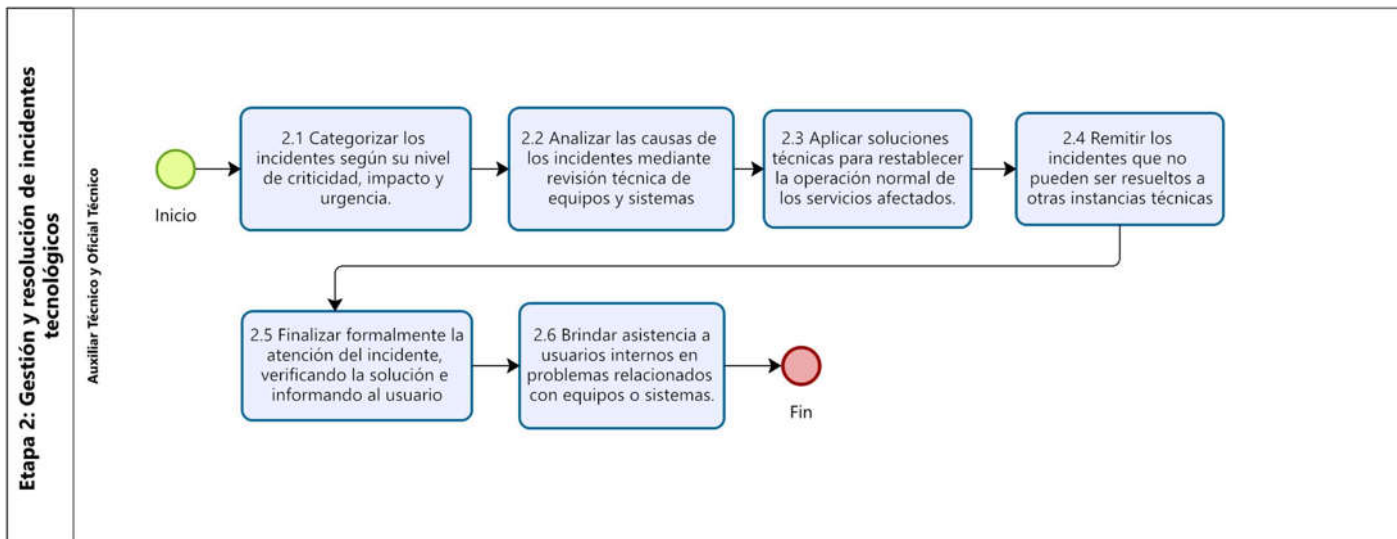
No.	Etapas del Proceso	Objetivo de la Etapa	Insumo	Actividad	Tiempo	Responsable	Producto	Envío a:		
1	Monitoreo, registro y detección de eventos tecnológicos	Supervisar continuamente redes, documentando eventos relevantes e identificando oportunamente fallas, alertas o interrupciones que afecten la operación tecnológica institucional.	Memorándum, sistema de ticket o correo electrónico.	1.1 Supervisar de forma continua el estado operativo de redes, servidores y sistemas, mediante herramientas de monitoreo, con el fin de detectar fallas, alertas o degradación del servicio.	1 día	Auxiliar Técnico y Oficial Técnico	Reporte del control de activos tecnológicos identificados	Auxiliar Técnico y Oficial Técnico		
				1.2 Documentar cronológicamente todos los eventos relevantes de la operación tecnológica (incidentes, mantenimientos, caídas, accesos), garantizando trazabilidad y evidencia del proceso.	3 días		Reporte del control de activos tecnológicos identificados			
				1.3 Identificar fallas o interrupciones en los servicios tecnológicos a través del monitoreo o reportes de usuarios.	1 día		Inventario actualizado			
2	Gestión y resolución de incidentes tecnológicos	Clasificar, analizar, atender, escalar y cerrar formalmente los incidentes tecnológicos, asegurando la recuperación del servicio, la asistencia a usuarios internos y la trazabilidad mediante el sistema de tickets.		2.1 Categorizar los incidentes según su nivel de criticidad, impacto y urgencia para priorizar su atención.	15 min	Auxiliar Técnico y Oficial Técnico	Inventario actualizado		Actas de asignación préstamo de equipo Vale de préstamo y devolución	
				2.2 Analizar las causas de los incidentes mediante revisión técnica de equipos, sistemas y configuraciones.	1 hora					
				2.3 Aplicar soluciones técnicas para restablecer la operación normal de los servicios afectados.	4 horas					
				2.4 Remitir los incidentes que no pueden ser resueltos en el primer nivel a instancias técnicas superiores o proveedores especializados.	3 días					
				2.5 Finalizar formalmente la atención del incidente, verificando la solución e informando al usuario, dejando evidencia en el sistema de ticket.	10 min					
				2.6 Brindar asistencia a usuarios internos en problemas relacionados con equipos, sistemas o conectividad.	1 hora					
3	Mantenimiento y restablecimiento de infraestructura	Ejecutar acciones preventivas y correctivas sobre equipos, sistemas y conectividad institucional, con el fin de prevenir fallas, restablecer servicios y mantener la disponibilidad y rendimiento de la infraestructura tecnológica.		3.1 Realizar acciones programadas para prevenir fallas en la infraestructura tecnológica (revisiones, limpieza, actualizaciones).	Semestral	Auxiliar Técnico y Oficial Técnico	Inventario actualizado			
				3.2 Intervenir equipos o sistemas que presentan fallas para restablecer su funcionamiento.	1 hora					
				3.3 Reestablecer la conectividad de la red institucional, asegurando su disponibilidad y rendimiento en caso de ser fallas internas.	1 hora					
4	Seguridad, respaldo y control de activos tecnológicos	Administrar permisos de acceso, aplicar medidas de protección tecnológica, realizar respaldos de configuraciones y mantener actualizado el inventario de activos tecnológicos para fortalecer la seguridad, integridad y continuidad operativa.		4.1 Asignar, modificar o revocar permisos de acceso a los recursos tecnológicos conforme a autorizaciones establecidas.	15 min	Auxiliar Técnico y Oficial Técnico	Reportes de incidencias			
				4.2 Aplicar medidas de protección como antivirus, firewalls, parches de seguridad y control de accesos para proteger la infraestructura.	1 hora					
				4.3 Realizar copias de seguridad de configuración de los equipos de redes, garantizando la integridad y disponibilidad de los respaldos realizados.	1 hora					
				4.4 Registrar y mantener actualizado el control de activos tecnológicos (equipos, servidores, dispositivos de red).	1 hora		Auxiliar Técnico y Oficial Técnico		Reportes de incidencias	

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 66 de 183

10. Diagrama de Flujo del Procedimiento



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 67 de 183



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 68 de 183

Etapas 4: Seguridad, respaldo y control de activos tecnológicos

Auxiliar Técnico y Oficial Técnico



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 69 de 183

11. Gestión del Riesgo

PGR		PROCURADURÍA GENERAL DE LA REPÚBLICA										NCI-TSC/22-06; NCI-TSC/23-08; NCI-TSC/24-08	
MATRIZ PARA LA EVALUACIÓN, ANÁLISIS Y RESPUESTA A LOS RIESGOS												Formulario 27 PGR	
PROCESO:		Operación de Infraestructura Tecnológica y Redes.											
NOMBRE DEL SUBPROCESO:		Operación de Infraestructura Tecnológica y Redes.											
OBJETIVO:		Garantizar la operación continua, segura, eficiente y disponible de la infraestructura tecnológica y de redes institucional, mediante la administración, monitoreo, mantenimiento y mejora de los recursos tecnológicos, asegurando el soporte a los procesos institucionales y la prestación oportuna de servicios a la ciudadanía.											
(1) No.	(2) Etapa del proceso	(3) Descripción del Riesgo	Riesgo inherente		(4) Zona de Riesgo Preliminar	(7) Controles obligatorios para mitigar los riesgos	(8) Controles que existen en la entidad	(9) Controles pendientes por establecer para mitigar los riesgos	Riesgo Residual		(12) Zona de Riesgo Final	(13) Respuesta a los Riesgos	
			(4) P	(5) I					(10) P	(11) I			
1	Monitoreo, registro y detección de eventos tecnológicos	1.1 No se monitorean oportunamente las redes, lo que puede impactar detectando a tiempo fallas, caídas o disminución en la calidad del servicio.	1	3	M	Implementar herramientas de monitoreo continuo. Definir responsables y límites de revisión. Configurar alertas automáticas por criticidad. Elaborar reportes periódicos de disponibilidad, eventos e incidencias detectadas.	Implementar herramientas de monitoreo continuo. Definir responsables y límites de revisión. Configurar alertas automáticas por criticidad. Elaborar reportes periódicos de disponibilidad, eventos e incidencias detectadas.		1	2	6	Aceptar	
2	Gestión y resolución de incidentes tecnológicos	2.1 Los incidentes pueden cesarse antes de ser resueltos o no escalarse oportunamente cuando el proveedor no pueda solucionarlos en el primer nivel de atención.	1	4	A	Definir procedimiento de atención y escalamiento al proveedor y documentar diagnósticos, solución aplicada y responsable.	Definir procedimiento de atención y escalamiento al proveedor y documentar diagnósticos, solución aplicada y responsable.		1	3	M	Mitigar	
3	Mantenimiento y restablecimiento de infraestructura	3.1 La falta de mantenimiento preventivo puede provocar fallas recurrentes, interrupciones del servicio o deterioro de los equipos tecnológicos.	1	2	U	Elaborar plan anual o mensual de mantenimiento preventivo. Programar revisiones, limpieza, actualizaciones y verificación de equipos.	Elaborar plan anual o mensual de mantenimiento preventivo. Programar revisiones, limpieza, actualizaciones y verificación de equipos.		1	1	3	Aceptar	
		3.2 Los equipos, sistemas o servicios de conectividad pueden restablecerse de forma tardía o inadecuada por parte del proveedor, afectando la continuidad operativa institucional.	1	4	A	Documentar causa raíz, acciones correctivas y validación del servicio restablecido.	Documentar causa raíz, acciones correctivas y validación del servicio restablecido.		1	3	M	Mitigar	
4	Seguridad, resiliencia y control de activos tecnológicos	4.1 Los permisos de acceso pueden mantenerse activos después del período autorizado, debido a que el usuario no notifica oportunamente su finalización, generando riesgo de acceso no autorizado o uso indebido de recursos tecnológicos.	2	2	B	Requerir autorización formal para altas, bajas y modificaciones de usuarios. Aplicar perfiles de acceso por rol. Revisar periódicamente usuarios activos y privilegios. Revocar accesos de personal trasladado o desvinculado.	Requerir autorización formal para altas, bajas y modificaciones de usuarios. Aplicar perfiles de acceso por rol. Revisar periódicamente usuarios activos y privilegios. Revocar accesos de personal trasladado o desvinculado.		1	1	5	Aceptar	
		4.2 El inventario tecnológico puede estar desactualizado, dificultando el control, mantenimiento, ubicación, custodia y reposición de los activos tecnológicos.	1	2	B	Mantener inventario actualizado de equipos, servidores y dispositivos de red. Registrar responsable, ubicación, estado, número de serie y fecha de mantenimiento. Realizar verificaciones físicas periódicas. Conciliar inventario técnico con registros administrativos.	Mantener inventario actualizado de equipos, servidores y dispositivos de red. Registrar responsable, ubicación, estado, número de serie y fecha de mantenimiento. Realizar verificaciones físicas periódicas. Conciliar inventario técnico con registros administrativos.		1	1	6	Aceptar	
Elaborado por:			Revisado por:			Aprobado por:							
Anaelito Alados García-Rivera Oficial Técnico			Ingrid Karina López Fuentes Directora de Administración y Finanzas			Subdirector de Gestión de Recursos Tecnológicos							
Fecha: 19 de mayo de 2026			Fecha: 20 de mayo de 2026			Fecha: 20 de mayo de 2026							

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 70 de 183

	PROCURADURÍA GENERAL DE LA REPÚBLICA MAPA PARA LA VALORACIÓN PRELIMINAR Y FINAL DE LOS RIESGOS		NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00 Formulario 28 PGR		
PROPÓSITO:	Facilitar la valoración y determinación de la zona de riesgos, de acuerdo con la explicación que consta en el Anexo 22 Instructivo para la gestión de riesgos				
PROBABILIDAD					
Muy Alta (5)	A	A	E	E	E
Alta (4)	M	A	A	E	E
Moderada (3)	B	M	A	E	E
Baja (2)	B	4.1 B	M	A	E
Muy Baja (1)	B	3.1 B 4.2	1.1 M	2.1 A 3.2	A
	Muy Bajo (1)	Bajo (2)	Moderado (3)	Alto (4)	Muy Alto(5)
	IMPACTOS				
ZONA DE RIESGO:					
B:	Zona de Riesgo Baja: Respuesta, Aceptar el riesgo				
M:	Zona de Riesgo Moderada: Respuestas, Aceptar el riesgo o reducir el riesgo. Costo Beneficio				
A:	Zona de Riesgos Alta: Respuestas, Reducir el riesgo, o evitar, o compartir, o transferir				
E:	Zona de Riesgo Extrema: Respuestas, Reducir el riesgo (costo beneficio), o evitar, o compartir o transferir				

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UEM 71 de 183

12. Elementos Transversales del Procedimiento



Matriz de Verificación

Inclusión de Elementos Transversales Estratégicos

Manual de Procedimientos de la Subdirección de Infotecnología



Denominación del Proceso: Operación de Infraestructura Tecnológica y Redes			
Preguntas de Verificación	Si	No	Respuestas de Verificación
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Control Interno y anticorrupción</u> ?	X		El proceso contempla controles sobre inventario tecnológico, accesos administrativos, monitoreo de redes, bitácoras de incidencias, respaldos, autorizaciones para cambios y mantenimiento preventivo/correctivo. Estas medidas reducen riesgos de uso indebido de equipos, accesos no autorizados, pérdida de información y alteraciones sin trazabilidad.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Descentralización</u> ?		X	No se identifican actividades descentralizadas hacia regionales u otras dependencias. La operación de infraestructura tecnológica y redes se concentra en la Subdirección de Infotecnología.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Participación Ciudadana</u> ?		X	No se contempla consulta directa a la ciudadanía, ya que el proceso es principalmente interno y técnico.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Transparencia y Acceso a la Información Pública</u> ?	X		El proceso contribuye a mantener disponibles los sistemas, redes y servicios tecnológicos que soportan la publicación de información institucional y la atención de solicitudes de información pública. También debe incluir controles para proteger datos reservados, confidenciales o sensibles alojados en la infraestructura tecnológica.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Archivo Documental</u> ?	X		Se deben conservar reportes físicos o digitales sobre inventarios, configuraciones, mantenimientos, incidencias, respaldos, cambios de red, garantías, licencias, informes técnicos y actas de recepción de servicios o equipos como buenas prácticas.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al cumplimiento de los indicadores de <u>PEI Institucional</u> ?	X		El proceso se vincula con indicadores de modernización, continuidad operativa, disponibilidad de servicios tecnológicos, seguridad de la información, atención de incidencias y fortalecimiento institucional. Su seguimiento debe asociarse a metas del PEI, POA, planes tecnológicos y reportes de desempeño de la infraestructura.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 72 de 183

13. Bibliografía

- Carbonell, M. (2019). *Teoría del derecho*. Porrúa.
- Cisco Systems. (2024). *Networking Fundamentals*. . Cisco Press.
- De la Torre, J. (2018). *Técnicas de redacción jurídica*. Jurídica Universitaria.
- International Organization for Standardization. (2018). *ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary*. ISO.
- INational Institute of Standards and Technology. (2020). *Glossary of Key Information Security Terms*. Obtenido de https://csrc.nist.gov/glossary/term/access_control
- Office of Government Commerce. (2019). *IT Service Management Practices*. . AXELOS.
- *Real Academia Española*. (2023). Obtenido de Diccionario de la lengua española (23.^a ed.): <https://dle.rae.es>
- Standardization, I. O. (2015). *ISO 9000: Quality management systems — Fundamentals and vocabulary*. . ISO.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 73 de 183

14. Anexos

14.1. M-PGR-SDIT-XXX-202X

MEMORÁNDUM PGR-SDIT-LI-00X-202X

Tegucigalpa M.D.C. XX de enero de 202X

PARA: Nombre

Cargo

C.c.: Nombre

Cargo

DE: Nombre

Cargo

ASUNTO:

Cc: Archivo

Residencial El Trapiche, Edificio PGR, Tegucigalpa, M.D.C.

Tel.: 2235-2022 / 2235-2025 / 2235-2049 / 2235-2050

www.pgr.gob.hn

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UEM 74 de 183

14.2. Sistema de ticket o correo electrónico



SISTEMA TICKETS

Ingrese la información para atender su solicitud

Empezar ahora

SISTEMA TICKETS

Cuando envíe este formulario, no recopilará automáticamente sus detalles, como el nombre y la dirección de correo electrónico, a menos que lo proporcione usted mismo.

* Obligatorio

1. Nombre *

Escriba su respuesta

2. Correo Institucional *

Escriba una dirección de correo electrónico

3. Dependencia *

Selecciona la respuesta

4. Detalle *

Escriba su respuesta

Enviar

No revele nunca su contraseña. [Notificar abuso](#)

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 75 de 183

14.3. F-SDIT-002 Reporte de consumo de ancho de banda

 PROCURADURÍA GENERAL DE LA REPÚBLICA F-SDIT-002 V 1.0 Fecha:20 de mayo de 2026 SUBDIRECCIÓN DE INFOTECNOLOGÍA REPORTE DE CONSUMO DE ANCHO DE BANDA							
REPORTE TRIMESTRAL							
MES DE XXX 2026							
	Proveedor del servicio	Tipo de enlace	Ancho de banda contratado	Consumo promedio	Incidencias identificadas	Recomendaciones/acciones	Observaciones
	<i>Empresa que proporciona el enlace</i>	<i>Internet, enlace dedicado, datos, etc.</i>	<i>Capacidad contratada, expresada en Mbps o Gbps</i>	<i>Utilización promedio registrada durante el periodo</i>	<i>Porcentaje de disponibilidad durante el periodo, si se dispone del dato</i>	<i>Recomendaciones de las acciones que se deben tomar</i>	<i>Explicación de comportamientos atípicos o aspectos relevantes</i>
TRIMESTRE							
TRIMESTRE							
TRIMESTRE							
TRIMESTRE							

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-002 Versión 1.0	Operación de Infraestructura Tecnológica y Redes Fecha: 20 de mayo 2026	UDEM 76 de 183

15. Control de Cambios al Procedimiento

Historial de Cambios al Procedimiento

Fecha	Versión	Autor		Descripción del cambio	Cambio Autorizado por:	
		Cargo	Área		Cargo	Firma

PROCURADURÍA GENERAL DE LA REPÚBLICA

SUBDIRECCIÓN DE INFOTECNOLOGÍA

PROCEDIMIENTO SOPORTE TÉCNICO A USUARIOS

**CÓDIGO
PR-SDIT-003**

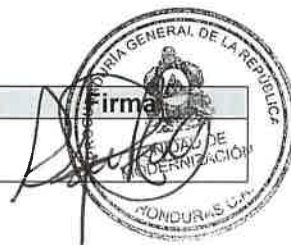
22 DE MAYO DE 2026

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 78 de 183

Responsables de los Cambios al Procedimiento

Elaboración del Documento

Elaborado por:	Cargo	Área de Trabajo	Fecha	Firma
Suyapa del Mar Andino Ordoñez	Jefa de Unidad	Unidad de Modernización	22 de mayo de 2026	



Revisión del Documento

Revisado por:	Cargo	Área de Trabajo	Fecha	Firma
Abel Fernando Perez Vargas	Auxiliar Técnico	Subdirección de Infotecnología	25 de mayo de 2026	
Daniel Isaac Membreño Anariba	Auxiliar Técnico	Subdirección de Infotecnología	25 de mayo de 2026	

Verificación del Documento

Verificado por:	Cargo	Área de Trabajo	Fecha	Firma
Jorge Efrain Salgado	Subdirector de Infotecnología	Subdirección de Infotecnología	26 de mayo de 2026	
Ingrid Karina López Fuentes	Directora	Dirección de Administración y Finanzas	26 de mayo de 2026	



Aprobación del Documento

Aprobado por:	Cargo	Área de Trabajo	Fecha	Firma
José Francisco Quiroz Mejía	Sub-Procurador General de la República	Despacho de la Sub-Procuraduría General de la República	28 de mayo de 2026	



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UEM 79 de 183

Tabla de Contenido

1.	Objetivo del Procedimiento	80
2.	Alcance del Procedimiento	80
3.	Marco Legal del Procedimiento	80
4.	Políticas y Lineamientos del Procedimiento	80
5.	Responsables del Procedimiento	81
6.	Insumos del Procedimiento	82
7.	Productos o Resultados del Procedimiento	82
8.	Definición de Glosario de Términos, Siglas y Abreviaturas	82
9.	Descripción del Procedimiento	84
10.	Diagrama de Flujo del Procedimiento	86
11.	Gestión del Riesgo	88
12.	Elementos Transversales del Procedimiento	90
13.	Bibliografía	91
14.	Anexos	92
15.	Control de Cambios al Procedimiento	98

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003	Soporte Técnico a Usuarios	UDEM
Versión 1.0	Fecha: 22 de mayo 2026	80 de 183

1. Objetivo del Procedimiento

Brindar ayuda a los usuarios para resolver problemas con equipos, sistemas o servicios tecnológicos, de forma rápida y eficiente, para que puedan realizar su trabajo sin interrupciones.

2. Alcance del Procedimiento

Este proceso inicia cuando un usuario reporta un problema o solicita ayuda relacionada con equipos, sistemas o servicios tecnológicos, y finaliza cuando el problema ha sido resuelto, la solicitud ha sido atendida satisfactoriamente o con un dictamen técnico.

3. Marco Legal del Procedimiento

No.	Código	Documento
1	Decreto 131-82	Constitución de la República
2	Decreto 74-61	Ley Orgánica de la Procuraduría General de la República
3	Decreto 146-86	Ley General de la Administración Pública
4	N/A	Reglamento Interno de Trabajo PGR
5	N/A	Modelo OSI
6	ISO/IEC 27000	Seguridad de la información

4. Políticas y Lineamientos del Procedimiento

4.1. Alcance del soporte

El servicio de soporte técnico se brindará exclusivamente a los usuarios internos de la institución, en relación con los equipos, sistemas, aplicaciones y servicios tecnológicos oficialmente autorizados.

4.2. Canales oficiales de solicitud

- Toda solicitud de soporte técnico deberá ser registrada a través de los canales oficiales definidos por la Subdirección de Infotecnología por el sistema de tickets.
- No se atenderán solicitudes verbales o informales que no cuenten con registro oficial, salvo autorización expresa de la Subdirección de Infotecnología.

4.3. Registro y trazabilidad

- Cada solicitud de soporte técnico deberá quedar debidamente registrada, asignándose un número de ticket que permita su seguimiento, control y cierre.
- El registro deberá contener, como mínimo, los datos del usuario solicitante, descripción del incidente o requerimiento, fecha y hora de recepción.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 81 de 183

4.4. Priorización de solicitudes

- Las solicitudes de soporte técnico serán atendidas conforme al orden de llegada.
- Las incidencias que afecten servicios críticos institucionales tendrán prioridad sobre las solicitudes de carácter operativo o individual.

4.5. Asignación del soporte

- Las solicitudes serán asignadas al personal técnico correspondiente, de acuerdo con su especialidad, carga de trabajo y disponibilidad.
- El técnico asignado será responsable de la atención, seguimiento y cierre del ticket.

4.6. Tiempos de atención

- Los tiempos de respuesta y solución estarán sujetos a la complejidad del incidente y disponibilidad de recursos.
- La Subdirección de Infotecnología informará al usuario sobre el estado de su solicitud cuando sea requerido.

4.7. Responsabilidad del usuario

- El usuario deberá proporcionar información clara, veraz y completa sobre la falla o requerimiento presentado.
- El usuario será responsable del uso adecuado de los recursos tecnológicos asignados y de cumplir las normas y políticas institucionales de tecnología.

4.8. Cierre del servicio

Una vez solucionada la solicitud, el técnico deberá registrar las acciones realizadas y proceder al cierre del ticket.

5. Responsables del Procedimiento

Área	Puesto de Trabajo	Responsabilidad
Subdirección de Infotecnología	Subdirector(a)	Dirigir y supervisar el servicio de soporte técnico, aprobar lineamientos y asegurar que los recursos necesarios estén disponibles para una atención oportuna y eficiente.
Subdirección de Infotecnología	Auxiliar Técnico	Atender, diagnosticar y solucionar las solicitudes de soporte técnico de los usuarios, registrando las acciones realizadas y escalando los casos que lo requieran.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 82 de 183

Subdirección de Infotecnología	Asistente Administrativo	Recibir y registrar las solicitudes de soporte técnico, asignar los tickets correspondientes y dar seguimiento administrativo hasta su cierre.
--------------------------------	--------------------------	--

6. Insumos del Procedimiento

Código	Insumos	Lugar de Guarda	Tiempo de Guarda
M- PGR-SDIT-XXX-202X	Memorándum	Subdirección de Infotecnología	5 años
N/A	Sistema de ticket o correo electrónico	Subdirección de Infotecnología	5 años

7. Productos o Resultados del Procedimiento

Código	Productos	Lugar de Guarda	Tiempo de Guarda
N/A	Reportes de incidencias atendidas por medio de tickets	Subdirección de Infotecnología	5 años
F-SDIT-004	Dictamen Técnico de Equipos Tecnológicos	Subdirección de Infotecnología	5 años
F-SDIT-005	Reporte de mantenimiento semestral	Subdirección de Infotecnología	5 años
F-SDIT-006	Reportes periódicos de soporte trimestral	Subdirección de Infotecnología	5 años

8. Definición de Glosario de Términos, Siglas y Abreviaturas

8.1. Términos

Atención Remota: Modalidad de soporte técnico que permite al personal de Infotecnología brindar asistencia a los usuarios sin desplazarse físicamente, mediante herramientas de acceso remoto y comunicación digital. (Wikipedia, 2025)

Bitácora de Soporte Técnico: Registro donde se documentan las solicitudes atendidas, acciones realizadas, fechas, responsables y resultados del servicio de soporte técnico, con fines de control y seguimiento. (HubSpot., 2024)

Confidencialidad de la Información: Principio de seguridad que garantiza que la información solo sea accesible a personas autorizadas, evitando su divulgación no autorizada durante la atención del soporte técnico. (ISO, 2022)

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UEM 83 de 183

Escalamiento de Incidencias: Proceso mediante el cual una incidencia o solicitud técnica es transferida a un nivel superior de soporte cuando no puede ser resuelta en el nivel inicial de atención. (AXELOS, 2019).

Help Desk (Mesa de Ayuda): Servicio centralizado que actúa como punto único de contacto entre los usuarios y el área de Infotecnología para la recepción, registro y seguimiento de solicitudes de soporte técnico.

