



MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS

**SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL**

10 DE AGOSTO DE 2026

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 2 de 150

ÍNDICE

	Página
I FIRMAS	8
II INTRODUCCIÓN	10
III OBJETIVOS DEL MANUAL	11
IV MARCO JURÍDICO Y NORMATIVO	12
V ALCANCE O NIVEL DE APLICACIÓN	14
V DEFINICIONES	14
VII POLÍTICAS GENERALES	19
Políticas de servicios de la Dirección de Tecnologías	19
Lineamientos para la adquisición de tecnología	23
Adquisición de hardware	24
Adquisición de software	25
Políticas de seguridad lógica	25
Bases de datos	25
Recursos de cómputo – seguridad de cómputo	26
Usos de servicios de red – áreas administrativas	26
Usuarios o usuarias	28
Responsabilidades personales	29



**SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL**

DIRECCIÓN DE TECNOLOGÍAS

**MANUAL DE POLÍTICAS Y PROCEDIMIENTOS
DE LA DIRECCIÓN DE TECNOLOGÍAS**

Codificación:

SAIA-DT-MPP-01-V3

Versión: 3

Emisión: 1 de agosto de 2018

Actualización: 10 de agosto de 2026

Página: 3 de 150

Uso apropiado de los recursos de tecnología	30
Sistemas de Detección de Intrusos (IDS)	31
Políticas de dispositivos móviles	31
Responsabilidades de la Dirección de Tecnologías	33
Responsabilidades de las personas usuarias resguardantes de dispositivos de la Administración Pública Municipal	34
Políticas de teletrabajo	35
Políticas de seguridad de los recursos humanos	37
Políticas de gestión de los activos	39
Políticas de control de accesos	42
Políticas de seguridad física y del entorno	42
Políticas de seguridad en las operaciones	44
Gestión de cambios	45
Gestión de la capacidad	46
Separación de los ambientes de desarrollo, prueba y operación	46
Protección ante software malicioso	47
Requisitos para los usuarios	47
Requisitos para los sistemas	47
Respaldo – copias de seguridad	48
Registro de eventos	49
Protección de la información de registros (logs)	50
Sincronización de relojes	50
Control de software en la producción	50
Gestión de vulnerabilidades técnicas	51
Controles de auditoría de sistemas de información	51
Políticas de seguridad de las comunicaciones	52
Seguridad de los servicios de Red	53
Mensajería electrónica	54



**SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL**

DIRECCIÓN DE TECNOLOGÍAS

**MANUAL DE POLÍTICAS Y PROCEDIMIENTOS
DE LA DIRECCIÓN DE TECNOLOGÍAS**

Codificación:
SAIA-DT-MPP-01-V3

Versión: 3

Emisión: 1 de agosto de 2018

Actualización: 10 de agosto de 2026

Página: 4 de 150

	Acuerdos de confidencialidad y no divulgación	55
	Políticas de controles criptográficos	55
	Gestión de claves	56
	Políticas de adquisición, desarrollo y mantenimiento de sistemas	57
	Análisis y especificaciones de los requisitos de seguridad de los sistema de información	57
	Aseguramiento de los servicios de aplicación en las redes públicas	58
	Seguridad en los procesos de desarrollo y soporte	59
	Procedimientos de control de cambios del sistema	59
	Revisión técnica de aplicaciones después de cambios de las plataformas operativas	61
	Restricciones a los cambios en los paquetes de software	62
	Principios de ingeniería de sistemas seguros	62
	Ambiente de desarrollo seguro	62
	Desarrollo subcontratado	63
	Pruebas de seguridad de sistema	63
	Pruebas de aceptación del sistema	63
	Datos de prueba	64
	Protección de datos de prueba	64
	Políticas en las relaciones con los proveedores	64
	Seguridad de la información en la relaciones con los proveedores	64
	Políticas de seguridad de la información para las relaciones con los proveedores	65
	Análisis de riesgos	65
	Selección de controles	65
	Acuerdos de prestación de servicios	66



SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL

DIRECCIÓN DE TECNOLOGÍAS

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS
DE LA DIRECCIÓN DE TECNOLOGÍAS

Codificación:
SAIA-DT-MPP-01-V3

Versión: 3

Emisión: 1 de agosto de 2018

Actualización: 10 de agosto de 2026

Página: 5 de 150

	Control de accesos	66
	Monitores	66
	Finalización del servicio	66
	La seguridad en los acuerdos con proveedores	67
	Cadena de suministro de tecnología de la información y las comunicaciones	67
	Gestión de la entrega de servicios por terceras partes	68
	Seguimiento y revisión de los servicios de proveedores	68
	Gestión de cambios en los servicios de los proveedores	68
	Políticas de gestión de incidentes de seguridad de la información	69
	Políticas de cumplimiento	70
	Cumplimiento de los requisitos legales y contractuales	70
	Derechos de Propiedad Intelectual y Software Institucional	71
	Protección de riesgos	73
	Políticas de los datos y privacidad de la información personal	74
	Regulación de los controles criptográficos	74
	Cifrado obligatorio	76
	Uso de datos a gran escala	77
	Código de Ética y Conducta	77
	Revisiones de seguridad de la información	78
	Revisión independiente de la seguridad de la información	78
	Cumplimiento de la política y normas de seguridad	79
	Revisión del cumplimiento técnico	79
VIII	PROCESOS	80
	<u>SAIA-DT-MPP-01-PROC-01-V3</u>	81
	PROCESO DESARROLLO DE UN NUEVO SISTEMA DE INFORMACIÓN	81



SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL

DIRECCIÓN DE TECNOLOGÍAS

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS
DE LA DIRECCIÓN DE TECNOLOGÍAS

Codificación:
SAIA-DT-MPP-01-V3

Versión: 3

Emisión: 1 de agosto de 2018

Actualización: 10 de agosto de 2026

Página: 6 de 150

	DESCRIPCIÓN DEL PROCESO	
	DIAGRAMA DE FLUJO DEL PROCESO	85
	<u>SAIA-DT-MPP-01-PROC-02-V3</u>	87
	PROCESO SOPORTE DE SISTEMAS	87
	DESCRIPCIÓN DEL PROCESO	
	DIAGRAMA DE FLUJO DEL PROCESO	96
	<u>SAIA-DT-MPP-01-PROC-03-V3</u>	98
	PROCESO SOLICITUD DE SOPORTE TÉCNICO	98
	DESCRIPCIÓN DEL PROCESO	
	DIAGRAMA DE FLUJO DEL PROCESO	103
	<u>SAIA-DT-MPP-01-PROC-04-V3</u>	105
	PROCESO SOLICITUD DE PRÉSTAMO TEMPORAL DE EQUIPO DE CÓMPUTO	105
	DESCRIPCIÓN DEL PROCESO	
	DIAGRAMA DE FLUJO DEL PROCESO	107
	<u>SAIA-DT-MPP-01-PROC-05-V3</u>	108
	PROCESO DEVOLUCIÓN DEL EQUIPO DE CÓMPUTO	108
	DESCRIPCIÓN DEL PROCESO	
	DIAGRAMA DE FLUJO DEL PROCESO	111
IX	ANEXOS	112
	<u>SAIA-DT-MPP-01-FORM-01-V3</u>	113
	SOLICITUD DE SOPORTE TÉCNICO	114
	<u>SAIA-DT-MPP-01-FORM-02-V3</u>	115
	SOLICITUD DE SOPORTE DE SISTEMAS	116
	<u>SAIA-DT-MPP-01-FORM-03-V3</u>	117
	RECEPCIÓN/ENTREGA EQUIPO DE CÓMPUTO	118
	<u>SAIA-DT-MPP-01-FORM-04-V3</u>	119
	CONSTRUCCIÓN DE CONTRASEÑAS SEGURAS	120
	<u>SAIA-DT-MPP-01-FORM-05-V3</u>	123



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 7 de 150

CONVENIO DE CONFIDENCIALIDAD	124
<u>SAIA-DT-MPP-01-FORM-06-V3</u>	135
REPORTE DE DIAGNÓSTICO DE EQUIPO DE CÓMPUTO	136
<u>SAIA-DT-MPP-01-FORM-07-V3</u>	137
REGISTRO DE RESPALDOS	138
<u>SAIA-DT-MPP-01-FORM-08-V3</u>	139
PLAN PARA RESPALDO DE INFORMACIÓN EN EQUIPO DE USUARIOS (DISASTER RECOVERY PLAN, DRP)	140
<u>SAIA-DT-MPP-01-FORM-09-V3</u>	143
PLAN DE RESPALDOS DE INFORMACIÓN DEL CENTRO DE DATOS (DISASTER RECOVERY PLAN, DRP)	144
<u>SAIA-DT-MPP-01-FORM-10-V3</u>	147
SOLICITUD DE PRÉSTAMO TEMPORAL DE EQUIPO DE CÓMPUTO	148

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 8 de 150

El *Manual de Políticas y Procedimientos de la Dirección de Tecnologías*, el cual, corresponde aplicar a la Dirección de Tecnologías adscrita a la Secretaría de Administración e Inteligencia Artificial de San Pedro Garza García, Nuevo León queda formalizado con las firmas de autorización de los siguientes funcionarios públicos:

I. FIRMAS



Licenciado Daniel Iván Ruiz Chávez
Secretario de la Contraloría y Transparencia de
San Pedro Garza García, Nuevo León



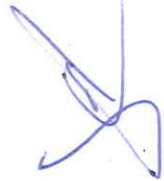
Licenciado Jonathan Daniel Martínez de la Rosa
Consejero General de Asuntos Jurídico de
San Pedro Garza García, Nuevo León



Licenciado Alberto Herrera Hernández
Secretario de Administración e Inteligencia Artificial
de San Pedro Garza García, Nuevo León

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 9 de 150

Mediante las firmas de las y los servidores públicos que aparecen en los recuadros, se da el crédito a los participantes en la elaboración y/o actualización, revisión, verificación y validación del presente Manual.

	NOMBRE Y CARGO	FIRMA
Actualizó:	Ingeniero Francisco Javier Coronado Sandoval Control de Calidad y Procesos de la Dirección de Tecnologías	
Revisó:	Contadora Pública Sonia Edna Martínez Cárdenas Coordinadora de Normatividad de la Dirección de Normatividad, Evaluación y Capacitación	
Verificó:	Licenciada Claudia Esther Cervantes Alanís Directora de Tecnologías de la Secretaría de Administración e Inteligencia Artificial	
Validó:	Francisco Javier Castillo Santana Encargado del Despacho de la Dirección de Normatividad, Evaluación y Capacitación de la Secretaría de la Contraloría y Transparencia	

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 10 de 150

II. INTRODUCCIÓN

En el marco del compromiso inquebrantable con la excelencia institucional, la innovación tecnológica y la administración pública de vanguardia, la Dirección de Tecnologías adscrita a la Secretaría de Administración e Inteligencia Artificial de San Pedro Garza García, Nuevo León presenta el Manual de Políticas y Procedimientos como una obra normativa y operativa que consolida el orden, la disciplina técnica y la coherencia organizacional en el ámbito de las tecnologías de la información y la gestión digital.

Este instrumento, de carácter estratégico y normativo, tiene como propósito articular con rigor metodológico los principios, políticas y directrices que orientan la actuación de la Dirección de Tecnologías, con la finalidad de asegurar la estandarización de procesos, la trazabilidad de las acciones institucionales y la plena observancia de los valores del servicio público.

A través de su contenido, se promueve un modelo de gobernanza tecnológica alineado con los más altos estándares nacionales e internacionales en materia de eficiencia, seguridad de la información, transformación digital y calidad en la gestión pública.

Más que un documento administrativo, este manual representa una declaración de principios y un compromiso institucional con la legalidad, la transparencia, la rendición de cuentas y la mejora continua. En el convergen la visión estratégica del Municipio, la responsabilidad ética de sus servidores públicos y la convicción de que el uso inteligente y ordenado de las tecnologías es un pilar fundamental para el desarrollo sostenible, la competitividad municipal y el bienestar de la ciudadanía.

Se exhorta a todas las personas servidoras públicas adscritas a esta Administración Pública Municipal a observar con diligencia, integridad y profesionalismo el contenido de este manual, por lo cual, se asume que su correcta aplicación no solo fortalece la estructura operativa de la Administración Pública Municipal, sino que enaltece el propósito superior del servicio público, consistente en servir con excelencia, innovación y compromiso a la comunidad de San Pedro Garza García.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 11 de 150

III. OBJETIVOS DEL MANUAL

El presente Manual de Políticas y Procedimientos tiene por objeto establecer y dar a conocer los lineamientos normativos, operativos y administrativos que rigen el actuar de la Dirección de Tecnologías, adscrita a la Secretaría de Administración e Inteligencia Artificial de San Pedro Garza García, Nuevo León.

Constituye una herramienta institucional que promueve la eficiencia, transparencia y responsabilidad en la gestión de los recursos tecnológicos, al tiempo que garantiza el cumplimiento de los principios rectores del servicio público.

Su finalidad es proporcionar una guía clara y estructurada sobre las funciones, responsabilidades y procesos que competen a esta Dirección de Tecnologías, en concordancia con el marco normativo vigente, los planes estratégicos del Municipio y las mejores prácticas en materia de gobernanza digital y transformación tecnológica.

La Dirección de Tecnologías asume el compromiso de fortalecer la infraestructura tecnológica, optimizar los servicios digitales y salvaguardar la información institucional mediante el cumplimiento riguroso de las políticas aquí establecidas.

Asimismo, este manual contribuye al orden institucional, a fin de facilitar la toma de decisiones fundamentadas, la rendición de cuentas y la mejora continua de los procesos internos. De igual forma, busca proporcionar soluciones tecnológicas eficientes, seguras e innovadoras que fortalezcan los servicios públicos, optimicen los procesos administrativos y garanticen la protección de los datos personales, para contribuir al desarrollo inteligente y sostenible del municipio de San Pedro Garza García.

Nuestra labor se orienta a apoyar con infraestructura, soporte técnico, gestión de la información y sistemas de información a las distintas dependencias municipales, con el objetivo de impulsar una administración pública moderna y transparente centrada en la ciudadanía.

La Dirección aspira a consolidarse como líder en la transformación digital del gobierno municipal, mediante el uso estratégico de las tecnologías de la información para una administración eficiente, proactiva y confiable, con altos estándares de innovación, seguridad de la información y mejora continua en el servicio público.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 12 de 150

IV. MARCO JURÍDICO Y NORMATIVO

El *Manual de Políticas y Procedimientos de la Dirección de Tecnologías* se fundamenta en el marco jurídico aplicable en materia de transparencia, protección de datos personales, gobierno digital, administración de bienes, gestión documental, seguridad de la información y responsabilidades administrativas.

Las disposiciones citadas establecen las bases normativas que facultan a San Pedro Garza García, para regular el uso, administración, protección y aprovechamiento de los activos tecnológicos, la operación de los sistemas institucionales y el tratamiento adecuado de la información pública, reservada, confidencial y personal.

A continuación, se describen los fundamentos legales aplicables, su contenido esencial y su relación con las funciones de esta Dirección:

LEGISLACIÓN FEDERAL:

- *Constitución Política de los Estados Unidos Mexicanos;*
- *Ley General de Responsabilidades Administrativas;*
- *Ley General de Transparencia y Acceso a la Información Pública;*
- *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;*
- *Ley General de Archivos;*
- *Ley de Firma Electrónica Avanzada;*
- *Ley Federal de Protección a la Propiedad Industrial; y*
- *Ley Federal del Derecho de Autor.*

LEGISLACIÓN ESTATAL:

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 13 de 150

- *Constitución Política del Estado Libre y Soberano de Nuevo León;*
- *Ley de Gobierno Municipal del Estado de Nuevo León;*
- *Ley Sobre Gobierno Electrónico y Fomento al Uso de las Tecnologías del Estado de Nuevo León;*
- *Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León;*
- *Ley de Responsabilidades Administrativas del Estado de Nuevo León;*
- *Ley de Archivos del Estado de Nuevo León; y*
- *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.*

REGLAMENTOS MUNICIPALES:

- *Reglamento Orgánico de la Administración Pública Municipal de San Pedro Garza García Nuevo León;*
- *Reglamento de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Gobierno Abierto del Municipio de San Pedro Garza García, Nuevo León;*
- *Reglamento de Archivos para el Municipio de San Pedro Garza García, Nuevo León;*
- *Reglamento de Entrega – Recepción para el Municipio de San Pedro Garza García, Nuevo León;*
- *Reglamento para la Conservación y Protección de los Bienes de Propiedad Municipal de San Pedro;*
- *Reglamento Interior de la Secretaría del Republicano Ayuntamiento;*
- *Código de Ética y Conducta para el Municipio de San Pedro Garza García, Nuevo León; y*

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 14 de 150

- *Manual de Organización de la Secretaría de Administración e Inteligencia Artificial.*

V. ALCANCE O NIVEL DE APLICACIÓN

Las políticas y procedimiento establecidos en este manual son de observancia obligatoria para:

- Todo el personal servidor público adscrito a la Dirección de Tecnologías, independientemente de su categoría, función o modalidad de contratación;
- Las unidades administrativas, dependencias y entidades municipales que requieran, utilicen o gestionen servicios, sistemas o activos tecnológicos provistos, administrados o supervisados por la Dirección;
- Las personas usuarias internas que, en el ejercicio de sus funciones, tengan acceso a infraestructura tecnológica; sistemas institucionales, información digital o equipos de cómputo propiedad del Municipio;
- Proveedores contratistas y terceros que, mediante relación contractual, tengan interacción con servicios, proyectos o activos tecnológicos administrados por la Dirección de Tecnologías, por lo que, deberán observar en todo momento las obligaciones establecidas en el presente manual y los instrumentos jurídicos aplicables; y
- Para personas que presten servicio social o estén haciendo prácticas profesionales en la Administración Pública Municipal, se les podrá facilitar acceso a activos informáticos e inclusive contraseñas temporales, deberán considerar en todo momento la responsabilidad de los activos al resguardante.

El incumplimiento de las disposiciones aquí contenidas será sujeto a las responsabilidades administrativas, civiles o penales correspondientes, conforme al marco jurídico municipal, estatal y federal aplicable.

VI. DEFINICIONES

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 15 de 150

Activos hardware. Los activos de hardware incluyen cualquier equipo o material tecnológico que los empleados utilizan para acceder a la información. Esto incluye computadoras personales, computadoras de escritorio, teléfonos móviles, servidores, equipos de red, equipo periférico como impresoras, monitores, etcétera.

Activos de software. Los activos de software se refieren a cualquier programa, aplicación o licencia que la Administración Pública Municipal utiliza con fines operativos. El uso de activos de software conlleva diversos riesgos, como la seguridad de los datos y el cumplimiento normativo.

Activos personales y servicios tercerizados. Empleados, técnicos externos, proveedores de correo o nube. Todos los que tengan acceso o responsabilidad sobre la información también.

Activo de información. Los activos de información incluyen, entre otros, información en formato físico o electrónico, bases de datos, sistemas de información, aplicaciones, credenciales de acceso, configuraciones, metadatos y cualquier tipo de información operativa, administrativa, técnica o estratégica.

Amenaza para la seguridad de la información. Se refiere a cualquier cosa que tenga el potencial de causar daños graves a un sistema o activo de información. Una amenaza es algo que puede suceder o no, pero tiene el potencial de causar daños graves.

Activos de tecnología (Activos de TI): Cualquier elemento tangible o intangible que una organización posee o utiliza y que tiene valor para sus operaciones, incluidos hardware (computadoras, servidores, etcétera), software (aplicaciones, licencias, etcétera), datos, suscripciones a la nube, entre otros.

Aplicación móvil, app: App es la abreviatura de “aplicación” en inglés (application) y se refiere a un programa de software diseñado para funcionar en dispositivos móviles como teléfonos inteligentes y tabletas.

Acuerdo de confidencialidad: También conocido como NDA (Non-Disclosure Agreement) por sus siglas en inglés, es un contrato legal que obliga a las partes firmantes a no divulgar información sensible, secreta o de propiedad exclusiva a la que tengan acceso durante una relación comercial, laboral o de colaboración.

Datos: Cualquier forma de información, ya sea en forma electrónica o sobre papel. En forma electrónica “datos” se refiere a archivos, bases de datos, documentos de texto, imágenes, voz y video codificados en forma digital.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 16 de 150

Datos en reposo: Se refieren a los datos almacenados o archivados en dispositivos de almacenamiento físico o electrónicos. Estos datos no se acceden ni se procesan activamente. Algunos ejemplos incluyen archivos, discos duros, copias de seguridad o datos almacenados en la nube.

Datos en tránsito: Se refieren a los datos que se mueven entre los diferentes ubicaciones o redes. Algunos ejemplos incluyen datos enviados por correo electrónico o transferidos entre servidores.

Dirección: Dirección de Tecnologías. Unidad Administrativa que organizacionalmente está adscrita a la Secretaría de Administración e Inteligencia Artificial de San Pedro Garza García. Bajo esta Dirección, girará este documento al respecto de políticas y procedimientos. La Dirección de Tecnologías es responsable de gestionar, desarrollar, implementar, mantener la infraestructura de tecnologías de información y telecomunicaciones a los usuarios de la Administración Pública Municipal de San Pedro Garza García.

El deber de secreto: Es la obligación legal y ética de mantener en reserva la información confidencial, datos o hechos conocidos durante el desarrollo de una actividad profesional, cargo público o relación laboral. Su propósito principal es proteger la intimidad de las personas y fomentar la confianza en los servicios.

Equipo aislado: Son todos aquellos equipos de cómputo que están fuera del dominio de la red o configurados en una red aislada, para observación de seguridad u operación especial.

Equipo de telecomunicaciones: Hardware utilizado principalmente para las telecomunicaciones, como líneas de transmisión, multiplexores y estaciones transceptoras base.

Evento de seguridad de la información. Es un cambio en las operaciones diarias de una red o servicio de tecnología de la información que indica que una política de seguridad puede haber sido violada o una protección de seguridad puede haber fallado.

Partes Interesadas: Cualquier organización, grupo o individuo que pueda afectar o ser afectado por las actividades de la Dirección de Tecnologías.

Personas: Incluye administradores, usuarios y cualquier otro desarrollador, así como el comportamiento organizacional y las políticas que concurren cuando las personas interactúan unas con otras.

Plan de recuperación de datos. Disaster Recovery Plan (DRP): Es la capacidad de recuperar la información en el punto anterior. Es decir, cuántos datos puede perder el área antes de que se paralice su funcionamiento de trabajo.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 17 de 150

Política: Prescribe los lineamientos generales dentro de los cuales han de realizarse las actividades y tareas asignadas.

Problemas: Situaciones de tecnología indeseables que no permiten lograr sus propósitos, metas y objetivos de la Administración Pública Municipal.

Puesta a punto: Operación consistente en regular un mecanismo, un dispositivo, etcétera, a fin de que funcione correctamente.

Punto de recuperación objetivo. Recovery Point Objective (PRO): Es la capacidad de recuperar la información en el punto anterior. Es decir, cuántos datos puede perder el área antes de que se paralice su funcionamiento de trabajo.

Responsable del activo. Es el servidor público, área o unidad administrativa que tiene la titularidad operativa y administrativa sobre un activo de información, es la instancia facultada para autorizar supervisar y asegurar su correcto uso protección, mantenimiento, actualización y resguardo. Tiene la obligación de garantizar que el activo sea gestionado conforme a las normas aplicables, políticas internas, controles de seguridad, disposiciones jurídicas y mejores prácticas, así como de vigilar que los usuarios que acceden a dicho activo cumplan con las responsabilidades y restricciones establecidas.

Resguardante del activo. Es el servidor público que tiene bajo su custodia física y operativa un activo asignado, es el responsable de su buen uso, conservación, integridad y resguardo cotidiano. Su función implica emplear el activo exclusivamente para fines institucionales, mantenerlo en condiciones adecuadas de operación, reportar incidencias o anomalías y, cumplir con las políticas, procedimientos y controles establecidos para su protección.

Seguridad informática: Técnicas desarrolladas para proteger los bienes informáticos frente a daños accidentales o intencionados.

Seguridad de la información: Se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan.

Servidor: Genéricamente, dispositivo de un sistema que resuelve las peticiones de otro elemento, denominado cliente. Computadora conectada a una red que pone sus recursos a disposición del resto de los integrantes de la red.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 18 de 150

Sistema de información: Es un conjunto de personas, datos, procesos, interfaces y distribución geográfica que son integrados para soportar y mejorar la operación día a día en la Administración Pública Municipal de San Pedro Garza García; así como proveer información para la solución de problemas y toma de decisiones de los administradores de la unidad administrativa.