Incidente Informático: Evento no planificado que interrumpe o reduce la calidad de un servicio tecnológico, afectando los sistemas, equipos o información institucional. (ISO, 2022).

Memorándum: Comunicación escrita breve utilizada en el ámbito institucional o empresarial para informar, recordar o instruir sobre asuntos específicos. (Real Academia Española, 2023)

Normativa: Conjunto de normas jurídicas que regulan una materia específica dentro de un ordenamiento legal. (Carbonell, 2019)

Nivel de Soporte: Clasificación del soporte técnico según la complejidad del incidente, que determina si la atención se realiza en primer nivel o requiere escalamiento.

Oficio: Documento formal mediante el cual una autoridad comunica decisiones, solicitudes o información a otra autoridad o entidad. (De la Torre, Técnicas de redacción jurídica, 2018)

Soporte Técnico: Conjunto de actividades orientadas a asistir a los usuarios en la solución de problemas relacionados con equipos, sistemas y servicios tecnológicos institucionales. (Definición.de. , 2024).

Ticket de Soporte Técnico: Registro electrónico que documenta una solicitud o incidencia de soporte técnico, permitiendo su control, seguimiento y cierre. (Zendesk, 2024)

8.2. Siglas

ISO: International Organization for Standardization

NIST: National Institute of Standards and Technology

PGR: Procuraduría General de la República.

SDIT: Subdirección de Infotecnología.

TIC: Tecnologías de la Información y la Comunicación.

UEM: Unidad de Modernización.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 84 de 183

9. Descripción del Procedimiento

Auxiliar Técnico

- 9.1. Recibir la solicitud o incidencia del usuario por orden de llegada (vía memorándum, sistema de tickets y correo electrónico), a través de los medios oficiales establecidos por la Subdirección de Infotecnología, respetando el orden en que ingresan.
- 9.2. Registrar la solicitud en el sistema de tickets, se ingresa la información de la solicitud en el sistema, asignándole un número de ticket para su control y seguimiento.
- 9.3. Clasificar la incidencia según tipo, prioridad y nivel de impacto, se analiza la solicitud para determinar el tipo de problema, su urgencia y el impacto que tiene en las labores del usuario o de la institución.

Asistente Administrativo

- 9.4. Asignar el caso al personal técnico correspondiente, que cuenta con el conocimiento y disponibilidad para atender el problema.

Auxiliar Técnico

- 9.5. Diagnosticar la causa del problema reportado. El personal técnico revisa el equipo, sistema o servicio para identificar el origen de la falla reportada por el usuario.
- 9.6. Determinar la solución técnica adecuada, se define la acción técnica más conveniente para resolver el problema detectado, considerando las normas institucionales.
- 9.7. Ejecutar la solución o intervención técnica (remota o presencial). Se aplica la solución aprobada, ya sea de forma remota o en el lugar donde se encuentra el equipo del usuario.
- 9.8. Escalar el caso a un nivel superior o proveedor externo, cuando no pueda resolverse en primera instancia. Si el problema no puede resolverse, se traslada el caso a un nivel técnico superior o a un proveedor autorizado.
- 9.9. Verificar el funcionamiento correcto del equipo, sistema o servicio intervenido. Se comprueba que el equipo o sistema funcione correctamente después de aplicar la solución.
- 9.10. Confirmar con el usuario la solución del problema. Se consulta al usuario para confirmar que la solución aplicada resolvió satisfactoriamente la incidencia.
- 9.11. Registrar las acciones realizadas y la solución aplicada en el sistema de tickets. Se documentan en el sistema todas las acciones realizadas y la solución final aplicada al caso.
- 9.12. Cerrar la solicitud o ticket de soporte técnico. Una vez confirmada la solución, se procede al cierre formal del ticket en el sistema.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 85 de 183

- 9.13.** Generar los Dictámenes Técnicos cuando corresponda. Se elaboran dictámenes técnicos cuando la incidencia lo requiera, dejando constancia formal de la intervención realizada.
- 9.14.** Analizar las incidencias recurrentes para proponer mejoras preventivas. Se revisan las fallas repetitivas para identificar causas y proponer acciones que eviten su recurrencia.



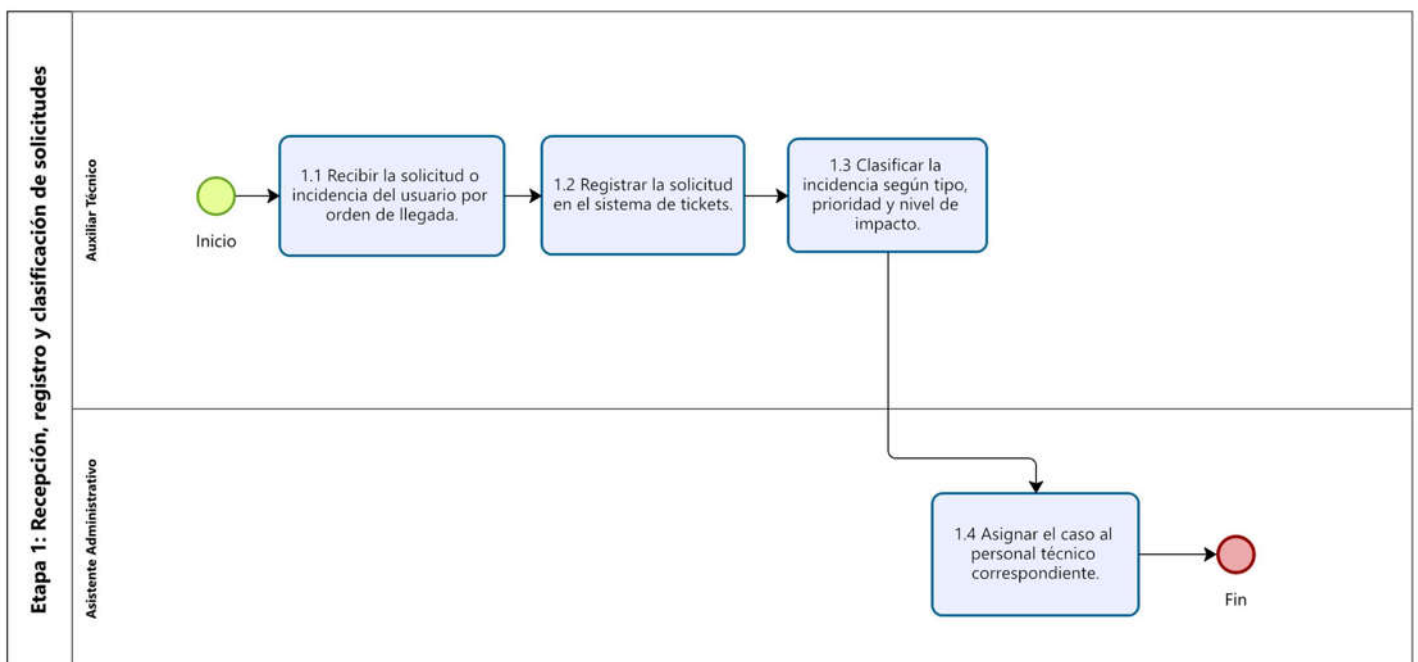
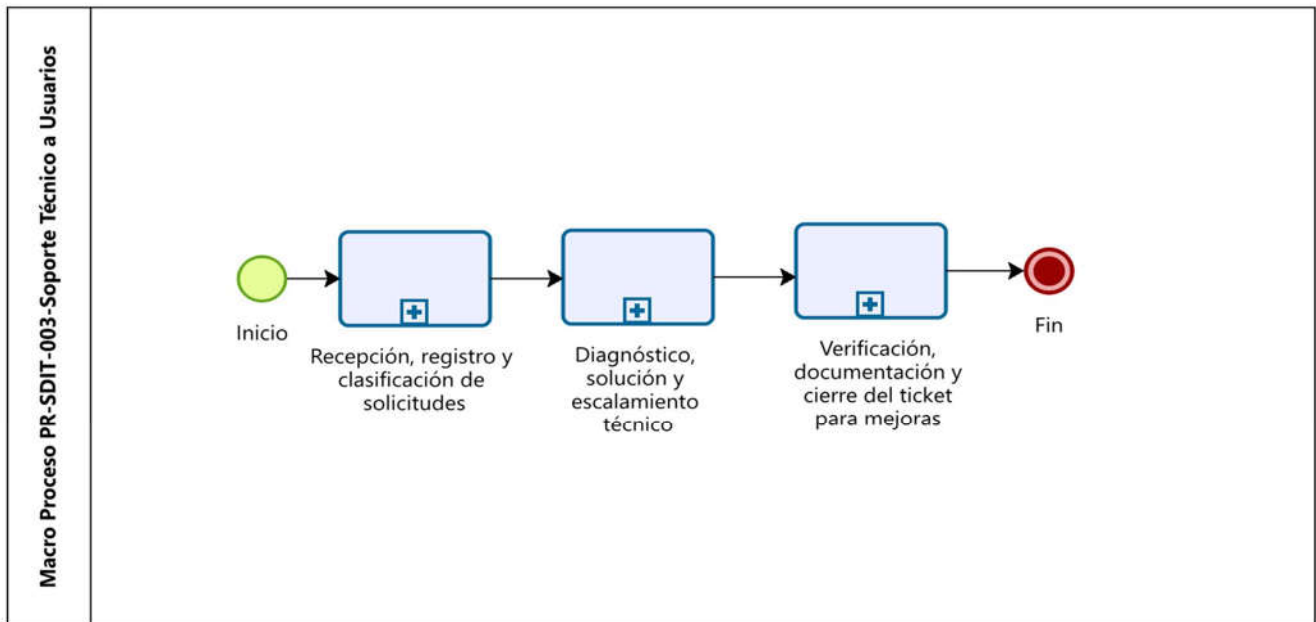
Matriz de Actividades, Responsables y Formularios
Manual de Procedimientos de la Subdirección de Infotecnología
Proceso de Soporte Técnico a Usuarios



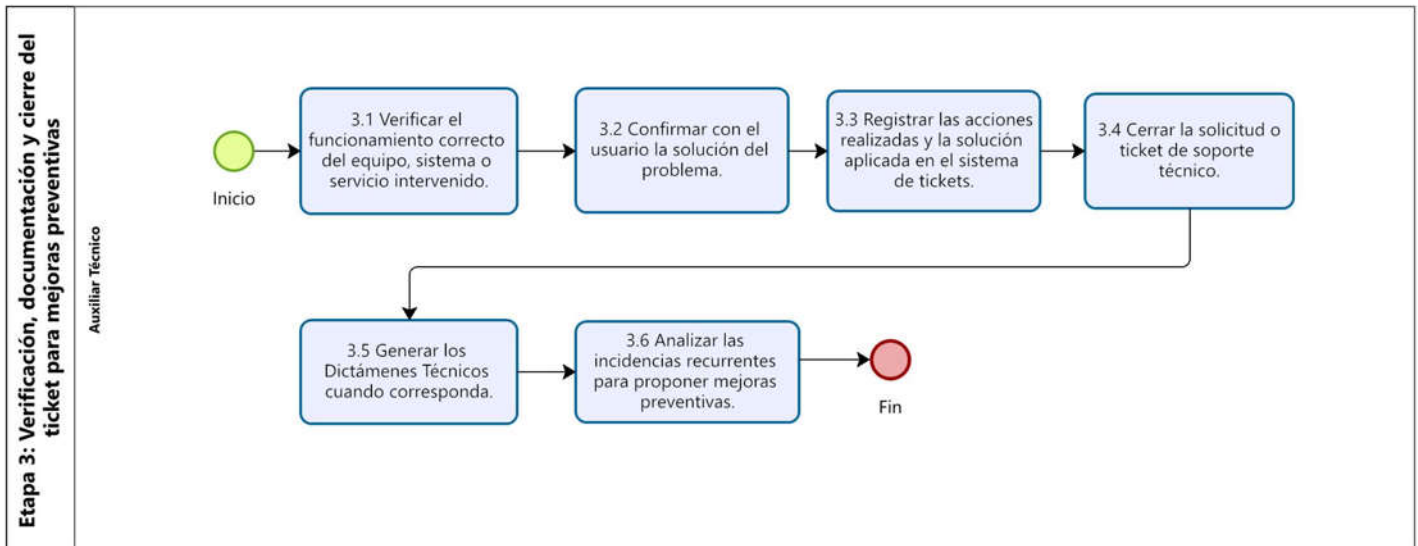
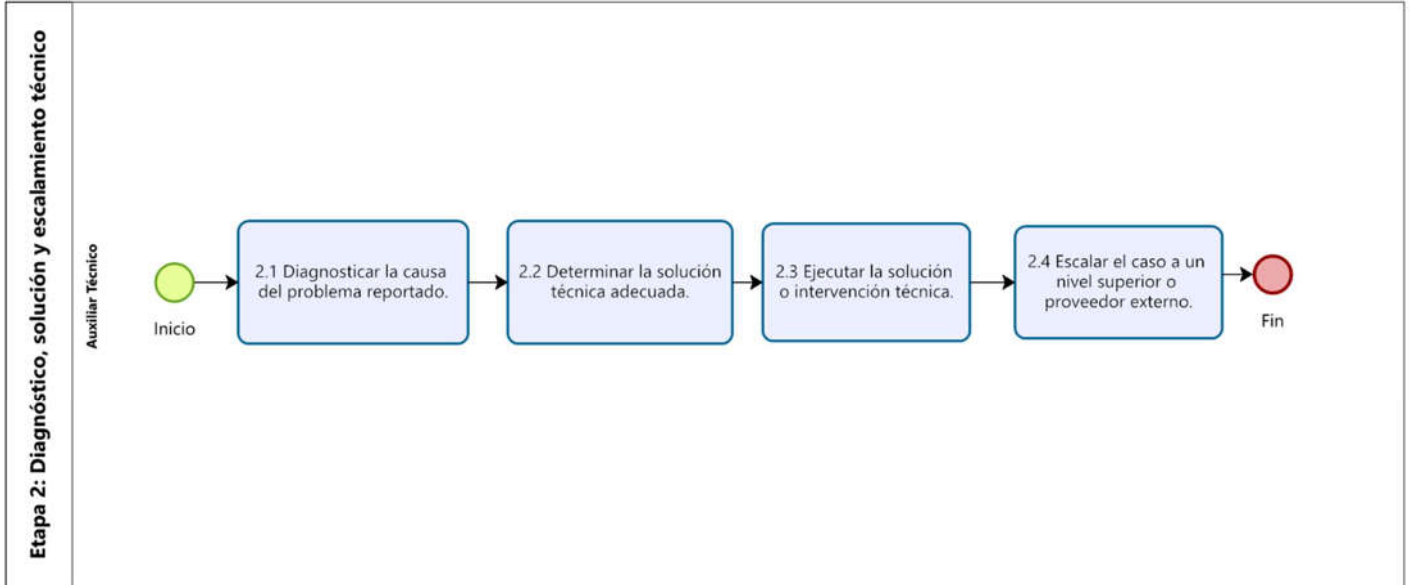
No.	Etapas del Proceso	Objetivo de la Etapa	Insumo	Actividad	Tiempo	Responsable	Producto	Envío a:			
1	Recepción, registro y clasificación de solicitudes	Recibir, registrar, clasificar y asignar las solicitudes o incidencias de soporte técnico, asegurando orden de atención, trazabilidad y asignación al personal competente.	Memorándum, sistema de ticket o correo electrónico, herramientas de precisión, aspiradoras, aire comprimido, estación de calor, pasta térmica, taladros, herramientas para red y hacer diagnósticos, entre otros.	1.1 Recibir la solicitud o incidencia del usuario por orden de llegada (vía memorándum, sistema de tickets y correo electrónico).	10 min	Auxiliar Técnico	Reportes de incidencias atendidas por medio de tickets	Auxiliar Técnico			
				1.2 Registrar la solicitud en el sistema de tickets.	5 min						
				1.3 Clasificar la incidencia según tipo, prioridad y nivel de impacto.	10 min	Auxiliar Técnico	Asistente Administrativo				
				1.4 Asignar el caso al personal técnico correspondiente.	10 min	Asistente Administrativo					
2	Diagnóstico, solución y escalamiento técnico	Identificar la causa del problema, determinar y ejecutar la solución técnica correspondiente, o escalar el caso cuando no pueda resolverse en primera instancia.		2.1 Diagnosticar la causa del problema reportado.	30 min	Auxiliar Técnico	Reportes de incidencias atendidas por medio de tickets Reportes periódicos de soporte trimestral	Auxiliar Técnico			
				2.2 Determinar la solución técnica adecuada.	1 día						
				2.3 Ejecutar la solución o intervención técnica (remota o presencial).	1 día						
				2.4 Escalar el caso a un nivel superior o proveedor externo, cuando no pueda resolverse en primera instancia.	1 día						
3	Verificación, documentación y cierre del ticket para mejoras preventivas	Verificar el funcionamiento del equipo, sistema o servicio intervenido, confirmar la solución con el usuario, registrar las acciones realizadas, cerrar el ticket y emitir dictamen técnico cuando corresponda.		3.1 Verificar el funcionamiento correcto del equipo, sistema o servicio intervenido.	30 min				Auxiliar Técnico	Dictamen Técnico de Equipos Tecnológicos	Asistente Administrativo
				3.2 Confirmar con el usuario la solución del problema.	5 min						
				3.3 Registrar las acciones realizadas y la solución aplicada en el sistema de tickets.	10 min						
				3.4 Cerrar la solicitud o ticket de soporte técnico.	5 min						
			3.5 Generar los Dictámenes Técnicos cuando corresponda.	1 hora	Auxiliar Técnico						
			3.6 Analizar las incidencias recurrentes para proponer mejoras preventivas.	20 min							

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 86 de 183

10. Diagrama de Flujo del Procedimiento

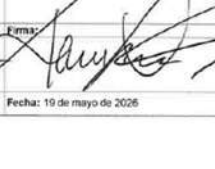


	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 87 de 183



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 88 de 183

11. Gestión del Riesgo

PGR		PROCURADURÍA GENERAL DE LA REPÚBLICA										NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00	
		MATRIZ PARA LA EVALUACIÓN, ANÁLISIS Y RESPUESTA A LOS RIESGOS										Formulario 27 PGR	
PROCESO:		Soporte Técnico a Usuarios											
NOMBRE DEL SUBPROCESO:		Soporte Técnico a Usuarios											
OBJETIVO:		Brindar ayuda a los usuarios para resolver problemas con equipos, sistemas o servicios tecnológicos, de forma rápida y eficiente, para que puedan realizar su trabajo sin interrupciones.											
(1) No.	(2) Etapa del proceso	(3) Descripción del Riesgo	Riesgo Inherente		(6) Zona de Riesgo Preliminar	(7) Controles obligatorios para mitigar los riesgos	(8) Controles que existen en la entidad	(9) Controles pendientes por establecer para mitigar los riesgos	Riesgo Residual		(12) Zona de Riesgo Final	(13) Respuesta a los Riesgos	
			(4) P	(5) I					(10) P	(11) I			
1	Recepción, registro y clasificación de solicitudes	1.1 La incidencia puede clasificarse incorrectamente según su tipo, prioridad o nivel de impacto, afectando su atención oportuna.	1	3	M	Establecer criterios de clasificación por tipo, prioridad e impacto.	Establecer criterios de clasificación por tipo, prioridad e impacto.		1	2	II	Aceptar	
2	Diagnóstico, solución y escalamiento técnico	2.1 No contar con las herramientas técnicas o insumos para solucionar el problema.	2	3	M	Registrar causa identificada y pruebas realizadas. Validar casos complejos con personal técnico superior antes de ejecutar cambios.	Registrar causa identificada y pruebas realizadas. Validar casos complejos con personal técnico superior antes de ejecutar cambios.		1	2	II	Aceptar	
3	Verificación, documentación y cierre del ticket	3.1 La falta de análisis de incidencias recurrentes puede impedir identificar causas comunes, prevenir fallas futuras y mejorar la calidad del soporte técnico.	1	3	M	Generar reportes periódicos de incidencias por tipo, usuario, dependencia y causa. Proponer acciones preventivas.	Generar reportes periódicos de incidencias por tipo, usuario, dependencia y causa. Proponer acciones preventivas.		1	2	II	Aceptar	
Revisado por: Abel Fernando Pérez Vargas Auxiliar Técnico Daniel Isaac Membreño Anariba Auxiliar Técnico Suyapa del Mar Andino Ordóñez Jefa de la Unidad de Modernización						Aprobado por: Ingrid Karina López Fuentes Directora de Administración y Finanzas Jorge Elías... Subdirector de... José Francisco Quintanilla Subprocurador General de la República							
Firma:  Fecha: 18 de mayo de 2026						Firma:  Fecha: 19 de mayo de 2026							

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 89 de 183

	PROCURADURÍA GENERAL DE LA REPÚBLICA		NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00 Formulario 28 PGR		
	MAPA PARA LA VALORACIÓN PRELIMINAR Y FINAL DE LOS RIESGOS				
PROPÓSITO: Facilitar la valoración y determinación de la zona de riesgos, de acuerdo con la explicación que consta en el Anexo 22 Instructivo para la gestión de riesgos					
PROBABILIDAD					
Muy Alta (5)	A	A	E	E	E
Alta (4)	M	A	A	E	E
Moderada (3)	B	M	A	E	E
Baja (2)	B	B	2.1 M	A	E
Muy Baja (1)	B	B	1.1 M 3.1	A	A
	Muy Bajo (1)	Bajo (2)	Moderado (3)	Alto (4)	Muy Alto (5)
IMPACTOS					
ZONA DE RIESGO:					
B: Zona de Riesgo Baja: Respuesta, Aceptar el riesgo					
M: Zona de Riesgo Moderada: Respuestas, Aceptar el riesgo o reducir el riesgo. Costo Beneficio					
A: Zona de Riesgos Alta: Respuestas, Reducir el riesgo, o evitar, o compartir, o transferir					
E: Zona de Riesgo Extrema: Respuestas, Reducir el riesgo (costo beneficio), o evitar, o compartir o transferir					

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003	Soporte Técnico a Usuarios	UDEM
Versión 1.0	Fecha: 22 de mayo 2026	90 de 183

12. Elementos Transversales del Procedimiento



Matriz de Verificación

Inclusión de Elementos Transversales Estratégicos

Manual de Procedimientos de la Subdirección de Infotecnología



Denominación del Proceso: Soporte Técnico a Usuarios

Preguntas de Verificación	Si	No	Respuestas de Verificación
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Control Interno y anticorrupción</u> ?	X		El proceso contempla registro de solicitudes mediante ticket, asignación de responsables, control de tiempos de atención, validación del servicio brindado y cierre documentado. Estas medidas reducen riesgos de atención discrecional, manipulación de equipos, uso indebido de accesos y falta de trazabilidad.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Descentralización</u> ?		X	No se identifican actividades descentralizadas hacia regionales u otras dependencias territoriales. La atención de soporte técnico se concentra en la Subdirección de Infotecnología, por lo que podría valorarse la designación de enlaces o puntos focales regionales para reportes básicos.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Participación Ciudadana</u> ?		X	No se contempla consulta directa a la ciudadanía, ya que el proceso está orientado principalmente a usuarios internos.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Transparencia y Acceso a la Información Pública</u> ?	X		El proceso contribuye a la continuidad de equipos, sistemas y servicios tecnológicos que respaldan la atención institucional y el acceso a información pública. Además, debe proteger información reservada, confidencial o sensible durante la asistencia técnica a usuarios.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Archivo Documental</u> ?	X		Se deben conservar registros de tickets, solicitudes de soporte, diagnósticos, acciones realizadas, responsables, fechas de atención, evidencias de cierre y reportes de incidencias. Esta documentación permite trazabilidad, control posterior y respaldo ante revisiones internas o auditorías.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al cumplimiento de los indicadores de <u>PEI Institucional</u> ?	X		El proceso se vincula con indicadores de eficiencia operativa, continuidad de servicios, atención de incidencias, satisfacción de usuarios internos y modernización institucional. Su seguimiento debe asociarse a metas del PEI, POA y reportes periódicos de desempeño del soporte técnico.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 91 de 183

13. Bibliografía

- AXELOS. (2019). *ITIL® Foundation: ITIL 4 Edition*. TSO.
- Carbonell, M. (2019). *Teoría del derecho*. Porrúa.
- De la Torre, J. (2018). *Técnicas de redacción jurídica*. Jurídica Universitaria.
- *Definición.de.* . (2024). Obtenido de Soporte técnico: <https://definicion.de/soporte-tecnico/>
- *HubSpot.* (2024). Obtenido de Qué es el soporte técnico: <https://blog.hubspot.es/service/que-es-soporte-tecnico>
- ISO. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.
- *Real Academia Española.* (2023). Obtenido de Diccionario de la lengua española (23.ª ed.): <https://dle.rae.es>
- *Ticket de soporte técnico: definición y funciones.* (2024). Obtenido de Ticket de soporte técnico: definición y funciones: <https://www.zendesk.es/blog/customer-service/ticketing-system/ticket-de-soporte-tecnico/>
- *Wikipedia.* (2025). Obtenido de Soporte técnico: https://es.wikipedia.org/wiki/Soporte_t%C3%A9cnico

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 92 de 183

14. Anexos

14.1. M- PGR-SDIT-XXX-202X



MEMORÁNDUM PGR-SDIT-LI-00X-202X

Tegucigalpa M.D.C. XX de enero de 202X

PARA: Nombre _____
Cargo _____

C.c.: Nombre _____
Cargo _____

DE: Nombre _____
Cargo _____

ASUNTO: _____

Co: Archivo

📍 Residencial El Trapiche, Edificio PGR, Tegucigalpa, M.D.C.

☎ Tel: 2235-2022 / 2235-2025 / 2235-2049 / 2235-2050

🌐 www.pgr.gob.hn

📱 📺 📷 📞

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UEM 93 de 183

14.2. Sistema de ticket o correo electrónico



Notificar abuso'." data-bbox="510 259 920 789"/>

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 94 de 183

14.3. F-SDIT-004 Dictamen Técnico de Equipos Tecnológicos

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
INF-SDIT-004 Versión 1.0	DICTAMEN TÉCNICO No. XXXX-202X Fecha: 20 de mayo de 2026	SDIT 2 de 4

1. Datos Generales

Fecha: _____

Dependencia solicitante: _____

Asunto: _____

2. Objetivo del Dictamen

Indicar brevemente la finalidad de la evaluación.

3. Identificación del equipo

Campo	Información
Tipo de equipo	
Marca	
Modelo	
Número de serie	
Código de inventario	
Ubicación	
Usuario o dependencia asignada	
Año de adquisición	
Estado físico	

4. Características técnicas

Registrar únicamente las características que correspondan al tipo de equipo:

- Procesador.
- Memoria RAM.
- Capacidad y tipo de almacenamiento.
- Sistema operativo.
- Tarjeta de red/conectividad.
- Periféricos.
- Capacidad o especificaciones particulares del equipo.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
INF-SDIT-004 Versión 1.0	DICTAMEN TÉCNICO No. XXXX-202X Fecha: 20 de mayo de 2026	SDIT 3 de 4

- Otras características relevantes.

5. Evaluación técnica

Aspecto evaluado	Resultado	Observaciones
Estado físico		
Encendido y funcionamiento		
Rendimiento		
Almacenamiento		
Conectividad		
Sistema operativo		
Componentes		

6. Hallazgos

Describir concretamente las condiciones encontradas.

Por ejemplo:

- Fallas identificadas.
- Componentes deteriorados.
- Obsolescencia tecnológica.
- Incompatibilidad de hardware o software.
- Rendimiento insuficiente.
- Daños físicos.
- Ausencia o dificultad de repuestos.
- Condiciones que representen riesgo para la continuidad del servicio.

7. Diagnóstico técnico

Presentar el resultado integral de la evaluación.

Clasificación sugerida:

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 95 de 183

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
INF-SDIT-004 Versión 1.0	DICTAMEN TÉCNICO No. XXXX-202X Fecha: 20 de mayo de 2026	SDIT 4 de 4

- ☐ Apto para continuar en uso
- ☐ Apto con mantenimiento
- ☐ Requiere reparación
- ☐ Requiere actualización de componentes
- ☐ Requiere reemplazo
- ☐ Técnicamente no funcional

De acuerdo con las pruebas y verificaciones realizadas, se determina que el equipo presenta _____. En consecuencia, técnicamente se considera _____, recomendándose _____.

8. Evidencia y anexos

Fotografías del equipo, Reportes de pruebas, Cotización o estimación de reparación, si procede.

9. Responsables

Responsabilidad	Nombre y Cargo	Firma	Fecha
Elaborado por			
Revisado por			
Aprobado por			

 PROCURADURÍA GENERAL DE LA REPÚBLICA	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	 UNIDAD DE MODERNIZACIÓN
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 96 de 183

14.4. F-SDIT-005 Reporte de mantenimiento semestral

PROCURADURÍA GENERAL DE LA REPÚBLICA								
	SUBDIRECCIÓN DE INFOTECNOLOGÍA REPORTE DE MANTENIMIENTO							F-SDIT-005 V 1.0 Fecha: 20 de mayo de 2026
REPORTE SEMESTRAL								
MES DE XXX 2026								
Periodo	Fecha	Dependencia	Tipo de equipo	Marca y modelo	Número de serie	Código de inventario	Actividades realizadas	Observaciones
	Fecha en que se prepara el reporte de mantenimiento.	Área administrativa donde se encuentra asignado o ubicado el equipo.	Clasificación del equipo intervenido, por ejemplo: computadora, impresora, servidor, UPS u otro.	Datos que permiten identificar las características comerciales del equipo.	Código único asignado por el fabricante para identificar el equipo.	Número o código institucional utilizado para el control patrimonial del equipo.	Descripción breve de las acciones de revisión, limpieza, configuración, reparación o actualización efectuadas.	Información complementaria que resulte relevante para el seguimiento del equipo.
SEMESTRE								
SEMESTRE								
SEMESTRE								
SEMESTRE								

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 97 de 183

14.5. F-SDIT-006 Reportes periódicos de soporte trimestral

PROCURADURÍA GENERAL DE LA REPÚBLICA

SUBDIRECCIÓN DE INFOTECNOLOGÍA

REPORTE DE MANTENIMIENTO

F-SDIT-006

V 1.0

Fecha:20 de mayo de 2026

REPORTE TRIMESTRAL

MES DE XXX 2026

Período	Fecha	Dependencia	Tipo de equipo	Marca y modelo	Número de serie	Código de inventario	Actividades realizadas	Observaciones
	Fecha en que se prepara el reporte de mantenimiento.	Área administrativa donde se encuentra asignado o ubicado el equipo.	Clasificación del equipo intervenido, por ejemplo: computadora, impresora, servidor, UPS u otro.	Datos que permiten identificar las características comerciales del equipo.	Código único asignado por el fabricante para identificar el equipo.	Número o código institucional utilizado para el control patrimonial del equipo.	Descripción breve de las acciones de revisión, limpieza, configuración, reparación o actualización efectuadas.	Información complementaria que resulte relevante para el seguimiento del equipo.
TRIMESTRE								
TRIMESTRE								
TRIMESTRE								
TRIMESTRE								

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-003 Versión 1.0	Soporte Técnico a Usuarios Fecha: 22 de mayo 2026	UDEM 98 de 183

15. Control de Cambios al Procedimiento

Historial de Cambios al Procedimiento

Fecha	Versión	Autor		Descripción del cambio	Cambio Autorizado por:	
		Cargo	Área		Cargo	Firma

PROCURADURÍA GENERAL DE LA REPÚBLICA

SUBDIRECCIÓN DE INFOTECNOLOGÍA

PROCEDIMIENTO ADMINISTRACIÓN DE ACTIVOS TECNOLÓGICOS

**CÓDIGO
PR-SDIT-004**

25 DE MAYO DE 2026

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UDEM 100 de 183

Responsables de los Cambios al Procedimiento

Elaboración del Documento

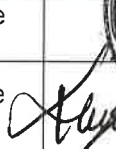
Elaborado por:	Cargo	Área de Trabajo	Fecha	Firma
Suyapa del Mar Andino Ordoñez	Jefa de Unidad	Unidad de Modernización	25 de mayo de 2026	



Revisión del Documento

Revisado por:	Cargo	Área de Trabajo	Fecha	Firma
Lilian Iveth Galo Andrade	Asistente Administrativo	Subdirección de Infotecnología	26 de mayo de 2026	

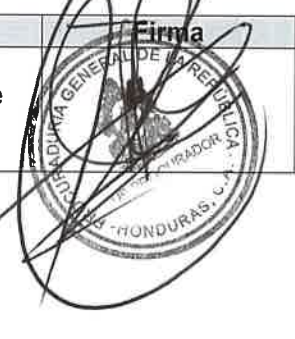
Verificación del Documento

Verificado por:	Cargo	Área de Trabajo	Fecha	Firma
Jorge Efraín Salgado	Subdirector de Infotecnología	Subdirección de Infotecnología	27 de mayo de 2026	
Ingrid Karina López Fuentes	Directora	Dirección de Administración y Finanzas	27 de mayo de 2026	



Aprobación del Documento

Aprobado por:	Cargo	Área de Trabajo	Fecha	Firma
José Francisco Quiroz Mejía	Sub-Procurador General de la República	Despacho de la Sub-Procuraduría General de la República	29 de mayo de 2026	



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UEM 101 de 183

Tabla de Contenido

1.	Objetivo del Procedimiento	102
2.	Alcance del Procedimiento	102
3.	Marco Legal del Procedimiento	102
4.	Políticas y Lineamientos del Procedimiento	102
5.	Responsables del Procedimiento	103
6.	Insumos del Procedimiento	103
7.	Productos o Resultados del Procedimiento	103
8.	Definición de Glosario de Términos, Siglas y Abreviaturas	104
9.	Descripción del Procedimiento	105
10.	Diagrama de Flujo del Procedimiento	110
11.	Gestión del Riesgo	113
12.	Elementos Transversales del Procedimiento	115
13.	Bibliografía	116
14.	Anexos	117
15.	Control de Cambios al Procedimiento	121

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-004	Administración de Activos Tecnológicos	UDEM
Versión 1.0	Fecha: 25 de mayo 2026	102 de 183

1. Objetivo del Procedimiento

Administrar y controlar los activos tecnológicos institucionales durante su ciclo de vida, incluyendo su asignación y préstamo a otras dependencias, para garantizar su registro, custodia, seguimiento, mantenimiento, devolución y disposición final, conforme a la normativa vigente.

2. Alcance del Procedimiento

El presente proceso comprende desde la recepción o incorporación de los activos tecnológicos a la institución, su verificación, registro e identificación en los controles correspondientes, así como su asignación, préstamo temporal a otras dependencias, traslado, mantenimiento preventivo y correctivo, seguimiento, devolución, reasignación, verificación física y control de custodios, hasta su baja, descarte o disposición final, conforme a la normativa administrativa, patrimonial y de control interno vigente.

3. Marco Legal del Procedimiento

No.	Código	Documento
1	Decreto 131-82	Constitución de la República
2	Decreto 74-61	Ley Orgánica de la Procuraduría General de la República
3	Decreto 146-86	Ley General de la Administración Pública
4	Decreto 152-87	Ley del Procedimiento Administrativos
5	Decreto 274- 2010	Creación de la Dirección General de Bienes Nacionales
6	Acuerdo Ejecutivo 226-2017	Reglamento de Organización y Funcionamiento de la Dirección Nacional de Bienes del Estado (DNBE)
7	N/A	Disposiciones Generales del Presupuesto vigentes y demás leyes de aplicación general

4. Políticas y Lineamientos del Procedimiento

- 4.1. La administración de los activos tecnológicos es de cumplimiento obligatorio para todas las unidades administrativas que utilicen, gestionen o resguarden bienes tecnológicos de la institución.
- 4.2. Ningún activo tecnológico podrá ser adquirido, asignado, trasladado, modificado o dado de baja sin seguir el procedimiento establecido por la Subdirección de Bienes Nacionales.
- 4.3. Los activos tecnológicos son bienes institucionales y deben ser utilizados exclusivamente para el cumplimiento de las funciones oficiales.
- 4.4. La persona usuaria asignada será responsable del uso adecuado, custodia y conservación del activo tecnológico que se le haya entregado.
- 4.5. La Subdirección de Infotecnología será la encargada de coordinar, supervisar y mantener actualizado el inventario de activos tecnológicos en su custodia.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UDEM 103 de 183

4.6. Toda acción relacionada con préstamos de un día de los activos tecnológicos deberá quedar debidamente registrada y documentada.

4.7. Los registros deberán permitir identificar el estado, ubicación, responsable y vida útil del activo.

5. Responsables del Procedimiento

Área	Puesto de Trabajo	Responsabilidad
Subdirección de Infotecnología	Subdirector(a)	Aprueba decisiones relacionadas con la asignación, traslado y baja de activos tecnológicos. Garantiza el cumplimiento de la normativa institucional y legal.
Subdirección de Infotecnología	Asistente Administrativo	Registra, organiza y resguarda la documentación de los activos tecnológicos. Da seguimiento administrativo a solicitudes de asignación, mantenimiento y baja.
Subdirección de Infotecnología	Oficial Técnico	Administra técnicamente los activos tecnológicos durante todo su ciclo de vida. Mantiene actualizado el inventario institucional.
Subdirección de Infotecnología	Auxiliar Técnico	Apoya en la identificación física y control de los activos tecnológicos. Colabora en inventarios y verificaciones.

6. Insumos del Procedimiento

Código	Insumos	Lugar de Guarda	Tiempo de Guarda
M- PGR-SDIT-XXX-202X	Memorándum	Subdirección de Infotecnología	5 años
N/A	Sistema de ticket	Subdirección de Infotecnología	5 años

7. Productos o Resultados del Procedimiento

Código	Productos	Lugar de Guarda	Tiempo de Guarda
F-SDIT-007	Reporte del control de activos tecnológicos identificados	Subdirección de Infotecnología	5 años
	Inventario actualizado	Subdirección de Infotecnología	5 años
N/A	Actas de asignación préstamo de equipo	Subdirección de Infotecnología	5 años

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-004	Administración de Activos Tecnológicos	UDEM
Versión 1.0	Fecha: 25 de mayo 2026	104 de 183

F-SDIT-008	Vale de préstamo y devolución	Subdirección de Infotecnología	5 años
F-SDIT-009	Reportes de incidencias	Subdirección de Infotecnología	5 años
F-SDIT-010	Conciliación de inventario	Subdirección de Infotecnología	5 años

8. Definición de Glosario de Términos, Siglas y Abreviaturas

8.1. Términos

Activo Tecnológico: Bien tangible o intangible de tecnología de la información que es propiedad de la institución y que se utiliza para apoyar el cumplimiento de sus funciones, tales como equipos de cómputo, software, licencias, dispositivos de red y servicios tecnológicos. (IBM Cloud Education, s.f.)

Administración de Activos Tecnológicos: Proceso sistemático para identificar, registrar, asignar, controlar, mantener y disponer los activos tecnológicos de una institución durante todo su ciclo de vida, con el fin de asegurar su uso eficiente, seguro y conforme a la normativa vigente. (IBM Cloud Education, s.f.)

Baja de Activos Tecnológicos: Proceso formal mediante el cual un activo tecnológico es retirado del inventario institucional por obsolescencia, daño irreparable o fin de su vida útil, previa evaluación técnica y autorización correspondiente. (ServiceNow, s.f.)

Inventario de Activos Tecnológicos: Registro formal, estructurado y actualizado que contiene la información de todos los activos tecnológicos de la institución, incluyendo su identificación, ubicación, estado y responsable asignado. (NinjaOne, 2025)

Responsable del Activo: Persona o unidad administrativa a la que se le asigna un activo tecnológico y que es responsable de su uso adecuado, custodia y conservación

Seguridad de la Información: Conjunto de medidas destinadas a proteger la confidencialidad, integridad y disponibilidad de la información contenida o procesada por los activos tecnológicos. (ServiceNow, s.f.)

Memorándum: Comunicación escrita breve utilizada en el ámbito institucional o empresarial para informar, recordar o instruir sobre asuntos específicos. (Real Academia Española, 2023)

Normativa: Conjunto de normas jurídicas que regulan una materia específica dentro de un ordenamiento legal. (Carbonell, 2019)

Oficio: Documento formal mediante el cual una autoridad comunica decisiones, solicitudes o información a otra autoridad o entidad. (De la Torre, Técnicas de redacción jurídica, 2018)

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-004	Administración de Activos Tecnológicos	UEM
Versión 1.0	Fecha: 25 de mayo 2026	105 de 183

8.2. Siglas

ISO: International Organization for Standardization

NIST: National Institute of Standards and Technology

PGR: Procuraduría General de la República.

SDIT: Subdirección de Infotecnología.

TIC: Tecnologías de la Información y la Comunicación.

UEM: Unidad de Modernización.

9. Descripción del Procedimiento

Auxiliar Técnico y Oficial Técnico

- 9.1. Recibir los activos tecnológicos adquiridos, donados, transferidos o reasignados. Esta actividad consiste en recibir físicamente los activos tecnológicos provenientes de compras, donaciones u otras dependencias, objetivo es asegurar que los activos ingresen formalmente a la institución cuando son comprados y en caso de ser devueltos por otras dependencias se entregan a la Subdirección de Infotecnología y verifica su estado físico y funcionamiento básico.
- 9.2. Verificar que los activos tecnológicos cumplan con las especificaciones técnicas, cantidad, estado físico y documentación soporte correspondiente, aquí se revisa que los activos coincidan con lo establecido en órdenes de compra, actas o documentos de transferencia, a la vez se valida su estado físico y funcionamiento básico, confirmando que cuenten con la documentación soporte correspondiente.
- 9.3. Clasificar los activos tecnológicos según su tipo, estado, ubicación y responsable asignado, organizándose de acuerdo con su naturaleza (hardware, software, red, entre otros), para el control de la Subdirección se identifica el estado de uso y la dependencia donde esta asignado.
- 9.4. Asignar los activos tecnológicos al usuario de la dependencia correspondiente. Se identifica al usuario que utilizará el activo según las necesidades de la dependencia. La asignación se realiza la Subdirección de Bienes Nacionales con base en la normativa vigente.
- 9.5. Formalizar la entrega del activo tecnológico mediante acta de recibo o documento de resguardo por la Subdirección de Bienes Nacionales, una vez asignado el activo se configura y proporciona las credenciales de acceso al usuario.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-004	Administración de Activos Tecnológicos	UEM
Versión 1.0	Fecha: 25 de mayo 2026	106 de 183

Asistente Administrativo

- 9.6.** Recibir las solicitudes de préstamo temporal de activos tecnológicos de otras dependencias, estas presentan la solicitud correspondiente y se revisa que la solicitud esté debidamente justificada, luego se registra para el seguimiento del activo.

Asistente Administrativo, Auxiliar Técnico y Oficial Técnico

- 9.7.** Verificar la disponibilidad del activo tecnológico solicitado para préstamo, se revisa el inventario para confirmar la existencia del activo solicitado, validando que no esté asignado o comprometido para otro uso.
- 9.8.** Autorizar el préstamo temporal del activo tecnológico, cuando corresponda, se consideran el tiempo solicitado y la finalidad del uso, esto garantiza el control y uso adecuado del activo.
- 9.9.** Registrar el préstamo del activo tecnológico, indicando dependencia solicitante, responsable, fecha de entrega, plazo de uso y condiciones de devolución, este registro permite la trazabilidad del activo durante el período de uso, a la vez facilita el control y seguimiento administrativo.
- 9.10.** Entregar el activo tecnológico en calidad de préstamo a la dependencia autorizada, se realiza la entrega física del activo al responsable designado también se verifican las condiciones del activo antes de su entrega asegurando que el usuario conozca las condiciones de uso y devolución.
- 9.11.** Actualizar los registros de ubicación, custodia y responsable del activo tecnológico prestado, se registra la nueva ubicación y responsable temporal manteniendo la información actualizada y confiable.
- 9.12.** Dar seguimiento a los activos tecnológicos prestados a otras dependencias, se supervisa el cumplimiento del plazo de préstamo autorizado, manteniendo la comunicación con la dependencia prestataria, con el objetivo es evitar pérdidas o uso indebido del activo.
- 9.13.** Recibir los activos tecnológicos devueltos por las dependencias prestatarias, se verifica que la devolución se realice en el plazo establecido y se confirma la entrega de la dependencia solicitante.
- 9.14.** Verificar el estado físico y funcional de los activos tecnológicos al momento de su devolución, se revisa que el activo conserve su estado original validando su correcto funcionamiento y cualquier anomalía se registra para las acciones correspondientes.
- 9.15.** Atender las solicitudes de traslado, devolución o reasignación de activos tecnológicos. Las solicitudes se reciben y analizan conforme a las necesidades institucionales, a la vez se verifica que cuenten con la autorización correspondiente y se actualizan los registros según el movimiento realizado.
- 9.16.** Registrar el mantenimiento preventivo de los activos tecnológicos conforme a su uso, criticidad y vida útil, también se consideran criterios técnicos y planes establecidos para contribuir a prolongar la vida útil de los activos.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-004	Administración de Activos Tecnológicos	UEM
Versión 1.0	Fecha: 25 de mayo 2026	107 de 183

Asistente Administrativo

- 9.17.** Conciliar la existencia física de los activos tecnológicos con los registros administrativos o patrimoniales, con la Subdirección de Bienes Nacionales se comparan los activos físicos con los registros existentes, identificando diferencias o inconsistencias. Se realizan las aclaraciones necesarias.
- 9.18.** Identificar los activos tecnológicos en desuso, obsoletos, dañados o no reparables. Se revisa el estado general del inventario e identifican activos que ya no cumplen su función.

Auxiliar Técnico y Oficial Técnico

- 9.19.** Evaluar la procedencia de la baja, descarte, reposición o disposición final de los activos tecnológicos, conforme a la normativa aplicable, se realiza un análisis técnico y administrativo del activo en cumplimiento del marco legal vigente, emitiendo la recomendación correspondiente.

Asistente Administrativo

- 9.20.** Archivar y resguardar la documentación soporte relacionada con la recepción, asignación, préstamo, traslado, devolución, mantenimiento y baja de los activos tecnológicos. La documentación se organiza de forma ordenada y segura para garantizar su disponibilidad para auditorías o revisiones, esto fortalece la transparencia y el control interno.

Asistente Administrativo, Auxiliar Técnico y Oficial Técnico

- 9.21.** Emitir reportes periódicos sobre inventario, préstamos, asignaciones, estado, mantenimiento y movimiento de los activos tecnológicos. Los reportes apoyan la toma de decisiones institucionales, también facilitan el control y la rendición de cuentas.

	PROCURADURÍA GENERAL DE LA REPÚBLICA	
	SUBDIRECCIÓN DE INFOTECNOLOGÍA	
	Administración de Activos Tecnológicos	UEM
PR-SDIT-004	Fecha: 25 de mayo 2026	108 de 183
Versión 1.0		



Matriz de Actividades, Responsables y Formularios
Manual de Procedimientos de la Subdirección de Infotecnología
Proceso de Administración de Activos Tecnológicos



No.	Etapas del Proceso	Objetivo de la Etapa	Insumo	Actividad	Tiempo	Responsable	Producto	Envío a:	
1	Recepción, verificación y clasificación de activos	Recibir los activos tecnológicos, verificar sus especificaciones técnicas, cantidad, estado físico y documentación soporte, y clasificarlos según tipo, estado, ubicación y responsable inicial.	Documentos de control, memorándum, sistema de ticket o correo electrónico.	1.1 Recibir los activos tecnológicos adquiridos, donados, transferidos o reasignados.	2 días	Auxiliar Técnico y Oficial Técnico	Reporte del control de activos tecnológicos identificados	Auxiliar Técnico y Oficial Técnico	
				1.2 Verificar que los activos tecnológicos cumplan con las especificaciones técnicas, cantidad, estado físico y documentación soporte correspondiente.	2 días		Reporte del control de activos tecnológicos identificados		
				1.3 Clasificar los activos tecnológicos según su tipo, estado, ubicación y responsable asignado.	2 días		Inventario actualizado		
2	Asignación y formalización de custodia	Asignar los activos tecnológicos al usuario o dependencia correspondiente y formalizar la entrega mediante un correo electrónico a la Subdirección de Bienes Nacionales, dejando evidencia de la responsabilidad de custodia.		2.1 Asignar los activos tecnológicos al usuario de la dependencia correspondiente.	2 días	Asistente Administrativo	Actas de asignación préstamo de equipo Vale de préstamo y devolución	Auxiliar Técnico y Oficial Técnico	
				2.2 Formalizar la entrega del activo tecnológico mediante acta, recibo, vale, formulario o documento de resguardo.	1 día				
3	Gestión de préstamos, traslados y reasignaciones	Atender solicitudes de préstamo, traslado, devolución o reasignación; verificar disponibilidad, autorizar cuando corresponda, registrar condiciones de uso, entregar los activos y actualizar los registros de ubicación, custodia y responsable.		3.1 Recibir las solicitudes de préstamo temporal de activos tecnológicos de otras dependencias.	1 hora	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	Inventario actualizado	Asistente Administrativo	
				3.2 Verificar la disponibilidad del activo tecnológico solicitado para préstamo.	1 hora				
				3.3 Autorizar el préstamo temporal del activo tecnológico, cuando corresponda.	1 hora				
				3.4 Registrar el préstamo del activo tecnológico, indicando dependencia solicitante, responsable, fecha de entrega, plazo de uso y condiciones de devolución.	30 min	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico			Reportes de Incidencias
				3.5 Entregar el activo tecnológico en calidad de préstamo a la dependencia autorizada.	30 min				
				3.6 Actualizar los registros de ubicación, custodia y responsable del activo tecnológico prestado.	30 min				
				3.7 Dar seguimiento a los activos tecnológicos prestados a otras dependencias.	30 min				
4	Devolución, mantenimiento, conciliación y control físico	Recibir activos devueltos, verificar su estado físico y funcional, registrar mantenimientos preventivos y conciliar la existencia física con los registros administrativos o patrimoniales.		4.1 Recibir los activos tecnológicos devueltos por las dependencias prestatarias.	30 min	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico	Reportes de Incidencias		
				4.2 Verificar el estado físico y funcional de los activos tecnológicos al momento de su devolución.	30 min				
				4.3 Atender las solicitudes de traslado, devolución o reasignación de activos tecnológicos.	30 min				
				4.4 Registro del mantenimiento preventivo de los activos tecnológicos conforme a su uso, criticidad y vida útil.	1 día				

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UDEM 109 de 183



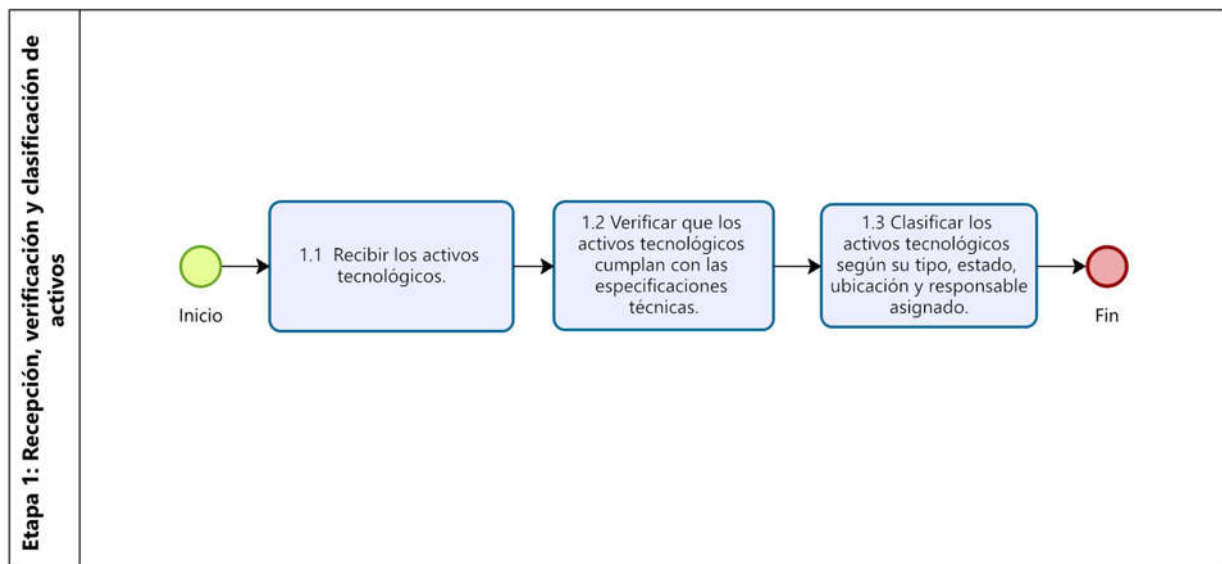
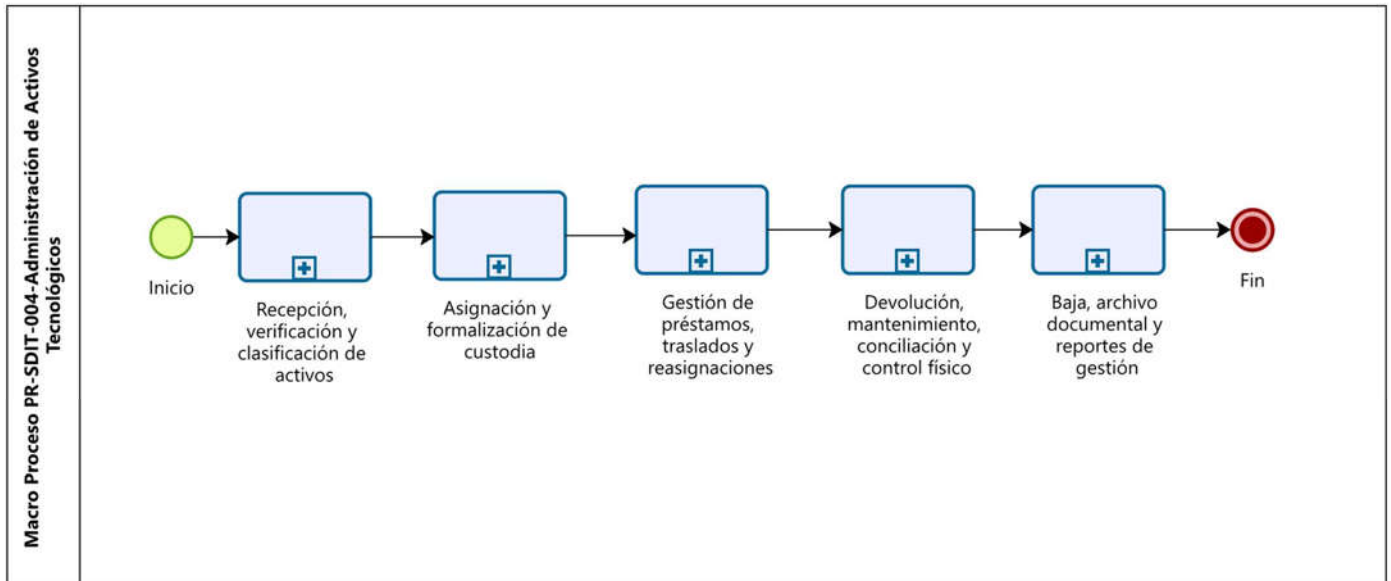
Matriz de Actividades, Responsables y Formularios
Manual de Procedimientos de la Subdirección de Infotecnología
Proceso de Administración de Activos Tecnológicos