Sistema operativo: Conjunto de programas fundamentales sin los cuales no sería posible hacer funcionar el equipo de cómputo con los programas de aplicaciones o software que se desee utilizar.

Software o programas base: Consideramos como software o programas base a las aplicaciones de uso común para la Administración Pública Municipal; como el office, windows, programas de libre uso y sistemas de información o aplicaciones creados por la Dirección de Tecnologías.

Sistemas de telecomunicaciones. Colección de hardware y software compatible dispuesto para comunicar información de un lugar a otro. Estos sistemas pueden transmitir textos, gráficos, voz, documentos o información de video en movimiento completo.

Tecnologías de la información (TI): Son aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información. La tecnología de la información se encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones. Es un término que comprende todo lo que está vinculado con el almacenamiento, protección, procesamiento y transmisión de la información. Este concepto engloba todo lo relacionado con la informática, la electrónica y las telecomunicaciones. Los avances tecnológicos como el internet, las comunicaciones móviles, los satélites, etcétera.

La infraestructura de tecnologías de la información y telecomunicaciones (TIC): Se refiere al conjunto de recursos, herramientas, equipos, software, redes y servicios que permiten la gestión, procesamiento, almacenamiento y transmisión de información. En esencia, es la base tecnológica sobre la que se construyen y operan los sistemas de información y comunicación de San Pedro Garza García.

Tiempo de recuperación del trabajo. - Work Recovery Time (TWR): Es el tiempo de recuperación de trabajo que determina el tiempo que se necesita para verificar el sistema, la integridad de los datos, comprobar las bases de datos y asegurarse de que las aplicaciones o servicios se están ejecutando bien. Cuando los sistemas o datos afectados por el desastre son verificados, se reanuda de nuevo la producción.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 19 de 150

Tiempo de recuperación objetivo. - Recovery Time Objective (RTO): Es el tiempo que se tarda en reanudar el servicio. Es decir, cuánto tiempo tiene el usuario para contar nuevamente con la información en el sistema después de una pérdida de información.

Tiempo máximo tolerable sin servicio. Maximum Tolerable Downtime (TMSS): El TMSS es el tiempo máximo tolerable sin servicio para cada proceso en cada instalación, con el fin de ayudar en la definición de las estrategias de recuperación.

Usuario: En informática, los usuarios son personas que interactúan habitualmente con ciertos programas, aplicaciones y sistemas de un dispositivo, ya sea, una computadora o un dispositivo móvil.

Vulnerabilidad en la seguridad de la información. Se refiere a una debilidad o defecto en un sistema o activo de información que puede ser expuesto a una amenaza o ataque. También puede referirse a cualquier tipo de debilidad en un sistema de información en sí mismo, en un conjunto de procedimientos o en cualquier cosa que deje la seguridad de la información expuesta a una amenaza.

VII. POLÍTICAS GENERALES

Políticas de servicios de la Dirección de Tecnologías

La Dirección de Tecnologías actualmente cuenta con personal, el cual, tiene a su cargo diversas funciones relativas a la gestión, administración, soporte técnico y mantenimiento de la infraestructura de tecnologías de información y telecomunicaciones; además de personal de desarrollo y mantenimiento de sistemas de información, gestión y administración de recursos de tecnología, administradores de redes y área administrativa. Por lo anterior, se emiten lineamientos en cuanto a los procedimientos de cada área y las políticas de seguridad informática para el conjunto de recursos de infraestructura y de servicios asociados a ellos.

Con fundamento en lo dispuesto en el artículo 43, inciso e), del *Reglamento Orgánico de la Administración Pública Municipal de San Pedro Garza García*, la Dirección de Tecnologías tiene las siguientes atribuciones:

- Determinar, validar y autorizar la adquisición y administración de licencias de software comercial de índole administrativo para las diversas áreas, en beneficio de las operaciones de la Administración Pública Municipal Centralizada;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 20 de 150

- b. Gestionar, administrar y proveer a las y los usuarios de la Administración Pública Municipal Centralizada, los servicios administrados de recursos tecnológicos que requieran para mejorar y eficientar sus funciones administrativas;
- c. Dictar las políticas, lineamientos y requerimientos técnicos para la sistematización, captura, control, seguimiento y resguardo de documentos digitales en poder de la Administración Pública Municipal Centralizada;
- d. Desarrollar, administrar y actualizar los Sistemas de Administración de Recursos Gubernamentales de la Administración Pública Municipal Centralizada;
- e. Validar la adquisición de nuevos equipos de cómputo, dispositivos móviles y equipo de telecomunicaciones, vigilando que el bien a adquirir sea compatible con la infraestructura existente y que cumpla con los estándares de calidad requeridos;
- f. Gestionar la actualización de los equipos, programas, sistemas y redes de voz, datos e imágenes, así como en materia de telefonía fija y acceso a Internet;
- g. Coordinar la capacitación del personal de la Administración Pública Municipal, respecto a los Sistemas de Administración de Recursos Gubernamentales, así como al equipo de cómputo y móvil;
- h. Favorecer e impulsar la adquisición y establecimiento de tecnología de última generación, que permita la constante modernización de la Administración Pública Municipal en su infraestructura tecnológica;
- i. Establecer los lineamientos para el uso adecuado de la tecnología por parte de las y los colaboradores dentro de la Administración Pública Municipal;
- j. Fomentar el desarrollo y establecimiento de sistemas de calidad a los procesos y servicios al respecto del uso de la tecnología;
- k. Proporcionar a la Administración Pública Municipal Centralizada lo necesario en materia de equipos, software comercial de índole administrativo y redes de voz, datos e imágenes, telefonía fija y acceso a internet, así como el mantenimiento y soporte técnico necesarios para los mismos;
- l. Definir, si es necesario con otras áreas, los proyectos de infraestructura tecnológica que ayuden a la eficiencia y mejora continua de la Administración Pública Municipal Centralizada;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 21 de 150

- m. Establecer sistemas de seguridad informática y sistemas de recuperación de desastres (DRP) que permitan la continuidad de los servicios informáticos;
- n. Dictar, promover y hacer cumplir las políticas, lineamientos y requerimientos técnicos para la adquisición y el uso de los recursos informáticos de la Administración Pública Municipal Centralizada; y
- o. Colaborar en el establecimiento de adecuaciones de tecnología para el cumplimiento de requerimientos de leyes y reglamentos que nos obliga en su cumplimiento.

La Dirección de Tecnologías proporciona los servicios descritos en las siguientes secciones, los cuales podrán ser solicitados por las personas usuarias de la Administración Pública Municipal a través de los canales establecidos en el *Manual de Servicios de la Dirección de Tecnologías*, conforme a las siguientes condiciones:

- a. Los plazos de resolución se definen de acuerdo al tipo de servicio; en su mayoría de uno a tres días. Habrá otros en los que demorará más tiempo, por ejemplo, el desarrollo de un nuevo sistema o cambios para los sistemas de información que implican cambios de gran impacto en tiempo y recursos utilizados;
- b. Todos los servicios proporcionados por la Dirección de Tecnologías, invariablemente deberán registrarse en un reporte para su atención, seguimiento y conclusión. Asimismo, deberá proporcionarse la información requerida para su atención, a fin de garantizar la protección de los datos personales, apegada siempre a las normas establecidas para el correcto tratamiento de dicha información, lo que favorece al desarrollo inteligente y sostenible del Municipio;
- c. Los canales por los cuales se deberán solicitar estos servicios son:

- ❖ **Vía registro electrónico en la página:** <https://sanpedrocontigo.mx>; y
- ❖ **Vía aplicación móvil:** San Pedro Contigo

En caso de no contar con acceso a los servicios anteriores, puede utilizar las siguientes formas alternas:

- ❖ **Vía correo electrónico:** Deberá enviar a soporte.tecnico@sanpedro.gob.mx; los datos requeridos para iniciar el proceso de servicio técnico (ver apartado de anexos); y **presencial**; cuando el usuario no cuente con los recursos para realizar el reporte de manera electrónica, puede realizarlo de manera presencial. Para ello,

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 22 de 150

deberá presentar identificación vigente con fotografía emitida por la Dirección de Recursos Humanos adscrita a la Secretaría de Administración e Inteligencia Artificial de San Pedro Garza García, Nuevo León.

- d. Para los servicios que indiquen resolver una falla que esté produzca un impacto importante en los procesos y servicios de la Administración Pública Municipal, se actuará de inmediato para corregir el problema;
- e. Para los mantenimientos evolutivos o gestiones para el desarrollo de nueva aplicación o sistema de información, es necesario presentar el formato correspondiente, (ver apartado de anexos) con la información requerida lo más claro posible, con el objetivo de iniciar las actividades para su concepción, desarrollo, implantación y ejecución. De ser necesario se llevarán a cabo reuniones de trabajo con los solicitantes del servicio;
- f. Los horarios de atención son de lunes a viernes, días laborables, de 8:00 a 16:00 horas y horario extraordinario, sólo cuando la situación lo demande.
- g. La Dirección de Tecnologías deberá de contar con un sistema de información para el registro y seguimiento de solicitudes de servicios técnicos.
- h. La Dirección de Tecnologías, a través de su reporte de diagnóstico (ver anexo: Reporte de Diagnóstico de Equipo de Cómputo) indica al usuario responsable del activo informático sobre las condiciones operativas del activo evaluado. En caso necesario, se indicarán mediante este reporte las refacciones a adquirir para su reparación.
- i. La reparación de un activo informático podrá requerir del reemplazo de piezas o bien el reemplazo del activo por uno nuevo, y para ello la Dirección de Tecnologías apoyará a las personas usuarias en las especificaciones técnicas para su adquisición.
- j. La compra de refacciones se efectuará mediante el proceso de adquisiciones, por conducto del área administrativa correspondiente.
- k. Para los casos en los que se requiera los servicios de un proveedor externo, para el diagnóstico y/o reparación del activo, la Dirección de Tecnologías se encargará de dar seguimiento.
- l. El personal de la Dirección de Tecnologías es el único autorizado para dar servicios o seguimiento de mantenimiento y soporte técnico a resolución de fallas a los equipos de cómputo de la Administración Pública Municipal.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 23 de 150

- m. Para proporcionar una atención más rápida en el seguimiento de algún reporte deberán indicar el folio único, el cual será proporcionado a la persona usuaria durante el registro del reporte.
- n. Para quejas, comentarios o sugerencias respecto a los servicios proporcionados, podrán hacerlo de manera electrónica al correo calidad.tecnologias@sanpedro.gob.mx.
- o. En caso de ser necesario la persona usuaria responsable del activo informático, deberá de presentarlo al domicilio conocido de la Dirección de Tecnologías, para su diagnóstico y/o reparación.
- p. Con el uso de aplicaciones de software de conexión remota, el técnico o cualquier otro empleado de la Dirección de Tecnologías, podrá realizar soporte técnico remoto para reparar fallas reportadas e inclusive proporcionar asesoría remota.
- q. En caso de disponer de los activos informáticos en las instalaciones de la Dirección de Tecnologías, ésta deberá llevar a cabo registro electrónico o físico de los activos recibidos. De igual manera, actualizará el registro cuando sean entregados a la persona responsable o representante del responsable, de vuelta la entrega de activos informáticos.
- r. El proceso de entrega-recepción de activos informáticos, los registros electrónicos generados deberán relacionarse a un ticket de servicio.

Lineamientos para la adquisición de tecnología

La Dirección de Tecnologías en lo relativo a la adquisición de bienes informáticos, en su selección deberá tomar en cuenta lo siguiente:

- **Calidad:** Parámetro cualitativo que especifica las características técnicas de los recursos informáticos;
- **Experiencia:** Presencia en el mercado, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente;
- **Desarrollo tecnológico:** Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 24 de 150

- **Estándares:** Toda adquisición se basa en los estándares; es decir, la arquitectura del fabricante. Esta arquitectura tiene una permanencia mínima de dos a cinco años; y
- **Capacidades:** Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área.

Adquisición de hardware

Para la adquisición de hardware se tendrá en cuenta lo siguiente:

- El equipo que desee adquirir, deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares de la Dirección de Tecnologías;
- En la adquisición de equipos de cómputo, en la medida de lo posible se buscará que éstos incluyan el software preinstalado con su licenciamiento correspondiente;
- Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país;
- La marca de los equipos o componentes deberán contar con presencia y permanencia demostrada en el mercado nacional; así como con asistencia técnica certificada y de repuestos local. Tratándose de computadoras, a fin de mantener actualizada la arquitectura informática de la Administración Pública Municipal;
- Los dispositivos de almacenamiento, así como las interfaces de entrada/salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos como en procesamiento;
- Las impresoras deberán apegarse a los estándares de hardware y software vigentes en el mercado y de la Administración Pública Municipal, por lo que, es importante corroborar que los suministros se consigan fácilmente en el mercado local o nacional;
- Conjuntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento, de acuerdo con las especificaciones de los fabricantes, y que ésta adquisición se refleje en el costo de la partida inicial;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 25 de 150

- h. Los equipos adquiridos deberán contar con asistencia técnica certificada durante la instalación de los mismos; y
- i. En lo que se refiere a los servidores, equipos de comunicaciones, concentradores, conmutadores y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deberán contar con un programa de soporte técnico certificado que incluya el suministro de repuestos al vencer su período de garantía.

Adquisición de software

- Todos los productos de software utilizados, deberán contar con su licencia de uso respectiva; por lo que se realizará la regularización y/o eliminación de los productos que no cuenten con el debido licenciamiento;
- La Dirección de Tecnologías propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros;
- La Dirección de Tecnologías, periódicamente realiza auditorías de Software instalado;
- La Dirección de Tecnologías, promueve la compra de licenciamientos por volumen, ya que esto lleva a beneficios económicos y de control del licenciamiento; y
- La Dirección de Tecnologías llevará el inventario del software (programas) instalados en la Administración Pública Municipal.

Políticas de seguridad lógica

Bases de datos

- La persona administradora de la base de datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema;
- La persona administradora de la base de datos es la encargada de asignar las cuentas a las y los usuarios para el uso;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 26 de 150

- Las contraseñas serán asignadas por la persona administradora de la base de datos en el momento en que la o el usuario desee activar su cuenta, previa solicitud a la persona responsable de acuerdo con el procedimiento generado;
- En caso de olvido de contraseña de una o un usuario, será necesario crear un registro de soporte técnico para que la persona administradora de la base de datos reasigne su contraseña; y
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales. Verificar anexo Construcción de contraseñas seguras.

Recursos de cómputo

Seguridad de cómputo

Las siguientes políticas realizadas por la Dirección de Tecnologías puede realizarlas con el outsourcing de un proveedor experto en seguridad o de manera independiente.

- La Dirección de Tecnologías es la única encargada de definir, suministrar y administrar medidas de seguridad contra la intrusión o daños a la información almacenada en los sistemas; y
- Asimismo, la Dirección de Tecnologías, es la única responsable para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios.

Uso de servicios de red

Áreas administrativas:

- A todas las personas usuarias que se les brinda el derecho de acceso a la información privilegiada, deberán firmar un documento de confidencialidad del uso de la información (véase anexo Convenio de Confidencialidad), contenido en este manual;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 27 de 150

- b. Las personas servidoras públicas adscritas a la Dirección de Tecnologías son las responsables de la administración de contraseñas y deberán guardar su confidencialidad y seguir el procedimiento para manejo de contraseñas;
- c. No se otorgará equipo, contraseñas ni cuentas de correo a personas que presten servicio social o se encuentren en prácticas profesionales dentro de la Administración Pública Municipal, excepto por orden escrita del Director del área correspondiente;
- d. La Dirección de Tecnologías realizará las siguientes actividades en los servidores de la Administración Pública Municipal
- Respaldo de información conforme a los procedimientos establecidos.
- e. Revisión de los "logs" y reporte de cualquier eventualidad;
- Implementar de forma inmediata las recomendaciones de seguridad y reportar posibles faltas a las políticas de seguridad de cómputo; y
 - Monitoreo de los servicios de red proporcionados por los servidores a su cargo.
- f. Organizar y supervisar al personal encargado del mantenimiento preventivo y correctivo de los servidores;
- g. La Dirección de Tecnologías son los únicos autorizados para asignar las cuentas de acceso a las y los usuarios; y
- h. La Dirección de Tecnologías podrá aislar cualquier servidor de red, notificando a las áreas correspondientes, en las condiciones siguientes:
- Si los servicios proporcionados por el servidor implican un tráfico adicional que impida un buen desempeño de la red;
 - Si se reporta un tráfico adicional que comprometa a la red de la Administración Pública Municipal;
 - Si se detecta alguna vulnerabilidad que pueda comprometer la seguridad en la red;
 - Si se detecta la utilización de programas que alteren la legalidad y/o consistencia de los servidores;
 - Si se detectan accesos no autorizados que comprometan la integridad de la información; y

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 28 de 150

- Si se violan las políticas de uso de los servidores.

Usuarios o usuarias

Identificación de usuarios o usuarias y contraseñas:

- Todas las personas usuarias con acceso a un sistema de información o a la red de la Administración Pública Municipal, dispondrán de una única autorización de acceso compuesta de clave de usuario y contraseña;
- Ningún usuario recibirá un identificador de acceso a la red municipal, recursos informáticos o sistemas de información hasta que no acepte formalmente las políticas de seguridad vigente (ver anexo Convenio de Confidencialidad) y, todas las políticas y normas que competen a los usuarios en el uso de los recursos informáticos en el presente manual;
- Todo usuario o usuaria deberá definir su clave de contraseña de acuerdo al procedimiento establecido para tal efecto y será responsable de la confidencialidad de la misma (ver anexos Construcción de Contraseñas Seguras y Convenio de Confidencialidad);
- Las personas usuarias tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones y, así lo autorice el Director del área correspondiente conforme a los procedimientos;
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres especiales, alfabéticos y numéricos;
- Los accesos para personas usuarias temporales se configurarán para un corto período de tiempo;
- La o el usuario deberá renovar su contraseña y colaborar en lo que sea necesario, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:
 - Cuando ésta sea una contraseña débil o de fácil acceso; y
 - Cuando crea que ha sido violada la contraseña de alguna manera.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 29 de 150

- h. Todo usuario o usuaria deberá notificar a los administradores del sistema de información, a la Dirección de Tecnologías, o a las personas titulares de las Direcciones del área, según corresponda en los siguientes casos:
- Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual); y
 - Si tiene problemas en el acceso a los servicios proporcionados.
- i. Si un usuario o usuaria viola las políticas de uso de los servidores, la Dirección de Tecnologías podrá cancelar totalmente su cuenta de acceso, para ello, deberá notificarle a los administradores o personas titulares de las Direcciones del área correspondiente.

Responsabilidades personales:

- a. Las personas usuarias son responsables de toda actividad relacionada con el uso de su acceso autorizado a los recursos de tecnología;
- b. Las personas usuarias no deben revelar bajo ningún concepto sus cuentas de acceso y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros;
- c. Los usuarios o las usuarias no deben utilizar ningún acceso autorizado de otra persona usuaria, aunque dispongan de la autorización del propietario;
- d. Si un usuario o usuaria tiene sospechas de que su acceso autorizado (clave de usuario y contraseña) se ha utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato, al administrador del sistema y/o al administrador de la Dirección de Tecnologías;
- e. Todo usuario o usuaria debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales;
- f. La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas y teléfonos;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 30 de 150

- g. En caso que el sistema no lo solicite automáticamente, la o el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema;
- h. En caso que el sistema no lo solicite automáticamente, la o el usuario debe cambiar su contraseña como mínimo una vez cada 160 días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador, el proceso de bloqueo de la cuenta;
- i. Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos;
- j. Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos y fuera del alcance de terceros;
- k. Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros;
- l. Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos; y
- m. Las personas administradoras de los sistemas de información, deberán notificar por correo electrónico, a la Dirección de Tecnologías, los datos de la o el usuario que ha dejado de tener una relación laboral con la Administración Pública Municipal (baja de personal). Esto, con el objetivo de que los accesos a los distintos recursos de tecnología asignados al usuario le sean retirados.

Uso apropiado de los recursos de tecnología:

Los recursos de tecnología, datos, software, red y sistemas de comunicación de la Administración Pública Municipal, están disponibles exclusivamente para complementar las funciones del personal de la Administración Pública Municipal.

Queda prohibido:

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 31 de 150

1. El uso de estos recursos de tecnología para actividades no relacionadas con los propósitos de la Administración Pública Municipal;
2. Las actividades, equipos o aplicaciones que no estén directamente especificadas como parte del software o de los estándares de los recursos de tecnología propios de la Administración Pública Municipal.
3. Introducir en los sistemas de información o la red municipal contenidos obscenos, amenazadores, inmorales u ofensivos;
4. Introducir voluntariamente programas, virus, macros, "applets", controles "Activex" o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración, obtención de contraseñas, obtención de información confidencial o daño a los recursos de tecnología;
5. Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos;
6. Albergar datos de carácter personal en las unidades locales de disco de las computadoras de trabajo; y
7. Cualquier archivo introducido en la red municipal o en el puesto de trabajo del usuario a través de soportes automatizados, internet, sistema de información, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas políticas y, en especial, las referidas a propiedad intelectual y control de virus.

Sistemas de Detección de Intrusos (IDS):

Un sistema de detección de intrusos (IDS por sus siglas en inglés de Intrusion Detection System) es una aplicación usada para detectar accesos no autorizados a un equipo de cómputo o a una red.

Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas.

Políticas de dispositivos móviles

- a. Para tales efectos se consideran dispositivos móviles los USB, discos duros externos, teléfonos celulares inteligentes, tabletas, lectores del tipo PDA, hand held, computadoras portátiles, etcétera;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 32 de 150

- b. Para cualquier reasignación de dispositivo móvil deberá realizarse a través de la creación de un ticket gestionado por el coordinador administrativo, Director o jefatura del área;
- c. Para el caso de robo o extravío de los dispositivos más significativos por valor económico o con datos clasificados como críticos, deberá gestionarse una denuncia ante el Ministerio Público e informar a las áreas correspondientes. En tales casos, la Dirección de Tecnologías iniciará el proceso de borrado o restablecimiento del dispositivo de manera remota, en la medida de lo posible;
- d. Cualquier aplicativo base necesario en los dispositivos móviles deberá ser provisto sólo por la Dirección de Tecnologías;
- e. Los dispositivos móviles provistos por la Administración Pública Municipal son de uso exclusivo para el desempeño de las actividades laborales encomendadas;
- f. Se asignará un usuario responsable del dispositivo móvil, quién será responsabilizará de su resguardo, buen uso y de cualquier mantenimiento, soporte necesario, asimismo, realizará la gestión del servicio ante la Dirección de Tecnologías;
- g. Es responsabilidad de la o el usuario resguardante el dispositivo móvil, para prevenir cualquier daño, pérdida o robo del dispositivo;
- h. Es responsabilidad de la o el resguardante notificar a la Dirección de Tecnologías, mediante la generación de un ticket de soporte técnico, cuando detecte un funcionamiento incorrecto o detecte una desactivación u otra anomalía del dispositivo móvil;
- i. Si el dispositivo está perdido, robado o se sospecha que está comprometido en cualquier sentido, la persona usuaria debe notificar inmediatamente mediante el procedimiento establecido (reporte de soporte, robo o extravío de dispositivos móviles);
- j. Para el caso de adquisición de dispositivos móviles por nueva compra o reposición, deberá iniciarse el proceso administrativo de adquisición establecido;
- k. Es responsabilidad de la persona usuaria resguardante del dispositivo móvil mantener respaldos de la información contenida de estos dispositivos;
- l. No está permitido que los usuarios realicen cambios de parámetros o de configuración de los dispositivos móviles, cuando estas configuraciones vienen establecidas de fábrica o son establecidas por la Dirección de Tecnologías, esta última es la única que autorizará y realizará nominalmente la realización de estos cambios;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 33 de 150

- m. La persona usuaria resguardante no debe compartir el dispositivo móvil con personas externas a la Administración Pública Municipal, a fin de prevenir que tengan acceso a los recursos asociados de los mismos;
- n. La persona usuaria resguardante no debe compartir el dispositivo, compartir credenciales de acceso u otras llaves. Y en caso que se vaya a reasignar o retirar el dispositivo, asegurarse que no se queden llaves o credenciales guardadas en el dispositivo;
- o. El área administrativa que realice la recepción de dispositivos móviles deberá coordinarse con la Dirección de Tecnologías para su preparación, inventario y medidas de seguridad establecidas por la Dirección de Tecnologías para su uso seguro;
- p. Las personas usuarias deben respetar las siguientes medidas preventivas de seguridad para proteger la información y las aplicaciones instaladas en los dispositivos asignados:
 - 1. Los dispositivos no deben quedar a la vista en un vehículo desatendido, aunque sea por un periodo corto de tiempo;
 - 2. Los dispositivos no deben dejarse en un vehículo durante toda la noche;
 - 3. Si en la pantalla del dispositivo móvil se está mostrando información sensible en un lugar público, se deberá posicionar de tal manera que la información no pueda ser vista por otros;
 - 4. En situaciones que impliquen mayor exposición o riesgo, tales como eventos en colonias, áreas de atención al público, centros de conferencias u otros espacios similares, el dispositivo no deberá quedar desatendido bajo ninguna circunstancia;
 - 5. Para asegurar el almacenamiento adecuado, solo se almacenarán los datos necesarios para propósitos laborales; y
 - 6. En lugares públicos deberá evitar conectarse a redes wifi públicas.