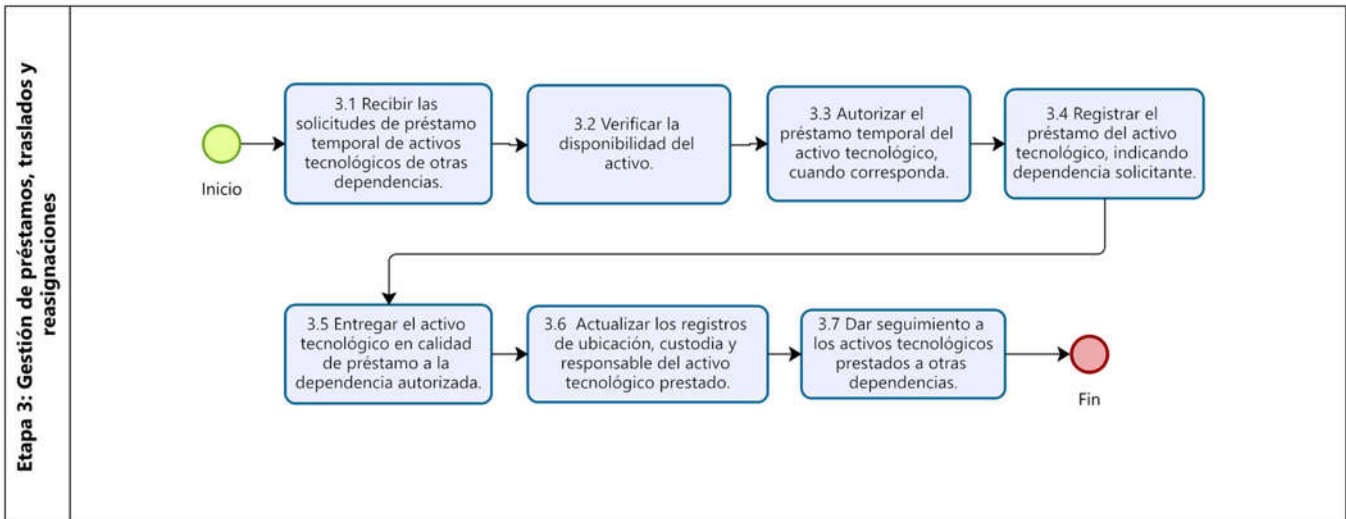
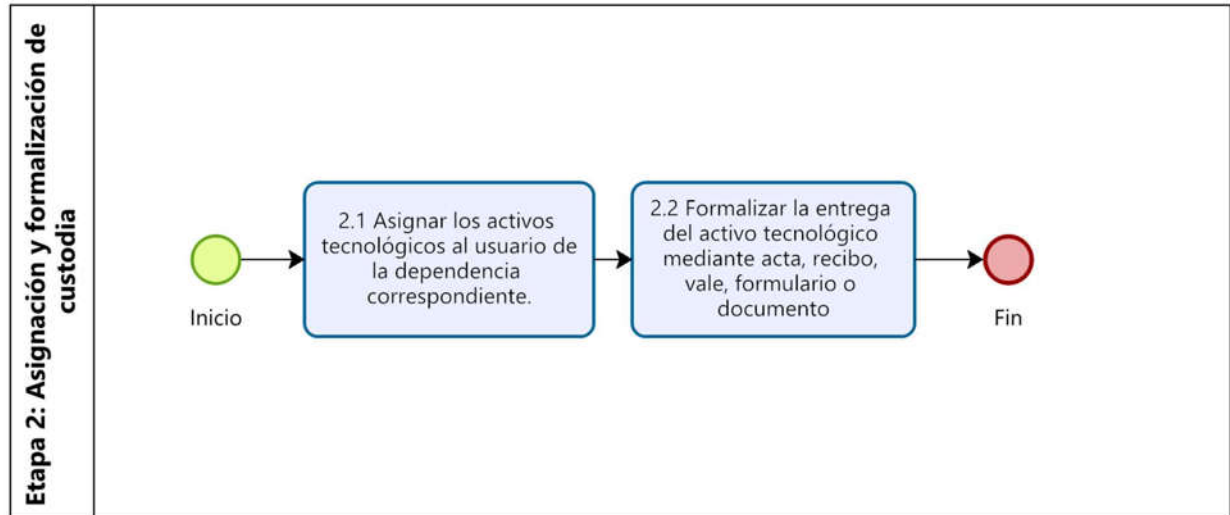
No.	Etapas del Proceso	Objetivo de la Etapa	Insumo	Actividad	Tiempo	Responsable	Producto	Envío a:
5	Baja, archivo documental y reportes de gestión	Identificar activos en desuso, obsoletos, dañados o no reparables, evaluar su baja o disposición final, resguardar la documentación soporte y emitir reportes periódicos sobre inventario, asignaciones, préstamos, estado, mantenimiento y movimientos.		4.5 Conciliar la existencia física de los activos tecnológicos con los registros administrativos o patrimoniales.	5 días	Asistente Administrativo	Conciliación de inventario	Auxiliar Técnico y Oficial Técnico
				5.1 Identificar los activos tecnológicos en desuso, obsoletos, dañados o no reparables.	5 días		Reportes de incidencias	
				5.2 Evaluar la procedencia de la baja, descarte, reposición o disposición final de los activos tecnológicos, conforme a la normativa aplicable.	1 día	Auxiliar Técnico y Oficial Técnico		
				5.3 Archivar y resguardar la documentación soporte relacionada con la recepción, asignación, préstamo, traslado, devolución, mantenimiento y baja de los activos tecnológicos.	1 hora	Asistente Administrativo	Reporte del control de activos tecnológicos identificados	Subdirector de Infotecnología
				5.4 Emitir reportes periódicos sobre inventario, préstamos, asignaciones, estado, mantenimiento y movimiento de los activos tecnológicos.	Trimestral	Asistente Administrativo, Auxiliar Técnico y Oficial Técnico		

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UDEM 110 de 183

10. Diagrama de Flujo del Procedimiento

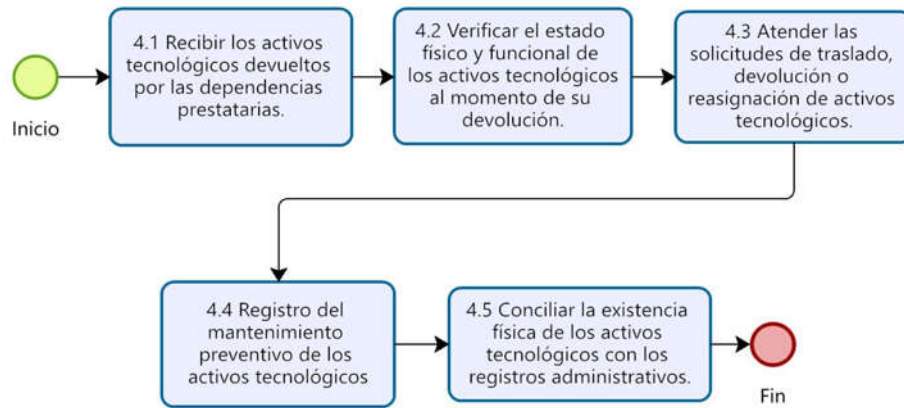


	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UDEM 111 de 183

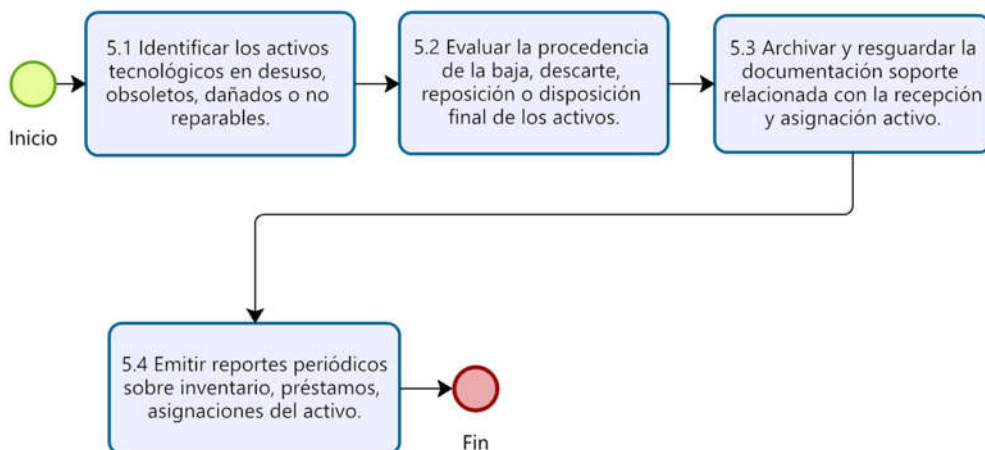


	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UDEM 112 de 183

Etapas 4: Devolución, mantenimiento, conciliación y control físico



Etapas 5: Baja, archivo documental y reportes de gestión



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UDEM 113 de 183

11. Gestión del Riesgo

PGR		PROCURADURÍA GENERAL DE LA REPÚBLICA										NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00	
MATRIZ PARA LA EVALUACIÓN, ANÁLISIS Y RESPUESTA A LOS RIESGOS													
Formulario 27 PGR													
PROCESO:		Administración de Activos Tecnológicos											
NOMBRE DEL SUBPROCESO:		Administración de Activos Tecnológicos											
OBJETIVO:		Administrar y controlar los activos tecnológicos institucionales durante su ciclo de vida, incluyendo su asignación y préstamo a otras dependencias, para garantizar su registro, custodia, seguimiento, mantenimiento, devolución y disposición final, conforme a la normativa vigente.											
(1) No.	(2) Etapa del proceso	(3) Descripción del Riesgo	Riesgo Inherente		(6) Zona de Riesgo Preliminar	(7) Controles obligatorios para mitigar los riesgos	(8) Controles que existen en la entidad	(9) Controles pendientes por establecer para mitigar los riesgos	Riesgo Residual		(12) Zona de Riesgo Final	(13) Respuesta a los Riesgos	
			(4) P	(5) I					(10) P	(11) I			
1	Recepción, verificación y clasificación de activos	1.1 Los activos fueron recibidos sin verificar previamente el cumplimiento de las especificaciones técnicas requeridas.	3	4	E	Realizar verificación física y técnica contra orden de compra, donación, traslado o documento de entrega, con la Subdirección de Compras y Suministros y la Subdirección de Bienes Nacionales.	Realizar verificación física y técnica contra orden de compra, donación, traslado o documento de entrega, con la Subdirección de Compras y Suministros y la Subdirección de Bienes Nacionales.		2	3	M	Mitigar	
2	Asignación y formalización de custodia	2.1 Los activos pueden usarse indebidamente, perdidos o ser sustraídos, generando afectación al patrimonio institucional.	2	4	A	Mantener registro actualizado del responsable, ubicación y estado del activo. Informar al custodio sus obligaciones de uso y conservación.	Mantener registro actualizado del responsable, ubicación y estado del activo. Informar al custodio sus obligaciones de uso y conservación.		1	3	M	Mitigar	
3	Gestión de préstamos, asignación y reasignaciones	3.1 Los activos se devuelven fuera del plazo establecido o en condiciones diferentes a las autorizadas.	3	4	E	Utilizar formulario de solicitud y autorización de préstamo, traslado o reasignación.	Utilizar formulario de solicitud y autorización de préstamo, traslado o reasignación.		2	3	M	Mitigar	
4	Devolución, mantenimiento, conciliación y control físico	4.1 Pueden existir diferencias entre el inventario físico y los registros administrativos, dificultando el control y la trazabilidad de los activos	2	2	B	Realizar conciliaciones periódicas entre inventario físico y registros patrimoniales a con la implementación del sistema informático para la Subdirección de Bienes Nacionales.	Realizar conciliaciones periódicas entre inventario físico y registros patrimoniales a con la implementación del sistema informático para la Subdirección de Bienes Nacionales.		1	1	B	Acestar	
5	Baja, archivo documental y reportes de gestión	N/A				N/A	N/A					N/A	
Elaborado por:						Revisado por:						Aprobado por:	
Lilian Iveth Galo Andrade Asistente Administrativo Suyapa del Mar Andino Ordóñez Jefa de la Unidad de Modernización						Ingrid Karina López Fuentes Directora de Administración y Finanzas Jorge Elías Subdirección						José Francisco Quiroz Vella Sub-Procurador General de la República	
Firma: Fecha: 20 de mayo de 2026						Firma: Fecha: 21 de mayo de 2026						Firma: Fecha: 22 de mayo de 2026	

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UDEM 114 de 183

	PROCURADURÍA GENERAL DE LA REPÚBLICA			NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00	
	MAPA PARA LA VALORACIÓN PRELIMINAR Y FINAL DE LOS RIESGOS			Formulario 28 PGR	
PROPÓSITO: Facilitar la valoración y determinación de la zona de riesgos, de acuerdo con la explicación que consta en el Anexo 22 Instructivo para la gestión de riesgos					
PROBABILIDAD					
Muy Alta (5)	A	A	E	E	E
Alta (4)	M	A	A	E	E
Moderada (3)	B	M	A	1.1 E 3.1	E
Baja (2)	B	4.1 B	M	2.1 A	E
Muy Baja (1)	B	B	M	A	A
	Muy Bajo (1)	Bajo (2)	Moderado (3)	Alto (4)	Muy Alto(5)
IMPACTOS					
ZONA DE RIESGO:					
B: Zona de Riesgo Baja: Respuesta, Aceptar el riesgo					
M: Zona de Riesgo Moderada: Respuestas, Aceptar el riesgo o reducir el riesgo. Costo Beneficio					
A: Zona de Riesgos Alta: Respuestas, Reducir el riesgo, o evitar, o compartir, o transferir					
E: Zona de Riesgo Extrema: Respuestas, Reducir el riesgo (costo beneficio), o evitar, o compartir o transferir					

	PROCURADURÍA GENERAL DE LA REPÚBLICA	
PR-SDIT-004	SUBDIRECCIÓN DE INFOTECNOLOGÍA	UEM
Versión 1.0	Administración de Activos Tecnológicos	115 de 183
	Fecha: 25 de mayo 2026	

12. Elementos Transversales del Procedimiento



Matriz de Verificación

Inclusión de Elementos Transversales Estratégicos

Manual de Procedimientos de la Subdirección de Infotecnología



Denominación del Proceso: Administración de Activos Tecnológicos			
Preguntas de Verificación	Si	No	Respuestas de Verificación
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Control Interno y anticorrupción</u> ?	X		Incluye registro único, asignación formal, responsables de custodia y verificaciones físicas. Permite trazabilidad de activos, control de movimientos y prevención de pérdida, uso indebido o discrecionalidad.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Descentralización</u> ?	X		Las dependencias usuarias participan en solicitudes, custodia, reporte de fallas y devolución de activos. La dependencia responsable mantiene el control técnico, inventario y seguimiento institucional.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Participación Ciudadana</u> ?		X	No aplica directamente, por ser un proceso interno de soporte.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Transparencia y Acceso a la Información Pública</u> ?	X		Genera información verificable sobre inventario, asignaciones, movimientos, mantenimientos y bajas. Sirve para auditoría, rendición de cuentas y atención de solicitudes de información pública.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Archivo Documental</u> ?	X		Resguarda controles de registro préstamo y devolución. La documentación debe mantenerse ordenada, codificada y disponible para control interno o auditoría.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al cumplimiento de los indicadores de <u>PEI Institucional</u> ?	X		Se vincula con indicadores de activos inventariados, reportes y atención de fallas. Apoya la eficiencia institucional, continuidad operativa y modernización administrativa.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UEM 116 de 183

13. Bibliografía

- Carbonell, M. (2019). *Teoría del derecho*. Porrúa.
- De la Torre, J. (2018). *Técnicas de redacción jurídica*. Jurídica Universitaria.
- IBM Cloud Education. (s.f.). *¿Qué es la gestión de activos de TI (ITAM)? IBM*. Obtenido de <https://www.ibm.com/es-es/think/topics/it-asset-management>
- NinjaOne. (2025). Obtenido de La gestión del ciclo de vida de activos de TI: <https://www.ninjaone.com/es/blog/que-saber-sobre-gestion-de-ciclo-de-vida-de-activos-de-ti/>
- ServiceNow. (s.f.). *¿Qué es el ciclo de vida de los activos de TI?* . Obtenido de <https://www.servicenow.com/es/products/it-asset-management/what-is-it-asset-lifecycle.htm>

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UDEM 117 de 183

14. Anexos

14.1. M- PGR-SDIT-XXX-202X

MEMORÁNDUM PGR-SDIT-LI-00X-202X

Tegucigalpa M.D.C. XX de enero de 202X

PARA: Nombre _____

Cargo _____

C.c.: Nombre _____

Cargo _____

DE: Nombre _____

Cargo _____

ASUNTO: _____

Co: Archivo

📍 Residencial El Trapiche, Edificio PGR, Tegucigalpa, M.D.C.

☎ Tel: 2235-2022 / 2235-2025 / 2235-2049 / 2235-2050

🌐 www.pgr.gob.hn

📱 📧 📞 📠

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UDEM 119 de 183

14.3. F-SDIT-008 Vale de préstamo y devolución

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
INF-SDIT-008	VALE DE PRÉSTAMO Y DEVOLUCIÓN DE ACTIVOS TECNOLÓGICOS	SDIT
Versión 1.0	Fecha: 20 de mayo 2026	1 de 1

1. DATOS DE LA PERSONA QUE RECIBE EL ACTIVO

Nombre completo:		Cargo:	
Dependencia:		Fecha de préstamo:	___/___/___
Correo institucional:		Motivo del préstamo:	
Estado al devolver:	☐ Bueno ☐ Regular ☐ Con daño	Fecha de devolución:	___/___/___

2. IDENTIFICACIÓN DEL ACTIVO PRESTADO

N.º	Tipo de activo	Marca / Modelo	N.º de serie	Código de inventario	Accesorios	Estado al entregar

3. ENTREGA DEL ACTIVO

Entrega / Unidad responsable	Recibe / Usuario
Nombre: _____	Nombre: _____
Firma: _____	Firma: _____

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-004 Versión 1.0	Administración de Activos Tecnológicos Fecha: 25 de mayo 2026	UEM 121 de 183

15. Control de Cambios al Procedimiento

Historial de Cambios al Procedimiento

Fecha	Versión	Autor		Descripción del cambio	Cambio Autorizado por:	
		Cargo	Área		Cargo	Firma

PROCURADURÍA GENERAL DE LA REPÚBLICA

SUBDIRECCIÓN DE INFOTECNOLOGÍA

PROCEDIMIENTO ADMINISTRACIÓN DE BASES DE DATOS Y RESPALDOS

**CÓDIGO
PR-SDIT-005**

27 DE MAYO DE 2026

 PGR PROCURADURÍA GENERAL DE LA REPÚBLICA	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-005	Administración de Bases de Datos y Respaldos	UDEM
Versión 1.0	Fecha: 27 de mayo 2026	123 de 183

Responsables de los Cambios al Procedimiento

Elaboración del Documento

Elaborado por:	Cargo	Área de Trabajo	Fecha	Firma
Suyapa del Mar Andino Ordoñez	Jefa de Unidad	Unidad de Modernización	27 de mayo de 2026	



Revisión del Documento

Revisado por:	Cargo	Área de Trabajo	Fecha	Firma
Lisandro Alfredo Suárez Salinas	Oficial Técnico	Subdirección de Infotecnología	28 de mayo de 2026	
Pablo Javier Padilla Avilés	Oficial Técnico	Subdirección de Infotecnología	28 de mayo de 2026	
Cristian Alexander Martínez Ochoa	Oficial Técnico	Subdirección de Infotecnología	28 de mayo de 2026	

Verificación del Documento

Verificado por:	Cargo	Área de Trabajo	Fecha	Firma
Jorge Efraín Salgado	Subdirector de Infotecnología	Subdirección de Infotecnología	29 de mayo de 2026	
Ingrid Karina López Fuentes	Directora	Dirección de Administración y Finanzas	29 de mayo de 2026	



Aprobación del Documento

Aprobado por:	Cargo	Área de Trabajo	Fecha	Firma
José Francisco Quiroz Mejía	Sub-Procurador General de la República	Despacho de la Sub-Procuraduría General de la República	01 de junio de 2026	



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-005	Administración de Bases de Datos y Respaldos	UEM
Versión 1.0	Fecha: 27 de mayo 2026	124 de 183

Tabla de Contenido

1. Objetivo del Procedimiento	125
2. Alcance del Procedimiento.....	125
3. Marco Legal del Procedimiento	125
4. Políticas y Lineamientos del Procedimiento.....	125
5. Responsables del Procedimiento.....	126
6. Insumos del Procedimiento.....	126
7. Productos o Resultados del Procedimiento.....	126
8. Definición de Glosario de Términos, Siglas y Abreviaturas	127
9. Descripción del Procedimiento	128
10. Diagrama de Flujo del Procedimiento	131
11. Gestión del Riesgo	134
12. Elementos Transversales del Procedimiento	136
13. Bibliografía	137
14. Anexos.....	138
15. Control de Cambios al Procedimiento.....	139

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-005	Administración de Bases de Datos y Respaldos	UDEM
Versión 1.0	Fecha: 27 de mayo 2026	125 de 183

1. Objetivo del Procedimiento

Garantizar la disponibilidad, integridad, confidencialidad y recuperación de la información institucional contenida en las bases de datos, mediante la administración eficiente, segura y controlada de los sistemas gestores de bases de datos, así como la ejecución, verificación y resguardo de los respaldos, asegurando la continuidad operativa de los servicios tecnológicos institucionales.

2. Alcance del Procedimiento

El proceso inicia con la configuración, administración y monitoreo de las bases de datos institucionales, incluyendo la definición y ejecución de políticas de respaldo, y finaliza con la garantía de disponibilidad, seguridad, integridad y recuperación de la información institucional.

3. Marco Legal del Procedimiento

No.	Código	Documento
1	Decreto 131-82	Constitución de la República
2	Decreto 74-61	Ley Orgánica de la Procuraduría General de la República
3	Decreto 146-86	Ley General de la Administración Pública
4	N/A	Reglamento Interno de Trabajo PGR,
5	ISO 27001	
6	ISO 27701	

4. Políticas y Lineamientos del Procedimiento

- 4.1. Las bases de datos institucionales deberán ser administradas de forma segura, organizada y controlada, garantizando la confidencialidad, integridad y disponibilidad de la información.
- 4.2. La administración de bases de datos y respaldos será responsabilidad exclusiva del personal autorizado de la Subdirección de Infotecnología.
- 4.3. El acceso a las bases de datos se otorgará únicamente a usuarios autorizados, según su rol y funciones.
- 4.4. Los usuarios deberán utilizar credenciales personales e intransferibles para acceder a los sistemas de bases de datos.
- 4.5. Se deberá registrar y monitorear cualquier acceso, modificación o eliminación de información en las bases de datos.
- 4.6. Todas las bases de datos productivas deberán contar con copias de respaldo periódicas, de acuerdo con su nivel de criticidad.
- 4.7. Los respaldos deberán realizarse de forma automática, evitando la intervención manual siempre que sea posible.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-005	Administración de Bases de Datos y Respaldos	UDEM
Versión 1.0	Fecha: 27 de mayo 2026	126 de 183

- 4.8.** Los respaldos deberán almacenarse en repositorios seguros, distintos al servidor principal de la base de datos y protegerse mediante mecanismos de seguridad, como cifrado y control de accesos.
- 4.9.** La restauración de bases de datos solo podrá realizarse previa solicitud formal y autorización correspondiente.
- 4.10.** El proceso de recuperación deberá ejecutarse minimizando el impacto en la operación institucional y se deberán realizar pruebas periódicas de restauración para verificar la validez de los respaldos.

5. Responsables del Procedimiento

Área	Puesto de Trabajo	Responsabilidad
Subdirección de Infotecnología	Subdirector	Supervisar y asegurar la correcta administración de las bases de datos institucionales y coordinar acciones ante incidentes, fallas o riesgos que afecten la información.
Subdirección de Infotecnología	Oficial Técnico	Administrar técnicamente las bases de datos y ejecutar los respaldos programados. Monitorear el funcionamiento, disponibilidad y seguridad de las bases de datos, a la vez realizar restauraciones de información autorizadas. Mantener actualizados los registros, bitácoras y evidencias del procedimiento. Informar oportunamente sobre incidentes, riesgos o anomalías detectadas.

6. Insumos del Procedimiento

Código	Insumos	Lugar de Guarda	Tiempo de Guarda
N/A	Sistemas gestores de bases de datos (DBMS)	Subdirección de Infotecnología	5 años
N/A	Sistemas de Información	Subdirección de Infotecnología	5 años

7. Productos o Resultados del Procedimiento

Código	Productos	Lugar de Guarda	Tiempo de Guarda
F-SDIT-011	Control de respaldos	Subdirección de Infotecnología	5 años
F-SDIT-012	Control de permisos asignados o revocados	Subdirección de Infotecnología	5 años

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-005 Versión 1.0	Administración de Bases de Datos y Respaldos Fecha: 27 de mayo 2026	UDEM 127 de 183

8. Definición de Glosario de Términos, Siglas y Abreviaturas

8.1. Términos

Administrador de Bases de Datos (DBA): Persona responsable de la gestión técnica, operación, seguridad, mantenimiento y disponibilidad de las bases de datos. (Red de Responsables TIC – UNAM, s.f.)