Responsabilidades de la Dirección de Tecnologías:

- a. Identificar e inventariar los dispositivos móviles propiedad de la Administración Pública Municipal, los cuales deberán etiquetarse por la Dirección de Tecnologías para su identificación visible, mediante el uso de etiquetas resistentes y durables;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 34 de 150

- b. Establecer las condiciones de uso de los dispositivos móviles y comunicarlas a las personas responsables de su resguardo y utilización;
- c. Garantizar que las tecnologías, aplicaciones, así como los medios de comunicación utilizados sean seguros y confiables;
- d. Asegurar que las aplicaciones para dispositivos móviles estén disponibles y optimizadas;
- e. Bloquear el acceso a los dispositivos móviles sin una autorización previa o cuando se comprometa la integridad, disponibilidad y confidencialidad de la información; y
- f. No es responsabilidad de la Dirección de Tecnologías recuperar ningún tipo de información en caso de que el dispositivo se haya perdido, robado o dañado.

Responsabilidades de las personas usuarias resguardantes de dispositivos de la Administración Pública Municipal:

- a. El cumplimiento de las condiciones de uso de los dispositivos establecidos por la Dirección de Tecnologías, aun cuando sean utilizados dentro o fuera de las instalaciones de la Administración Pública Municipal;
- b. Llevar el dispositivo a la Dirección de Tecnologías, cuando sea solicitado por el personal de esta Dirección, ya sea por razones de auditoría, administración, configuración, seguridad, soporte técnico, etcétera;
- c. Deberá llenar el formato de entrega-recepción de equipo de cómputo y presentar copia de identificación oficial con fotografía, toda vez que acuda a recoger equipo de cómputo a la Dirección de Tecnología;
- d. Tener el debido cuidado de la integridad física del dispositivo;
- e. Tomar las precauciones apropiadas para prevenir cualquier daño, pérdida o robo del dispositivo;
- f. En caso de robo o extravío, el usuario responsable del dispositivo deberá notificar inmediatamente a su superior, a la Dirección de Tecnologías de la situación y realizar la denuncia correspondiente;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 35 de 150

- g. Realizar los respaldos y atender los mensajes del equipo de cómputo, en caso de requerir apoyo, deberá inmediatamente notificar por los canales establecidos a la Dirección de Tecnologías;
- h. Evitar el bloqueo de las limitaciones del fabricante y/o proveedor, o realizar cualquier otro método de cambio de las protecciones que se han establecido en el dispositivo;
- i. Será obligatorio firmar el acta de entrega-recepción de activos informáticos y presentar copia de una identificación oficial con fotografía al momento de la asignación de activos informáticos o cuando se formalice un cambio de resguardante;
- j. Los usuarios deberán cuidar, respetar y hacer uso adecuado de los activos informáticos y de la infraestructura de la red de la Administración Pública Municipal, de acuerdo con las políticas que en este documento se mencionan;
- k. El usuario deberá proteger los activos informáticos contra el acceso, divulgación, modificación, destrucción o interferencia no autorizada; y
- l. Atender a las demás disposiciones de este y otros reglamentos, así como de leyes aplicables al comportamiento y buen uso de los dispositivos móviles dentro y fuera de las instalaciones de la Administración Pública Municipal.

Políticas de teletrabajo

La Administración Pública Municipal, mediante la Dirección de Tecnologías cuenta con herramientas y condiciones para permitir el teletrabajo a los empleados que así lo ameriten, por situaciones de terminación de proyectos a tiempo, pandemia, o incapacidad temporal de acudir a las oficinas de la Administración Pública Municipal a laborar de manera presencial.

- a. Los empleados que desarrollen sus funciones de manera remota, es necesario que soliciten una conexión de red privada (VPN's, Virtual Private Network) mediante la creación de un ticket de soporte técnico en la página <https://sanpedrocontigo.mx>;
- b. Los empleados que soliciten las herramientas para laborar de manera remota, es imprescindible que su jefe Director o Secretario le autorice trabajar en estas condiciones;
- c. Los empleados que requieran desarrollar sus funciones de manera remota, es necesario que cuenten con dispositivos móviles, proporcionados por la Administración Pública Municipal;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 36 de 150

- d. La Dirección de Tecnologías deberá asegurarse que el o los dispositivos móviles a cargo del empleado, cuenten con las herramientas necesarias de ciberseguridad para poder laborar remotamente de manera segura;
- e. Las condiciones ambientales idóneas en las que se deberán operar los dispositivos móviles en sitio, así como las conexiones de internet, las deberá proveer el empleado;
- f. La instalación y/o revisión de las herramientas de conexión segura, la realizará la Dirección de Tecnologías mediante un soporte técnico con conexión remota o presencial al dispositivo móvil del empleado;
- g. En el reporte de soporte deberá proporcionar adicionalmente los datos propios del formulario de soporte, el periodo de tiempo y horario en el que realizarán las conexiones para trabajo remoto;
- h. En caso que se requiera más tiempo de trabajo remoto, deberá generarse nuevamente un ticket de soporte con la información de los nuevos periodos. Por lo que, esto puede considerarse como una renovación a las credenciales de acceso a los recursos información de la Administración Pública Municipal;
- i. De conformidad con lo dispuesto en la fracción VI, del artículo 330-E de la *Ley Federal del Trabajo*, relativo al derecho de las personas trabajadoras a la desconexión digital y al respeto de sus periodos de descanso, asimismo, relativo a que la modalidad de trabajo a distancia podrá implementarse de manera excepcional, y en atención a las necesidades del servicio y previa autorización de la autoridad competente, se establecen las siguientes disposiciones:
 1. Cuando el personal adscrito a Administración Pública Municipal desempeñe sus funciones bajo la modalidad de trabajo a distancia o esquema híbrido autorizado, el Municipio no asumirá la obligación de proporcionar mobiliario, bienes inmobiliarios, adecuaciones físicas en el domicilio particular de la persona servidora pública, ni el pago o reembolso de gastos derivados del consumo de energía eléctrica, servicio de internet u otros servicios domésticos necesarios para la prestación del servicio remoto;
 2. La adopción de la modalidad de trabajo a distancia implica que la persona servidora pública acepta realizar sus actividades desde un espacio propio, bajo su responsabilidad y con los recursos domésticos disponibles, salvo que exista disposición expresa contrario mediante instrumento jurídico, lineamiento específico o acuerdo formal debidamente autorizado por la autoridad competente; y
 3. Lo anterior, no exime a la persona servidora pública del cumplimiento de sus obligaciones laborales, ni modifica las responsabilidades institucionales relacionadas con la seguridad de la información, uso adecuado activos tecnológicos municipales y la observancia del marco normativo aplicable.
- j. El empleado deberá acatar las políticas sobre uso de dispositivos móviles, uso de infraestructura informática del Municipio.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 37 de 150

Políticas de seguridad de los recursos humanos

Las personas son el activo más importante de una organización, a su vez, podemos considerar que los errores humanos son normalmente el mayor riesgo para la seguridad de la información:

- Para todo personal seleccionado, se deberán implementar competencias de seguridad de la información a cada uno de ellos;
- Todos los empleados o proveedores de servicios con acceso a información sensible, firmarán acuerdos de confidencialidad o de no divulgación antes de que tengan los permisos para acceder a dicha información;
- Una vez que finalice la relación contractual entre la organización y los empleados o proveedores de servicios, deberán verificarse y eliminar los accesos establecidos a ellos. Para el caso que se necesite proporcionar información o acceso a los activos de la organización a personas físicas o morales sin relación contractual con la organización para realización de pruebas de concepto o de funcionalidad, será necesario firmar acuerdos de confidencialidad;
- Los empleados y proveedores de servicios tendrán que informarse de las acciones a tomar, si el empleado o proveedor de servicios desatiende los requisitos de la seguridad de la organización;
- El área encargada de la contratación y terminación o finiquito laboral con los empleados, deberá informar a la Dirección de Tecnologías, cualquiera de estos eventos. En el caso de terminación de la relación laboral, automáticamente se le retirarán los derechos y accesos con que contaba en ese momento; y
- Al momento de la terminación laboral, los activos informáticos asignados al empleado que concluye la relación laboral, en caso de que no haya un reemplazo, se deberán reasignar a un responsable de los mismos. El responsable podrá ser de la misma área del empleado finiquitado o bien un responsable de la Dirección de Tecnologías.

La forma en que la Dirección exige se cumplan con las políticas, normas y procedimientos establecidos para la seguridad de la información.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 38 de 150

Condiciones de cumplimiento:

- Capacitación a los empleados en sus responsabilidades sobre la seguridad de la información antes de que tengan acceso a los activos de información;
- Informar sobre los resultados que la organización espera de sus funciones en relación a la seguridad de la información;
- Establecer canales de comunicación para mantener la conciencia y la motivación suficiente a los empleados para que cumplan con sus obligaciones en las tareas de la seguridad de la información;
- Establecer canales de comunicación para que los empleados comenten sobre los métodos de trabajo y la parte que les afecta de las políticas de la seguridad de la información;
- Mantener el proceso de formación continua para mantener las habilidades en el desarrollo de las tareas de seguridad de la información; y
- Establecer canal de comunicación que garantice el anonimato para denunciar los fallos y violaciones a las normas sobre la seguridad de la información.

En la formación y concientización deben de incluirse:

- Compromiso de la Dirección de Tecnologías con la seguridad de la información en toda la organización;
- Conocimiento y el cumplimiento de las obligaciones aplicables de seguridad de la información contenida en las políticas, normas, contratos, etcétera;
- Responsabilidad de los empleados y proveedores de servicios de sus propias acciones u omisiones en la protección de la información; y
- Los procedimientos básicos de la seguridad de la información, por ejemplo:
 - Procedimiento de notificación de incidentes de seguridad;
 - Procedimientos sobre uso de contraseñas seguras;
 - Controles sobre software malicioso;
 - Escritorios limpios;
 - Respaldos en la nube;
 - Manuales;
 - Puntos de contacto; y
 - Entre otros

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 39 de 150

Proceso disciplinario

Con el propósito de promover el cumplimiento de las disposiciones en materia de seguridad de la información, se establecerá un sistema disciplinario aplicable a los incumplimientos de las políticas, lineamientos, procedimientos y controles de seguridad de la información. Dicho proceso deberá ser formal y comunicado a los empleados.

El proceso disciplinario al menos debe incluir:

- El aseguramiento con evidencia de la infracción que se ha cometido;
- Evitar tratamiento injustos o incorrectos a los empleados; y
- Considerar respuestas graduales en consideración de la gravedad, el impacto, si es deliberado o existe antecedente.

Responsabilidades en la desvinculación laboral

Se trata de establecer y comunicar al empleado las responsabilidades sobre la seguridad de la información después de finalizar un contrato o ante el cambio de empleo.

Cuestiones que se deben incluir durante en el proceso de desvinculación laboral:

- Responsabilidades de la desvinculación;
- Responsabilidades incluidas en los acuerdos de confidencialidad;
- Periodo de vigencia de accesos a activos de la organización;
- Deberes y responsabilidades que permanecen válidos después de la desvinculación; y
- Cambiar o actualizar las responsabilidades en los términos y condiciones del empleo, ante cambios de empleo dentro de la organización.

Políticas de gestión de los activos

- La gestión de los activos tiene como objetivo responsabilizarse de los activos, mediante una protección que incluya la identificación de los propietarios, también asegurar la clasificación, según un nivel adecuado de protección;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 40 de 150

- La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados, así como elaborarse y mantenerse en inventario;
- La Dirección de Tecnologías es responsable de elaborar, mantener y actualizar el inventario de activos de tecnología de la Administración Pública Municipal;
- Se deberá tener un propietario para cada activo, alguien que se haga responsable de su uso y protección;
- Las áreas administrativas conjuntamente con la Dirección de Tecnologías, deberán colaborar para actualizar y mantener el inventario de los activos de información;
- Para cada uno de los activos de la organización, se deben clasificar según el tipo y sensibilidad basados en las normas de gestión los podremos clasificar en bajo, moderado y alto (NIST) o bien en pública, interna, confidencial (ISO/IEC 27011:2022 – Anexo A 5.12);
- La Dirección de Tecnologías deberá contar con un sistema para el control del ciclo de vida de los activos, de acuerdo a la *Norma ISO 27001*, se considerarán para el registro de los activos, entre otros datos, los siguientes:
 - Identificador único:** etiqueta de TI y/o etiqueta de patrimonio;
 - Tipo de activo:** hardware, software, datos o humano;
 - Nivel de criticidad:** basado en el impacto que tendrá su pérdida, mal uso o compromiso;
 - Responsable asignado:** una persona o rol que se encargue de su protección y uso correcto; y
 - Información clave:** ubicación, nivel de confidencialidad, valor estimado y estado dentro del ciclo de vida (activo, fuera de servicio, dado de baja, entre otros).

La Dirección de Tecnologías deberá tener visibilidad sobre cada etapa del ciclo de vida de los activos para asegurar su correcto uso, mantenimiento y eliminación. Por lo que, se considerará cada una de las siguientes etapas:

- Documentar y controlar:** registro desde el proceso de adquisición, uso, mantenimiento, transferencia, baja o eliminación;
- Uso y mantenimiento:** mantener actualizados los parches de seguridad, configuración, accesos y permisos;
- Transferencia o reutilización:** si un activo cambia de área o usuario, debe quedar registro de quien entrega y recibe y, bajo qué condiciones;
- Registro de eventos importantes asociados al activo:** incidentes de seguridad, cambios técnicos o movimientos físicos;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 41 de 150

- e. **Aplicación de políticas de eliminación segura:** cuando el activo ya no se usa por obsolescencia, incosteabilidad de reparación, falta de refacciones en el mercado para su reparación, etcétera, debe eliminarse correctamente. En el caso de dispositivos, esto incluye métodos como el borrado seguro de discos, para evitar fugas de información; y
- f. La Dirección de Tecnologías dispone a los propietarios o usuarios de los activos la página www.sanpedrocontigo.mx, en la que podrán registrar la solicitud de algún soporte para la resolución de mal funcionamiento, acceso a servicios, etcétera.

Adquisición y controles de licenciamiento

- a. Todos los productos de software utilizados deberán contar con su licencia de uso respectiva, por lo que, se realizará la regularización y/o eliminación de los productos que no cuenten con el debido licenciamiento;
- b. La Dirección de Tecnologías propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros;
- c. La Dirección de Tecnologías realizará periódicamente auditorías de software instalado;
- d. La Dirección de Tecnologías promueve la compra de licenciamientos por volumen, ya que esto lleva a beneficios económicos y de control del licenciamiento;
- e. La Dirección de Tecnologías llevará el inventario del software (programas) instalados en la Administración Pública Municipal;
- f. La Dirección de Tecnologías, contará con herramientas de ciberseguridad para monitoreo continuo de aplicaciones, en caso de detectar alguna aplicación maliciosa, virus u otro programa que ponga en peligro la información y los recursos informáticos de la Administración Pública Municipal, el equipo se pondrá en cuarentena, lo anterior, será requerido para su revisión; y
- g. Si un usuario desea utilizar programas informáticos, deberá consultar previamente con la Dirección de Tecnologías para su aprobación, gestión y uso.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 42 de 150

Políticas de control de acceso

Las políticas de control de acceso son un conjunto de reglas y directrices que definen quién, cómo, y cuándo pueden acceder a sistemas, datos o recursos protegidos.

Para garantizar la protección de la información y el acceso adecuado a los sistemas institucionales, el control de acceso deberá regirse por los siguientes principios y disposiciones:

- La persona usuaria tiene acceso a la información requerida para realizar sus funciones con previa autorización; así mismo, deberá evitar incurrir en alguna violación en materia de seguridad;
- Los sistemas de información adquiridos o desarrollados internamente, cuando éstos son transversales a distintas dependencias o áreas administrativas de la Administración Pública Municipal, la responsabilidad del control de accesos estará a cargo de la Dirección de Tecnologías;
- Para los sistemas de información desarrollados internamente o adquiridos con alcance mayoritariamente a los empleados pertenecientes a la Secretaría de quien ejerce el presupuesto para adquisición o desarrollo del sistema de información, se identificará un empleado o área responsable para el control de accesos a la información; y
- Primordialmente el control de acceso estará basado en Accesos Basados en Roles (RBAC).

Políticas de seguridad física y del entorno

Acceso físico:

La Dirección de Tecnologías cuenta con un Centro de Datos Principal (Data Center), en el que se ubica la información centralizada de los sistemas de información, servidores y la administración de la red principal de datos y telefonía, así como centros de datos secundarios que distribuyen cargas de servicio y administración en áreas específicas.

Todos los sistemas de telecomunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no autorizado tenga acceso físico directo.

El acceso a terceras personas deberá vigilarse, identificarse y controlarse con el uso de la identificación, que les será asignada por el área de recepción de la oficina de la Dirección de Tecnologías.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 43 de 150

Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de la Dirección de Tecnologías.

Las visitas a las instalaciones físicas de los centros de telecomunicaciones estarán autorizadas, organizadas y se harán en el horario establecido por la Dirección de Tecnologías.

Para los proveedores de servicios que muevan, cambien, entreguen o extraigan equipo para reemplazo o mantenimiento del centro de cómputo, deberán ser autorizados por la Dirección de Tecnología.

La Dirección de Tecnologías, deberá establecer mecanismos de registro y de control de acceso en sus instalaciones, de toda persona externa visitante con motivos de trabajo y reunión a las distintas áreas operativas críticas.

Un empleado designado de la Dirección de Tecnologías deberá dar acceso a los visitantes por motivos de visita para mantenimiento o reparación. Por ningún motivo, se proporcionarán las claves de acceso a los externos a menos que éstas sean temporales.

Las claves de acceso temporales permanecerán activas sólo durante el periodo de trabajo.

Protección física

El centro de datos deberá:

- Tener una puerta de acceso de vidrio templado transparente, para favorecer el control de uso de los recursos de cómputo;
- Ser un área restringida. Contar con un sistema de control de acceso que garantice la entrada solo al personal autorizado por la Dirección de Tecnologías;
- Recibir limpieza al menos una vez por semana, a fin de mantenerse libre de polvo;
- Estar libre de contactos e instalaciones eléctricas en mal estado;
- Contar con climas de precisión que permita mantener siempre constante la misma temperatura;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 44 de 150

- f. Asignar un técnico para llevar un registro de estos controles de mantenimiento de los equipos;
- g. Contar con respaldo de energía redundante;
- h. Seguir los estándares de protección eléctrica vigente para minimizar el riesgo de daños físicos a los equipos de telecomunicaciones y servidores;
- i. Contar con sistemas de tierra física, sistemas de protección e instalaciones eléctricas, los cuales deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema;
- j. Contar con algún esquema que asegure la continuidad del servicio;
- k. Contar con controles de humedad;
- l. Contar detectores contra incendios; y
- m. Contar por lo menos con dos extintores contra incendio adecuado y cercano al centro de datos.

Políticas de seguridad en las operaciones

Se trata de asegurar la operación de forma correcta y segura en las instalaciones de procesamiento de información.

Los procedimientos deberán estar documentados y disponibles. La documentación de procedimientos al menos debe abarcar aquellas actividades que afectarán al procesamiento de la información y aquellas que la protegen.

De acuerdo a este principio se debe de incluir:

- a. Los procesos de verificación, instalación, configuración, así como la administración de sistemas y aplicaciones;
- b. La forma en que se procesa y maneja la información;
- c. Documentación de la gestión de los respaldos de la información, incluidas las pruebas y la verificación de copias de seguridad;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 45 de 150

- d. La gestión de la programación operación en el caso de procesos que requieran programación de tiempos;
- e. Manejo de errores y condiciones excepcionales que puedan definirse como incidentes de seguridad;
- f. Instrucciones especiales de manejo de medios para información confidencial, incluida la eliminación segura, recuperación / reinicio del sistema;
- g. Los procesos de gestión de registros y elementos de seguimiento de auditoría; y
- h. Los procedimientos de monitoreo de red y activos de información.

Gestión de los cambios

Los procesos de cambio pueden conllevar riesgos asociados con la seguridad de la información. Es por ello que, la Dirección de Tecnologías deberá analizar los procesos de cambio en instalaciones o infraestructuras de equipos y software, sistemas de procesamiento de información. Asimismo, la Dirección debe analizar los riesgos y la aplicabilidad de los cambios.

Tratándose de activos en los que la Dirección de Tecnologías no es responsable, gestionará la autorización formal ante la instancia correspondiente para la realización de los cambios.

La Dirección de Tecnologías establecerá una planificación para los cambios a realizar en equipos, sistemas software, etcétera, e invariablemente realizará pruebas y notificará los resultados de estas a todos los involucrados.

Finalmente, la Dirección de Tecnologías mantendrá un registro que contenga al menos la información siguiente:

- a. Quien autoriza los cambios;
- b. Quien o quienes realizan los cambios;
- c. Fecha de ejecución;
- d. Descripción de las tareas;
- e. Validaciones de los cambios; y
- f. Otros que considere relevantes.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 46 de 150

Esta información será útil en las auditorías, con la finalidad de tener certeza de que los cambios se han realizado de manera controlada.

Gestión de la capacidad

Tiene como finalidad evitar la pérdida de disponibilidad o rendimiento de los sistemas por falta de capacidad.

Gestionar la capacidad se refiere a tener un control del uso de los recursos. Esto se traduce en controles para:

- Medición y seguimiento del uso de los recursos;
- Previsión de uso a futuro (prever cuello de botella);
- Planificar las ampliaciones de capacidad de los recursos cuando sea necesario; y
- Optimizar el uso de los recursos, por ejemplo, optimizar las consultas de las bases de datos, deberá realizar procesos por lotes fuera de horario de carga de trabajo, eliminación de archivo de datos antiguos y aceleración del ancho de banda para accesos no críticos.

Separación de los ambientes de desarrollo, prueba y operación

En base a la *Norma ISO 27001* y buenas prácticas, se requiere separar los entornos de desarrollo de los entornos de producción para evitar problemas de indisponibilidad o fallos en el servicio.

Los entornos de desarrollo, código fuente y herramientas de desarrollo, no deben estar disponibles para los entornos de producción, a fin de evitar problemas de seguridad.

Por otro lado, relativo a los datos utilizados en entornos de desarrollo, no podrán copiar datos de producción a menos que se hayan previsto controles de seguridad (acuerdo de confidencialidad, etcétera) similares a los entornos de desarrollo.

La Dirección de Tecnologías implementará controles para prevenir la incorporación de código malicioso, no autorizado o no validado en los desarrollos de software, mediante la adopción de metodologías y prácticas como el Ciclo de Vida de Desarrollo Seguro (Secure Software Development Life Cycle, SSDLC), el Ciclo de Vida de Desarrollo de Software (Software Development Life Cycle, SDLC) y enfoques de Operaciones de Seguridad (Security

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 47 de 150

Operations, SecOps), que contemplen el monitoreo continuo, la detección y respuesta ante incidentes, la automatización de procesos, la colaboración entre áreas y la integración de controles de seguridad en cada fase del proceso de desarrollo.

Protección ante software malicioso

La Dirección de Tecnologías actualmente cuenta con un área encargada de la ciberseguridad y con herramientas que, en su implementación, monitoreo, procedimientos y seguimiento permite aminorar los riesgos de ser atacados por software malicioso. Asimismo, implementa sistemas de detección de código malicioso en los servidores y equipos de trabajo. Además, ejecuta programas de concientización dirigidos a los servidores públicos del Municipio con la finalidad de aminorar los riesgos de seguridad de la información.