Backup (Respaldo): Copia de seguridad de la información almacenada en una base de datos, creada para permitir su recuperación en caso de pérdida, daño o falla del sistema. (Departamento Administrativo de la Función Pública., 2025))

Base de Datos: Conjunto organizado de información estructurada que se almacena y gestiona mediante sistemas informáticos para facilitar su consulta, actualización y control. (Red de Responsables TIC – UNAM, s.f.)

Cifrado: Proceso mediante el cual la información es protegida mediante algoritmos de seguridad para impedir su acceso por personas no autorizadas.

Disponibilidad de la Información: Principio que garantiza que la información esté accesible y utilizable cuando los usuarios autorizados la requieran.

Integridad de la Información: Propiedad que asegura que los datos se mantengan completos, exactos y sin alteraciones no autorizadas durante su almacenamiento o procesamiento. (Unidad Administrativa Especial de Alimentación Escolar., 2021)

Memorándum: Comunicación escrita breve utilizada en el ámbito institucional o empresarial para informar, recordar o instruir sobre asuntos específicos. (Real Academia Española, 2023)

Normativa: Conjunto de normas jurídicas que regulan una materia específica dentro de un ordenamiento legal. (Carbonell, 2019)

Repositorio de Respaldos: Medio físico, virtual o servicio en la nube destinado al almacenamiento, organización y custodia de las copias de seguridad de las bases de datos.

Restauración: Proceso mediante el cual se recupera una base de datos o información a partir de un respaldo previamente generado. (Microsoft, s.f.)

Seguridad de la Información: Conjunto de medidas técnicas y administrativas destinadas a proteger la confidencialidad, integridad y disponibilidad de la información institucional. (Unidad Administrativa Especial de Alimentación Escolar., 2021)

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-005	Administración de Bases de Datos y Respaldos	UEM
Versión 1.0	Fecha: 27 de mayo 2026	128 de 183

8.2. Siglas

ISO: International Organization for Standardization

NIST: National Institute of Standards and Technology

PGR: Procuraduría General de la República.

SDIT: Subdirección de Infotecnología.

TIC: Tecnologías de la Información y la Comunicación.

UEM: Unidad de Modernización

9. Descripción del Procedimiento

Oficial Técnico

- 9.1. Administrar las bases de datos institucionales para garantizar su disponibilidad y correcto funcionamiento. Esto implica asegurar que las bases de datos estén siempre accesibles para los usuarios autorizados, incluye la revisión periódica de su estado operativo para evitar interrupciones en los sistemas institucionales.
- 9.2. Configurar los sistemas gestores de bases de datos conforme a los requerimientos institucionales. Consiste en ajustar los parámetros técnicos del sistema de base de datos, se realiza según las necesidades de los sistemas y normativas vigentes esto permite que las bases de datos operen de forma segura y eficiente.
- 9.3. Monitorear el desempeño de las bases de datos para detectar problemas de rendimiento o capacidad. Se revisa el uso de recursos como memoria, almacenamiento y tiempo de respuesta, permitiendo identificar fallas antes de que afecten a los usuarios y tomar acciones preventivas oportunamente.
- 9.4. Optimizar las bases de datos mediante ajustes en estructuras, consultas e índices. Incluye mejorar la forma en que se almacenan y consultan los datos. Reduce tiempos de respuesta y uso innecesario de recursos, esto contribuye a un mejor desempeño de los sistemas institucionales.
- 9.5. Gestionar los usuarios y permisos de acceso a las bases de datos conforme a autorizaciones establecidas. Se asignan accesos según las funciones de cada usuario evitando el accesos no autorizados a la información, garantiza que cada persona solo utilice la información necesaria
- 9.6. Implementar controles de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información. Incluye medidas técnicas y administrativas de protección. Previene accesos indebidos, pérdida o alteración de datos. Asegura el cumplimiento de las políticas de seguridad institucional.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-005 Versión 1.0	Administración de Bases de Datos y Respaldos Fecha: 27 de mayo 2026	UEM 129 de 183

- 9.7. Definir la programación de respaldos de acuerdo con las políticas institucionales. Se establece la frecuencia y tipo de respaldos a realizar, considerando la importancia y criticidad de cada base de datos, esto garantiza que la información pueda recuperarse oportunamente
- 9.8. Ejecutar respaldos de las bases de datos (completos, diferenciales o incrementales). Consiste en generar copias de seguridad de la información, se realiza conforme a la programación establecida permite proteger la información ante fallas o pérdidas.
- 9.9. Verificar la correcta ejecución de los respaldos realizados. Se comprueba que los respaldos se hayan generado correctamente incluyendo la revisión de registros y alertas del sistema. Asegura que los respaldos sean confiables y utilizables.
- 9.10. Almacenar los respaldos en medios seguros conforme a los lineamientos establecidos, se evita su pérdida, daño o acceso no autorizado. Cumple con los lineamientos de custodia de la información.
- 9.11. Realizar pruebas de restauración de respaldos para validar su integridad y disponibilidad. Se simula la recuperación de información desde los respaldos, permitiendo confirmar que los datos pueden restaurarse correctamente y reduce riesgos ante incidentes reales.
- 9.12. Restaurar bases de datos en caso de fallas, incidentes o pérdida de información. Se recupera la información utilizando los respaldos disponibles, esto busca restablecer la operación normal de los sistemas con la autorización correspondiente.
- 9.13. Diagnosticar las causas de fallas en bases de datos. Se analizan errores, alertas y comportamientos anómalos para identificar el origen del problema y lograr facilitar la aplicación de soluciones adecuadas.
- 9.14. Escalar incidentes complejos a los proveedores cuando corresponda. Se contacta a proveedores especializados cuando el problema lo requiere y se le brinda la documentación del incidente para asegurar una atención técnica especializada.
- 9.15. Registrar en control todas las operaciones realizadas sobre bases de datos y respaldos. Se documentan las actividades ejecutadas permitiendo la trazabilidad y control de las acciones realizadas esto facilita auditorías y revisiones posteriores.
- 9.16. Evaluar el cumplimiento de políticas de respaldo y seguridad. Se revisa que las actividades se realicen conforme a lo establecido, esto permite detectar incumplimientos o áreas de mejora.
- 9.17. Implementar mejoras en la administración de bases de datos y gestión de respaldos. Se proponen ajustes técnicos y operativos. Busca optimizar procesos y reducir riesgos para fortalecer la continuidad y seguridad de la información.

	PROCURADURÍA GENERAL DE LA REPÚBLICA	
	SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-005	Administración de Bases de Datos y Respaldos	UDEM
Versión 1.0	Fecha: 27 de mayo 2026	130 de 183



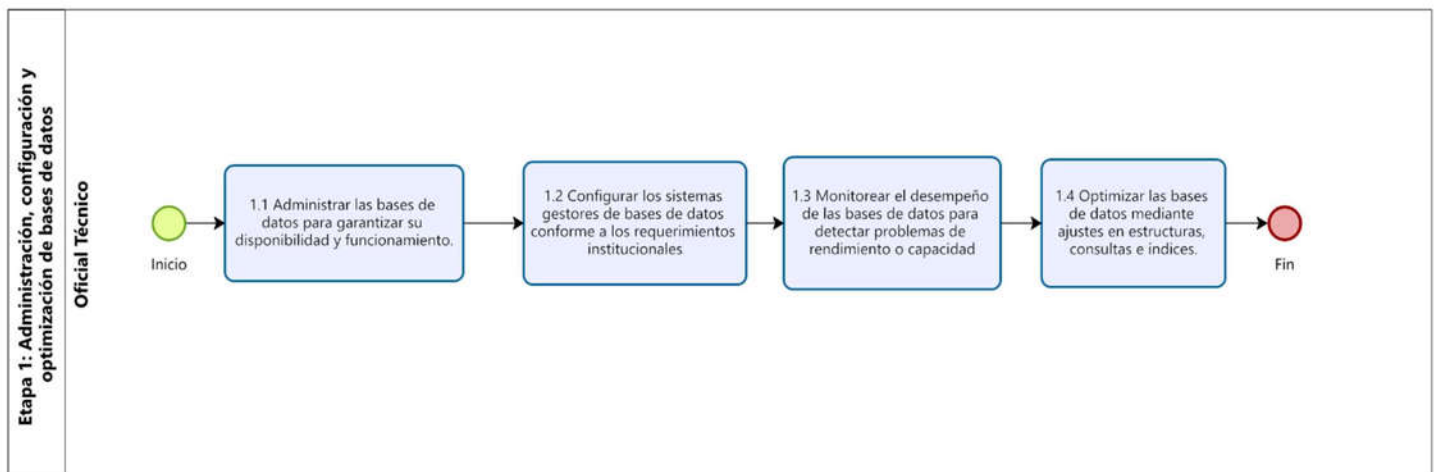
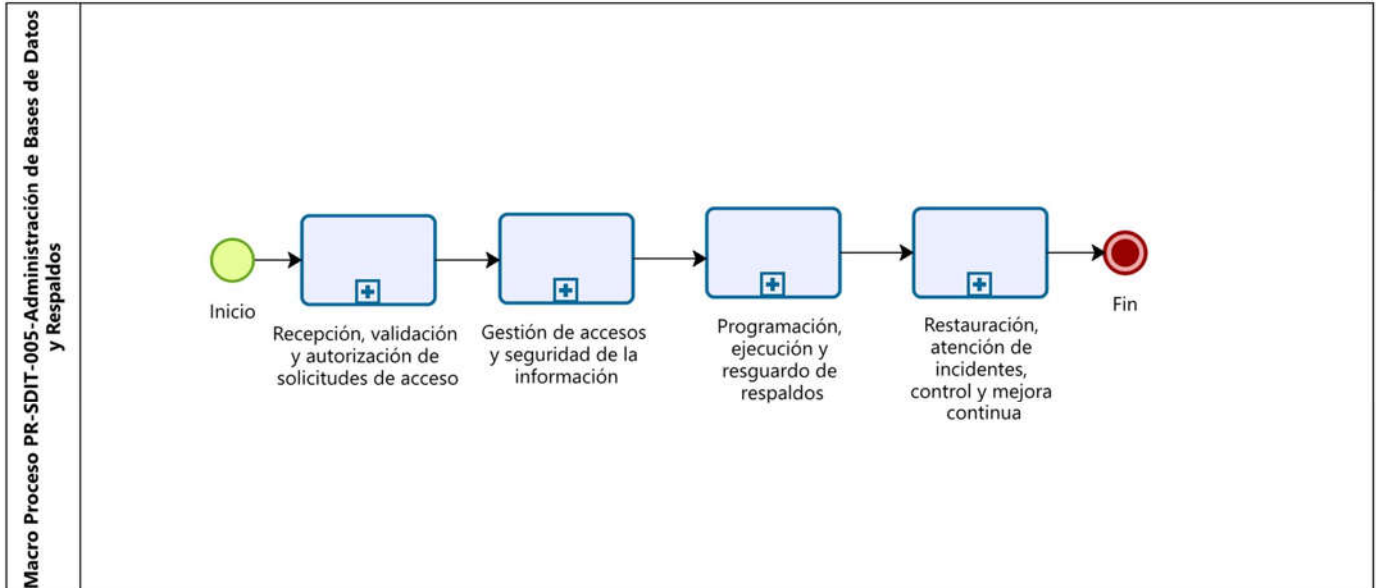
Matriz de Actividades, Responsables y Formularios
Manual de Procedimientos de la Subdirección de Infotecnología
Proceso de Administración de Bases de Datos y Respaldos



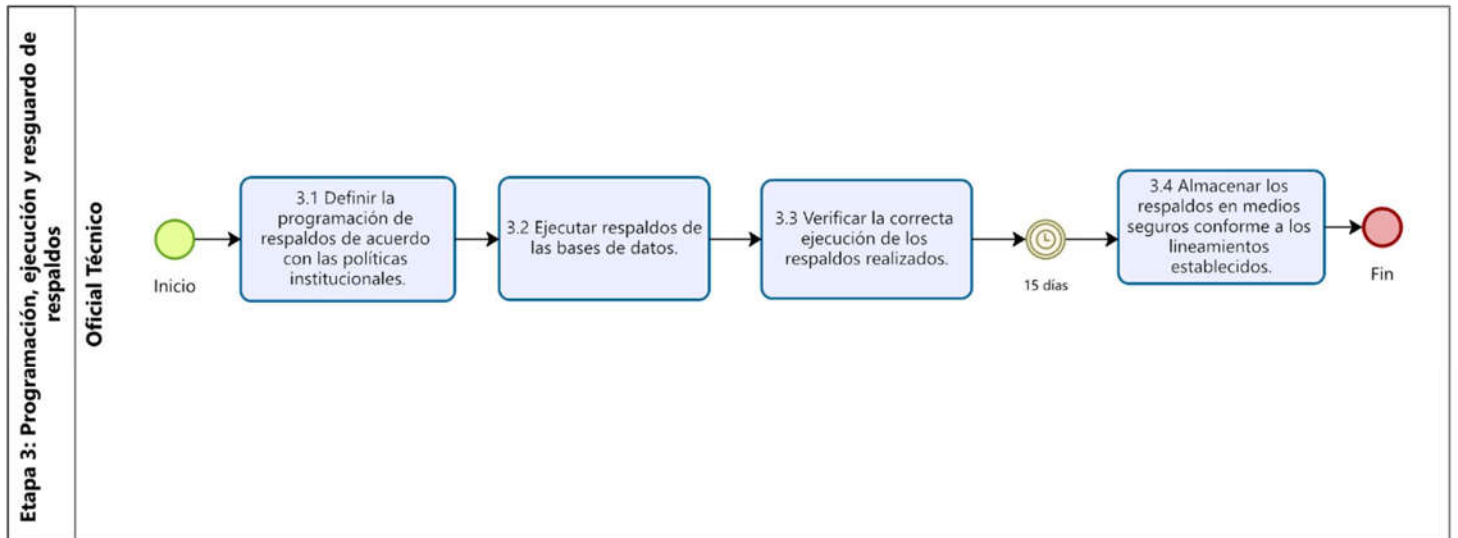
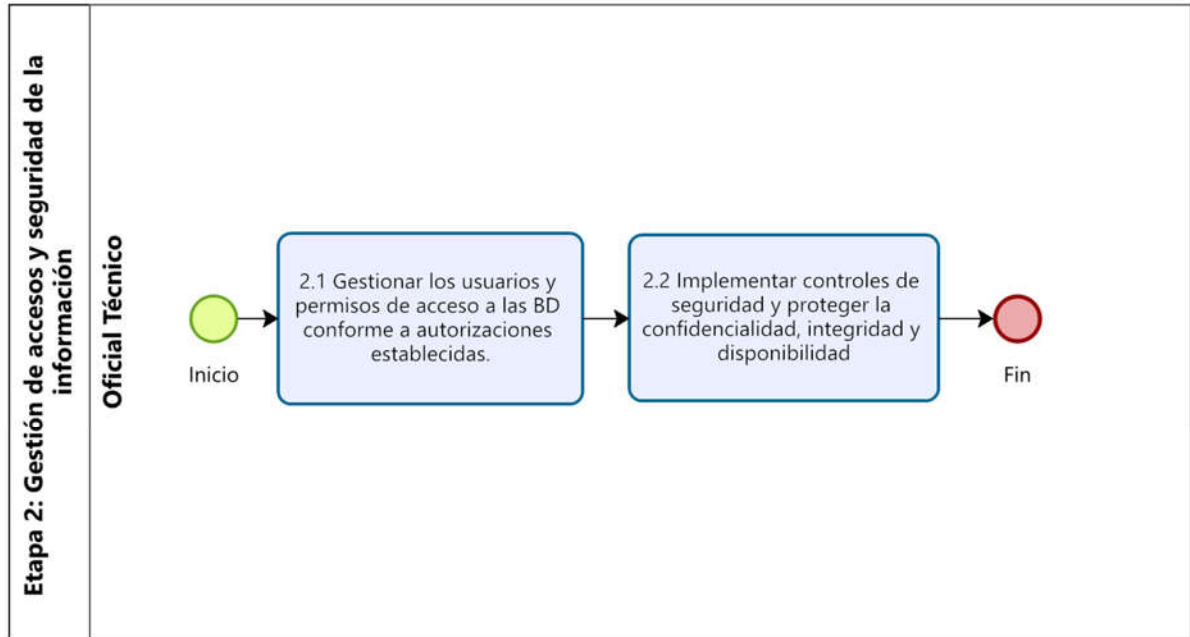
No.	Etapas del Proceso	Objetivo de la Etapa	Insumo	Actividad	Tiempo	Responsable	Producto	Envío a:			
1	Administración, configuración y optimización de bases de datos	Garantizar la disponibilidad, correcto funcionamiento y rendimiento de las bases de datos institucionales mediante su administración, configuración, monitoreo y optimización técnica.	Sistemas gestores de bases de datos (DBMS) y Sistemas de Información	1.1 Administrar las bases de datos institucionales para garantizar su disponibilidad y correcto funcionamiento.	Diario	Oficial Técnico	Control de respaldos	Subdirector de Infotecnología			
				1.2 Configurar los sistemas gestores de bases de datos conforme a los requerimientos institucionales.	Mensual						
				1.3 Monitorear el desempeño de las bases de datos para detectar problemas de rendimiento o capacidad.	Diario						
				1.4 Optimizar las bases de datos mediante ajustes en estructuras, consultas e índices.	Mensual						
2	Gestión de accesos y seguridad de la información	Controlar los usuarios, permisos y medidas de seguridad aplicables a las bases de datos, asegurando la confidencialidad, integridad y disponibilidad de la información institucional.		2.1 Gestionar los usuarios y permisos de acceso a las bases de datos conforme a autorizaciones establecidas.	Mensual	Oficial Técnico	Control de Permisos asignados o revocados	Dependencia PGR solicitante			
				2.2 Implementar controles de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información.	Mensual						
3	Programación, ejecución y resguardo de respaldos	Definir, ejecutar, verificar y almacenar los respaldos de bases de datos conforme a las políticas institucionales, reduciendo el riesgo de pérdida de información crítica.		3.1 Definir la programación de respaldos de acuerdo con las políticas institucionales.	Semanal		Oficial Técnico	Control de respaldos	Subdirector de Infotecnología		
				3.2 Ejecutar respaldos de las bases de datos (completos, diferenciales o incrementales).	Semanal						
				3.3 Verificar la correcta ejecución de los respaldos realizados.	Semanal						
				3.4 Almacenar los respaldos en medios seguros conforme a los lineamientos establecidos.	15 días						
4	Restauración, atención de incidentes, control y mejora continua	Restaurar la información y los servicios afectados por incidentes, atenderlos de manera oportuna, aplicar controles de verificación y promover la mejora continua, con el fin de asegurar la disponibilidad, integridad y continuidad operativa de los servicios institucionales.		4.1 Realizar pruebas de restauración de respaldos para validar su integridad y disponibilidad.	Semestral				Oficial Técnico	Control de respaldos	Dependencia PGR afectada
				4.2 Pruebas de restaurar bases de datos en caso de fallas, incidentes o pérdida de información	Semestral						Subdirector de Infotecnología
				4.3 Diagnosticar las causas de fallas en bases de datos.	Trimestral						Proveedores
				4.4 Escalar incidentes complejos a los proveedores cuando corresponda.	Anual						
				4.5 Registrar en control todas las operaciones realizadas sobre bases de datos y respaldos.	Semanal						Subdirector de Infotecnología
				4.6 Evaluar el cumplimiento de políticas de respaldo y seguridad.	Semanal						
				4.7 Implementar mejoras en la administración de bases de datos y gestión de respaldos.	Mensual						

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-005 Versión 1.0	Administración de Bases de Datos y Respaldos Fecha: 27 de mayo 2026	UDEM 131 de 183

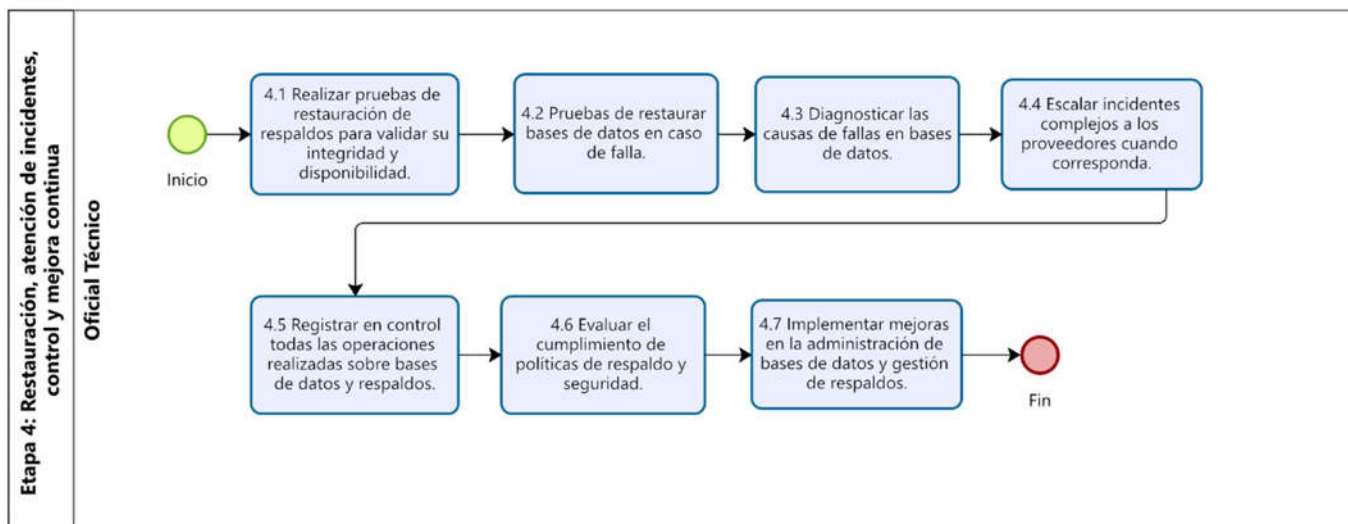
10. Diagrama de Flujo del Procedimiento



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-005 Versión 1.0	Administración de Bases de Datos y Respaldos Fecha: 27 de mayo 2026	UDEM 132 de 183



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-005 Versión 1.0	Administración de Bases de Datos y Respaldos Fecha: 27 de mayo 2026	UDEM 133 de 183



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-005 Versión 1.0	Administración de Bases de Datos y Respaldos Fecha: 27 de mayo 2026	UDEM 134 de 183

11. Gestión del Riesgo

PGR		PROCURADURÍA GENERAL DE LA REPÚBLICA								NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00		
MATRIZ PARA LA EVALUACIÓN, ANÁLISIS Y RESPUESTA A LOS RIESGOS												
Formulario 27 PGR												
PROCESO:		Administración de Bases de Datos y Respaldos										
NOMBRE DEL SUBPROCESO:		Administración de Bases de Datos y Respaldos										
OBJETIVO:		Garantizar la disponibilidad, integridad, confidencialidad y recuperación de la información institucional contenida en las bases de datos, mediante la administración eficiente, segura y controlada de los sistemas gestores de bases de datos, así como la ejecución, verificación y resguardo de los respaldos, asegurando la continuidad operativa de los servicios tecnológicos institucionales.										
(1) No.	(2) Etapa del proceso	(3) Descripción del Riesgo	Riesgo inherente		(5) Zona de Riesgo Preliminar	(7) Controles obligatorios para mitigar los riesgos	(8) Controles que existen en la entidad	(9) Controles pendientes por establecer para mitigar los riesgos	Riesgo Residual		(12) Zona de Riesgo Final	(13) Respuesta a los Riesgos
			(4) P	(5) I					(10) P	(11) I		
1	Administración, configuración y optimización de bases de datos	1.1 No tener acceso a la base de datos impidiendo la disponibilidad o rendimiento de la información, debido a que se depende de un proveedor.	1	3	M	Implementar un dominio institucional para el manejo de base de datos en el Data Center de la PGR.	Implementar un dominio institucional para el manejo de base de datos en el Data Center de la PGR.		1	2	II	Aceptar
2	Gestión de accesos y seguridad de la información	2.1 Las credenciales pueden compartirse por los usuarios, generando riesgo de accesos no autorizados.	1	1	II	Prohibir cuentas compartidas y vincular alias, bajas y modificaciones de accesos con la Gerencia de Recursos Humanos o la dependencia responsable del personal.	Prohibir cuentas compartidas y vincular alias, bajas y modificaciones de accesos con la Gerencia de Recursos Humanos o la dependencia responsable del personal.		1	1	II	Aceptar
3	Programación, ejecución y resguardo de respaldos	3.1 Los respaldos de información pueden dañarse, retrasando la restauración de la información.	1	1	II	Mantener varios respaldos de la información para garantizar la disponibilidad de los datos.	Mantener varios respaldos de la información para garantizar la disponibilidad de los datos.		1	1	II	Aceptar
4	Restauración, atención de incidentes, control y mejora continua	4.1 La información puede no recuperarse de manera completa ante fallas, errores, ataques informáticos o desastres.	1	1	II	Definir puntos de recuperación de la información.	Definir puntos de recuperación de la información.		1	1	II	Aceptar
Elaborado por:						Revisado por:			Aprobado por:			
Lisandro Alfredo Suárez Salinas Oficial Técnico Pablo Javier Padilla Avilés Oficial Técnico Cristian Alexander Martínez Ochoa Oficial Técnico Suyapa del Mar Andino Cróchez Jefa de la Unidad de Modernización						Ingrid Karina López Fuentes Directora de Administración y Finanzas Jorge Efraín Salgado Subdirector de Infotecnología			José Francisco Quintanilla Sub-Procurador General de la República Procurador General de la República			
Firma: Fecha: 19 de mayo de 2026						Firma: Fecha: 20 de mayo de 2026			Firma: Fecha: 21 de mayo de 2026			

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-005 Versión 1.0	Administración de Bases de Datos y RespalDOS Fecha: 27 de mayo 2026	UDEM 135 de 183

	PROCURADURÍA GENERAL DE LA REPÚBLICA			NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00	
	MAPA PARA LA VALORACIÓN PRELIMINAR Y FINAL DE LOS RIESGOS			Formulario 28 PGR	
PROPÓSITO: Facilitar la valoración y determinación de la zona de riesgos, de acuerdo con la explicación que consta en el Anexo 22 Instructivo para la gestión de riesgos					
PROBABILIDAD					
Muy Alta (5)	A	A	E	E	E
Alta (4)	M	A	A	E	E
Moderada (3)	B	M	A	E	E
Baja (2)	B	B	M	A	E
Muy Baja (1)	2.1 3.1 4.1 B	B	1.1 M	A	A
	Muy Bajo (1)	Bajo (2)	Moderado (3)	Alto (4)	Muy Alto(5)
IMPACTOS					
ZONA DE RIESGO:					
B: Zona de Riesgo Baja: Respuesta, Aceptar el riesgo					
M: Zona de Riesgo Moderada: Respuestas, Aceptar el riesgo o reducir el riesgo. Costo Beneficio					
A: Zona de Riesgos Alta: Respuestas, Reducir el riesgo, o evitar, o compartir, o transferir					
E: Zona de Riesgo Extrema: Respuestas, Reducir el riesgo (costo beneficio), o evitar, o compartir o transferir					

	PROCURADURÍA GENERAL DE LA REPÚBLICA	
	SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-005	Administración de Bases de Datos y Respaldos	UEM
Versión 1.0	Fecha: 27 de mayo 2026	136 de 183

12. Elementos Transversales del Procedimiento



Matriz de Verificación

Inclusión de Elementos Transversales Estratégicos

Manual de Procedimientos de la Subdirección de Infotecnología

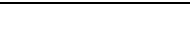
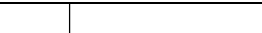


Denominación del Proceso: Administración de Bases de Datos y Respaldos			
Preguntas de Verificación	Si	No	Respuestas de Verificación
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Control Interno y anticorrupción</u> ?	X		Incluye controles de acceso, perfiles de usuario, segregación de funciones, bitácoras de cambios, autorización de respaldos y restauraciones, así como monitoreo de accesos no autorizados. Estas medidas reducen riesgos de manipulación, pérdida, alteración o uso indebido de la información institucional.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Descentralización</u> ?		X	No permite que las dependencias responsables de sistemas soliciten respaldos, restauraciones o accesos conforme a sus competencias, mientras la Subdirección de Infotecnología mantiene la administración técnica, seguridad, trazabilidad y control centralizado de las bases de datos.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Participación Ciudadana</u> ?		X	No aplica directamente, por ser un proceso técnico interno de soporte.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Transparencia y Acceso a la Información Pública</u> ?	X		Garantiza disponibilidad, integridad y trazabilidad de la información institucional contenida en las bases de datos. Facilita la generación de reportes confiables para rendición de cuentas, auditoría y atención de solicitudes de información pública, protegiendo datos reservados o sensibles.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Archivo Documental</u> ?	X		Contempla el resguardo de bitácoras, políticas de respaldo, registros de restauración, autorizaciones, reportes de incidencias, evidencias de pruebas de recuperación y documentación técnica. Esta información debe conservarse ordenada y disponible para control interno y auditoría.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al cumplimiento de los indicadores de <u>PEI Institucional</u> ?	X		Se vincula con indicadores de disponibilidad de sistemas, cumplimiento del plan de respaldos, tiempo de recuperación, integridad de datos, continuidad operativa y reducción de incidentes tecnológicos. Estos indicadores apoyan la modernización, eficiencia y seguridad institucional.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-005 Versión 1.0	Administración de Bases de Datos y Respaldos Fecha: 27 de mayo 2026	UEM 137 de 183

13. Bibliografía

- Carbonell, M. (2019). *Teoría del derecho*. Porrúa.
- Departamento Administrativo de la Función Pública. (2025)). *Obtenido de Política de respaldo y recuperación de la información*: <https://www1.funcionpublica.gov.co>
- Microsoft. (s.f.). *Back up and restore of SQL Server databases*. Obtenido de 2024: <https://learn.microsoft.com>
- Real Academia Española. (2023). *Obtenido de Diccionario de la lengua española (23.^a ed.)*: <https://dle.rae.es>
- Red de Responsables TIC – UNAM. (s.f.). *Obtenido de Lineamientos y recomendaciones para la administración de bases de datos*: . <https://www.red-tic.unam.mx>
- Unidad Administrativa Especial de Alimentación Escolar. (2021). *Obtenido de Política de respaldo, custodia y/o restauración de información.*: <https://www.alimentosparaaprender.gov.co>

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-005	Administración de Bases de Datos y Respaldos	UEM
Versión 1.0	Fecha: 27 de mayo 2026	138 de 183

14. Anexos

14.1. F-SDIT-011 Control de respaldos

[illegible]

14.2. F-SDIT-012 Control de permisos asignados o revocados

[illegible]

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-005 Versión 1.0	Administración de Bases de Datos y Respaldos Fecha: 27 de mayo 2026	UEM 139 de 183

15. Control de Cambios al Procedimiento

Historial de Cambios al Procedimiento

Fecha	Versión	Autor		Descripción del cambio	Cambio Autorizado por:	
		Cargo	Área		Cargo	Firma

PROCURADURÍA GENERAL DE LA REPÚBLICA

SUBDIRECCIÓN DE INFOTECNOLOGÍA

PROCEDIMIENTO SEGURIDAD TECNOLÓGICA Y CONTROL DE ACCESO

**CÓDIGO
PR-SDIT-006**

29 DE MAYO DE 2026

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UDEM 141 de 183

Responsables de los Cambios al Procedimiento

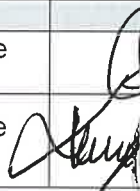
Elaboración del Documento

Elaborado por:	Cargo	Área de Trabajo	Fecha	Firma
Suyapa del Mar Andino Ordóñez	Jefa de Unidad	Unidad de Modernización	29 de mayo de 2026	

Revisión del Documento

Revisado por:	Cargo	Área de Trabajo	Fecha	Firma
Pablo Javier Padilla Avilés	Oficial Técnico	Subdirección de Infotecnología	01 de junio de 2026	

Verificación del Documento

Verificado por:	Cargo	Área de Trabajo	Fecha	Firma
Jorge Efrain Salgado	Subdirector de Infotecnología	Subdirección de Infotecnología	02 de junio de 2026	
Ingrid Karina López Fuentes	Directora	Dirección de Administración y Finanzas	02 de junio de 2026	

Aprobación del Documento

Aprobado por:	Cargo	Área de Trabajo	Fecha	Firma
José Francisco Quiroz Mejía	Sub-Procurador General de la República	Despacho de la Sub-Procuraduría General de la República	04 de junio de 2026	

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UEM 142 de 183

Tabla de Contenido

1. Objetivo del Procedimiento	143
2. Alcance del Procedimiento.....	143
3. Marco Legal del Procedimiento	143
4. Políticas y Lineamientos del Procedimiento.....	143
5. Responsables del Procedimiento.....	144
6. Insumos del Procedimiento.....	144
7. Productos o Resultados del Procedimiento.....	145
8. Definición de Glosario de Términos, Siglas y Abreviaturas	145
9. Descripción del Procedimiento	146
10. Diagrama de Flujo del Procedimiento	151
11. Gestión del Riesgo	154
12. Elementos Transversales del Procedimiento	156
13. Bibliografía	157
14. Anexos.....	158
15. Control de Cambios al Procedimiento.....	160

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UDEM 143 de 183

1. Objetivo del Procedimiento

Proteger los sistemas, activos tecnológicos e información institucional mediante el control de accesos y la aplicación de medidas de seguridad tecnológica, para prevenir riesgos y fortalecer el control interno.

2. Alcance del Procedimiento

El presente proceso comprende la administración de accesos a sistemas, plataformas, equipos y recursos tecnológicos institucionales, así como la ejecución de controles de seguridad tecnológica sobre usuarios, credenciales, dispositivos y servicios, incluyendo el registro, monitoreo, revisión, actualización y revocación de accesos, así como la atención y documentación de incidentes de seguridad, conforme a la normativa aplicable.

3. Marco Legal del Procedimiento

No.	Código	Documento
1	Decreto 131-82	Constitución de la República
2	Decreto 74-61	Ley Orgánica de la Procuraduría General de la República
3	Decreto 146-86	Ley General de la Administración Pública
4	N/A	Normativas y Marcos de Referencia de Ciberseguridad
5	NIST	Cybersecurity Framework.
6	OWASP ASVS	Application Security Verification Standard.
7	ISO 27001-019	Sistema de Gestión de Seguridad de la Información.

4. Políticas y Lineamientos del Procedimiento

- 4.1. Toda la información institucional deberá protegerse garantizando su confidencialidad, integridad y disponibilidad, conforme a la normativa vigente.
- 4.2. El acceso a sistemas, equipos, redes e información se otorgará únicamente según las funciones y responsabilidades del puesto del usuario.
- 4.3. Cada usuario es responsable del uso adecuado, ético y seguro de los recursos tecnológicos que le sean asignados.
- 4.4. La institución implementará medidas preventivas, correctivas y de control para reducir riesgos tecnológicos y accesos no autorizados.
- 4.5. Todo acceso a sistemas deberá contar con autorización formal del jefe inmediato y validación de la Subdirección de Infotecnología.
- 4.6. Las credenciales de acceso (usuario y contraseña) son personales e intransferibles, por esto queda prohibido compartir contraseñas o utilizar credenciales de otros usuarios.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UDEM 144 de 183

- 4.7. El usuario deberá cambiar su contraseña cuando el sistema lo solicite o ante una sospecha de compromiso.
- 4.8. Los accesos deberán ser suspendidos o eliminados de forma inmediata cuando el usuario cambie de funciones, se ausente prolongadamente o finalice su relación laboral.
- 4.9. Los recursos tecnológicos (equipos, sistemas, redes, correo institucional) deberán utilizarse exclusivamente para fines institucionales.
- 4.10. Se prohíbe instalar software no autorizado, conectar dispositivos externos sin permiso o realizar acciones que pongan en riesgo la seguridad tecnológica.
- 4.11. El usuario deberá resguardar la información y evitar su divulgación, alteración o pérdida sin autorización.
- 4.12. Todo incidente o sospecha de violación de seguridad tecnológica deberá ser reportado de forma inmediata al área responsable.

5. Responsables del Procedimiento

Área	Puesto de Trabajo	Responsabilidad
Subdirección de Infotecnología	Subdirector(a)	Autorizar el acceso a sistemas, información y áreas restringidas según las funciones del personal. He de asegurar que se cumplan las políticas y lineamientos de seguridad tecnológica. Apoyar la toma de decisiones ante incidentes o riesgos relevantes de seguridad.
Subdirección de Infotecnología	Oficial Técnico	Ejecutar las actividades operativas de seguridad tecnológica y control de accesos. Administrar usuarios, permisos y credenciales en los sistemas institucionales. Vigilar el uso adecuado de los recursos tecnológicos y detectar accesos no autorizados. Reportar y apoyar en la atención de incidentes de seguridad tecnológica.

6. Insumos del Procedimiento

Código	Insumos	Lugar de Guarda	Tiempo de Guarda
M- PGR-SDIT-XXX-202X	Memorándum	Subdirección de Infotecnología	5 años
N/A	Sistema de ticket	Subdirección de Infotecnología	5 años
N/A	Buscadores u OSINT	Subdirección de Infotecnología	5 años

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UDEM 145 de 183

7. Productos o Resultados del Procedimiento

Código	Productos	Lugar de Guarda	Tiempo de Guarda
F-SDIT-013	Bitácoras y registros actualizados de accesos y cambios realizados.	Archivo Institucional	5 años
F-SDIT-014	Reportes de revisión periódica de usuarios, perfiles y privilegios.	Archivo Institucional	5 años
F-SDIT-015	Reportes periódicos de control de accesos y seguridad tecnológica.	Archivo Institucional	5 años

8. Definición de Glosario de Términos, Siglas y Abreviaturas

8.1. Términos

Acceso: Permiso otorgado a un usuario para ingresar, utilizar o interactuar con sistemas, información, recursos tecnológicos o áreas físicas, de acuerdo con su autorización y nivel asignado. (Microsoft, s.f.)

Control de Acceso: Conjunto de medidas y mecanismos que permiten autorizar, limitar o negar el ingreso de personas o el uso de recursos físicos y digitales, garantizando que solo usuarios autorizados tengan acceso. (López, s.f.)

Control de Acceso Físico: Medidas de seguridad destinadas a regular y supervisar la entrada y salida de personas a instalaciones, áreas restringidas o espacios donde se resguardan activos e infraestructura tecnológica. (Clave Ciberseguridad., s.f.)

Credenciales de Acceso: Conjunto de datos utilizados para verificar la identidad de un usuario y permitir su acceso a sistemas o servicios, generalmente compuesto por nombre de usuario y contraseña, y en algunos casos factores adicionales de autenticación. (Fortinet, s.f.)

Gestión de Accesos: Proceso mediante el cual se administran, controlan y supervisan los permisos de los usuarios para acceder a recursos tecnológicos, garantizando que solo cuenten con los privilegios necesarios para el desempeño de sus funciones. (IBM, s.f.)

Incidente de Seguridad: Evento que compromete o pone en riesgo la confidencialidad, integridad o disponibilidad de la información o de los sistemas tecnológicos, como accesos no autorizados, pérdida de información o ataques informáticos. (Banco Santander, s.f.)

Memorándum: Comunicación escrita breve utilizada en el ámbito institucional o empresarial para informar, recordar o instruir sobre asuntos específicos. (Real Academia Española, 2023)

Normativa: Conjunto de normas jurídicas que regulan una materia específica dentro de un ordenamiento legal. (Carbonell, 2019)

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UEM 146 de 183

Seguridad Tecnológica: Conjunto de medidas, políticas y controles orientados a proteger los recursos tecnológicos, sistemas de información e infraestructura digital frente a accesos no autorizados, daños, pérdidas o amenazas internas y externas. (IBM, s.f.)

Usuario Autorizado: Persona que ha sido formalmente aprobada para acceder y utilizar sistemas, información o áreas restringidas, de acuerdo con las políticas de seguridad de la información y las funciones asignadas a su puesto. (IBM., s.f.)

8.2. Siglas

ISO: International Organization for Standardization

NIST: National Institute of Standards and Technology

PGR: Procuraduría General de la República.

SDIT: Subdirección de Infotecnología.

TIC: Tecnologías de la Información y la Comunicación.

UEM: Unidad de Modernización

9. Descripción del Procedimiento

Oficial Técnico

- 9.1. Recibir solicitudes de creación, modificación, suspensión o cancelación de accesos a sistemas, plataformas, equipos o servicios tecnológicos. Esta actividad inicia el procedimiento y permite identificar la necesidad de acceso del usuario. Las solicitudes pueden recibirse por los medios institucionales establecidos (formato, correo, sistema). Se verifica que la solicitud contenga la información mínima requerida para su análisis.
- 9.2. Verificar que la solicitud esté debidamente justificada, autorizada y respaldada por la dependencia competente. Se revisa que la solicitud cuente con la aprobación del jefe inmediato o autoridad competente. Se valida que la justificación esté relacionada con funciones laborales reales. Las solicitudes incompletas o no autorizadas no continúan el proceso.
- 9.3. Validar el perfil, rol y nivel de acceso requerido conforme a las funciones del usuario solicitante. Se analiza el puesto del usuario y sus responsabilidades institucionales. Se determina el tipo de acceso necesario para el cumplimiento de sus funciones. Se evita otorgar accesos innecesarios o superiores a los requeridos

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UEM 147 de 183

- 9.4. Determinar si el acceso solicitado procede de acuerdo con las políticas y controles institucionales. Se revisa la solicitud conforme a las políticas de seguridad tecnológica vigentes. Se verifica que el acceso no represente un riesgo para la información institucional. En caso de no proceder, se informa a la dependencia solicitante.
- 9.5. Crear usuarios y credenciales en los sistemas, plataformas o recursos tecnológicos autorizados. Se registra al usuario en el sistema correspondiente de manera controlada. Se generan credenciales únicas conforme a los estándares de seguridad. La creación del usuario se documenta para fines de control y auditoría.
- 9.6. Asignar perfiles, privilegios y permisos de acceso según el nivel autorizado. Se configuran los permisos de acuerdo con el perfil aprobado. Se aplican los principios de mínimo privilegio y segregación de funciones. Se verifica que los accesos asignados funcionen correctamente.
- 9.7. Analizar la configuración y controles de seguridad sobre contraseñas, sesiones, autenticación y restricciones de acceso. Se valida que las contraseñas cumplan los criterios de seguridad establecidos. Se revisan los tiempos de sesión y mecanismos de autenticación. Se aplican restricciones adicionales cuando el nivel de riesgo lo amerita.
- 9.8. Entregar al usuario las credenciales o instrucciones de acceso bajo los mecanismos institucionales definidos. Las credenciales se entregan por medios seguros y autorizados. Se brindan instrucciones claras sobre el uso adecuado del acceso. Se recuerda al usuario su responsabilidad sobre la confidencialidad de las credenciales.
- 9.9. Restablecer contraseñas o accesos cuando exista solicitud debidamente autorizada. Se valida la identidad del solicitante antes de realizar el restablecimiento. Se genera una nueva contraseña conforme a los estándares de seguridad. Se notifica al usuario una vez realizado el restablecimiento.
- 9.10. Modificar privilegios de acceso cuando exista cambio de puesto, funciones, dependencia o nivel de responsabilidad. Se recibe la notificación oficial del cambio organizacional. Se ajustan los accesos conforme a las nuevas funciones asignadas. Se documentan los cambios realizados para control interno.
- 9.11. Suspender o cancelar accesos de usuarios desvinculados, trasladados o con cambios de función. Se actúa de forma inmediata para evitar accesos no autorizados. Se eliminan o suspenden credenciales que ya no sean necesarias. Esta actividad reduce riesgos de seguridad de la información.
- 9.12. Monitorear el uso de accesos y eventos de seguridad en sistemas, equipos o servicios tecnológicos. Se revisan registros de acceso y actividad de los usuarios. Se identifican comportamientos inusuales o fuera de lo autorizado. El monitoreo permite detectar riesgos de manera oportuna.
- 9.13. Identificar y analizar accesos no autorizados, perfiles incompatibles, intentos fallidos o incidentes de seguridad. Se analizan alertas y registros generados por los sistemas. Se determina la causa del evento o incidente detectado. Se documentan los hallazgos para su seguimiento.
- 9.14. Atender incidentes relacionados con accesos, credenciales o uso indebido de recursos tecnológicos. Se aplican acciones inmediatas para contener el incidente. Se coordinan acciones con las áreas correspondientes cuando sea necesario. Se restablece la seguridad del sistema afectado.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UEM 148 de 183

- 9.15. Aplicar medidas correctivas o preventivas ante hallazgos de seguridad o desviaciones de control. Se fortalecen controles para evitar la recurrencia del incidente, revisando periódicamente los permisos, perfiles y privilegios asignados a los usuarios. A la vez se identifican accesos innecesarios o desactualizados. Esta actividad fortalece el control y la seguridad institucional y las medidas aplicadas quedan debidamente documentadas.
- 9.16. Revisar periódicamente los permisos, perfiles y privilegios asignados a los usuarios. Se realizan revisiones programadas de accesos activos. Se identifican accesos innecesarios o desactualizados. Esta actividad fortalece el control y la seguridad institucional.
- 9.17. Depurar usuarios inactivos, duplicados o con accesos improcedentes. Se identifican cuentas sin uso o duplicadas en los sistemas. Se procede a su eliminación o bloqueo según corresponda. La depuración reduce riesgos y optimiza los recursos tecnológicos.
- 9.18. Documentar incidencias, revisiones, cambios de acceso y acciones correctivas ejecutadas. Se registra toda acción realizada durante el procedimiento. La documentación sirve como evidencia para auditorías y control interno. Se mantiene la trazabilidad de las decisiones tomadas.
- 9.19. Emitir reportes periódicos sobre accesos otorgados, modificados, cancelados e incidentes atendidos por sistemas. Se elaboran reportes conforme a los períodos establecidos. Los reportes apoyan la toma de decisiones y la supervisión. La información se remite a las autoridades correspondientes.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UEM 149 de 183



Matriz de Actividades, Responsables y Formularios
Manual de Procedimientos de la Subdirección de Infotecnología
Proceso de Seguridad Tecnológica y Control de Acceso



No.	Etapas del Proceso	Objetivo de la Etapa	Insumo	Actividad	Tiempo	Responsable	Producto	Envío a:		
1	Recepción, validación y autorización de solicitudes de acceso	Asegurar que toda solicitud de creación, modificación, suspensión o cancelación de acceso esté debidamente justificada, autorizada y alineada con las funciones del usuario y las políticas institucionales.	Memorándum, correos, ticks, buscadores u OSINT	1.1 Recibir solicitudes de creación, modificación, suspensión o cancelación de accesos a sistemas, plataformas, equipos o servicios tecnológicos.	5 min	Oficial Técnico de Infotecnología	Bitácoras y registros actualizados de accesos y cambios realizados.	Oficial Técnico de Infotecnología		
				1.2 Verificar que la solicitud esté debidamente justificada, autorizada y respaldada por la dependencia competente.	5 min			Dependencia PGR solicitante		
				1.3 Validar el perfil, rol y nivel de acceso requerido conforme a las funciones del usuario solicitante.	10 min			Subdirector de Infotecnología		
				1.4 Determinar si el acceso solicitado procede de acuerdo con las políticas y controles institucionales.	5 min					
2	Creación, configuración y entrega segura de acceso	Crear usuarios, credenciales y permisos conforme al nivel autorizado, aplicando configuraciones de seguridad sobre contraseñas, sesiones, autenticación y restricciones de acceso.		2.1 Crear usuarios y credenciales en los sistemas, plataformas o recursos tecnológicos autorizados.	5 min		Oficial Técnico de Infotecnología	Bitácoras y registros actualizados de accesos y cambios realizados.	Oficial Técnico de Infotecnología	
				2.2 Asignar perfiles, privilegios y permisos de acceso según el nivel autorizado.	15 min					
				2.3 Analizar la configuración, controles de seguridad sobre contraseñas, sesiones, autenticación y restricciones de acceso.	1 hora					
				2.4 Entregar al usuario las credenciales o instrucciones de acceso bajo los mecanismos institucionales definidos.	5 min			Reportes de revisión periódica de usuarios, perfiles y privilegios.		
3	Modificación, restablecimiento, suspensión y cancelación de accesos	Mantener actualizados los accesos de los usuarios conforme a cambios de puesto, funciones, dependencia, desvinculación o solicitud autorizada.		3.1 Restablecer contraseñas o accesos cuando exista solicitud debidamente autorizada.	5 min			Oficial Técnico de Infotecnología		Dependencia PGR solicitante
				3.2 Modificar privilegios de acceso cuando exista cambio de puesto, funciones, dependencia o nivel de responsabilidad.	15 min					
				3.3 Suspender o cancelar accesos de usuarios desvinculados, trasladados o con cambios de función.	5 min					
				4.1 Monitorear el uso de accesos y eventos de seguridad en sistemas, equipos o servicios tecnológicos.	30 min				Reportes periódicos de	Oficial Técnico de Infotecnología
				4.2 Identificar y analizar el accesos no autorizados, perfiles incompatibles, intentos fallidos o incidentes de seguridad.	1 hora					
				4.3 Atender incidentes relacionados con accesos, credenciales o uso indebido de recursos tecnológicos.	15 min					

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006	Seguridad Tecnológica y Control de Acceso	UEM
Versión 1.0	Fecha: 29 de mayo 2026	150 de 183



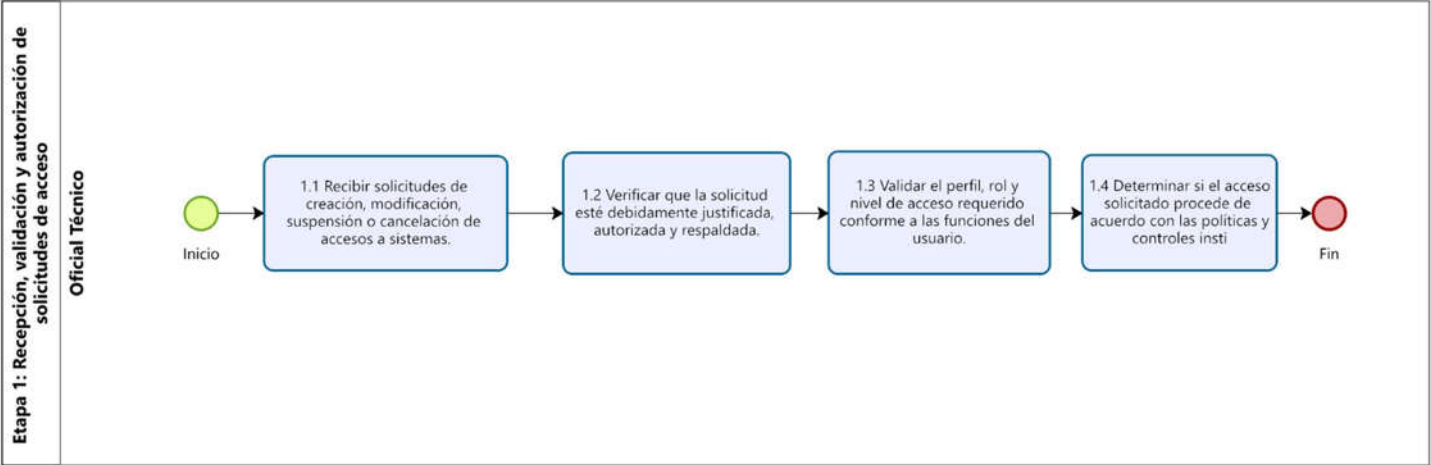
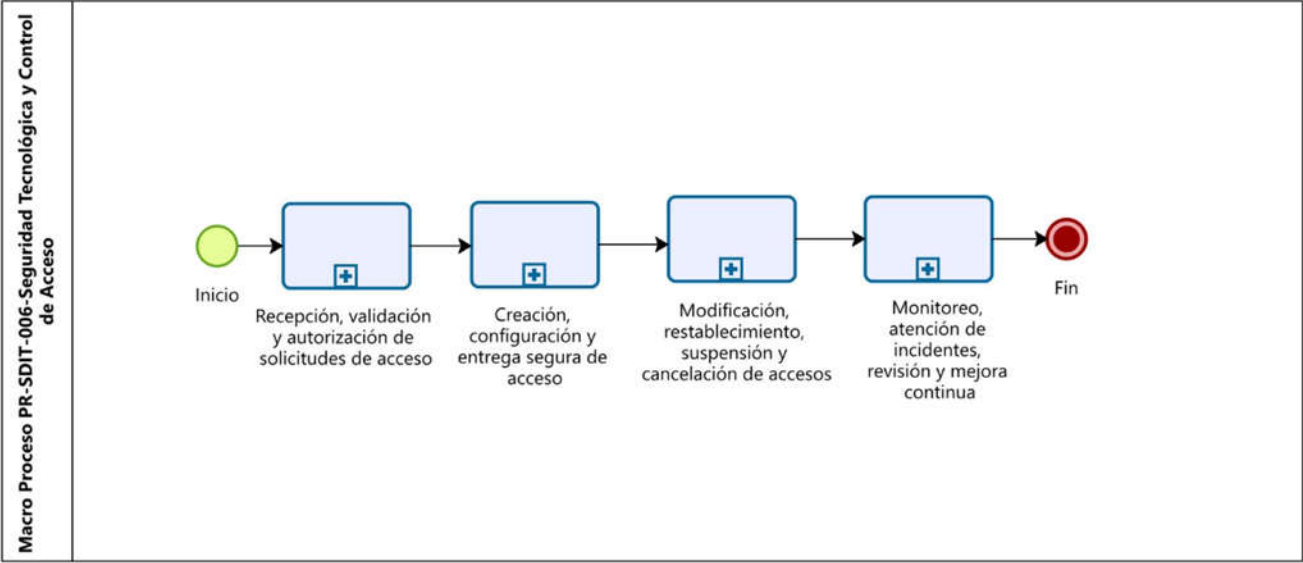
Matriz de Actividades, Responsables y Formularios
Manual de Procedimientos de la Subdirección de Infotecnología
Proceso de Seguridad Tecnológica y Control de Acceso