Requisitos para los usuarios

La Dirección de Tecnologías en conjunto con la Coordinación de Cultura Organizacional de la Dirección de Administración de Bienes Municipales y Cultura Organizacional adscrita a la Secretaría de Administración e Inteligencia Artificial, organiza y presenta en reunión remota y/o presenciales temas de seguridad de la información, con el objetivo de concientizar a los usuarios en el uso de la tecnología, esto, a fin de evitar prácticas que pongan en riesgo la información contenida en los distintos dispositivos a su cargo o responsabilidad. Además, se informa los medios o canales oficiales para reportar incidentes en la gestión y tratamiento diario de la información en sus áreas de trabajo.

Asimismo, se construyen, mantienen y actualizan día con día listas negras de sitios conocidos o se restringe el uso del internet en los puestos de trabajo si no es necesario para el desempeño de sus funciones.

Requisitos para los sistemas

Actualmente, la Dirección de Tecnologías implementa herramientas tecnológicas en los puestos de trabajo para restringir la ejecución de código malicioso alojado en dispositivos extraíbles, al ser éstos conectados a diversos dispositivos y puedan causar daño a la información e infraestructura tecnológica del Municipio. Asimismo, se utilizan herramientas de antivirus que verifican los archivos que se procesan o envían por correo.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 48 de 150

Por tal motivo, la Dirección cuenta con herramientas que son utilizadas en caso de presentarse algún incidente de seguridad en el equipo de trabajo, éste se ponga en cuarentena, a fin de evitar que se propague algún código malicioso por el resto de la infraestructura y dispositivos conectados a la red municipal.

En virtud de lo anterior, todo usuario tiene prohibido la introducción de software no autorizado por la Dirección de Tecnologías, o bien la desinstalación de software, previamente instalado a su equipo resguardado.

Ahora bien, a fin de aminorar los riesgos de sufrir un ataque provocado por un software malicioso, la Dirección ejecuta las siguientes acciones:

- El uso de herramientas para monitoreo de software y datos de la red;
- Se ejecutan procedimientos para la instalación de herramientas de escaneo de los equipos, servidores y estaciones de trabajo, en tanto se instala software o programado de manera diaria en búsqueda de software malicioso; y
- Los escaneos incluyen archivos adjuntos de correo electrónico, descargas y páginas web.

Respaldo - copias de seguridad

Tiene como finalidad, evitar la pérdida de datos mediante la aplicación de políticas de copias de seguridad que permitan asegurar la disponibilidad de la información ante incidentes.

Por tal motivo, se utiliza un software con la automatización de copias de seguridad de la información, datos y configuración de los distintos servidores críticos en la operación de los trámites, servicios o procesos de la Administración Pública Municipal.

La Dirección de Tecnologías llevará a cabo un proceso de comprobación de los respaldos, a manera de asegurar que los datos se restauren de forma completa y sin errores, asegurando así la confiabilidad del proceso del respaldo y restauración de los datos respaldados. Este proceso está alineado al de restauración del DRP en grupos de prueba.

Asimismo, se conservarán registros de las copias de seguridad conforme al cronograma o plan de mantenimiento correspondiente, así como de las pruebas realizadas para verificar su validez.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 49 de 150

Por otro lado, se mantendrán los mismos niveles de protección para las copias de seguridad que los requeridos para los datos operativos. Además, cuando sea necesario las copias de seguridad estarán encriptadas.

Para cada sistema de información se tendrá trazabilidad y monitorización sobre los eventos que se realizan en cada sistema de información. De esta forma, aplicamos un registro que nos permita identificar la autoría y los tipos de acciones que se han ejecutado en dicho sistema.

También, se instalarán herramientas que permitan el respaldo de información de las estaciones de trabajo en la nube. Específicamente la herramienta Google Drive, permitirá el respaldo de la información generada en las estaciones de trabajo, servicio bajo demanda y sobre todo para activos catalogados como críticos.

Registros de eventos

Para cada sistema podría variar los eventos a registrar, se consideran los siguientes:

- Intentos de acceso exitosos y fallidos;
- Desconexiones del sistema;
- Acciones ejecutadas;
- Dirección del equipo cliente;
- Alertas por fallos en el sistema;
- Fecha y hora en que se producen los eventos;
- Tiempos de detención (downtime); y
- Resultado de la ejecución, entre otros.

Definir a la persona usuaria responsable del sistema con funciones de administración operativa del mismo. Esta misma persona será la responsable de revisar de manera periódica, independientemente de si hay un incidente o no, detectar posibles actividades fraudulentas, o detectar el origen de fallos de funcionamiento, antes de que ocurran

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 50 de 150

incidentes importantes. Este usuario administrador operativo podrá reportar incidentes, cuando los descubra, a la Dirección de Tecnologías mediante los canales establecidos.

Protección de la información de registros (logs)

Los sistemas de información, tendrán el nivel de protección apropiado para evitar pérdidas, corrupción o cambios no autorizados. La Dirección de Tecnologías tendrá la obligación de establecer los controles para dicha protección.

En ningún caso, el administrador operativo o el usuario del sistema tendrá permiso para eliminar o desactivar el registro de sus propias actividades. Invariablemente, se guardarán copias de seguridad de los registros de eventos.

Sincronización de relojes

Todos los sistemas de desarrollo internos están sincronizados con el servidor del directorio activo de la red de la Administración Pública Municipal, el cual, es la única fuente de tiempo de referencia. Internamente, las redes utilizan el protocolo que sincronizan los relojes de todos los dispositivos informáticos con una fuente de tiempo precisa y fiable denominada Network Time Protocol (NTP)

Control de software en la producción

La Dirección de Tecnologías cuenta con herramientas para el control de instalación y uso de aplicaciones en los dispositivos de la Administración Pública Municipal, por lo que, todas las aplicaciones de los dispositivos pertenecientes al Municipio, deberán ser autorizados, instalados, mantenidos o desinstalados, solo por personal de la Dirección de Tecnologías.

Por lo anterior la Dirección de Tecnologías estableció los siguientes controles:

- Prueba las nuevas aplicaciones o software en entornos aislados especialmente preparados para pruebas;
- Comprueba previamente las necesidades de instalación (compatibilidad del entorno);
- Valorar la necesidad de actualización o instalación;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 51 de 150

- d. Planificar la forma de volver a versiones anteriores, en caso de ser necesario;
- e. Los entornos de desarrollo deben permanecer aislados de los entornos operativos;
- f. La instalación de software debe realizarse exclusivamente por personal autorizado de la Dirección de Tecnologías;
- g. Establecer procedimientos o herramientas de monitoreo del software para detectar cambios no autorizados; y
- h. Las pruebas posteriores a la implementación deben incluir una supervisión de la red para identificar cualquier tráfico inesperado que pueda exponer errores o suponga un empeoramiento de la velocidad de las transmisiones.

Gestión de vulnerabilidades técnicas

La Dirección de Tecnologías, con el objetivo de reducir el número de ataques informáticos a nuestros activos de información, activos informáticos, etcétera, realiza de manera programada pruebas de ataques simulados (hacking ético), escaneos periódicos de vulnerabilidades, mantiene actualizados los sistemas de seguridad y operativos, entre otras acciones.

Asimismo, la Dirección podrá requerir la presentación y/o retención de los activos de tecnología cuando lo considere necesario, por motivos de seguridad, mantenimiento o por cualquier otro motivo que considere conveniente.

Exclusivamente Directores o niveles superiores encargados del área administrativa, podrán gestionar ante la Dirección de Tecnologías el retiro de las credenciales de acceso a los distintos activos informáticos asignados a un empleado de su área, por los motivos que considere pertinentes derivados de investigación, seguridad, auditoría, pérdida de confianza, etcétera.

Controles de auditoría de sistemas información

En este caso, nos referimos a las auditorías de los sistemas de información para evaluar los siguientes casos:

- a. Que los usuarios estén trabajando con los privilegios correctos;
- b. La estabilidad y confiabilidad en la infraestructura tecnológica sobre la que opera el sistema de información;
- c. Que la infraestructura cuente con suficiente capacidad (memoria, procesamiento, almacenamiento, ancho de banda);

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 52 de 150

- d. Buscar mejoras del sistema;
- e. Lograr la efectividad de las pruebas realizadas;
- f. Programación de actividades de mantenimiento, monitoreo y gestión; y
- g. Monitoreo de acciones de los usuarios del sistema.

Políticas de seguridad de las comunicaciones

El objetivo es establecer controles para proteger la infraestructura tecnológica de telecomunicaciones de la Administración Pública Municipal, con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información transmitida a través de redes internas y externas.

El alcance es aplicable a todas las redes de telecomunicaciones utilizadas en la Administración Pública Municipal, incluidas las redes LAN, WAN, VPN, enlaces inalámbricos, redes móviles y cualquier otro medio de transmisión de datos. Por tal motivo, se consideran los siguientes criterios:

- a. La Dirección de Tecnologías es la encargada de establecer controles de seguridad para salvaguardar la confidencialidad, integridad y disponibilidad de la información, a través de la infraestructura tecnológica establecida en la Administración Municipal;
- b. Las telecomunicaciones deben estar protegidas contra accesos no autorizados, interceptores, alteraciones y pérdidas de servicio;
- c. La Dirección de Tecnologías implementa controles técnicos y administrativos para asegurar la transmisión segura de la información;
- d. Toda conexión con redes externas debe estar debidamente autorizadas, controladas y monitoreadas;
- e. En la seguridad de la infraestructura de la red se utilizarán firewalls, sistemas de detección y prevención de intrusos (IDS/IPS), y segmentación de red para proteger los perímetros;
- f. La red del Municipio solo podrá acceder a los parámetros que el Firewall tenga permitido o posibilite mediante su configuración;
- g. En la infraestructura de la red, las redes críticas estarán separadas lógicamente mediante VLANs o físicamente cuando sea necesario;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 53 de 150

- h. Toda la transmisión de información sensible deberá realizarse mediante protocolos seguros (por ejemplo, TLS, IPsec, SSH, VPN);
- i. Se utilizarán certificados digitales válidos y actualizados para garantizar la autenticidad de las conexiones;
- j. En las conexiones remotas a la red municipal, deberá realizarse exclusivamente mediante VPN's seguras y autenticación multifactor;
- k. Los usuarios de la Administración Pública Municipal podrán gestionar el uso de VPN's para gestión remota;
- l. Se registrarán y se monitorearán todas las sesiones remotas "bajo demanda"; esto significa que cuando se crea conveniente por la importancia del soporte técnico o como evidencia del trabajo realizado por la Dirección de Tecnologías o Proveedor del trabajo contratado, se graben en video o imágenes las acciones realizadas en los equipos de la administración pública municipal, a manera de evidencia, además de que el personal o aplicaciones estarán monitoreando las acciones realizadas;
- m. En la supervisión y monitoreo de redes se implementarán herramientas de monitoreo de tráfico y análisis de comportamiento para detectar actividades anómalas;
- n. Se mantendrán registros de los eventos de red para auditoría y respuesta a incidentes;
- o. Los proveedores de servicio de red contratados, deberán cumplir con los requisitos de seguridad establecidos por la Administración Pública Municipal, además de las distintas normas de seguridad de telecomunicaciones reconocidas mundialmente;
- p. Se comunicará a todas las dependencias para que utilicen medios de comunicación oficiales en cualquier intercambio de información oficial y de trabajo, tales como mensajes de correo electrónico, mensajes de conversación (por ejemplo Google Chat Unidades compartidas, aplicaciones de soporte remoto, uso de licenciamiento lícito de aplicaciones para seguimiento de proyectos, etcétera; y
- q. Se establecerá que en la autenticación de inicio de sesión para el uso de la red sea implementada mediante un sistema de garantía de factores múltiples.

Seguridad de los servicios de red

Independientemente si los servicios de red son internos o externos (subcontratados), deberán definirse requisitos en relación a la calidad de servicio mediante acuerdos de niveles de servicio o SLA.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 54 de 150

Estos aspectos son los que deben ser considerados en los proyectos en los que se tenga que intercambiar información:

- Los medios de transmisión;
- Las redes;
- Los soportes informáticos;
- Los soportes documentales, entre otros;

Las auditorías de la calidad de servicios prestados es el único modo en que se puede tener visibilidad sobre la disponibilidad de la red y evaluar los riesgos a los que se exponen con dichos servicios, ya que de ellos depende la operatividad de los sistemas de información. Además, la Dirección de Tecnologías aplica de manera planeada, auditorías de seguridad en la red y según los resultados solicita la remediación de los aspectos de mayor vulnerabilidad que representen riesgos a la Administración Pública Municipal.

Mensajería electrónica

El correo electrónico debe ser tratado como un activo más de información, en el que se aplicarán controles apropiados para mantener la confidencialidad, integridad y disponibilidad de la información.

En ese sentido, el correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios. Entendiéndose por correo masivo, todo aquel que sea ajeno a la Administración Pública Municipal, tales como cadenas, publicidad y propaganda comercial, política, social, etcétera.

Dentro de la mensajería electrónica también se consideran los mensajes generados en chats electrónicos, así como las redes sociales.

Los controles aplicables a la mensajería electrónica son:

- Protección ante acceso no autorizado (mensajes encriptados, etcétera);
- Asegurar el correcto direccionamiento y transporte de los mensajes;
- Confiabilidad y disponibilidad del servicio;
- Consideraciones legales (firmas electrónicas);

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 55 de 150

- e. Necesidad de autorización para usar servicios públicos externos (mensajería instantánea, redes sociales y compartición de archivos); y
- f. Medidas adicionales de autenticación en accesos desde redes públicas.

Acuerdos de confidencialidad y no divulgación

Se consideran acuerdos de confidencialidad tanto a la información propia de la Administración Pública Municipal, así como a la información proporcionada por terceras partes. En consecuencia, dichas obligaciones serán exigibles a todo el personal municipal, así como a ciudadanos y proveedores que, en el ejercicio de sus funciones tengan acceso a activos de información.

En ese sentido, los acuerdos de confidencialidad y el deber de secreto, deberán constar por escrito y estar debidamente firmados previo a iniciar una transferencia de información.

Los acuerdos de confidencialidad incluirán lo siguiente:

- a. La naturaleza de la información;
- b. La duración del acuerdo;
- c. Los procedimientos de rescisión;
- d. Las responsabilidades y las propiedades;
- e. El uso permitido de la información;
- f. El derecho de auditoría,
- g. Los procesos a seguir ante una infiltración; y
- h. Las cláusulas que obliguen a mantener el deber de secreto, incluso más allá de la relación profesional entre las entidades.

Políticas de controles criptográficos

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 56 de 150

Los controles criptográficos están enfocados a la protección de la información, en el caso de que un intruso acceda físicamente a la información, se establecerá un sistema de cifrado de la misma para dificultar la violación de su confidencialidad o su integridad.

En ese sentido, la Dirección de Tecnologías es la responsable de la gestión, implementación y administración de claves de cifrado criptográfico de datos.

Se considerará el cifrado de todos los tipos de medios extraíbles, así como aquellos que transmiten información interna y externa. La política de encriptación tendrá en cuenta los controles utilizados para detectar y eliminar malware.

La clave de la política de controles criptográficos consiste en identificar:

- La información que requiere protección mediante el uso de claves criptográficas, así como las circunstancias en las que su aplicación es necesaria;
- Los medios tecnológicos y mecanismos que se emplearán para su implementación; y
- La gestión, mantenimiento y actualización de dichos medios, con la finalidad de garantizar su adecuada operación.

Gestión de claves

En ese sentido, los medios de cifrado, implican mantener una adecuada gestión de las claves criptográficas utilizadas por los medios de cifrado. Por ello, dicha gestión debe considerar políticas que abarquen el ciclo de vida completo de las claves, incluida su generación, uso, protección, distribución, así como la renovación o destrucción. Como parte de la función de gestión, se establecerán las fechas de activación y desactivación de las claves, con el objetivo de reducir los riesgos previamente identificados.

En los casos en que las claves públicas sean emitidas por un proveedor externo, se deberá contar con un acuerdo de nivel de servicio que defina claramente las responsabilidades del proveedor. Asimismo, podrá considerarse el tratamiento de solicitudes legales por parte de autoridades competentes, en función de la clasificación de la información involucrada.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 57 de 150

Políticas de adquisición, desarrollo y mantenimiento de sistemas

El objetivo es garantizar que la seguridad de la información sea parte integral de los sistemas de información en todo su ciclo de vida, tanto propios como subcontratados.

Análisis y especificaciones de los requisitos de seguridad de los sistemas de información

Se deberán incluir las especificaciones de requerimientos funcionales o no funcionales en el desarrollo de un sistema. Para ello podemos tener en cuenta factores como:

- ¿Qué nivel de confianza requiere la aplicación?, con ello podemos determinar los requisitos de autenticación;
- Especificaciones de la provisión de accesos para las personas usuarias privilegiadas y técnicos de mantenimiento;
- ¿Qué funciones y responsabilidades requiere de las personas usuarias?;
- ¿Qué necesidades de protección tienen los activos involucrados? (análisis de riesgos);
- ¿Qué requisitos de seguridad se derivan de los procesos del negocio?, registros de transacciones o supervisión y monitoreo o requisitos de no-repudio u otros; y
- ¿Qué otros controles de seguridad son aplicables? o interfaces para el registro y supervisión o sistemas de detección de fugas de datos u otros.

En la especificación de los controles de seguridad, se deberán considerar los siguientes factores:

- Controles de acceso:** Detallar el nivel de acceso para cada tipo de usuario, por ejemplo, acceso basado en roles, RBAC, incluida la autenticación fuerte y autorización;
- Autenticación y autorización:** Especificar los mecanismos para verificar la identidad de los usuarios y definir las funciones que pueden realizar dentro del sistema;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 58 de 150

- c. **Protección de datos:** Definir las medidas para proteger la información, como el cifrado de datos tanto en tránsito como en reposo, así como el uso de firewalls y protección contra malware;
- d. **Auditoría y monitoreo:** Especificar la necesidad de registrar eventos, monitorear el sistema en tiempo real y detectar fugas de datos, incluyendo interfaces para la supervisión;
- e. **Continuidad y recuperación:** Definir los requisitos para la copia de seguridad de datos y su recuperación, en todo momento, deberán seguir las mejores prácticas del sector; y
- f. **Documentación:** Elaborar un documento de especificación de seguridad que sea preciso, completo y verificable, que sirva como guía para el desarrollo y el cumplimiento de los requisitos.

En el caso de compras de aplicaciones a terceros estableceremos como control de seguridad:

- a. Procesos de compra formales que incluyan periodos de prueba y validación de producto;
- b. Aplicar criterios de evaluación de riesgos para tomar medidas de control adicionales si el producto no satisface totalmente las necesidades de seguridad;
- c. A la hora de integrar un software en aplicaciones o sistemas propios, deberá considerarse si es necesario configurar las aplicaciones, sistemas y software a implantar en relación a la seguridad;
- d. Se definirán esquemas base de homologación y aceptación de productos, con la finalidad que se incluyan en todo momento los criterios de seguridad de la información; y
- e. Se revisarán y aprobarán las actualizaciones de software, así como las nuevas funcionalidades de productos en cuanto a criterios de seguridad.

Aseguramiento de los servicios de aplicación en las redes públicas

En caso de utilizar redes públicas para la transmisión de información sensible o para acceder a las aplicaciones, se establecerán controles adicionales, ya que las redes públicas representan un riesgo importante a la seguridad de la información.

Por lo anterior, deberán considerar los siguientes aspectos:

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 59 de 150

- a. El cifrado en las comunicaciones;
- b. Uso de sistemas de autenticación múltiple;
- c. Uso de certificados digitales (identificación segura de origen y destino);
- d. Sistemas de prevención de envío de información no permitida (Lost Data Prevention, DLP) en redes públicas; y
- e. Sistemas de protección para envíos involuntarios de archivos.

Seguridad en los procesos de desarrollo y soporte

Para el proceso de desarrollo seguro se toman en cuenta las siguientes reglas:

- a. La seguridad en el entorno de desarrollo;
- b. Uso de metodología en el desarrollo de software;
- c. Control de gestión de versiones de software;
- d. Gestión de vulnerabilidades del software;
- e. Gestión en el aseguramiento de controles de seguridad en software subcontratado; y
- f. Establecimiento de requisitos de seguridad en la fase de definición de funcionalidades del software.

Procedimientos de control de cambios del sistema

Las actualizaciones de software son un punto crítico a considerar, ya que pueden suponer un gran impacto en los entornos de desarrollo.

En virtud de lo anterior, deberán vigilarse los entornos de producción en la fase de desarrollo y controlar estrechamente la actualización de los navegadores en los sistemas operativos y la introducción de nuevas funcionalidades.

Para el control de cambios se considerará lo siguiente:

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 60 de 150

- a. El establecimiento formal documentado del proceso para ejecutar los cambios;
- b. La documentación técnica para la actualización de cambios;
- c. La evidencia de pruebas y control de calidad sobre los cambios introducidos;
- d. Gestión relativa a la implementación de cambios mediante procesos de autorización;
- e. Evaluación de riesgos previa a realizar y planificar los cambios;
- f. Control de los requisitos de seguridad de los sistemas afectados para que no se vean comprometidos en la fase de implementación de los cambios; procesos de aprobación formal, restricción de accesos, control de personal y de tiempos;
- g. Gestión de versiones de software;
- h. Control de impacto en las aplicaciones de servicio; y
- i. Limitación de actualizaciones automáticas en aplicaciones críticas

Se podrán realizar los siguientes tipos de cambios:

- a. Estándar: Cambio pre-autorizado a aplicaciones (cambio relacionado a algún componente de aplicaciones tecnológicas de la organización), o infraestructura (cambio relacionado a algún componente de la infraestructura tecnológica de la organización); para el cual el riesgo es bajo, sus efectos son conocidos y están documentados;
- b. Normal: Cambio que debe seguir completamente el proceso de soporte de sistema; y
- c. Emergencia: Cambio que requiere acciones inmediatas para restaurar servicios o prevenir interrupción de los mismos.

En virtud de lo anterior, deberá realizarse una evaluación del riesgo e impacto a los soportes que son aceptados. El nivel de impacto y la prioridad se asignará de acuerdo a las políticas establecidas.

En caso de requerir cambios urgentes, podrá solicitar una reunión con el Director de Tecnologías con la finalidad de informarle los motivos.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 61 de 150

Por tal motivo, los cambios normales de bajo impacto son valorados, evaluados, autorizados y priorizados por la persona titular de la Coordinación de Desarrollo de Sistemas. En esta actividad, la o el Coordinador autoriza o rechaza la solicitud de soporte de sistemas.

Bajo ese contexto, los cambios normales con impacto medio deberán ser valorados, evaluados, autorizados y priorizados en reunión con las personas involucradas en el seguimiento de las mejoras y modificaciones al sistema de información respecto del cual se solicita el cambio. Entre las personas participantes podrán encontrarse la o el Coordinador, el Analista de Tecnologías, la persona usuaria enlace del área y/o personas usuarias beneficiadas con la implementación del cambio en el proceso.

Como parte de esta actividad, la persona titular de la Coordinación de Desarrollo de Sistemas deberá registrar los resultados de la evaluación derivados de la reunión.

En virtud de lo anterior, la persona titular de la Coordinación de Desarrollo de Sistemas definirá, junto al equipo técnico, el plan del cambio o cambios de la aplicación. Dicho plan establece la duración del proyecto, los requerimientos del cambio y los desarrolladores que programarán e implementarán cada uno de estos requerimientos.

En cualquiera de los requerimientos de hardware asociados al cambio, el desarrollador asignado a cada requerimiento será notificado de su asignación y, una vez que, el desarrollo del requerimiento ha finalizado, se reportarán sus resultados.

Ahora bien, el éxito de cada requerimiento se deberá verificar en esta actividad y cuando todos los requerimientos funcionen como se espera, se guardan las pruebas para presentación y validación.

Una vez finalizada la implementación exitosa del cambio, se documenta como parte del mejoramiento continuo del soporte de sistemas. En esta actividad, el Coordinador revisa y evalúa el desarrollo del cambio, a fin de verificar si el usuario solicitante y las partes interesadas están satisfechas con los resultados; es decir, que el cambio fue ejecutado según lo planeado.

Revisión técnica de aplicaciones después de cambios de las plataformas operativas

Consiste en los procesos de revisión y aprobación de las aplicaciones para garantizar que los cambios no afecten a la operatividad, así como la planificación de los cambios para que haya tiempo para realizar pruebas.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 62 de 150

Restricciones a los cambios en los paquetes de software

Con el objetivo de minimizar la posibilidad de generar incidentes, se limitarán los cambios absolutamente necesarios en los paquetes de software.

Criterios de actualización a revisar antes de realizar los cambios o pensar en hacerlos:

- Evaluar los riesgos de actualización frente a los beneficios que se obtendrán de la actualización;
- Antes de realizar la actualización, revisar los alcances de los cambios;
- Evaluar el impacto sobre el mantenimiento de los activos a futuro; y
- Revisar compatibilidad del software a instalar con el software existente.