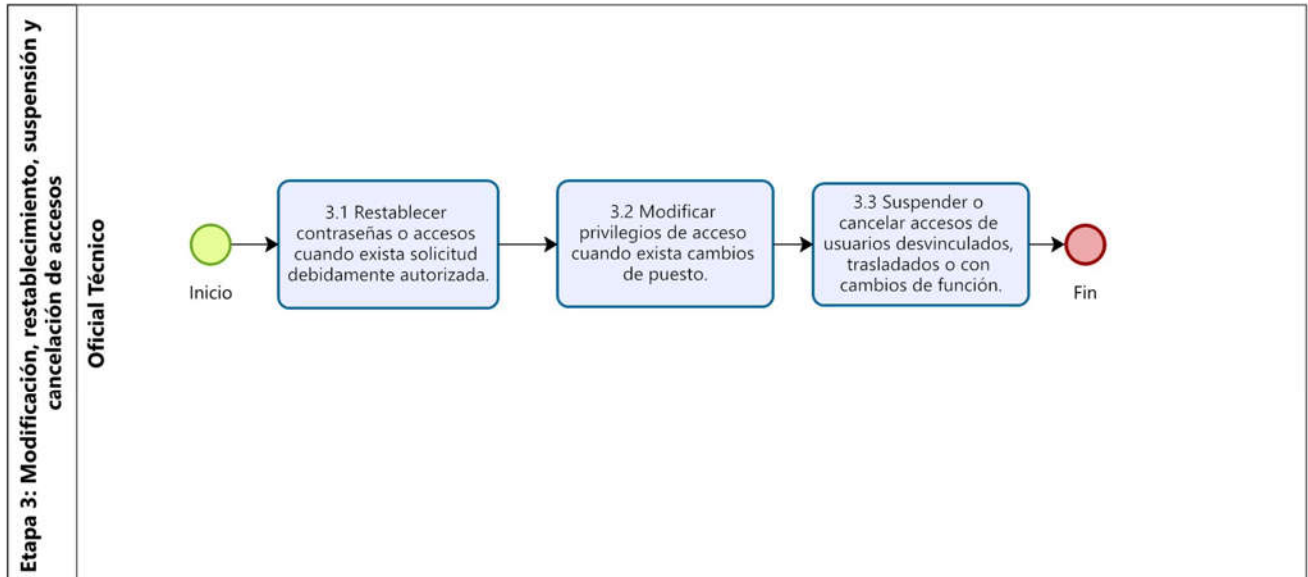
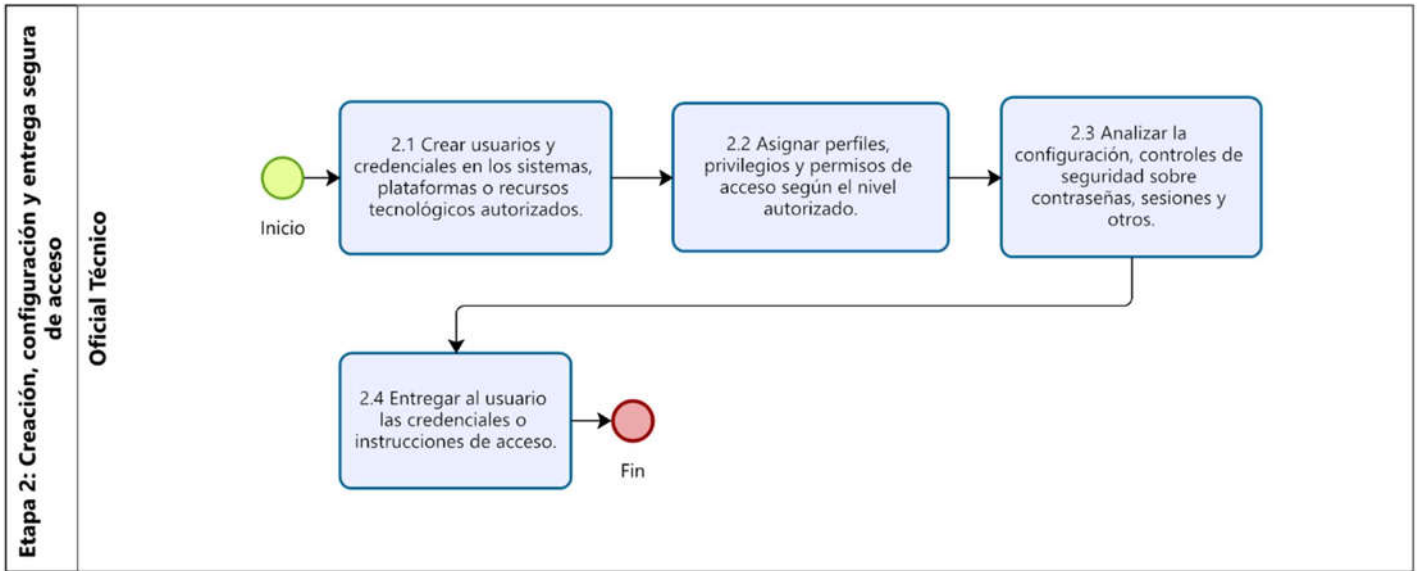
No.	Etapas del Proceso	Objetivo de la Etapa	Insumo	Actividad	Tiempo	Responsable	Producto	Envío a:
4	Monitoreo, atención de incidentes, revisión y mejora continua	Supervisar el uso de accesos, identificar eventos de seguridad, atender incidentes, depurar usuarios improcedentes y generar reportes para control interno y mejora continua a solicitud.		4.4 Aplicar medidas correctivas o preventivas ante hallazgos de seguridad o desviaciones de control.	1 hora		Reportes generados de control de accesos y seguridad tecnológica.	Subdirector de Infotecnología
				4.5 Revisar periódicamente los permisos, perfiles y privilegios asignados a los usuarios.	1 hora			
				4.6 Depurar usuarios inactivos, duplicados o con accesos improcedentes.	1 hora			
				4.7 Documentar incidencias, revisiones, cambios de acceso y acciones correctivas ejecutadas.	2 horas			
				4.8 Emitir reportes periódicos sobre accesos otorgados, modificados, cancelados e incidentes atendidos por sistemas.	1 hora		Bitácoras y registros actualizados de accesos y cambios realizados.	

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UDEM 151 de 183

10. Diagrama de Flujo del Procedimiento



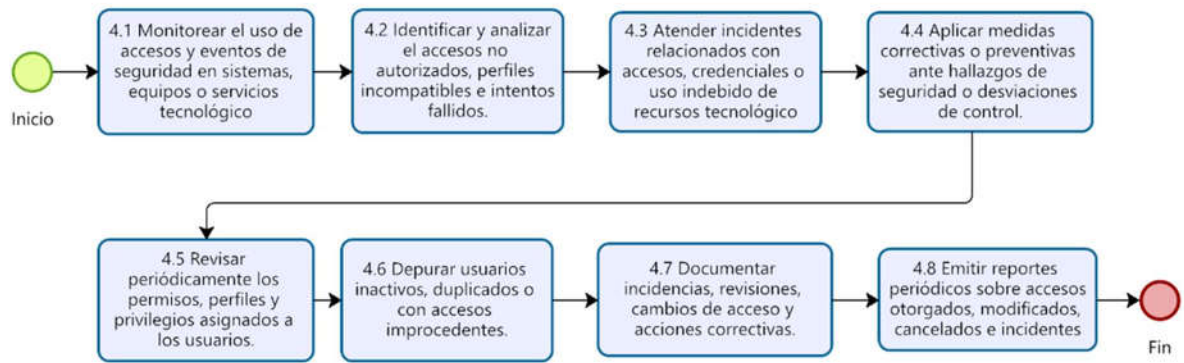
	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UDEM 152 de 183



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UDEM 153 de 183

Etapas 4: Monitoreo, atención de incidentes, revisión y mejora continua

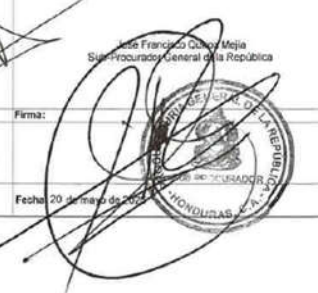
Oficial Técnico



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UDEM 154 de 183

11. Gestión del Riesgo

PGR		PROCURADURÍA GENERAL DE LA REPÚBLICA										NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00	
MATRIZ PARA LA EVALUACIÓN, ANÁLISIS Y RESPUESTA A LOS RIESGOS												Formulario 27 PGR	
PROCESO:		Seguridad Tecnológica y Control de Acceso											
NOMBRE DEL SUBPROCESO:		Seguridad Tecnológica y Control de Acceso											
OBJETIVO:		Proteger los sistemas, activos tecnológicos e información institucional mediante el control de accesos y la aplicación de medidas de seguridad tecnológica, para prevenir riesgos y fortalecer el control interno.											
(1) No.	(2) Etapa del proceso	(3) Descripción del Riesgo	Riesgo Inherente		(6) Zona de Riesgo Preliminar	(7) Controles obligatorios para mitigar los riesgos	(8) Controles que existen en la entidad	(9) Controles pendientes por establecer para mitigar los riesgos	Riesgo Residual		(12) Zona de Riesgo Final	(13) Respuesta a los Riesgos	
			(4) P	(5) I					(10) P	(11) I			
1	Recepción, validación y autorización de solicitudes de acceso	1.1 Los accesos pueden otorgarse sin justificación, autorización o documentación suficiente que respalde la solicitud.	1	3	M	Establecer formato oficial de solicitud, con firma o aprobación de la dependencia competente, justificación funcional y evidencia documental.	Establecer formato oficial de solicitud, con firma o aprobación de la dependencia competente, justificación funcional y evidencia documental.		1	2	B	Aceptar	
2	Creación, configuración y entrega segura de accesos	2.1 Las credenciales pueden entregarse sin contar con la información completa para el acceso.	1	3	M	Entregar credenciales mediante canales institucionales seguros y dejar constancia de la entrega, mediante un memorándum o correo electrónico.	Entregar credenciales mediante canales institucionales seguros y dejar constancia de la entrega, mediante un memorándum o correo electrónico.		1	2	B	Aceptar	
3	Modificación, restablecimiento, suspensión y cancelación de accesos	N/A				N/A	N/A	N/A				N/A	
4	Monitoreo, atención de incidentes, revisión y mejora continua	4.1 No verificar la caducidad del licenciamiento.	1	2	B	Documentar revisiones, incidentes, accesos otorgados, modificados o cancelados, y emitir reportes periódicos para supervisión institucional.	Documentar revisiones, incidentes, accesos otorgados, modificados o cancelados, y emitir reportes periódicos para supervisión institucional.		1	1	B	Aceptar	

Elaborado por: Pablo Javier Pacilla Avilés Oficial Técnico Suyapa del Mar Andino Ordóñez Jefe de la Unidad de Modernización Firma:  Fecha: 15 de mayo de 2026	Revisado por: Ingrid Karina López Fuentes Directora de Administración y Finanzas Jorge Elmar Solís Subdirector de Informática Firma:  Fecha: 19 de mayo de 2026	Aprobado por: José Francisco Gómez Mejía Subprocurador General de la República Firma:  Fecha: 20 de mayo de 2026
--	--	--

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UDEM 155 de 183

	PROCURADURÍA GENERAL DE LA REPÚBLICA		NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00		
	MAPA PARA LA VALORACIÓN PRELIMINAR Y FINAL DE LOS RIESGOS		Formulario 28 PGR		
PROPÓSITO: Facilitar la valoración y determinación de la zona de riesgos, de acuerdo con la explicación que consta en el Anexo 22 Instructivo para la gestión de riesgos					
PROBABILIDAD					
Muy Alta (5)	A	A	E	E	E
Alta (4)	M	A	A	E	E
Moderada (3)	B	M	A	E	E
Baja (2)	B	B	M	A	E
Muy Baja (1)	B	4.1 B	1.1 2.1 y 2.2 3.1 M	A	A
	Muy Bajo (1)	Bajo (2)	Moderado (3)	Alto (4)	Muy Alto(5)
IMPACTOS					
ZONA DE RIESGO:					
B: Zona de Riesgo Baja: Respuesta, Aceptar el riesgo					
M: Zona de Riesgo Moderada: Respuestas, Aceptar el riesgo o reducir el riesgo. Costo Beneficio					
A: Zona de Riesgos Alta: Respuestas, Reducir el riesgo, o evitar, o compartir, o transferir					
E: Zona de Riesgo Extrema: Respuestas, Reducir el riesgo (costo beneficio), o evitar, o compartir o transferir					

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UEM 156 de 183

12. Elementos Transversales del Procedimiento



Matriz de Verificación

Inclusión de Elementos Transversales Estratégicos

Manual de Procedimientos de la Subdirección de Infotecnología

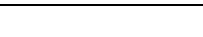
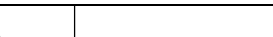


Denominación del Proceso: Seguridad Tecnológica y Control de Acceso			
Preguntas de Verificación	Si	No	Respuestas de Verificación
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Control Interno y anticorrupción</u> ?	X		El proceso incorpora controles de acceso por perfiles, segregación de funciones y autorización formal para usuarios privilegiados. Se mantienen bitácoras de accesos, cambios, incidentes y respaldos para asegurar trazabilidad. Estas medidas reducen riesgos de uso indebido de la información, manipulación no autorizada y abuso de privilegios.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Descentralización</u> ?		X	La Subdirección de Infotecnología, administra y mantiene el control técnico, pero las áreas responsables validan la necesidad funcional de cada permiso.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Participación Ciudadana</u> ?		X	No aplica de forma directa, debido a que el proceso es de carácter técnico interno.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Transparencia y Acceso a la Información Pública</u> ?	X		El proceso protege la integridad, disponibilidad y confidencialidad de la información pública administrada en los sistemas institucionales. Se aplican controles para evitar alteraciones, pérdidas o accesos indebidos a bases de datos y repositorios de información.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Archivo Documental</u> ?	X		El proceso contempla el resguardo de evidencias documentales como solicitudes de acceso, autorizaciones, bitácoras, reportes de respaldo e incidentes.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al cumplimiento de los indicadores de <u>PEI Institucional</u> ?	X		El proceso contempla el resguardo de evidencias documentales como solicitudes de acceso, autorizaciones, bitácoras, reportes de respaldo e incidentes.

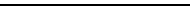
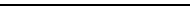
	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UDEM 157 de 183

13. Bibliografía

- Banco Santander. (s.f.). Obtenido de ¿Qué es un incidente de seguridad? : <https://www.bancosantander.es/glosario/incidente-seguridad> [bancosantander.es]
- Carbonell, M. (2019). Teoría del derecho. Porrúa.
- Clave Ciberseguridad. (s.f.). Obtenido de Control de acceso físico: importancia y definición actual.: <https://claveciberseguridad.com/infraestructura/control-de-acceso-fisico-importancia-y-definicion-actual/>
- Fortinet. (s.f.). Obtenido de ¿Qué son las credenciales de inicio de sesión? : <https://www.fortinet.com/lat/resources/cyberglossary/login-credentials>
- IBM. (s.f.). Obtenido de ¿Qué es la gestión de accesos? : <https://www.ibm.com/es-es/think/topics/access-management>
- IBM. (s.f.). Obtenido de ¿Qué es la seguridad de TI?: <https://www.ibm.com/es-es/think/topics/it-security>
- IBM Cloud Education. (s.f.). ¿Qué es la gestión de activos de TI (ITAM)? IBM. Obtenido de <https://www.ibm.com/es-es/think/topics/it-asset-management>
- IBM. (s.f.). Obtenido de ¿Qué es la seguridad de la información (InfoSec)? : <https://www.ibm.com/mx-es/think/topics/information-security>
- López, J. (s.f.). Obtenido de Control de acceso: definición, tipos y características: <https://definicion.de/control-de-acceso/>
- Microsoft. (s.f.). Obtenido de ¿Qué es el control de acceso?: <https://www.microsoft.com/es-mx/security/business/security-101/what-is-access-control>
- Real Academia Española. (2023). Obtenido de Diccionario de la lengua española (23.^a ed.): <https://dle.rae.es>

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006	Seguridad Tecnológica y Control de Acceso	UEM
Versión 1.0	Fecha: 29 de mayo 2026	158 de 183

[illegible]

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UEM 159 de 183

14.3. F-SDIT-015 Reportes periódicos de control de accesos y seguridad tecnológica

[illegible]

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-006 Versión 1.0	Seguridad Tecnológica y Control de Acceso Fecha: 29 de mayo 2026	UEM 160 de 183

15. Control de Cambios al Procedimiento

Historial de Cambios al Procedimiento

Fecha	Versión	Autor		Descripción del cambio	Cambio Autorizado por:	
		Cargo	Área		Cargo	Firma

PROCURADURÍA GENERAL DE LA REPÚBLICA

SUBDIRECCIÓN DE INFOTECNOLOGÍA

PROCEDIMIENTO SOPORTE TECNOLÓGICO A OFICINAS REGIONALES

**CÓDIGO
PR-SDIT-007**

01 DE JUNIO DE 2026

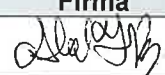
 PGR PROCURADURÍA GENERAL DE LA REPÚBLICA	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 162 de 183

Responsables de los Cambios al Procedimiento

Elaboración del Documento

Elaborado por:	Cargo	Área de Trabajo	Fecha	Firma
Suyapa del Mar Andino Ordóñez	Jefa de Unidad	Unidad de Modernización	01 de junio de 2026	 

Revisión del Documento

Revisado por:	Cargo	Área de Trabajo	Fecha	Firma
Abel Fernando Perez Vargas	Auxiliar Técnico	Subdirección de Infotecnología	02 de junio de 2026	
Daniel Isaac Membreño Anariba	Auxiliar Técnico	Subdirección de Infotecnología	02 de junio de 2026	

Verificación del Documento

Verificado por:	Cargo	Área de Trabajo	Fecha	Firma
Jorge Efrain Salgado	Subdirector de Infotecnología	Subdirección de Infotecnología	03 de junio de 2026	
Ingrid Karina López Fuentes	Directora	Dirección de Administración y Finanzas	03 de junio de 2026	 

Aprobación del Documento

Aprobado por:	Cargo	Área de Trabajo	Fecha	Firma
José Francisco Quiroz Mejía	Sub-Procurador General de la República	Despacho de la Sub-Procuraduría General de la República	05 de junio de 2026	 

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UEM 163 de 183

Tabla de Contenido

1.	Objetivo del Procedimiento	164
2.	Alcance del Procedimiento	164
3.	Marco Legal del Procedimiento	164
4.	Políticas y Lineamientos del Procedimiento	164
5.	Responsables del Procedimiento	165
6.	Insumos del Procedimiento	166
7.	Productos o Resultados del Procedimiento	166
8.	Definición de Glosario de Términos, Siglas y Abreviaturas	166
9.	Descripción del Procedimiento	168
10.	Diagrama de Flujo del Procedimiento	170
11.	Gestión del Riesgo	173
12.	Elementos Transversales del Procedimiento	175
13.	Bibliografía	176
14.	Anexos	177
15.	Control de Cambios al Procedimiento	183

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 164 de 183

1. Objetivo del Procedimiento

Brindar soporte tecnológico a las oficinas regionales para resolver problemas con equipos, sistemas y redes, de manera oportuna, asegurando que puedan operar de forma continua y eficiente.

2. Alcance del Procedimiento

Este proceso inicia cuando una oficina regional solicita soporte técnico o reporta un problema tecnológico, y finaliza cuando el problema ha sido resuelto o la solicitud ha sido atendida satisfactoriamente o se realiza el dictamen técnico.

3. Marco Legal del Procedimiento

No.	Código	Documento
1	Decreto 131-82	Constitución de la República
2	Decreto 74-61	Ley Orgánica de la Procuraduría General de la República
3	Decreto 146-86	Ley General de la Administración Pública
4	N/A	Modelo OSI
5	ISO 27000	Seguridad de la Información.

4. Políticas y Lineamientos del Procedimiento

4.1. Alcance del soporte

El servicio de soporte técnico se brindará exclusivamente a los usuarios internos de la institución, en relación con los equipos, sistemas, aplicaciones y servicios tecnológicos oficialmente autorizados.

4.2. Canales oficiales de solicitud

- Toda solicitud de soporte técnico deberá ser registrada a través de los canales oficiales definidos por la Subdirección de Infotecnología por el sistema de tickets.
- No se atenderán solicitudes verbales o informales que no cuenten con registro oficial, salvo autorización expresa de la Subdirección de Infotecnología.

4.3. Registro y trazabilidad

- Cada solicitud de soporte técnico deberá quedar debidamente registrada, asignándose un número de ticket que permita su seguimiento, control y cierre.
- El registro deberá contener, como mínimo, los datos del usuario solicitante, descripción del incidente o requerimiento, fecha y hora de recepción.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 165 de 183

4.4. Priorización de solicitudes

- Las solicitudes de soporte técnico serán atendidas conforme al orden de llegada.
- Las incidencias que afecten servicios críticos institucionales tendrán prioridad sobre las solicitudes de carácter operativo o individual.

4.5. Asignación del soporte

- Las solicitudes serán asignadas al personal técnico correspondiente, de acuerdo con su especialidad, carga de trabajo y disponibilidad.
- El técnico asignado será responsable de la atención, seguimiento y cierre del ticket.

4.6. Tiempos de atención

- Los tiempos de respuesta y solución estarán sujetos a la complejidad del incidente y disponibilidad de recursos.
- La Subdirección de Infotecnología informará al usuario sobre el estado de su solicitud cuando sea requerido.

4.7. Responsabilidad del usuario

- El usuario deberá proporcionar información clara, veraz y completa sobre la falla o requerimiento presentado.
- El usuario será responsable del uso adecuado de los recursos tecnológicos asignados y de cumplir las normas y políticas institucionales de tecnología.

4.8. Cierre del servicio

Una vez solucionada la solicitud, el técnico deberá registrar las acciones realizadas y proceder al cierre del ticket.

5. Responsables del Procedimiento

Área	Puesto de Trabajo	Responsabilidad
Subdirección de Infotecnología	Subdirector(a)	Dirigir y supervisar el servicio de soporte técnico, aprobar lineamientos y asegurar que los recursos necesarios estén disponibles para una atención oportuna y eficiente.
Subdirección de Infotecnología	Auxiliar Técnico	Atender, diagnosticar y solucionar las solicitudes de soporte técnico de los usuarios, registrando las acciones realizadas y escalando los casos que lo requieran.
Subdirección de Infotecnología	Asistente Administrativo	Recibir y registrar las solicitudes de soporte técnico, asignar los tickets correspondientes y dar seguimiento administrativo hasta su cierre.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 166 de 183

6. Insumos del Procedimiento

Código	Insumos	Lugar de Guarda	Tiempo de Guarda
M- PGR-SDIT-XXX-202X	Memorándum	Subdirección de Infotecnología	5 años
N/A	Sistema de ticket	Subdirección de Infotecnología	5 años

7. Productos o Resultados del Procedimiento

Código	Productos	Lugar de Guarda	Tiempo de Guarda
N/A	Reporte de soporte técnico a regionales en el sistema de tickets o memorándum	Subdirección de Infotecnología	5 años
F-SDIT-004	Dictamen Técnico de Equipos Tecnológicos	Subdirección de Infotecnología	5 años
F-SDIT-016	Reportes periódicos de soporte a regionales de mantenimiento	Subdirección de Infotecnología	5 años
INF-SDIT-002	Informe de incidencias atendidas a regionales	Subdirección de Infotecnología	5 años

8. Definición de Glosario de Términos, Siglas y Abreviaturas

8.1. Términos

Atención Remota: Modalidad de soporte técnico que permite al personal de Infotecnología brindar asistencia a los usuarios sin desplazarse físicamente, mediante herramientas de acceso remoto y comunicación digital. (Wikipedia, 2025)

Bitácora de Soporte Técnico: Registro donde se documentan las solicitudes atendidas, acciones realizadas, fechas, responsables y resultados del servicio de soporte técnico, con fines de control y seguimiento. (HubSpot., 2024)

Confidencialidad de la Información: Principio de seguridad que garantiza que la información solo sea accesible a personas autorizadas, evitando su divulgación no autorizada durante la atención del soporte técnico. (ISO, 2022)

Escalamiento de Incidencias: Proceso mediante el cual una incidencia o solicitud técnica es transferida a un nivel superior de soporte cuando no puede ser resuelta en el nivel inicial de atención. (AXELOS, 2019).

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UEM 167 de 183

Help Desk (Mesa de Ayuda): Servicio centralizado que actúa como punto único de contacto entre los usuarios y el área de Infotecnología para la recepción, registro y seguimiento de solicitudes de soporte técnico.

Incidente Informático: Evento no planificado que interrumpe o reduce la calidad de un servicio tecnológico, afectando los sistemas, equipos o información institucional. (ISO, 2022).

Memorándum: Comunicación escrita breve utilizada en el ámbito institucional o empresarial para informar, recordar o instruir sobre asuntos específicos. (Real Academia Española, 2023)

Normativa: Conjunto de normas jurídicas que regulan una materia específica dentro de un ordenamiento legal. (Carbonell, 2019)

Nivel de Soporte: Clasificación del soporte técnico según la complejidad del incidente, que determina si la atención se realiza en primer nivel o requiere escalamiento.

Oficio: Documento formal mediante el cual una autoridad comunica decisiones, solicitudes o información a otra autoridad o entidad. (De la Torre, Técnicas de redacción jurídica, 2018)

Soporte Técnico: Conjunto de actividades orientadas a asistir a los usuarios en la solución de problemas relacionados con equipos, sistemas y servicios tecnológicos institucionales. (Definición.de. , 2024).

Ticket de Soporte Técnico: Registro electrónico que documenta una solicitud o incidencia de soporte técnico, permitiendo su control, seguimiento y cierre. (Zendesk, 2024)

8.2. Siglas

ISO: International Organization for Standardization

NIST: National Institute of Standards and Technology

PGR: Procuraduría General de la República.

SDIT: Subdirección de Infotecnología.

TIC: Tecnologías de la Información y la Comunicación.