Principios de la ingeniería de sistemas seguros

Consiste en documentar los procedimientos para implementar las medidas de seguridad en las técnicas de desarrollo:

- Documentar los procedimientos seguros para el diseño y codificación;
- Documentar el diseño de mecanismos de autenticación;
- Documentar procesos de automatización de variables; y
- Documentar los procedimientos para el uso correcto de la criptografía, entre otros.

Ambiente de desarrollo seguro

La evaluación de riesgos para la seguridad de la información no solo debe realizarse a los activos de información como el software, datos o equipos y soporte, sino que también a los entornos de desarrollo, personas, procesos de desarrollo y las tecnologías utilizadas para determinar si es necesario aplicar medidas o controles de seguridad.

Para ello se tendrá cuenta:

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 63 de 150

- a. El grado de sensibilidad de los datos;
- b. Los niveles de seguridad aplicables;
- c. Los controles definidos para cada tipo de información;
- d. La confiabilidad del personal;
- e. Las necesidades de separar entornos de desarrollo;
- f. Los controles de acceso determinados para el entorno de desarrollo;
- g. Las necesidades de respaldo de información; y
- h. Los controles y políticas para el traslado de información

Desarrollo subcontratado

Para la subcontratación de desarrollo de software, se deberá tener en cuenta:

- a. Establecer y supervisar el cumplimiento de los requisitos de seguridad;
- b. Controlar y gestionar los aspectos de licenciamiento y propiedad de código fuente;
- c. Metodología y definición de las pruebas a realizar en el software subcontratado; y
- d. Todo lo anterior, se plasmará en acuerdos firmados y consensuados con el proveedor.

Pruebas de seguridad de sistema

Los requisitos para la seguridad de un sistema de software deben ser probados como si se tratase de una funcionalidad más del mismo. Por ello, deberá implementarse un plan de pruebas documentado. Las pruebas también se incluirán en los softwares subcontratados.

Pruebas de aceptación del sistema

El proceso de incorporación de nuevas aplicaciones, actualizaciones o nuevas versiones de software se sujetará a un proceso de aceptación, en el cual, se le realicen las pruebas funcionales y de seguridad planificadas.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 64 de 150

Los entornos de pruebas deben ser distintos a los entornos de operación para evitar fallos en sistemas reales.

Datos de prueba

Los entornos de prueba contarán con los mismos niveles de seguridad que los entornos de operación, por lo que se establecerán controles para seleccionar los datos de los sistemas de prueba o entornos de desarrollo.

En caso de realizar copias de datos de producción para datos de prueba, se requiere solicitar autorización previa al responsable del activo. Una vez realizada la acción de copia, en caso de existir datos críticos, deberán reemplazarse éstos por datos ficticios.

Protección de datos de prueba

Si no existe otra posibilidad en los entornos de prueba de los sistemas, se utilizarán datos no reales durante el desarrollo y pruebas previas al arranque de los sistemas.

De no ser posible lo anterior, se aplicarán los mismos controles de seguridad (acuerdo de confidencialidad, etcétera) aplicados a los datos reales.

Políticas en las relaciones con los proveedores

En caso que las empresas o personal externo a la organización tengan acceso a los sistemas de información o a los recursos que manejan activos de información, se establecerán de modo formal las condiciones para el uso de dichos activos y supervisar el cumplimiento de dichas condiciones.

Seguridad de la información en las relaciones con los proveedores

Consiste en el acceso a los activos de la organización por parte de personal externo, mediante el cual se plantean nuevos escenarios de riesgo para la seguridad de la información.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 65 de 150

Políticas de seguridad de la información para las relaciones con los proveedores

La relación con todo proveedor debe estar regulada por un contrato de prestación de servicios. En dicha relación contractual se deben reflejar las condiciones para el manejo adecuado de los activos de nuestra organización, en consideración de los requisitos de seguridad definidos.

Las condiciones de seguridad deben acordarse con el proveedor antes de firmar los contratos y documentarse si es necesario, en los anexos oportunos.

Además de la especificación de los servicios, productos, estructura empresarial, precios del proveedor, se especificarán, además, los procesos o auditorías previas a una posible relación comercial, así como los acuerdos de confidencialidad y los controles de seguridad aplicables.

Análisis de riesgos

Ante la subcontratación de servicios que implican el acceso a la información, se evaluarán los posibles impactos causados a la seguridad de la información.

Si nuestro proveedor accede a información clasificada como no pública, esto puede originar una situación comprometedora para la seguridad de la información, con el riesgo potencial de producir fugas de información cuyo origen sea el proveedor.

En consecuencia, para evaluar los riesgos, hemos de analizar que los activos están afectados por la subcontratación o cesión de datos a terceros, así como las posibles amenazas y el impacto que tendrían su pérdida de confidencialidad, integridad o disponibilidad.

Lo anterior, con la finalidad de seguir los procesos de evaluación de riesgos para cada activo, tales como aplicación, servicio, tarea o procesos, entre otros, que se hayan subcontratado o estén próximos a contratarse.

Selección de controles

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 66 de 150

El segundo paso, es el análisis o auditoría de los controles que debemos aplicar a los activos identificados para evitar o mitigar los riesgos identificados.

Bajo este contexto, los controles se establecerán desde la investigación de los antecedentes de nuestros socios y proveedores, mediante la verificación de la información financiera, antecedentes penales, auditorías de controles y procesos de seguridad del proveedor, etcétera.

Se deberán establecer criterios claros para la contratación de servicios externos y realizar evaluaciones periódicas para asegurar que la prestación del servicio sea tal como se acordó. Establecer los controles que se puedan incluir en los acuerdos de prestación de servicios.

Mantendremos las investigaciones realizadas dentro de la legalidad vigente y en cumplimiento con las leyes de protección de datos personales.

Acuerdos de prestación de servicios

En este punto, se identificarán los controles de seguridad aplicables en los acuerdos de confidencialidad.

Control de accesos

Definir y establecer la política de control, así como la restricción de acceso a la información, con la finalidad de garantizar que cada usuario cuente únicamente con los accesos e información estrictamente necesarios para el desempeño de sus funciones y el desarrollo de sus actividades laborales.

Monitoreo

Se supervisará y, si es necesario, auditará para verificar el cumplimiento de todas las cláusulas.

Finalización del servicio

La finalización de los acuerdos de servicio, trabajos o relación contractual no supone la finalización de las obligaciones en materia de confidencialidad, Lo anterior, deberá contemplarse en las cláusulas o anexos del contrato de prestación de servicios.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 67 de 150

Se establecerán controles para las siguientes acciones:

- a. Devolución de los activos;
- b. La eliminación o destrucción de datos; y
- c. La cancelación y revocación de los accesos.

La seguridad en los acuerdos con proveedores

Las condiciones de seguridad de la información, deberán reflejarse en los contratos de forma explícita y en un apartado específico para ello. Por ello, los documentos sobre los acuerdos para la seguridad de la información se firmarán por ambas partes.

Cadena de suministro de tecnología de la información y las comunicaciones

Se establecerán requisitos de seguridad en toda la cadena de suministro, es decir, los riesgos para la seguridad de la información serán afectados por lo que nuestros proveedores subcontraten.

Asimismo, se establecen los principios para sostener una cadena de suministro con garantías:

- a) Proveedores de confianza; y
- b) Exigir a los proveedores un control de seguridad a sus propios proveedores.

Los controles establecidos en la cadena de suministros son los siguientes:

- a) Criterios de seguridad para cada servicio, producto o tecnología de comunicación a subcontratar;
- b) Cláusulas para el subcontratista, relativos a la aplicación de requisitos de seguridad a sus proveedores y a toda la cadena de suministro;

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 68 de 150

- c) Procesos para comprobar que los productos o servicios suministrados cumplen con los requisitos establecidos para la seguridad de la información, al menos para los productos y servicios determinados como fundamentales y que son requeridos fuera de la organización;
- d) Trazabilidad de componentes críticos;
- e) Proceso para comunicarnos con nuestros proveedores y la cadena de suministro; y
- f) Proceso para revisión periódica y actualización de componentes, así como de las aplicaciones que entran en obsolescencia o quedan fuera del suministro por parte de proveedores.

Gestión de la entrega de servicio por terceras partes

Todo control de seguridad no sólo debe establecerse, sino que se mantendrá a lo largo del tiempo. El tema del control de proveedores seguirá el mismo patrón. En este sentido, no solo se trata de establecer requisitos, sino que, además, se verificará a lo largo del tiempo su cumplimiento, por lo que, será necesario controlar los servicios prestados y los cambios en los mismos.

Seguimiento y revisión de los servicios de proveedores

Siempre que sea posible y el esfuerzo no sea desproporcionado, se establecerá el mecanismo de monitorización de los servicios proporcionados por terceros, además, solicitarán los informes al proveedor sobre el nivel de servicio prestado.

Gestión de cambios en los servicios de los proveedores

Al realizar modificaciones a los servicios prestados por proveedores, se controlará lo siguiente:

- a) Aplicación del análisis de riesgo al nuevo escenario; y
- b) Evaluar la necesidad de modificar o ampliar los acuerdos de prestación de servicio para cubrir las nuevas necesidades de seguridad si así se estima oportuno.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 69 de 150

Políticas de gestión de incidentes de seguridad de la información

Consiste en gestionar los incidentes de manera ágil y eficiente para la organización. Cualquier usuario podrá detectar un evento que ponga en riesgo el funcionamiento de la organización, por lo que, deberá notificar la situación a su jefe inmediato superior y a la Dirección de Tecnologías mediante el correo direccion.tecnologias@sanpedro.gob.mx, o bien, notificar vía telefónica al encargado de ciberseguridad o al titular de la Dirección de Tecnologías. Lo anterior, dependerá de las circunstancias del tratamiento de la información del evento, por ello, la Dirección de Tecnologías generará un ticket de soporte técnico para el seguimiento del caso.

En ese sentido, puede clasificar el incidente de acuerdo a los datos que reciba del evento. El empleado que detecte el incidente, también podrá realizar una clasificación, sin embargo, será un experto técnico adscrito a la Dirección de Tecnologías quien lo clasifique de manera adecuada.

Una vez clasificado el incidente, conocida la gravedad y el tiempo para su resolución, el experto técnico decidirá las medidas necesarias para resolverlo.

En consecuencia, la Dirección de Tecnologías registrará toda la información generada durante el tratamiento y, finalmente, se notificará al empleado que envió la notificación del incidente finalizado.

Ahora bien, toda la información generada durante el tratamiento del incidente, será crítica para posibles incidentes futuros, así como para recopilar la evidencia necesaria. Por tal motivo, se implementarán y documentarán los procedimientos a seguir en el proceso de gestión de incidentes de seguridad de la información.

Bajo ese contexto, se definirá en la Dirección de Tecnologías a un responsable o responsables para la gestión de incidentes, mismo que, deberá garantizar que se desarrollen los procedimientos adecuados para realizar todas las tareas o procesos necesarios para gestionar los incidentes.

La Dirección deberá definir y asignar las responsabilidades de cada empleado adscrito, involucrados en la gestión de incidentes de seguridad de la información, incluida la detección, reporte, atención y seguimiento de los mismos.

Asimismo, deberá documentar y mantener actualizados los procedimientos para:

- La detección, análisis y elaboración de información de incidentes de la seguridad de la información; y

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 70 de 150

- Comunicación de los incidentes.

La Dirección de Tecnologías deberá establecer y mantener canales de comunicación internos y externos que permitan el reporte oportuno de eventos e incidentes de seguridad de la información, a fin de garantizar que las personas responsables de su gestión reciban la información necesaria para su atención.

Todos los usuarios internos y externos que tengan acceso a activos de información deberán conocer y utilizar los mecanismos establecidos para la notificación de eventos e incidentes.

Toda incidencia deberá registrarse y documentarse durante su ciclo de vida, desde su reporte hasta su cierre formal, por lo que, se dejará evidencia de las acciones realizadas y de la resolución implementada.

Políticas de cumplimiento

Consisten en controles que permitan garantizar el cumplimiento de las políticas, normas y legislación aplicable, enfocándose principalmente en lo relativo a seguridad de la información y tutela de programas de cómputo, bases de datos documentación técnica, desarrollos tecnológicos y contenidos digitales utilizados o generados por el Municipio.

Lo anterior, de conformidad con lo establecido en la *Ley Federal del Derecho de autor* a través de los artículos, 1, 4, 11, 13, 18, 19, 24, y 101 al 106, mismos que establecen la protección jurídica de estas obras, regula su uso, así como su licenciamiento y prohíbe la reproducción, modificación o distribución no autorizada, a fin de otorgar sustento a las políticas internas sobre software, propiedad intelectual y manejo de contenidos digitales de la Administración Pública Municipal.

Cumplimiento de los requisitos legales y contractuales

La finalidad es el cumplimiento de las leyes, reglamentos y las obligaciones contractuales requeridas para la seguridad de la información, por lo que el presente manual se fundamenta en lo siguiente:

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 71 de 150

- **Ley General de Responsabilidades Administrativas y su homóloga estatal**, en lo que respecta a la conducta de los servidores públicos en el uso de información, recursos y bienes tecnológicos, establecen el deber de integridad, legalidad, imparcialidad, honradez y eficiencia; tipifican faltas como uso indebido de información, abuso de funciones, negligencia, peculado y desvío de recursos públicos, por lo que, estas normas respaldan las políticas sobre uso institucional de los sistemas informáticos, confidencialidad de la información custodia de activos tecnológicos y reporte de incidentes o vulneraciones de seguridad;
- **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**. Que en sus disposiciones contenidas en los artículos 1, 23, 25 a 27 y 36 obligan a implementar controles tecnológicos, análisis de riesgos, políticas de acceso, mecanismos de seguridad y administración adecuada de bases de datos institucionales;
- **Ley General de Transparencia y Acceso a la Información Pública**, particularmente en sus artículos 1 y 6 que establecen el objeto, principios y obligaciones de los sujetos obligados en materia de acceso a la información. Estas disposiciones exigen implementar medidas y sistemas tecnológicos que garanticen la adecuada gestión, publicación, integridad y disponibilidad de la información pública, así como el cumplimiento de las obligaciones de transparencia del Municipio; y
- **Reglamento Orgánico de la Administración Pública Municipal de San Pedro Garza García, Nuevo León**. Define la estructura del Municipio y las atribuciones de la Dirección de Tecnologías, conforme a lo dispuesto en el artículo 43, inciso e), fracciones I a la XV.

Derechos de Propiedad Intelectual y Software Institucional

La Dirección de Tecnologías reconoce que los programas de cómputo, desarrollos informáticos, bases de datos, manuales, documentación técnica, sistemas digitales y demás creaciones intelectuales generadas dentro del ámbito de sus funciones constituyen obras protegidas bajo la *Ley Federal del Derecho de Autor*, en sus artículos 1, 13, 18, 19, 24, y 101 al 106.

En virtud de lo anterior, dichos bienes intelectuales software, código, documentación técnica, bases de datos, interfaces y desarrollos propios son considerados propiedad del Municipio. Su uso, reproducción, modificación, distribución o acceso están sujetos a las políticas, licencias y permisos determinados por la Dirección de Tecnologías, por lo que promueve el uso de software legal licenciado mediante las siguientes políticas:

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 72 de 150

a. Política de aseguramiento de la no violación de derechos de copia

La Dirección de Tecnologías, escanea continuamente sobre el uso de software apócrifo, e inmediatamente establece el equipo en cuarentena y realiza investigación para determinar hallazgos y define responsabilidades, por lo que, elimina todo residuo de software ilegal sobre los equipos de la Administración Municipal.

b. Política en la compra con distribuidores autorizados y certificados

La Dirección de Tecnologías promueve la adquisición de licencia de uso, con proveedores autorizados, certificados por el fabricante del software a usar. Además, buscará los servicios de garantía y soporte con escalamiento a fabricante para resolver problemas que pudieran presentarse en la operación diaria de la Administración Pública Municipal.

En ese sentido, la Dirección autoriza el uso de programas informáticos de diversas empresas externas, soportado por una adquisición de licencia, convenio-contrato, o donación y a menos que cuente con la autorización del creador de los programas informáticos, no tiene derecho a reproducirlos excepto con fines de respaldo.

c. Política en el control de uso máximo de usuarios por licencia

La Dirección de Tecnologías promueve el uso de licenciamiento solo en la cantidad de dispositivos autorizados; en las condiciones de uso, políticas de servicio y garantías indicadas por el fabricante.

d. Política de revisión periódica sobre uso de software con licencia

La Dirección de Tecnologías registra y utiliza controles de vigencias de licenciamiento, además de las licencias del tipo permanentes, para que, en caso de ser necesario se renueve los contratos de uso y continuar el uso de manera normal.

e. Política sobre el cumplimiento de uso de derechos de copia de material audiovisual, libros, informes, etcétera

La Dirección de Tecnologías deberá informar y difundir entre los usuarios la política de uso legal de software, así como establecer de manera clara las actividades, acciones y usos permitidos, así como aquellas conductas restringidas o prohibidas.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 73 de 150

Asimismo, deberá comunicar a todos los usuarios las consecuencias derivadas del incumplimiento de dicha política, incluida la aplicación de las medidas disciplinarias o administrativas que correspondan conforme a la normativa aplicable.

f. Identificar activos de información que están afectados por derechos de propiedad intelectual

Se identifican los activos en donde se resguardan las leyes o reglamentos implementados por la administración pública municipal, por ejemplo, *Ley de Imagen Institucional*, *Código de Ética y Conducta*, *Ley General de Archivos*, *Ley General de Protección de Datos en Posesión de Sujetos Obligados*, entre otras.

En caso de aplicar, se mantienen en físico la documentación que justifique o acredite la propiedad de las licencias (manuales, disco, accesos, usb's, etcétera), puesto que, actualmente la gran mayoría de los licenciamientos son por suscripción, con manuales de uso y garantías en la nube.

Protección de los registros

Mantener un análisis de los requisitos contractuales legales, en cuanto a las obligaciones de debido control sobre la protección de los registros relativos a evitar su pérdida, falsificación o acceso no autorizado.

Política de clasificación de los registros de información y aplicar los controles necesarios según los requisitos legales. Por ejemplo:

- Registros contables;
- Bases de datos;
- Bases de datos de transacciones;
- Registros de auditoría (propios del sistema de gestión de la seguridad de la información);
- Registros de procedimientos operativos;
- Registros documentales en papel, microfichas, archivos electrónicos; y
- Archivos cifrados (contraseñas y firmas digitales), entre otros.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 74 de 150

Para cumplimiento de la protección de los registros se requiere el cumplimiento de lo siguiente:

- La definición y publicación de las directrices sobre la retención, almacenamiento, tratamiento y eliminación de los registros y la información;
- Mantener un calendario de retenciones en el que se identifique los registros y los períodos de tiempo que deben retenerse; y
- Mantener un inventario de los registros de información clave o crítica.

Protección de los datos y privacidad de la información personal

Se establecen políticas de control para dar cumplimiento a la legislación en materia de protección de datos personales, fundamentadas en la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, conforme a lo dispuesto en sus artículos 1, 23, 25 al 27 y 36, así como en su ley homóloga estatal, la cual desarrolla y complementa, en el ámbito local, las disposiciones previstas en la ley general.

Regulación de los controles criptográficos

Los controles criptográficos se mantienen y actualizan conforme a las normativas sobre el uso de controles criptográficos vigentes, los cuales suelen derivarse de las siguientes disposiciones que se describen a continuación:

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, ya que en sus artículos 23 y 24 se establece la obligación esencial de proteger los datos personales, mientras que en los artículos, del 25 al 30 se regula cómo debe cumplirse esa obligación mediante medidas de seguridad, que si bien es cierto que el cifrado (controles criptográficos) no aparece expresamente mencionado en dicha ley, jurídicamente se justifica como una medida técnica de seguridad derivada de los artículos 25 al 30 y del análisis de riesgos previsto en la propia ley. Asimismo, en la legislación estatal aplicable: *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León*, en sus correlativos artículos 31 al 36 establecen las mismas disposiciones

Por lo que respecta a la descripción y síntesis de los principios y requisitos que se desprenden de la lectura conjunta de varios artículos de la *Ley de Firma Electrónica Avanzada (LFEA)*, así como del *Código de Comercio*, se abordan los requisitos funcionales y operativos que implican controles criptográficos avanzados para garantizar la seguridad y validez legal de las firmas electrónicas. En conclusión, se reconoce que la Firma Electrónica Avanzada produce

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 75 de 150

los mismos efectos jurídicos que la firma autógrafa, siempre y cuando cumpla con los requisitos establecidos por la *Ley de Firma Electrónica Avanzada*.

Si bien, la ley no suele especificar algoritmos criptográficos concretos (para permitir la actualización tecnológica), sí exige que se cumplan criterios técnicos rigurosos, tales como:

- **Vínculo exclusivo con el firmante:** Los datos de creación de la firma (la clave privada) deben estar bajo el control exclusivo del signatario. Esto se logra mediante el uso de criptografía de clave pública (PKI, por sus siglas en inglés), donde sólo el propietario tiene acceso a la clave privada;
- **Integridad del documento:** Debe ser posible detectar cualquier alteración del mensaje de datos o del documento electrónico después del momento de la firma. Los mecanismos criptográficos (como las funciones hash) son fundamentales para asegurar esta integridad;
- **Autenticidad y no repudio:** La ley busca asegurar que el firmante no pueda negar la firma en el documento (no repudio). La criptografía de clave pública, a través de certificados digitales emitidos por Prestadores de Servicios de Certificación (PSC) autorizados, vincula de manera fehaciente la identidad del firmante con el documento firmado;
- **Confidencialidad:** Aunque no es un requisito directo de la firma en sí misma, las disposiciones generales de la LFEA y otras normativas complementarias como la *NOM-151-SCFI-2016* que regulan la conservación de mensajes de datos, mencionan la capacidad de usar algoritmos y protocolos criptográficos compatibles con estándares industriales para garantizar la confidencialidad y la integridad de los mensajes de datos;
- **Certificados digitales:** La ley exige el uso de un certificado digital vigente, emitido por una autoridad certificadora reconocida (como el SAT para la e.firma, antes FIEL), que es la base tecnológica que sustenta la confianza en los controles criptográficos subyacentes; y
- La ley se centra en los resultados que los controles criptográficos deben garantizar, tales como la exclusividad, integridad, autenticidad y no repudio, dejando los detalles técnicos de los algoritmos a las normas técnicas y estándares internacionales que evolucionan con el tiempo.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 76 de 150

Los requisitos funcionales (vinculación única al firmante, control exclusivo de los datos de creación, detección de modificaciones) que implican el uso de controles criptográficos avanzados (como la criptografía de clave pública) se derivan de estos principios.

Asimismo, sirven de base las políticas internas en entidades gubernamentales y normas mexicanas, tales como las basadas en la serie ISO 27000, que establecen directrices sobre el uso de controles criptográficos para la protección de datos e información dentro de esas instituciones, pero no a nivel federal para usuarios generales.

Cifrado obligatorio

La normativa de protección de datos personales establece la obligatoriedad de implementar medidas de seguridad, incluido el cifrado de datos, especialmente para los datos personales sensibles.

Fundamento legal y tipos de datos

La *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* y sus lineamientos reconocen y protegen los datos personales y, de manera especial, los datos sensibles.

Se protegen los siguientes datos:

- El origen racial o étnico;
- Estado de salud presente o futuro;
- Información genética;
- Creencias religiosas, filosóficas y morales;
- Opiniones políticas; y
- Preferencia sexual.

Son considerados datos personales sensibles por la legislación mexicana, debido a que su uso indebido puede dar origen a discriminación o un riesgo grave para el titular.

Obligación de cifrado y medidas de seguridad

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 77 de 150

La ley exige a los responsables del tratamiento de datos personales implementar medidas de seguridad administrativas, técnicas y físicas para proteger esta información contra daños, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado.

Para ello, se deberán implementar medidas de seguridad adecuadas, tales como:

- **Medidas técnicas:** El cifrado de datos (tanto en reposo como en tránsito) es un ejemplo clave de medida de seguridad técnica que se recomienda y, en la práctica, se considera obligatorio para datos sensibles, ya que es fundamental para prevenir accesos no autorizados, especialmente en caso de robo o pérdida de dispositivos o bases de datos; y
- **Gestión de riesgos:** La Secretaría de Anticorrupción y Buen Gobierno adscrita al Gobierno de México emite guías y criterios que orientan sobre la implementación de estas medidas, por lo que, enfatizan que el nivel de seguridad debe ser proporcional al tipo de datos tratados, siendo el máximo nivel requerido para los datos sensibles.

Uso de datos a gran escala

En el caso del uso de datos a gran escala afectados por sistemas de acceso público, la ley establece que las fuentes de acceso público son aquellas que pueden ser consultadas lícitamente sin más exigencia que, en su caso, el pago de una contraprestación. Sin embargo, esto no exime al responsable de implementar medidas de seguridad si la información es obtenida o tratada de manera ilícita o si recaba datos sensibles que requieren un consentimiento expreso y por escrito del titular.

En resumen, aunque la ley no siempre menciona explícitamente la palabra "cifrado", la obligación de garantizar la seguridad de los datos personales sensibles, conforme a las guías y criterios de la autoridad garante competente, implica la aplicación de tecnologías como el cifrado para cumplir con el principio de seguridad y proteger adecuadamente la información.

Código de Ética y Conducta

Este Manual también fundamenta sus políticas en el *Código de Ética y Conducta para el Municipio de San Pedro Garza García*, toda vez que, dichas políticas se basan en los principios rectores que el Código establece dentro su capítulo segundo de Principios Rectores, tales como legalidad, honradez, lealtad, profesionalismo, transparencia,

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 78 de 150

rendición de cuentas, integridad, así como a su capítulo tercero denominado valores y directrices, mismos a los que deberán apegar su actuar los servidores públicos del Municipio, con ello delimitan un deber general de:

- Tratar con confidencialidad la información reservada y los datos personales;
- No utilizar dicha información para fines personales, partidistas o fuera del ámbito institucional; y
- Garantizar un manejo responsable de la información, lo que refuerza la necesidad de las políticas, controles y medidas normativas aquí integradas, que, si bien es cierto, el código establece en el principio de transparencia la máxima publicidad y, a su vez, la obligación de proteger los datos personales que estén bajo su custodia.

En conclusión, el *Código de Ética y Conducta* sirve como base "ética" muy útil, pues deja claro que existe un deber de confidencialidad, protección de información reservada, así como datos personales y factor de conducta esperada de los servidores públicos. Complementándose a su vez, con otros ordenamientos legales aplicables para el desarrollo de las políticas de este manual.

Revisiones de seguridad de la información

Consiste en garantizar que la seguridad de la información sea implementada y operada de acuerdo con las políticas y procedimientos organizacionales. Para ello se establecen los siguientes controles:

Revisión independiente de la seguridad de la información

De forma regular se realizan auditorías de cumplimiento de la seguridad de la información por personal externo.

Lo anterior, trae consigo los siguientes beneficios:

- Se garantiza la independencia de la revisión o auditorías;
- Aporta un punto de vista imparcial; y
- Aportan la experiencia de profesionales de la seguridad de la información que conocen otras organizaciones y pueden aportar mejoras.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 79 de 150

Cumplimiento de la política y normas de seguridad

Los responsables de cada área deben revisar que los procedimientos de la organización sean aplicados de acuerdo a los requisitos definidos.

Para ello, los responsables deberán determinar la forma para cumplir los requisitos de seguridad de la información definidos en las políticas, normas y otras regulaciones aplicables.

Cuando se identifiquen los incumplimientos deberán:

- Identificar las causas;
- Evaluar las necesidades de tomar medidas;
- Implementar las acciones correctivas apropiadas;
- Revisar la eficiencia de las acciones correctivas; y
- Identificar las deficiencias y debilidades del sistema.

Revisión del cumplimiento técnico

Consiste en evaluar los sistemas de información periódicamente, con la finalidad de verificar que están correctamente configurados de acuerdo a las reglas y políticas definidas.

El objetivo es identificar fallos en las actualizaciones de los sistemas y establecer medidas correctivas antes de que estos fallos supongan una amenaza real para el sistema.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 80 de 150

VIII. PROCESOS

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 81 de 150

SAIA-DT-MPP-01-PROC-01-V3

PROCESO DE DESARROLLO DE UN NUEVO SISTEMA DE INFORMACIÓN

DESCRIPCIÓN DEL PROCESO

PERSONA USUARIA O SOLICITANTE

- 1. Solicita por los medios establecidos la creación de un nuevo sistema de información.
- 2. Llena el formato de “Solicitud de Soporte de Sistemas”, *anexo (SAIA-DT-MPP-01-FORM-02-V3)* y lo envía a la Dirección de Tecnologías, por los distintos canales establecidos.

DIRECCIÓN DE TECNOLOGÍAS – La persona que desempeña el puesto de responsable administrativo.

- 3. Recibe la solicitud y confirma la solicitud para la creación de un nuevo sistema de información, vía correo electrónico.
- 4. Turna a la persona titular de la Coordinación de Desarrollo de Sistemas, para su revisión, verificación y evaluación.

DIRECCIÓN DE TECNOLOGÍAS – La persona titular de la Coordinación de Desarrollo de Sistemas

- 5. Revisa, verifica y evalúa la información contenida en la solicitud y, en caso que se requiera solicita complementar alguna información.

¿REQUIERE MÁS INFORMACIÓN?

sí



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 82 de 150

6. Envía, vía correo electrónico notificación a la persona usuaria o solicitante, en la que se requiere la necesidad de aclaración o más información para atender su solicitud.

PERSONA USUARIA O SOLICITANTE

7. Atiende la solicitud de la o el Coordinador de Desarrollo de Sistemas y, complementa la información y regresa de nuevo al punto 4.

DIRECCIÓN DE TECNOLOGÍAS – La persona titular de la Coordinación de Desarrollo de Sistemas

¿REQUIERE MÁS INFORMACIÓN?

NO

8. Promueve reunión técnica para evaluación, a fin de establecer los requerimientos, planes de trabajo, etcétera, en base a la metodología para el desarrollo de sistemas.
9. Realiza Estudio de Viabilidad (EV), para definir las condiciones, alcance y continuidad del proyecto.

¿ES VIABLE EL PROYECTO?

NO

10. Notifica a la persona usuaria o solicitante y justifica por qué no es viable el proyecto. Elabora minuta de reunión en la que se indica la razón por la cual resulta inconveniente el desarrollo del sistema; o bien, se sugiere alguna otra solución que cubra las necesidades de la o el usuario o solicitante.
11. Espera las condiciones oportunas para su desarrollo, por lo cual, lo asegura en la Dirección de Tecnologías.

FIN DEL PROCESO.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 83 de 150

DIRECCIÓN DE TECNOLOGÍAS – La persona titular de la Coordinación de Desarrollo de Sistemas

¿ES VIABLE EL PROYECTO?

SÍ

12. Notifica a la persona usuaria o solicitante la continuidad del proyecto.
13. Promueve reunión para validar conjuntamente con la persona usuaria o solicitante base al estudio de viabilidad, que es posible darle solución al proyecto, mediante la creación o la adquisición de nueva infraestructura y/o software comercial y bajo esas condiciones (en caso de ser aceptadas), validar la continuidad del proyecto.

¿APRUEBA LA CONTINUIDAD DEL PROYECTO?

SÍ

14. **Analiza.** Describe el sistema de información, a partir de los productos generados en el proceso del Estudio de Viabilidad del Sistema (EVS). Delimita su alcance, genera un catálogo de requisitos y describe el sistema mediante modelos iniciales de alto nivel.
15. **Diseña.** El propósito del Diseño del Sistema de Información (DSI), es obtener la definición de la arquitectura del sistema y del entorno tecnológico que le va a dar soporte, junto con la especificación detallada de los componentes del sistema de información.
16. **Construye.** La Construcción del Sistema de Información (CSI), tiene como objetivo final la construcción y prueba de los distintos componentes del sistema de información, a partir del conjunto de especificaciones lógicas y físicas del mismo. Se desarrollan los procedimientos de operación y seguridad y se elaboran los manuales de usuario final y técnico.
17. **Implanta y adapta.** Su principal objetivo es la entrega y aceptación del sistema en su totalidad, según lo establecido en el proceso de Estudio de Viabilidad del Sistema (EVS); así como la capacitación para la operación del sistema de información, al Usuario o Solicitante.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 84 de 150

PERSONA USUARIA O SOLICITANTE

18. **Valida y acepta el producto final.** Somete el sistema a las pruebas de implantación con la participación del usuario administrador designado para el sistema y realizan conjuntamente los ajustes necesarios.
19. **Realiza encuesta de satisfacción.** De manera electrónica, se envía una encuesta al usuario solicitante, en la que se pide que contribuya, con sus observaciones o comentarios, a mejorar la calidad del servicio proporcionado por la Dirección de Tecnologías.

FIN DEL PROCESO.

DIRECCIÓN DE TECNOLOGÍAS – La persona titular de la Coordinación de Desarrollo de Sistemas

¿APRUEBA LA CONTINUIDAD DEL PROYECTO?

NO

20. Elabora minuta de reunión en la que se indica la razón por la cual resulta inconveniente el desarrollo del sistema; o bien, se sugiere alguna otra solución que cubra las necesidades de la persona usuaria o solicitante.
21. Cierra el proyecto. Espera las condiciones oportunas para su inicio, por lo cual lo asegura en la Dirección de Tecnologías.

FIN DEL PROCESO.



SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL

DIRECCIÓN DE TECNOLOGÍAS

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS
DE LA DIRECCIÓN DE TECNOLOGÍAS

Codificación:
SAIA-DT-MPP-01-V3

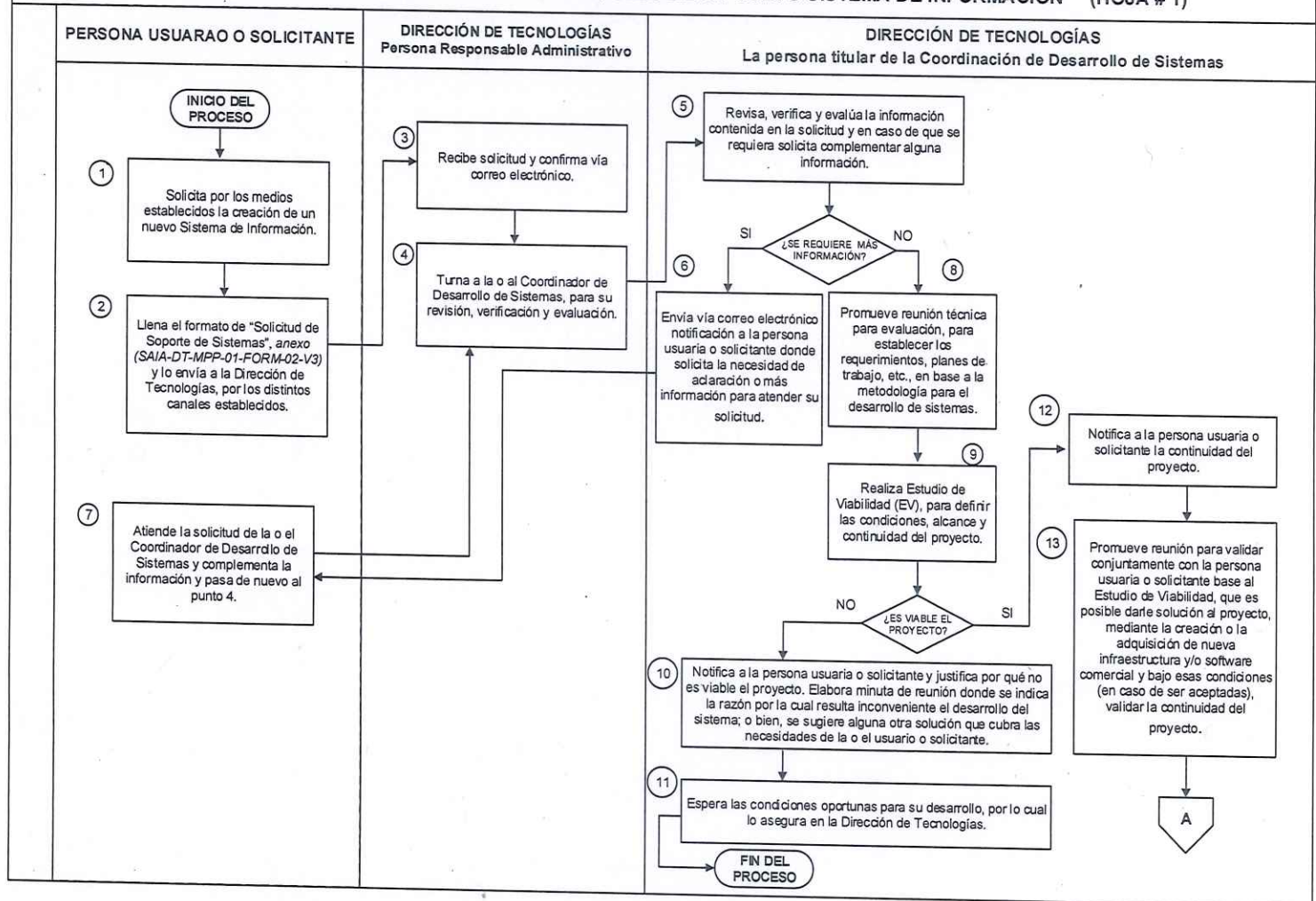
Versión: 3

Emisión: 1 de agosto de 2018

Actualización: 10 de agosto de 2026

Página: 85 de 150

DIAGRAMA DE FLUJO DEL PROCESO DESARROLLO DE UN NUEVO SISTEMA DE INFORMACIÓN (HOJA # 1)





SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL

DIRECCIÓN DE TECNOLOGÍAS

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS
DE LA DIRECCIÓN DE TECNOLOGÍAS

Codificación:
SAIA-DT-MPP-01-V3

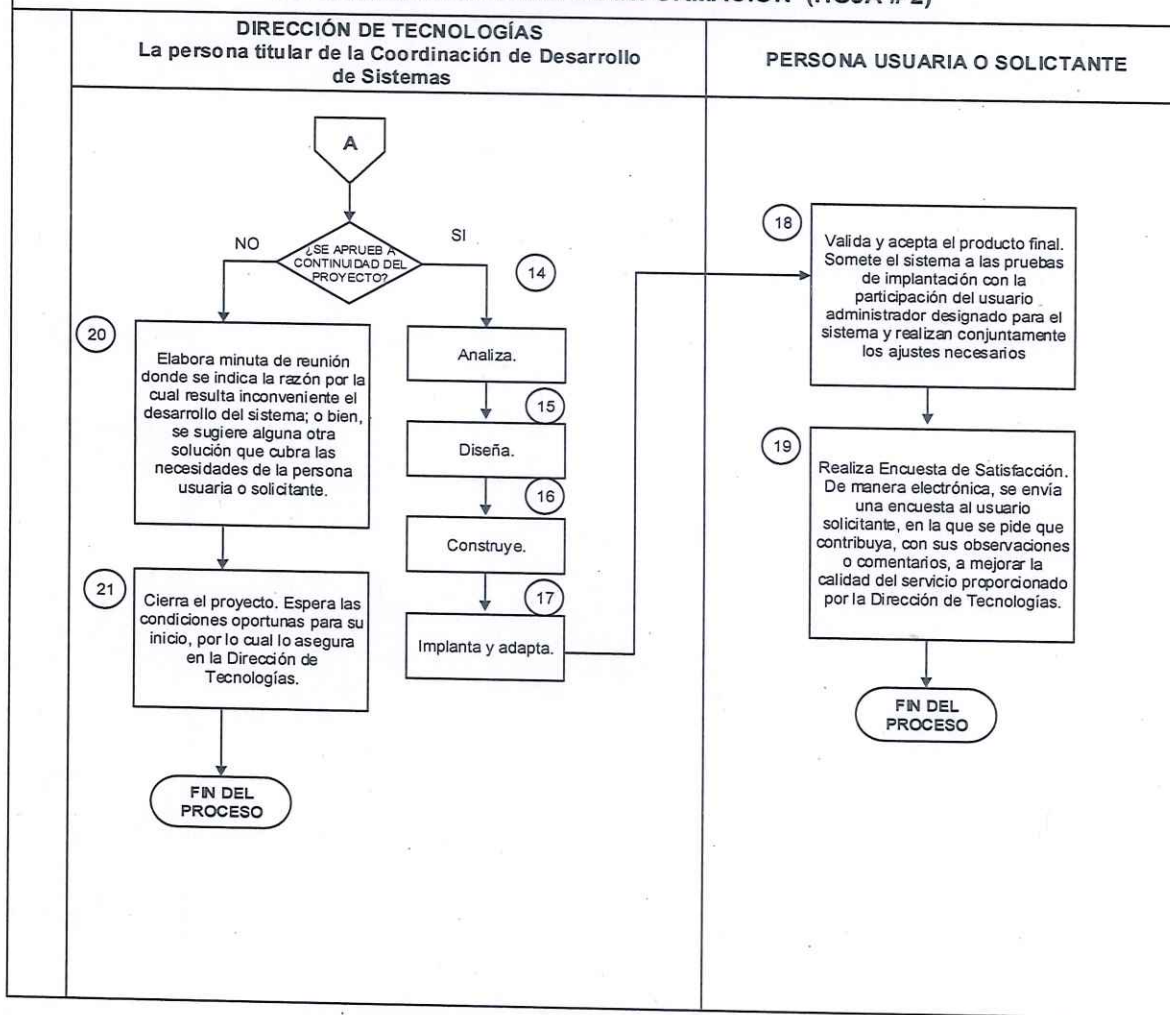
Versión: 3

Emisión: 1 de agosto de 2018

Actualización: 10 de agosto de 2026

Página: 86 de 150

DIAGRAMA DE FLUJO DEL PROCESO DESARROLLO
DE UN NUEVO SISTEMA DE INFORMACIÓN (HOJA # 2)



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 87 de 150

SAIA-DT-MPP-01-PROC-02-V3

PROCESO SOPORTE DE SISTEMAS

DESCRIPCIÓN DEL PROCESO

PERSONA USUARIA O SOLICITANTE

1. Ingresa la información para reportar una falla o inconveniente en la ejecución de algún sistema de información. El reporte lo realiza mediante una solicitud o formato de Soporte de Sistemas. (El nivel de detalle de la información es importante para resolver el problema).

“Los Tipos de Cambios pueden ser:

Estándar: Cambio pre-autorizado a aplicaciones (cambio relacionado a algún componente de aplicaciones tecnológicas de la organización), o infraestructura (cambio relacionado a algún componente de la infraestructura tecnológica de la organización); para el cual el riesgo es bajo, sus efectos son conocidos y están documentados.

Normal: Cambio que debe seguir completamente el proceso de Soporte de Sistema.

Emergencia: Cambio que requiere acciones inmediatas para restaurar servicios o prevenir interrupción de los mismos.”

DIRECCIÓN DE TECNOLOGÍAS – Persona Responsable Administrativo

2. Recibe la solicitud y confirma su recepción vía correo electrónico.
3. Turna a la persona titular de la Coordinación de Desarrollo de Sistemas, para su revisión y valoración.

DIRECCIÓN DE TECNOLOGÍAS – La persona titular de la Coordinación de Desarrollo de Sistemas



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 88 de 150

4. Revisa la solicitud de soporte de sistemas y evalúa si el o los cambios son factibles, si está relacionado a otros soportes ya radicados o si requiere que se complemente alguna información.

¿LA SOLICITUD ES ACEPTADA?

NO

5. Envía notificación a la persona usuaria o solicitante en la que se le explica al solicitante que no es factible su solicitud y el motivo por el cual fue rechazada.

FIN DEL PROCESO.

¿LA SOLICITUD ES ACEPTADA?

SÍ

DIRECCIÓN DE TECNOLOGÍAS – La persona titular de la Coordinación de Desarrollo de Sistemas

6. Envía notificación a la persona usuaria o solicitante para informarle que la solicitud de soporte de sistemas ha sido aceptada.
7. Continúa con la actividad de programar la solicitud de soporte.

“Se debe realizar una evaluación del riesgo e impacto a los soportes que son aceptados. El nivel de impacto y la prioridad deben ser asignados de acuerdo a las políticas establecidas”.

“Para el caso de solicitudes urgentes de cambios, podrá solicitar una reunión con el Director General de Tecnologías para conocimiento de las prioridades”.

¿EL TIPO DE SOPORTE ES ESTÁNDAR?

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 89 de 150

SÍ

8. El riesgo es bajo, sus efectos son conocidos y están documentados, por lo tanto, puede autorizar el cambio.

¿SE AUTORIZÓ EL CAMBIO?

SÍ

9. Continúa en el punto 23.

¿SE AUTORIZÓ EL CAMBIO?

NO

10. Notifica a la persona usuaria o solicitante que no se autorizó su solicitud y le explica el motivo.

FIN DEL PROCESO.

¿EL TIPO DE SOPORTE ES DE EMERGENCIA?

SÍ

11. Lo turna a la persona titular de la Dirección para su autorización.

DIRECCIÓN DE TECNOLOGÍAS – La persona titular

¿AUTORIZA EL SOPORTE DE EMERGENCIA?

SÍ

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 90 de 150

12. Continúa en el punto 23.

¿AUTORIZA EL SOPORTE DE EMERGENCIA?

NO

13. Notifica a la persona usuaria o solicitante que no se autorizó su solicitud y le explica el motivo.

FIN DEL PROCESO.

DIRECCIÓN DE TECNOLOGÍAS – La persona titular de la Coordinación de Desarrollo de Sistemas

¿EL TIPO DE SOPORTE ES NORMAL Y DE NIVEL DE IMPACTO BAJO?

SÍ

14. Analiza si no hay inconveniente en autorizar el cambio solicitado.

“Los cambios normales de bajo impacto son valorados, evaluados, autorizados y priorizados por la persona titular de la Coordinación de Desarrollo de Sistemas. En esta actividad la o el Coordinador autoriza o rechaza la Solicitud de Soporte de Sistemas”.

¿AUTORIZA EL CAMBIO?

SÍ

15. Continúa en el punto 23.

¿AUTORIZA EL CAMBIO?

NO

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 91 de 150

16. Notifica a la persona usuaria que no se autorizó su solicitud y le explica el motivo.

FIN DEL PROCESO.

¿EL TIPO DE SOPORTE ES NORMAL Y DE NIVEL DE IMPACTO MEDIO?

sí

DIRECCIÓN DE TECNOLOGÍAS – La persona titular de la Coordinación de Desarrollo de Sistemas

17. Determina conjuntamente con la persona usuaria o solicitante y el analista de tecnologías, la autorización del cambio.

“Los cambios normales con impacto medio deben ser valorados, evaluados, autorizados y priorizados; en reunión con los actores involucrados en el seguimiento de las mejoras y cambios al sistema de información, sobre el que se está pidiendo los cambios. Estos actores podrían ser la o el Coordinador, el Analista de Tecnologías y la persona Usuaria enlace del área y/o algunos usuarios beneficiados al nuevo cambio en el proceso. En esta actividad, la persona titular de la Coordinación de Desarrollo de Sistemas ingresa los resultados de la evaluación producto de la reunión”.

¿AUTORIZA EL CAMBIO?

sí

18. Continúa con el punto 23.

¿AUTORIZA EL CAMBIO?

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 92 de 150

NO

19. Notifica a la persona usuaria o solicitante que no se autorizó su solicitud y le explica el motivo.

FIN DEL PROCESO.

¿EL TIPO DE SOPORTE ES NORMAL Y EL NIVEL DE IMPACTO ES ALTO?

NO

FIN DEL PROCESO.

¿EL TIPO DE SOPORTE ES NORMAL Y EL NIVEL DE IMPACTO ES ALTO?

SÍ

20. Lo turna para autorización a la persona titular de la Dirección de Tecnologías.

¿AUTORIZA EL CAMBIO?

SÍ

21. Continúa en el punto 23.

¿AUTORIZA EL CAMBIO?

NO

22. Notifica a la persona usuaria o solicitante que no se autorizó su solicitud y le explica el motivo.

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 93 de 150

FIN DEL PROCESO.

¿EL CAMBIO IMPLICA HARDWARE Y DESARROLLO DE APLICACIONES?

SÍ

23. Programa cambios a desarrollo de aplicaciones, renta o adquisición de equipos.

24. Continúa en el punto 27.

¿EL CAMBIO IMPLICA HARDWARE?

NO

25. Recibe y planea el cambio considerando nuevas aplicaciones.

“La persona titular de la Coordinación de Desarrollo de Sistemas define, junto con el equipo técnico, el plan del cambio o cambios de la aplicación. Dicho plan establece la duración del proyecto, los requerimientos del cambio y los desarrolladores que programarán e implementarán cada uno de estos requerimientos”.

“En cualquiera de los requerimientos de hardware asociados al cambio, el desarrollador asignado a cada requerimiento es notificado de su asignación y, una vez que el desarrollo del requerimiento ha finalizado, se reportan sus resultados”.