UEM: Unidad de Modernización.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 168 de 183

9. Descripción del Procedimiento

Auxiliar Técnico

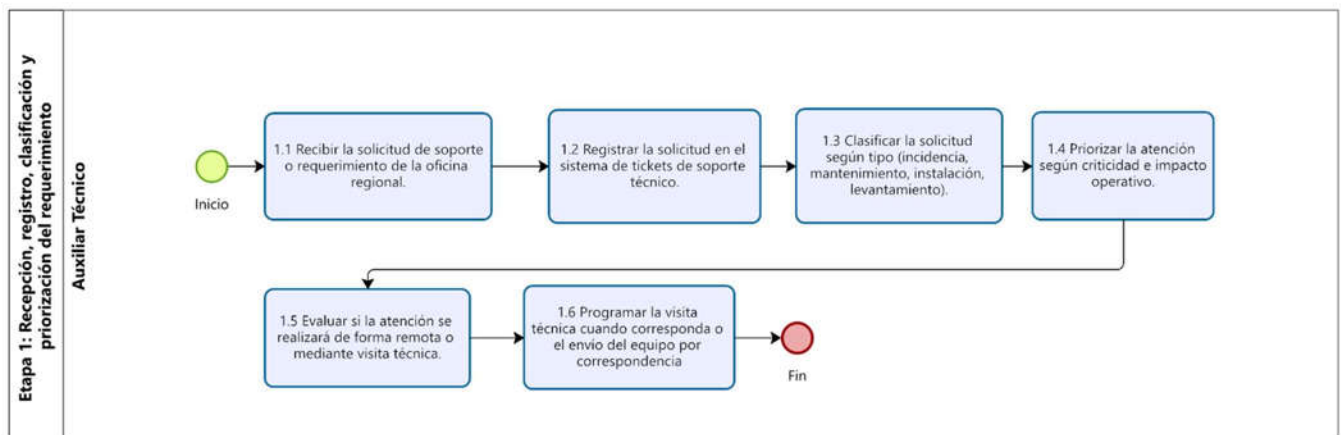
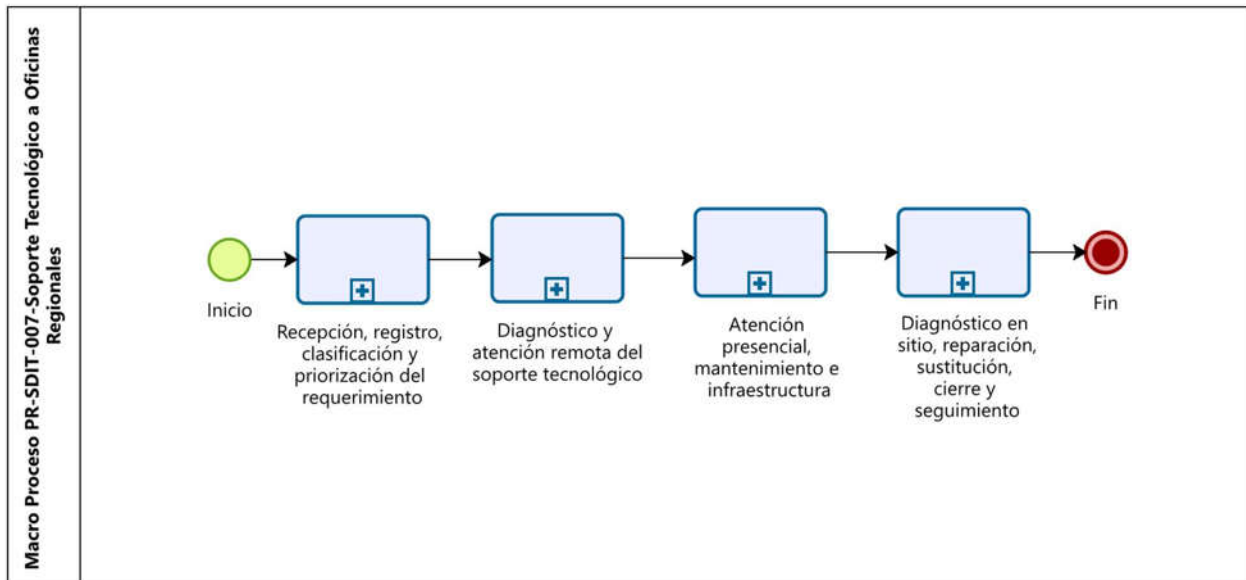
- 9.1. Recibir la solicitud o incidencia del usuario por orden de llegada (vía memorándum, sistema de tickets y correo electrónico), a través de los medios oficiales establecidos por la Subdirección de Infotecnología, respetando el orden en que ingresan.
- 9.2. Registrar la solicitud en el sistema de tickets, se ingresa la información de la solicitud en el sistema, asignándole un número de ticket para su control y seguimiento.
- 9.3. Clasificar la incidencia según tipo, (incidencia, mantenimiento, instalación, levantamiento), se analiza la solicitud para determinar el tipo de problema, su urgencia y el impacto que tiene en las labores del usuario o de la institución.
- 9.4. Priorizar la atención según criticidad e impacto operativo, analizar el nivel de afectación que el incidente o requerimiento genera sobre las operaciones institucionales.
- 9.5. Evaluar si la atención se realizará de forma remota o mediante visita técnica, se revisa las características técnicas del incidente para determinar la modalidad más eficiente de atención.
- 9.6. Programar la visita técnica cuando corresponda o el envío del equipo por correspondencia, gestionar la logística necesaria para el traslado de personal técnico, herramientas o equipos requeridos y notificar oportunamente a las partes involucradas sobre la programación y condiciones de la atención.
- 9.7. Diagnosticar el problema de forma remota, realizar pruebas técnicas mediante herramientas de monitoreo y acceso remoto autorizadas, a la vez se identifica las posibles causas del incidente mediante la revisión de configuraciones, registros y alertas del sistema.
- 9.8. Brindar asistencia técnica al usuario, orientarlo sobre los procedimientos necesarios para la solución del problema identificado. A la vez verificar la comprensión de las instrucciones y resolver dudas relacionadas con el incidente reportado.
- 9.9. Aplicar soluciones remotas a equipos, sistemas o redes, realizando ajustes de configuración, actualizaciones o restauraciones según corresponda al diagnóstico efectuado.
- 9.10. Verificar el funcionamiento correcto posterior a la intervención, sistema o servicio intervenido. Se comprueba que el equipo o sistema funcione correctamente después de aplicar la solución.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UEM 169 de 183

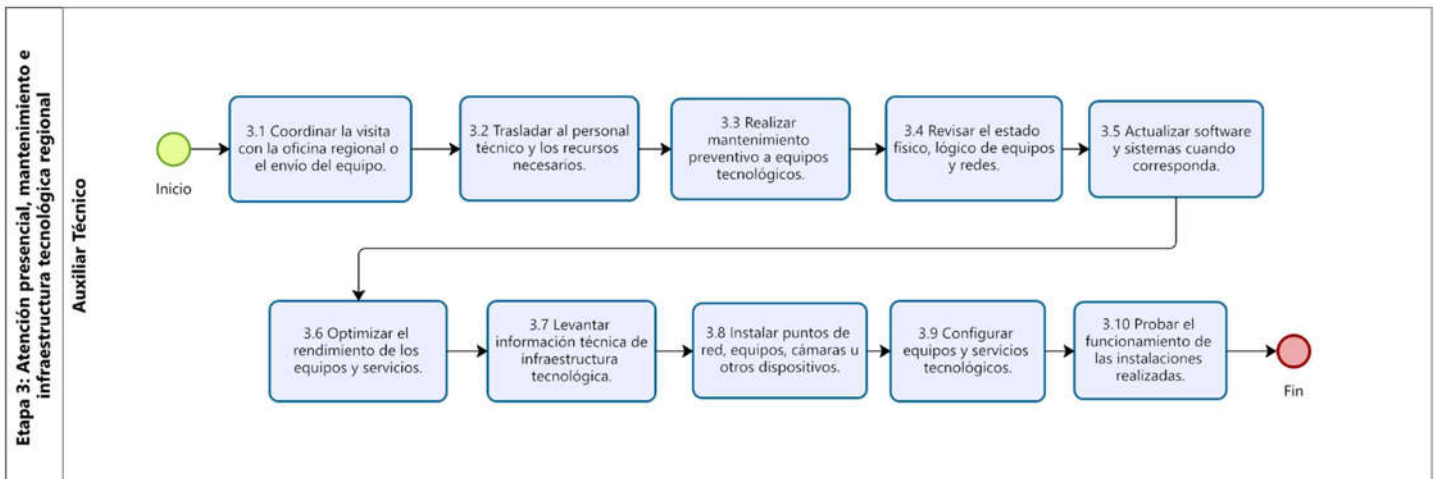
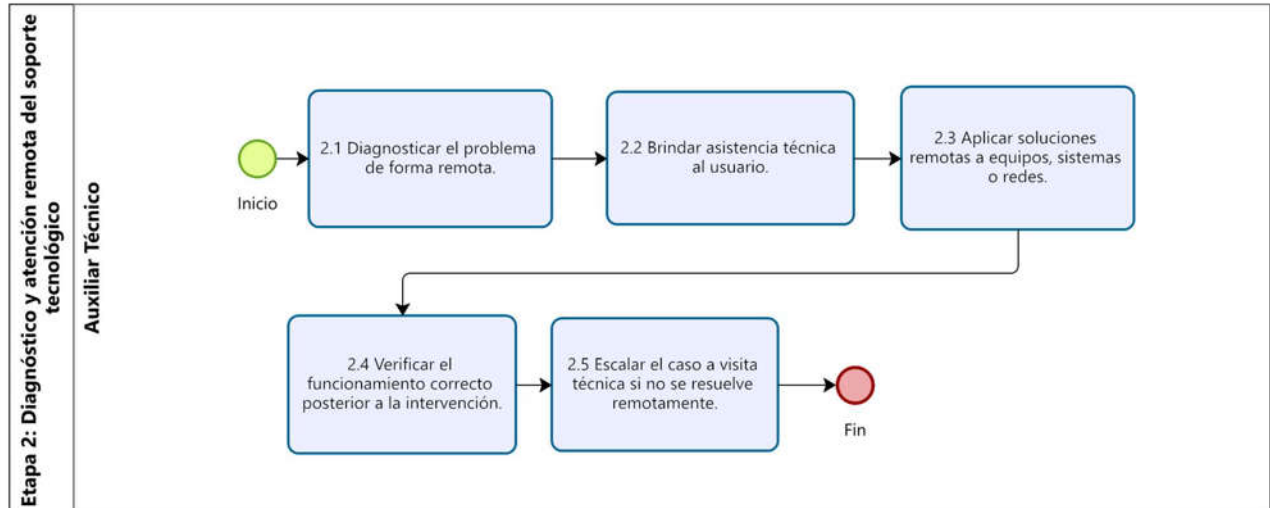
- 9.11. Escalar el caso a visita técnica si no se resuelve remotamente, analizar los resultados de las acciones remotas realizadas y determinar la necesidad de atención presencial.
- 9.12. Coordinar la visita con la oficina regional o el envío del equipo y establecer comunicación con los responsables locales para organizar la intervención técnica.
- 9.13. Trasladar al personal técnico y los recursos necesarios, gestionar el desplazamiento del personal asignado conforme a la programación aprobada, también verificar la disponibilidad de herramientas, repuestos y equipos requeridos para la intervención.
- 9.14. Realizar mantenimiento preventivo a equipos tecnológicos, aplicar procedimientos de limpieza, revisión y ajuste conforme a las especificaciones técnicas, es importante registrar las actividades realizadas y las observaciones identificadas durante el mantenimiento.
- 9.15. Revisar el estado físico, lógico de equipos y redes, a la vez inspeccionar las condiciones físicas de los equipos, conexiones y componentes tecnológicos para evaluar el estado lógico de sistemas operativos, aplicaciones, configuraciones y servicios de red.
- 9.16. Actualizar software y sistemas cuando corresponda, también se debe verificar la compatibilidad de las actualizaciones con la infraestructura tecnológica existente.
- 9.17. Optimizar el rendimiento de los equipos y servicios, realizar ajustes de configuración que permitan un mejor aprovechamiento de los recursos tecnológico, es importante verificar que las mejoras implementadas contribuyan a la estabilidad y eficiencia operativa.
- 9.18. Levantar información técnica de infraestructura tecnológica (redes, puntos, cámaras, etc.), detallada sobre la ubicación, características y estado de los componentes tecnológicos que faciliten la administración de la infraestructura.
- 9.19. Instalar puntos de red, equipos, cámaras u otros dispositivos, garantizando que la instalación cumpla con criterios de seguridad, funcionalidad y ordenamiento técnico.
- 9.20. Configurar equipos y servicios tecnológicos, validar que las configuraciones implementadas permitan el correcto funcionamiento de los servicios.
- 9.21. Probar el funcionamiento de las instalaciones realizadas, ejecutando pruebas técnicas para verificar la operatividad de los equipos y servicios instalados. Para la mejora continua es fundamental documentar los resultados obtenidos y las acciones correctivas realizadas, cuando corresponda.
- 9.22. Diagnosticar fallas en sitio, inspeccionar directamente los equipos, sistemas o redes afectados para identificar la causa raíz del problema, aplicando procedimientos de análisis técnico utilizando herramientas especializadas de diagnóstico.
- 9.23. Reparar equipos o componentes dañados, sustituir o reparar componentes defectuosos de acuerdo con los procedimientos técnicos establecidos y verificar el funcionamiento adecuado del equipo una vez finalizada la reparación.
- 9.24. Sustituir equipos o partes cuando sea necesario, instalar el nuevo equipo o componente garantizando su compatibilidad con la infraestructura existente.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 170 de 183

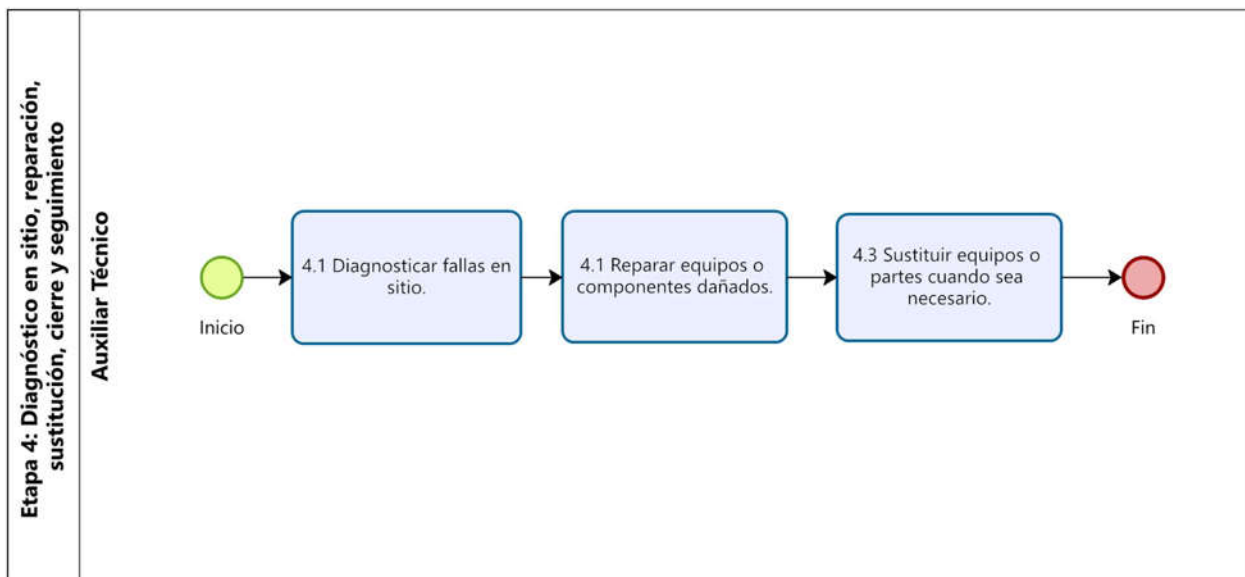
10. Diagrama de Flujo del Procedimiento



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 171 de 183



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 172 de 183



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 173 de 183

11. Gestión del Riesgo

PGR		PROCURADURÍA GENERAL DE LA REPÚBLICA										NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00	
MATRIZ PARA LA EVALUACIÓN, ANÁLISIS Y RESPUESTA A LOS RIESGOS													
Formulario 27 PGR													
PROCESO:		Soporte Tecnológico a Oficinas Regionales											
NOMBRE DEL SUBPROCESO:		Soporte Tecnológico a Oficinas Regionales											
OBJETIVO:		Brindar soporte tecnológico a las oficinas regionales para resolver problemas con equipos, sistemas y redes, de manera oportuna, asegurando que puedan operar de forma continua y eficiente.											
(1) No.	(2) Etapa del proceso	(3) Descripción del Riesgo	Riesgo inherente		(6) Zona de Riesgo Preliminar	(7) Controles obligatorios para mitigar los riesgos	(8) Controles que existen en la entidad	(9) Controles pendientes por establecer para mitigar los riesgos	Riesgo Residual		(12) Zona de Riesgo Final	(13) Respuesta a los Riesgos	
			(4) P	(5) I					(10) P	(11) I			
1	Recepción, registro, clasificación y priorización del requerimiento	1.1 Las solicitudes de soporte pueden no registrarse o atenderse sin evidencia, dificultando su seguimiento.	2	3	M	Registrar toda solicitud en sistema de tickets o formato oficial, indicando fecha, oficina regional, usuario, tipo de requerimiento, prioridad y responsable asignado.	Registrar toda solicitud en sistema de tickets o formato oficial, indicando fecha, oficina regional, usuario, tipo de requerimiento, prioridad y responsable asignado.		1	2	B	Aceptar	
2	Diagnóstico y atención remota del soporte tecnológico	2.1 El diagnóstico de la falla puede ser incorrecto o la solución aplicada puede ser parcial, provocando la reocurrencia del problema.	2	3	M	Utilizar checklist técnico de diagnóstico remoto y documentar causa identificada, acción aplicada y resultado de la verificación.	Utilizar checklist técnico de diagnóstico remoto y documentar causa identificada, acción aplicada y resultado de la verificación.		1	2	B	Aceptar	
3	Atención presencial, mantenimiento e infraestructura tecnológica regional	3.1 Las instalaciones, configuraciones o mantenimientos pueden ejecutarse sin pruebas o sin validación del usuario responsable.	1	3	M	Realizar pruebas de funcionamiento, levantar acta o reporte técnico de atención y obtener conformidad de la oficina regional.	Realizar pruebas de funcionamiento, levantar acta o reporte técnico de atención y obtener conformidad de la oficina regional.		1	2	B	Aceptar	
4	Diagnóstico en sitio, reparación, sustitución, cierre y seguimiento	4.1 El inventario de equipos puede no actualizarse oportunamente.	1	3	M	Actualizar inventario, actas de entrega-recepción, reportes de reparación y expediente del ticket antes del cierre definitivo.	Actualizar inventario, actas de entrega-recepción, reportes de reparación y expediente del ticket antes del cierre definitivo.		1	2	B	Aceptar	
Elaborado por:						Revisado por:						Aprobado por:	
Abel Fernando Perez Vargas Auxiliar Técnico Daniel Isaac Membreño Anarba Auxiliar Técnico Suyapa del Mar Andino Orozco Jefa de la Unidad de Modernización						Ingrid Karina López Fuentes Directora de Administración y Finanzas Jorge Elías... Subdirector						José Francisco Quirós Mejía Subprocurador General de la República	
Firma:  Fecha: 18 de mayo de 2026						Firma:  Fecha: 19 de mayo de 2026						Firma:  Fecha: 19 de mayo de 2026	

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 174 de 183

	PROCURADURÍA GENERAL DE LA REPÚBLICA		NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00		
	MAPA PARA LA VALORACIÓN PRELIMINAR Y FINAL DE LOS RIESGOS		Formulario 28 PGR		
PROPÓSITO: Facilitar la valoración y determinación de la zona de riesgos, de acuerdo con la explicación que consta en el Anexo 22 Instructivo para la gestión de riesgos					
PROBABILIDAD					
Muy Alta (5)	A	A	E		E
Alta (4)	M	A	A		E
Moderada (3)	B	M	A		E
Baja (2)	B	B	1.1 M 2.1	A	E
Muy Baja (1)	B	B	3.1 M 4.1	A	A
	Muy Bajo (1)	Bajo (2)	Moderado (3)		Muy Alto(5)
IMPACTOS					
ZONA DE RIESGO:					
B: Zona de Riesgo Baja: Respuesta, Aceptar el riesgo					
M: Zona de Riesgo Moderada: Respuestas, Aceptar el riesgo o reducir el riesgo. Costo Beneficio					
A: Zona de Riesgos Alta: Respuestas, Reducir el riesgo, o evitar, o compartir, o transferir					
E: Zona de Riesgo Extrema: Respuestas, Reducir el riesgo (costo beneficio), o evitar, o compartir o transferir					

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 175 de 183

12. Elementos Transversales del Procedimiento



Matriz de Verificación Inclusión de Elementos Transversales Estratégicos Manual de Procedimientos de la Subdirección de Infotecnología



Denominación del Proceso: Soporte Tecnológico a Oficinas Regionales			
Preguntas de Verificación	Si	No	Respuestas de Verificación
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Control Interno y anticorrupción</u> ?	X		El proceso contempla registro, asignación y seguimiento de solicitudes de soporte tecnológico.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Descentralización</u> ?		X	No aplica debido a que el soporte técnico es brindado por la Subdirección de Infotecnología, las oficinas regionales reportan incidencias, validan requerimientos y confirman la atención recibida.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Participación Ciudadana</u> ?		X	No aplica de forma directa, por tratarse de un proceso técnico interno de soporte institucional.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas a la <u>Transparencia y Acceso a la Información Pública</u> ?	X		El proceso contribuye a la disponibilidad y continuidad de los sistemas que soportan información pública institucional. La atención oportuna de fallas tecnológicas permite mantener operativos los canales de consulta, gestión y respuesta institucional.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al <u>Archivo Documental</u> ?	X		El proceso genera registros de solicitudes, diagnósticos, atenciones, autorizaciones y cierres de soporte.
¿La descripción del proceso incluye medidas concretas (actividades) orientadas al cumplimiento de los indicadores de <u>PEI Institucional</u> ?	X		El proceso aporta al cumplimiento de metas relacionadas con eficiencia operativa, modernización y continuidad de servicios regionales.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 176 de 183

13. Bibliografía

- AXELOS. (2019). ITIL® Foundation: ITIL 4 Edition. TSO.
- Carbonell, M. (2019). *Teoría del derecho*. Porrúa.
- De la Torre, J. (2018). *Técnicas de redacción jurídica*. Jurídica Universitaria.
- *Definición.de.* . (2024). Obtenido de Soporte técnico: <https://definicion.de/soporte-tecnico/>
- *HubSpot.* (2024). Obtenido de Qué es el soporte técnico: <https://blog.hubspot.es/service/que-es-soporte-tecnico>
- ISO. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.
- *Wikipedia.* (2025). Obtenido de Soporte técnico: https://es.wikipedia.org/wiki/Soporte_t%C3%A9cnico
- *Zendesk.* (2024). Obtenido de Ticket de soporte técnico: definición y funciones: <https://www.zendesk.es/blog/customer-service/ticketing-system/ticket-de-soporte-tecnico/>

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 177 de 183

14. Anexos

14.1. M- PGR-SDIT-XXX-202X



MEMORÁNDUM PGR-SDIT-LI-00X-202X

Tegucigalpa M.D.C. XX de enero de 202X

PARA: Nombre

Cargo

C.c.: Nombre

Cargo

DE: Nombre

Cargo

ASUNTO:

Cc: Archivo

 Residencial El Trapiche, Edificio PGR, Tegucigalpa, M.D.C.

 Tel: 2235-2022 / 2235-2025 / 2235-2049 / 2235-2050

 www.pgr.gob.hn



	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 178 de 183

14.2. Sistema de ticket o correo electrónico



Notificar abuso'." data-bbox="537 259 959 789"/>

 PGR PROCURADURÍA GENERAL DE LA REPÚBLICA	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 179 de 183

14.3. F-SDIT-004 Dictamen Técnico de Equipos Tecnológicos

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCION DE INFOTECNOLOGIA	
INF-SDIT-004 Versión 1.0	DICTAMEN TÉCNICO No. XXXX-202X Fecha: 20 de mayo de 2026	SDIT 2 de 4

1. Datos Generales

Fecha: _____

Dependencia solicitante: _____

Asunto: _____

2. Objetivo del Dictamen

Indicar brevemente la finalidad de la evaluación.

3. Identificación del equipo

Campo	Información
Tipo de equipo	
Marca	
Modelo	
Número de serie	
Código de inventario	
Ubicación	
Usuario o dependencia asignada	
Año de adquisición	
Estado físico	

4. Características técnicas

Registrar únicamente las características que correspondan al tipo de equipo:

- Procesador.
- Memoria RAM.
- Capacidad y tipo de almacenamiento.
- Sistema operativo.
- Tarjeta de red/conectividad.
- Periféricos.
- Capacidad o especificaciones particulares del equipo.

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCION DE INFOTECNOLOGIA	
INF-SDIT-004 Versión 1.0	DICTAMEN TÉCNICO No. XXXX-202X Fecha: 20 de mayo de 2026	SDIT 3 de 4

- Otras características relevantes.

5. Evaluación técnica

Aspecto evaluado	Resultado	Observaciones
Estado físico		
Encendido y funcionamiento		
Rendimiento		
Almacenamiento		
Conectividad		
Sistema operativo		
Componentes		

6. Hallazgos

Describir concretamente las condiciones encontradas.

Por ejemplo:

- Fallas identificadas.
- Componentes deteriorados.
- Obsolescencia tecnológica.
- Incompatibilidad de hardware o software.
- Rendimiento insuficiente.
- Daños físicos.
- Ausencia o dificultad de repuestos.
- Condiciones que representen riesgo para la continuidad del servicio.

7. Diagnóstico técnico

Presentar el resultado integral de la evaluación.

Clasificación sugerida:

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	UDEM UNIDAD DE MODERNIZACIÓN
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UDEM 180 de 183

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
INF-SDIT-004 Versión 1.0	DICTAMEN TÉCNICO No. XXXX-202X Fecha: 20 de mayo de 2026	SDIT 4 de 4

- ☐ Apto para continuar en uso
- ☐ Apto con mantenimiento
- ☐ Requiere reparación
- ☐ Requiere actualización de componentes
- ☐ Requiere reemplazo
- ☐ Técnicamente no funcional

De acuerdo con las pruebas y verificaciones realizadas, se determina que el equipo presenta _____. En consecuencia, técnicamente se considera _____, recomendándose _____.

8. Evidencia y anexos

Fotografías del equipo, Reportes de pruebas, Cotización o estimación de reparación, si procede.

9. Responsables

Responsabilidad	Nombre y Cargo	Firma	Fecha
Elaborado por			
Revisado por			
Aprobado por			

	PROCURADURÍA GENERAL DE LA REPÚBLICA SUBDIRECCIÓN DE INFOTECNOLOGÍA	
PR-SDIT-007 Versión 1.0	Soporte Tecnológico a Oficinas Regionales Fecha: 01 de junio 2026	UEM 183 de 183

15. Control de Cambios al Procedimiento

Historial de Cambios al Procedimiento

Fecha	Versión	Autor		Descripción del cambio	Cambio Autorizado por:	
		Cargo	Área		Cargo	Firma