26. Procede al desarrollo de requerimientos de cambios.

27. Realiza pruebas de certificación para asegurar que los cambios realizados cumplan con lo solicitado.

“El éxito de cada requerimiento se deberá verificar en esta actividad y cuando todos los requerimientos funcionen como se espera, se guardan las pruebas para presentación y validación”.

¿LAS PRUEBAS FUERON EXITOSAS?

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 94 de 150

NO

28. Regresa al punto 26.

¿LAS PRUEBAS FUERON EXITOSAS?

SÍ

29. Promueve una reunión con la persona usuaria o solicitante para presentar la operación y/o resultados de pruebas de certificación. También definirán; en caso de ser necesario, la programación de capacitación a usuarios finales implicados en el cambio.

30. Se programa la fecha de la capacitación y el tiempo estimado.

31. Se implementa el cambio y se envía notificación a los involucrados y da por finalizada la implementación.

PERSONA USUARIA O SOLICITANTE

32. Reporta los resultados de la implementación y evalúa el éxito del cambio.

¿AUTORIZA EL CIERRE?

SÍ

33. La implementación fue exitosa, según el cambio solicitado.

34. Notifica del cierre a la Dirección de Tecnologías.

“Una vez finalizada la implementación exitosa del cambio, se documenta como parte del mejoramiento continuo del Soporte de Sistemas. En esta actividad el Coordinador revisa y evalúa el desarrollo del cambio, verificando si el usuario solicitante y las partes



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LA DIRECCIÓN DE TECNOLOGÍAS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 1 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 95 de 150

interesadas están satisfechas con los resultados; es decir, que el cambio fue ejecutado según lo planeado”.

FIN DEL PROCESO.

PERSONA USUARIA O SOLICITANTE

¿AUTORIZA EL CIERRE?

NO

35. Evalúa fallas del cambio y explica a la Dirección de Tecnologías, los motivos por los cuales no fue exitosa la implementación del cambio.

DIRECCIÓN DE TECNOLOGÍAS – La persona titular de la Coordinación de Desarrollo de Sistemas

36. Revisa las razones por las cuales la persona usuaria o solicitante no autorizó el cierre del soporte de sistemas y reporta las acciones que se llevaron a cabo para remediar las fallas (evaluación del equipo de desarrollo, apertura de una nueva solicitud para deshacer los efectos del cambio actual, etcétera)

FIN DEL PROCESO.



SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL

DIRECCIÓN DE TECNOLOGÍAS

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS
DE LA DIRECCIÓN DE TECNOLOGÍAS

Codificación:
SAIA-DT-MPP-01-V3

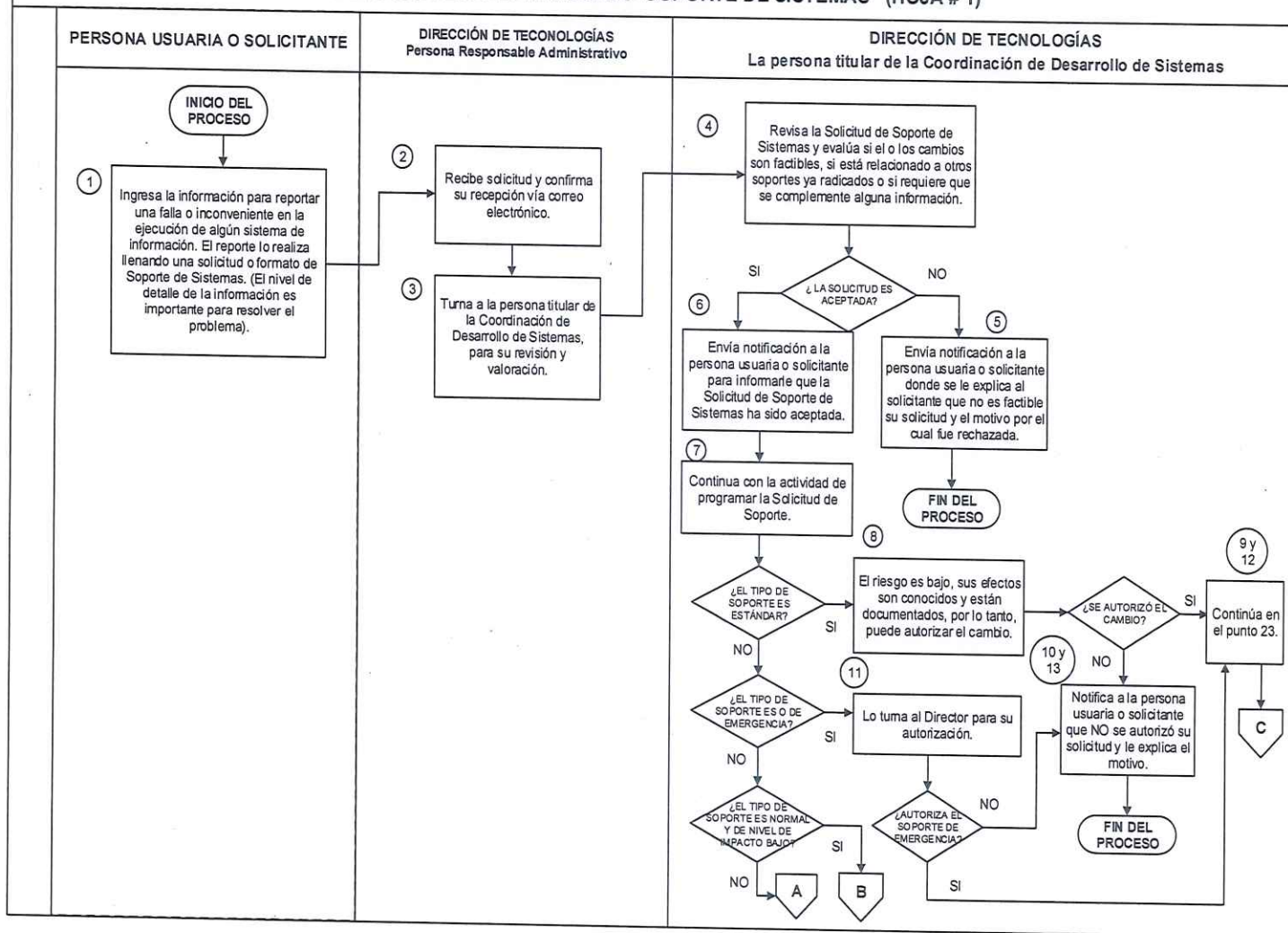
Versión: 3

Emisión: 1 de agosto de 2018

Actualización: 10 de agosto de 2026

Página: 96 de 150

DIAGRAMA DE FLUJO DEL PROCESO SOPORTE DE SISTEMAS (HOJA # 1)





**SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL**

DIRECCIÓN DE TECNOLOGÍAS

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS

Codificación:
SAIA-DT-MPP-01-V3

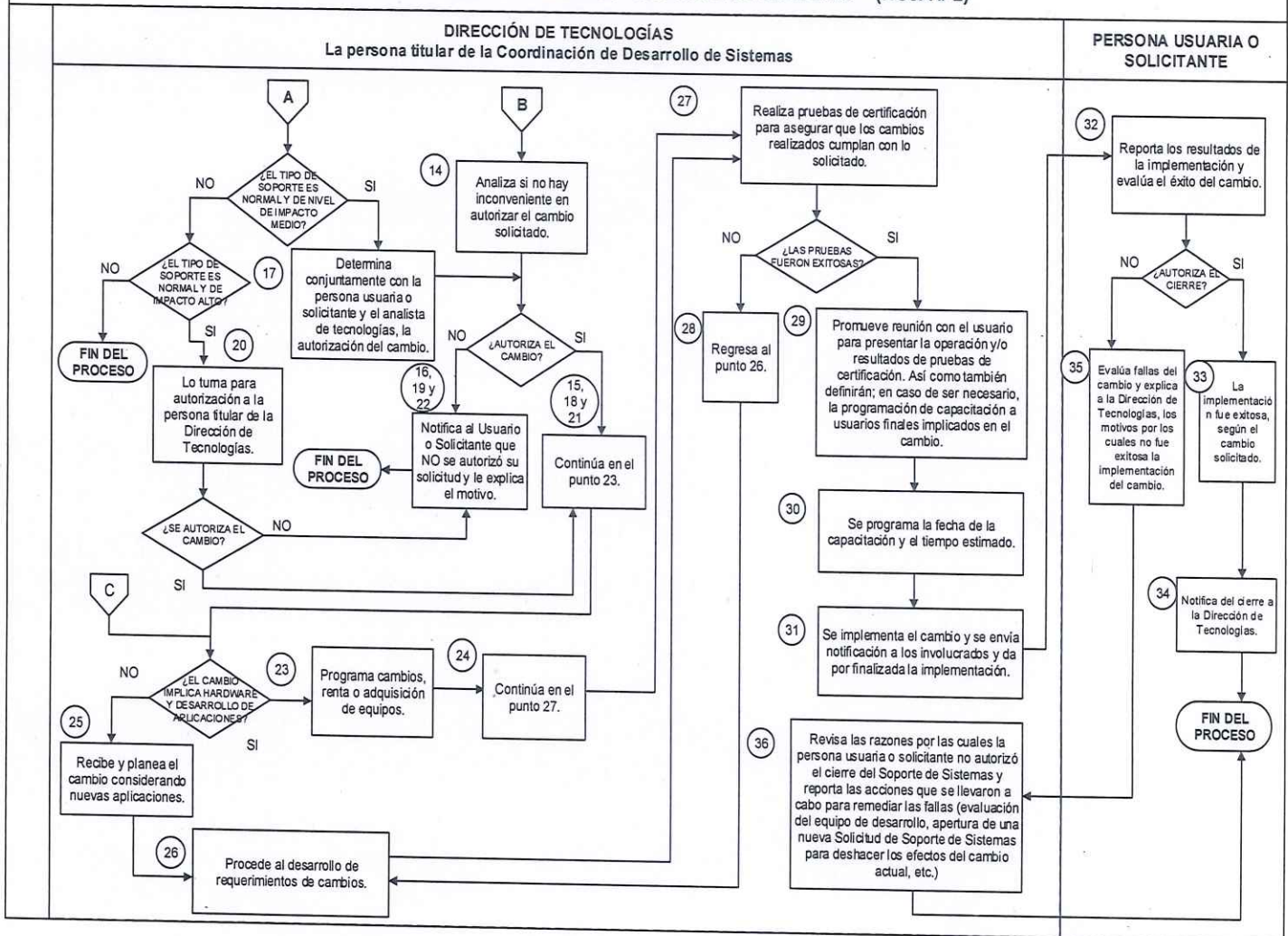
Versión: 3

Emisión: 01 de agosto de 2018

Actualización: 10 de agosto de 2026

Página: 97 de 150

DIAGRAMA DE FLUJO DEL PROCESO SOPORTE DE SISTEMAS (HOJA # 2)



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 98 de 150

SAIA-DT-MPP-01-PROC-03-V3

PROCESO SOLICITUD DE SOPORTE TÉCNICO

DESCRIPCIÓN DEL PROCESO

PERSONA USUARIA O SOLICITANTE

1. Solicita a través de los medios establecidos, atención de soporte técnico, formato "Solicitud de Soporte Técnico", *anexo (SAIA-DT-MPP-01-FORM-01-V3)*.

DIRECCIÓN DE TECNOLOGÍAS – Persona Responsable Administrativo

2. Recibe la solicitud y proporciona atención a los soportes.
3. Registra la información para abrir un nuevo caso.
4. Revisa y analiza el caso, con la finalidad de determinar si la información entregada por el usuario es suficiente para resolverlo.
5. Orienta las actividades para resolver el caso y adjunta documentación.

¿LA INFORMACIÓN ES SUFICIENTE?

SÍ

6. Resuelve la solicitud y pasa al número 8.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 99 de 150

¿LA INFORMACIÓN ES SUFICIENTE?

NO

7. Notifica a la persona usuaria o solicitante y espera complementa la información y, pasa de nuevo al numeral 4.

¿REQUIERE DE LA ASISTENCIA DE UN TÉCNICO?

NO

8. Revisa y registra en la base de datos del conocimiento.
9. Notifica a la persona usuaria o solicitante que ya fue atendido su reporte.
10. Cierra reporte y en su caso entrega el equipo.

FIN DEL PROCESO.

¿REQUIERE DE LA ASISTENCIA DE UN TÉCNICO?

SÍ

11. Asigna el reporte al técnico para resolver el caso.
12. En caso de ser necesario se le solicita el equipo a reparar.

COORDINACIÓN DE REDES Y SOPORTE TÉCNICO – Persona titular de la Coordinación de Redes y/o Soporte técnico



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 100 de 150

13. Analiza y evalúa el reporte.

¿EL EQUIPO ES PARA DAR DE BAJA?

SÍ

14. Determina que la falla del equipo no amerite reparación y por lo tanto es equipo para baja.

15. Elabora el formato "Reporte de Diagnóstico de Equipo de Cómputo", *anexo (SAIA-DT-MPP-01-FORM-06-V3)*.

16. Revisa y registra en la base de datos del conocimiento.

17. Notifica a la persona usuaria o solicitante y le entrega el formato "Reporte de Diagnóstico de Equipo de Cómputo", *anexo (SAIA-DT-MPP-01-FORM-06-V3)*.

18. Cierra reporte y en su caso entrega el equipo.

FIN DEL PROCESO.

¿EL EQUIPO ES PARA DAR DE BAJA?

NO

¿REQUIERE EVALUACIÓN DEL PROVEEDOR?

NO

¿REQUIERE REFACCIONES?

NO



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 101 de 150

19. Procede a realizar la reparación solicitada.
20. Revisa y registra en la base de datos del conocimiento.
21. Notifica a la persona usuaria o solicitante que ya fue atendido su reporte.
22. Cierra reporte y en su caso entrega el equipo.
23. Realiza encuesta de satisfacción del servicio.

FIN DEL PROCESO.

¿HAY EXISTENCIA DE REFACCIONES?

SÍ

24. Gestiona el requerimiento de refacciones en el stock de la Dirección de Tecnologías.
25. Realiza las actividades descritas en los puntos 19 al 23.

FIN DEL PROCESO.

¿HAY EXISTENCIA DE REFACCIONES?

NO

26. Notifica a la persona usuaria o solicitante sobre la necesidad de adquirir refacciones para atender su reporte.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 102 de 150

¿REQUIERE EVALUACIÓN DEL PROVEEDOR?

SÍ

27. Gestiona con el Proveedor evaluación de productos y/o servicios.

¿EL EQUIPO ES PARA DAR DE BAJA?

NO

28. Notifica a la persona usuaria o solicitante que realice el proceso de adquisición (productos y/o servicios).

29. El proveedor entrega refacciones o proporciona servicios solicitados.

30. El técnico repara equipo con refacciones requeridas al proveedor.

31. Procede a realizar las actividades descritas en los puntos 19 al 23.

FIN DEL PROCESO.

¿EL EQUIPO ES PARA DAR DE BAJA?

SÍ

32. El proveedor informa a la Dirección de Tecnologías que, según el diagnóstico, el equipo puede ser dado de baja.

33. Procede a realizar las actividades descritas en los puntos 19 al 23.

FIN DEL PROCESO.





SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL

DIRECCIÓN DE TECNOLOGÍAS

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS

Codificación:
SAIA-DT-MPP-01-V3

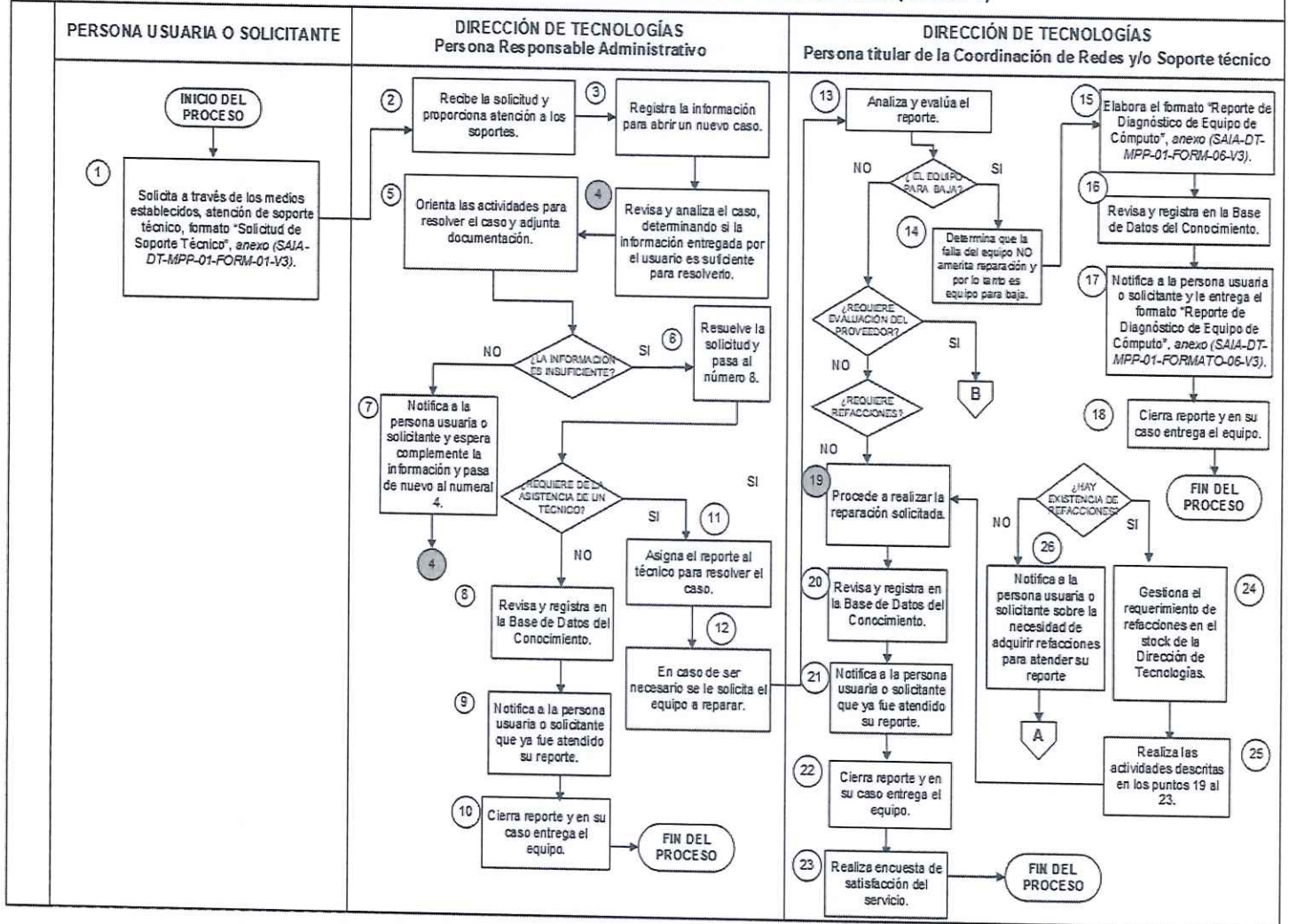
Versión: 3

Emisión: 01 de agosto de 2018

Actualización: 10 de agosto de 2026

Página: 103 de 150

DIAGRAMA DE FLUJO DEL PROCESO SOLICITUD DE SOPORTE TÉCNICO (HOJA # 1)





SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL

DIRECCIÓN DE TECNOLOGÍAS

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS

Codificación:

SAIA-DT-MPP-01-V3

Versión: 3

Emisión: 01 de agosto de 2018

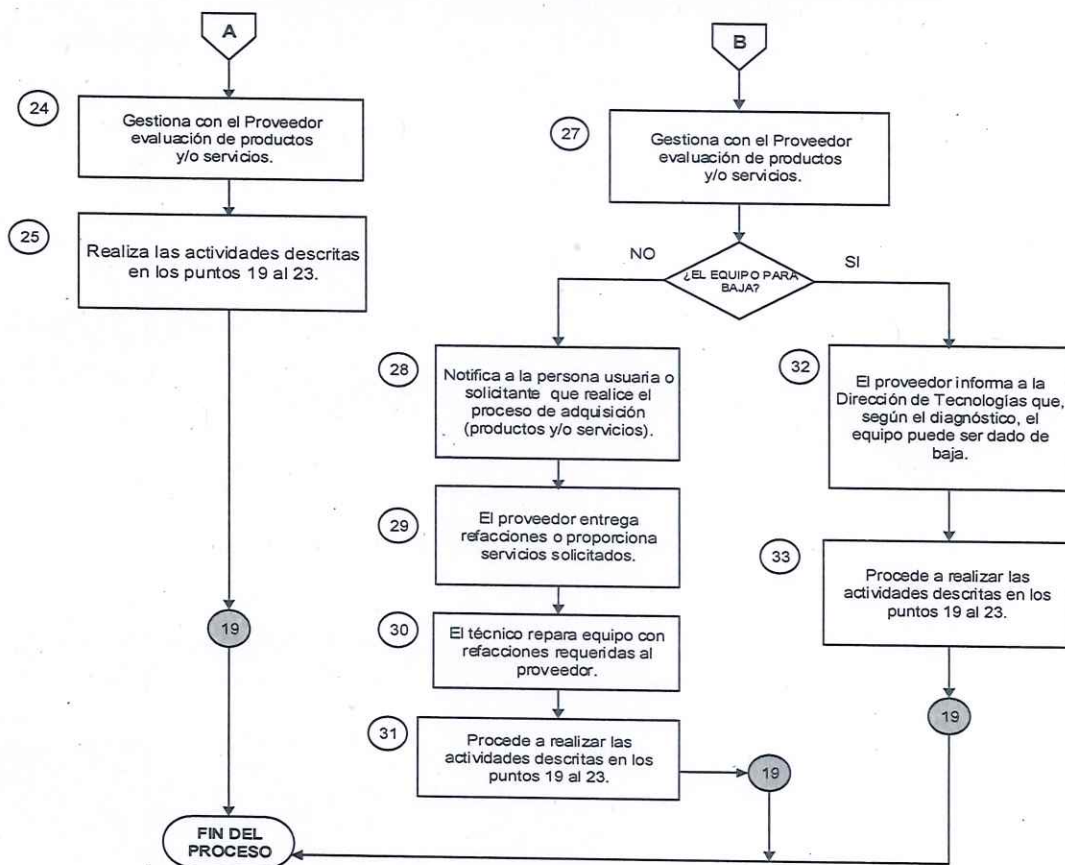
Actualización: 10 de agosto de 2026

Página: 104 de 150

DIAGRAMA DE FLUJO DEL PROCESO SOLICITUD DE SOPORTE TÉCNICO
(HOJA # 2)

DIRECCIÓN DE TECNOLOGÍAS

Persona titular de la Coordinación de Redes y/o Soporte Técnico



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 105 de 150

SAIA-DT-MPP-01-PROC-04-V3

PROCESO SOLICITUD DE PRÉSTAMO TEMPORAL DE EQUIPO DE CÓMPUTO

DESCRIPCIÓN DEL PROCESO

PERSONA USUARIA O SOLICITANTE

1. Verifica disponibilidad de equipo de cómputo con la persona responsable administrativo del servicio en la Dirección de Tecnologías.

¿HAY DISPONIBILIDAD?

Si

2. Captura o llena la información solicitada en el formato "Solicitud de Préstamo Temporal de Equipo de Cómputo" (*Anexo SAIA-DT-MPP-01-FORM-10-V3*).
3. Imprime y firma formato de solicitud.
4. Entrega el formato de solicitud a la persona responsable administrativo en la Dirección de Tecnologías.

DIRECCIÓN DE TECNOLOGÍAS – La persona Responsable Administrativo

5. Recibe formato "Solicitud de Préstamo Temporal de Equipo de Cómputo" (*Anexo SAIA-DT-MPP-01-FORM-10-V3*) debidamente lleno y firmado y le solicita a la persona usuaria su identificación oficial de empleado activo de la Administración Pública Municipal. Digitaliza documentos.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 106 de 150

6. Revisa el formato y entrega el equipo de cómputo solicitado.

FIN DEL PROCESO.

¿HAY DISPONIBILIDAD?

NO

7. Observa que no hay disponibilidad, por lo que esperará otro momento para verificar nuevamente la disponibilidad.

FIN DEL PROCESO.





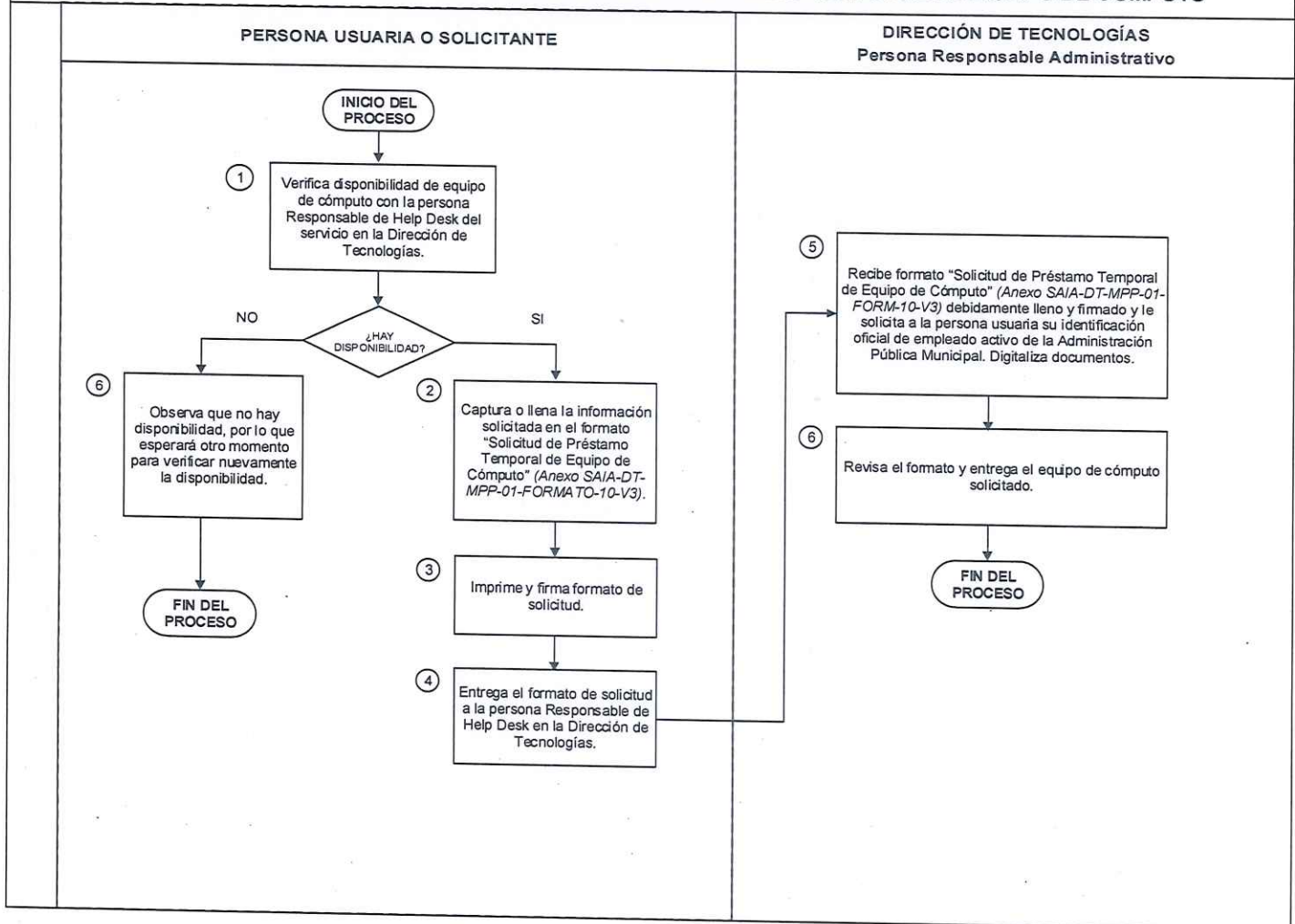
**SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL**

DIRECCIÓN DE TECNOLOGÍAS

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS

Codificación: SAIA-DT-MPP-01-V3
Versión: 3
Emisión: 01 de agosto de 2018
Actualización: 10 de agosto de 2026
Página: 107 de 150

DIAGRAMA DE FLUJO DEL PROCESO SOLICITUD DE PRÉSTAMO TEMPORAL DE EQUIPO DE CÓMPUTO



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 108 de 150

SAIA-DT-MPP-01-PROC-05-V3

PROCESO DE DEVOLUCIÓN DEL EQUIPO DE CÓMPUTO

DESCRIPCIÓN DEL PROCESO

PERSONA USUARIA O SOLICITANTE

1. Se presenta a realizar la devolución del equipo prestado.

DIRECCIÓN DE TECNOLOGÍAS – La persona que desempeña el puesto de Responsable Administrativo

2. Recibe y revisa condiciones físicas del equipo devuelto.

¿EL EQUIPO ESTÁ EN CONDICIONES ÓPTIMAS?

SI

3. Cierra el proceso del préstamo en el sistema.
4. Pone el equipo en estado de revisión.
5. Notifica a la Coordinación de Redes y Soporte Técnico.

DIRECCIÓN DE TECNOLOGÍAS – La persona titular de la Coordinación de Redes y Soporte Técnico

6. Espera el tiempo necesario para realizar la revisión del equipo.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 109 de 150

7. Revisa condiciones físicas y lógicas del equipo.

8. Elabora reporte de diagnóstico.

¿EL EQUIPO ESTÁ EN CONDICIONES DE SEGUIR OPERANDO?

SI

9. Lo pone en estado de disponibilidad.

FIN DEL PROCESO.

¿EL EQUIPO ESTÁ EN CONDICIONES DE SEGUIR OPERANDO?

NO

10. Notifica a la persona titular de la Dirección de Tecnologías.

11. Inhabilita equipo para préstamo.

FIN DEL PROCESO.

¿EL EQUIPO ESTÁ EN CONDICIONES ÓPTIMAS?

NO

DIRECCIÓN DE TECNOLOGÍAS – La persona que desempeña el puesto de Responsable Administrativo



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 110 de 150

12. Recibe el equipo y notifica a la persona usuaria o solicitante las observaciones.
13. Notifica a la persona titular de la Dirección de Tecnologías y pasa al numeral 4.

FIN DEL PROCESO.





**SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL**

DIRECCIÓN DE TECNOLOGÍAS

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS

Codificación:
SAIA-DT-MPP-01-V3

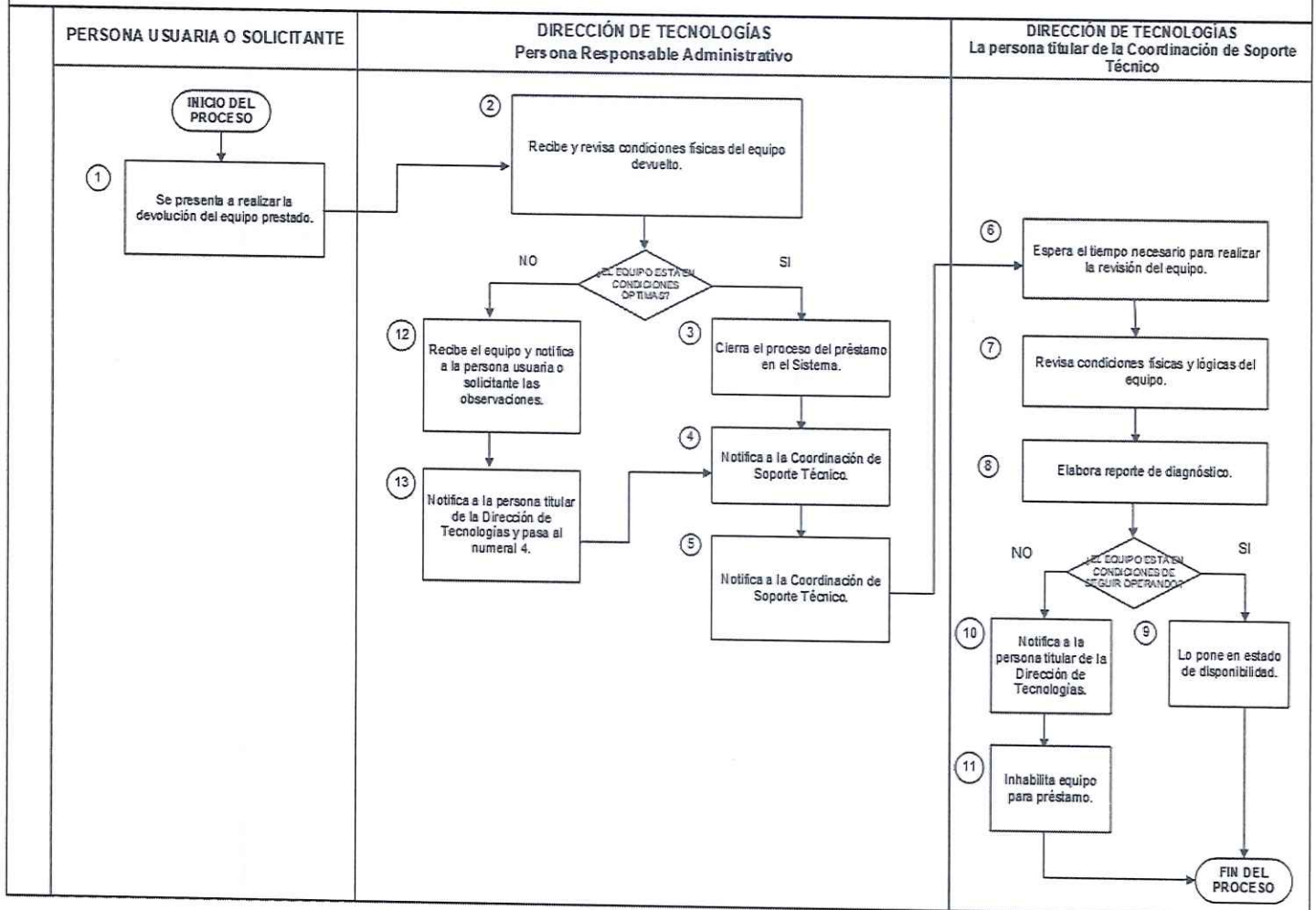
Versión: 3

Emisión: 01 de agosto de 2018

Actualización: 10 de agosto de 2026

Página: 111 de 150

DIAGRAMA DE FLUJO DEL PROCESO DE DEVOLUCIÓN DEL EQUIPO DE CÓMPUTO



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 112 de 150

IX. ANEXOS



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 113 de 150

SAIA-DT-MPP-01-FORM-01-V3

SOLICITUD DE SOPORTE TÉCNICO



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 114 de 150

 **TICKETS SOPORTE TÉCNICO**

Nombre:

Apellidos:

Email:

Teléfono / Extensión:

Describe el problema:

Activo Patrimonial:





	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 115 de 150

SAIA-DT-MPP-01-FORM-02-V3

SOLICITUD DE SOPORTE DE SISTEMAS



**SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL**

DIRECCIÓN DE TECNOLOGÍAS

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS

Codificación:
SAIA-DT-MPP-01-V3

Versión: 3

Emisión: 01 de agosto de 2018

Actualización: 10 de agosto de 2026

Página: 116 de 150

	PROCESO: Creación, Mantenimiento y Soporte Software		Código: _____	
	Formato Solicitud de Cambios, Ajustes y/o Creación de Nuevo Software		Versión: 1.0	
			Fecha: _____	
			Página: de	

Fecha de la Solicitud:	TICKET No.	
------------------------	-------------------	--

INFORMACIÓN DEL SOLICITANTE:			
Nombres completos del solicitante:		Apellidos completos del solicitante:	
Dependencia y/o Subdirección:		Cargo:	
Ubicación geográfica y/o número de oficina:		Teléfono y/o extensión:	
		Teléfono móvil:	

INFORMACIÓN SOBRE EL REQUERIMIENTO:			
Tipo de Requerimiento: Parametrización a software existente: ☐ Ajuste software existente: ☐ Nuevo componente a software existente: ☐ Nuevo desarrollo: ☐		Tipo de sistema a modificar o crear: Uso Interno: ☐ Uso Externo: ☐ Ambos: ☐	
		Nombre del sistema a modificar o crear: Prioridad: Alta ☐ Media ☐ Baja ☐	
		Referencia funcional: (Persona que acompañará el proceso): Nombre: _____ Identificación: _____ Teléfono: _____ Código: _____	

OBJETIVO GENERAL:	BENEFICIOS / BENEFICIARIOS:
Describa el objetivo general claro, puntual, utilice letra clara y legible, sin enmendaduras	Describa los beneficios que obtendrá con el sistema y los beneficiarios del mismo.

DEFINICIÓN DEL REQUERIMIENTO			

Indicadores resultantes y nombre del plan al que se alinean	REFERENTE SOLICITANTE	JEFE REFERENTE SOLICITANTE	ANALISTA (FIRMA EL RECIBO)
Nombre:	Fecha:		
Nombre:	Nombre:		
Nombre:	Cargo:		
Nombre:	Firma:		



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 117 de 150

SAIA-DT-MPP-01-FORM-03-V3 **RECEPCIÓN/ENTREGA EQUIPO DE CÓMPUTO**





SECRETARÍA DE ADMINISTRACIÓN E
INTELIGENCIA ARTIFICIAL

DIRECCIÓN DE TECNOLOGÍAS

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS

Codificación:
SAIA-DT-MPP-01-V3

Versión: 3

Emisión: 01 de agosto de 2018

Actualización: 10 de agosto de 2026

Página: 118 de 150

MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN
SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL
DIRECCIÓN DE TECNOLOGÍAS

ACTA DE ENTREGA-RECEPCIÓN DE ACTIVOS INFORMÁTICOS

Fecha: _____

El suscrito C. _____ en mi carácter de servidor público de la Administración Municipal de San Pedro Garza García, adscrito al departamento _____ con número de nómina _____ y como usuario de los activos informáticos que se me han asignado para el desarrollo de mis actividades de trabajo, respetuosamente manifiesto:

Que, a partir de la fecha de recibido indicada en este documento, me obligo a mantener en condiciones físicas óptimas los activos informáticos que recibo.

Acepto dar uso y cuidado adecuado de los activos informáticos: equipo de cómputo, periféricos, accesorios, software, etc., que a continuación se describe:

Nombre / IP	Descripción activo	Marcas/Modelo	Serie/No. parte	No. Patrimonio	No. Dir. Tec.
ACCESORIOS:					

Acepto que, al permitir la instalación y/o uso de software apócrifo en los equipos de cómputo o cualquier otro equipo perteneciente o bajo resguardo de la Administración Municipal que atenten o violenten las leyes de los derechos de autor, me hace acreedor de sanciones administrativas y económicas. Sanciones emitidas por las dependencias correspondientes de la Administración Municipal de San Pedro Garza García.

Acepto que solamente el personal adscrito a la Dirección de Tecnologías, es el único autorizado para brindar soporte técnico al hardware y software, bajo los procedimientos establecidos por la Dirección de Tecnologías.

Reconozco que durante el desempeño de mis funciones, en caso de tener acceso a información confidencial, sensible o reservada, relacionada con el Municipio de San Pedro Garza García, sus dependencias o sus servidores públicos, me comprometo de manera expresa e irrevocable a guardar la confidencialidad y seguridad de la información que por esta vía asumo; y a no divulgar, compartir, copiar, almacenar, transferir o utilizar indebidamente dicha información por ningún medio físico, electrónico o verbal, garantizando la confidencialidad, integridad y disponibilidad de la información a la que tenga acceso, así como observar en todo momento lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y las políticas y lineamientos internos a los que me obligo. Este compromiso subsistirá, incluso después de la conclusión de la relación laboral o contractual, de manera permanente, y su incumplimiento podrá derivar en responsabilidades administrativas, civiles o penales, según corresponda.

En caso de pérdida, robo o extravío del equipo bajo mi resguardo, me apegaré a lo señalado en el Manual de Políticas y Procedimientos para Bienes Muebles.

En caso de cambio de resguardante de alguno o todos los activos informáticos aquí descritos, estoy obligado a realizarlo mediante ticket de servicio en la aplicación sanpedrocontigo.mx.

Confirmando que he realizado respaldo de información de los activos que estoy entregando. Respaldo realizado en la nube con Google Drive. Además de aceptar y estar de acuerdo en que se realice el formateo correspondiente a estos activos.

Por último, reconozco que el equipo es un bien del Municipio de San Pedro Garza García, por lo que deberá ser entregado al momento de que yo, como empleado, cause baja, sea removido o separado del empleo, cargo o comisión.

Entrega

Personal de la Dirección de Tecnologías.

de conformidad nombre y firma
No. de nómina
Fecha y hora

Recibe

Resguardante de activos.

de conformidad nombre y firma
No. de nómina
Fecha y hora



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 119 de 150

SAIA-DT-MPP-01-FORM-04-V3

CONSTRUCCIÓN DE CONTRASEÑAS SEGURAS



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 120 de 150

La Dirección de Tecnologías pone a su disposición las siguientes políticas y acciones en el uso y construcción de las contraseñas para los usuarios de equipos de cómputo del Municipio de San Pedro Garza García.

- a) Se deben utilizar al menos 8 caracteres para crear la clave.
- b) Se recomienda utilizar en una misma contraseña dígitos, letras y caracteres especiales.
- c) Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas.
- d) Las contraseñas hay que cambiarlas con una cierta regularidad.
- e) Procurar no general reglas secuenciales de cambio. Por ejemplo: crear una nueva contraseña mediante un incremento secuencial del valor en relación a la última contraseña. Por ejemplo: pasar de "01Juitnx" o "02Juitnx".
- f) Utilizar signos de puntuación especiales, por ejemplo: "Tr-.3Fre". En este caso incluir otros caracteres que no sean alfanuméricos en la contraseña. Dentro de ese consejo se incluirá utilizar símbolos como: | " # \$ % & () * + , - . / : ; < = > ¿ @ [] ^ _ ` { } ~
- g) Existen algunos trucos para plantear una contraseña que no sea débil y se pueda recordar más fácilmente. Por ejemplo: se pueden elegir palabras sin sentido pero que sean pronunciables, etc. Nos podemos ayudar combinando esta selección con números o letras e introducir alguna letra mayúscula. Otro método sencillo de creación de contraseñas consiste en elegir la primera letra de cada una de las palabras que componen una frase conocida, de una canción, película, etc. Con ello, mediante esta sencilla mnemotecnica es más fácil recordarla. De la frase "Comí mucho chocolate el domingo 3, por la tarde", resultaría la contraseña: "cmCeD3-xLt". En ella se ha introducido alguna mayúscula, se ha cambiado el "por" en una "x" y, si el sistema lo permite, se puede colocar algún signo de puntuación (-).



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 121 de 150

Acciones que deben evitarse en la gestión de contraseñas seguras:

1. Evitar utilizar la misma contraseña siempre en todos los sistemas o servicios. Por ejemplo, si se utilizan varias cuentas de correo, se debe recurrir a contraseñas distintas para cada una de las cuentas.
2. No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento; y, por supuesto, en ninguna ocasión utilizar datos como el número de su nómina o número de teléfono.
3. Evitar utilizar secuencias básicas de teclado (por ejemplo: "qwerty", "asdf" o las típicas en numeración "1234" o "98765").
4. No repetir los mismos caracteres en la misma contraseña. (Ej. "111222").
5. Evitar utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.
6. No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.
7. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (Ejemplo: no poner como contraseñas apodos, el nombre del actor o de un personaje de ficción preferido, etc.).
8. No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma a la vista. Tampoco se deben guardar en documentos de texto en la computadora o dispositivo (Ejemplo: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto en la computadora).
9. No se deben utilizar palabras que se contengan en diccionarios en ningún idioma. Hoy en día existen programas de ruptura de claves que basan su ataque en probar una a una las palabras que extraen de diccionarios. Este método de ataque es conocido como "ataque por diccionario".



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 122 de 150

10. No enviar nunca la contraseña por correo electrónico o en un "sms". Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
11. Evitar mantener o almacenar contraseñas en correo electrónico.
12. No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.
13. No escribir las contraseñas en las computadoras de uso público (bibliotecas, cibercafés, telecentros, etc.).
14. No utilizar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.
15. No elegir una contraseña que se haya empleado anteriormente.

Lo anterior se hace del conocimiento de los usuarios de sistemas de información y de los equipos de cómputo del Municipio de San Pedro Garza García.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 123 de 150

SAIA-DT-MPP-01-FORM-05-V3

CONVENIO DE CONFIDENCIALIDAD



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 124 de 150

MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN

CONVENIO DE CONFIDENCIALIDAD

El presente Convenio de Confidencialidad (en adelante, el "Convenio") se celebra entre el **Municipio de San Pedro Garza García, Nuevo León** (en adelante, el "Municipio"), representado por _____, y **[NOMBRE COMPLETO DEL SERVIDOR PÚBLICO]**, en su carácter de servidor público (en adelante, el "Servidor Público"), de conformidad con las siguientes Declaraciones y Cláusulas:

DECLARACIONES:

I. Declara el Municipio:

- Que es una entidad de la administración pública municipal, con personalidad jurídica y patrimonio propios, facultado para celebrar el presente Convenio.
- Que, en el ejercicio de sus funciones, tiene acceso y genera información institucional y datos personales que deben ser protegidos de conformidad con la normativa aplicable.

II. Declara el Servidor Público:

- Que es servidor público del Municipio de San Pedro Garza García, desempeñando el cargo de **[CARGO DEL SERVIDOR PÚBLICO]**.
- Que, en razón de su cargo, tendrá acceso a información institucional y datos personales que, por su naturaleza, se consideran confidenciales y/o reservados.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 125 de 150

c) Que tiene conocimiento de las obligaciones y responsabilidades que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León, así como demás normatividad aplicable, imponen respecto del manejo, resguardo y protección de dicha información.

CLÁUSULAS:

PRIMERA.

El objeto del presente Convenio es establecer las obligaciones de confidencialidad y no divulgación a cargo del Servidor Público respecto de la información institucional y los datos personales a los que tenga acceso o conocimiento en el desempeño de sus funciones dentro del Municipio de San Pedro Garza García.

SEGUNDA. Para los efectos del presente Convenio, se entenderá por "**información confidencial**" toda aquella información a la que el Servidor Público tenga acceso, conocimiento o posesión, de forma oral, escrita, electrónica, visual o por cualquier otro medio, que sea propiedad del Municipio o que se encuentre bajo su resguardo, incluyendo, sin limitación:

a) **Información Institucional:** Proyectos, planes, estrategias, procesos internos, manuales, bases de datos, informes, estadísticas, información financiera, presupuestal, administrativa, técnica, legal, y cualquier otra información generada o utilizada por el Municipio en el cumplimiento de sus atribuciones que no sea de carácter público por disposición legal o por su propia naturaleza.

b) **Datos Personales:** Cualquier información concerniente a una persona física identificada o identificable (titular), incluyendo, sin limitación, nombre, domicilio, teléfono, correo electrónico, RFC, CURP, información patrimonial, financiera, académica, laboral, de salud, biométricos, ideológicos, raciales, sexuales, entre otros, que obren en posesión del Municipio.

TERCERA. El Servidor Público se obliga a:

a) Mantener la más estricta confidencialidad sobre la **información confidencial** a la que tenga acceso, durante y después de la terminación de su relación laboral o contractual con el Municipio.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 126 de 150

b) No divulgar, revelar, reproducir, copiar, distribuir, modificar, usar o permitir el uso de la **información confidencial** a terceros no autorizados, ya sean personas físicas o morales, públicas o privadas.

c) Utilizar la **información confidencial** exclusivamente para el cumplimiento de sus funciones y responsabilidades inherentes a su cargo dentro del Municipio.

d) Implementar las medidas de seguridad administrativas, físicas y técnicas necesarias para garantizar la protección de la **información confidencial**, de conformidad con la normativa aplicable y las políticas internas del Municipio.

e) Informar de manera inmediata al Municipio sobre cualquier divulgación, acceso, uso o tratamiento no autorizado de la **información confidencial** de la que tenga conocimiento.

f) Resguardar la **información confidencial** en los lugares y bajo las condiciones de seguridad que el Municipio determine.

g) Devolver al Municipio, al término de su relación laboral o cuando así le sea requerido, toda la **información confidencial** que obre en su poder, en cualquier formato.

CUARTA.

Las obligaciones de confidencialidad establecidas en el presente Convenio no serán aplicables a aquella información que:

a) Sea del dominio público al momento de su revelación o que posteriormente pase a serlo sin incumplimiento del presente Convenio.

b) Sea legalmente requerida por autoridad competente, previa notificación al Municipio para que este ejerza sus derechos.

c) Sea proporcionada a terceros con la autorización previa y por escrito del Municipio.

QUINTA.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 127 de 150

El incumplimiento de las obligaciones establecidas en el presente Convenio por parte del Servidor Público será causa de responsabilidad administrativa, sin perjuicio de las responsabilidades civiles y penales a que haya lugar, de conformidad con la legislación aplicable.

SEXTA.

El presente Convenio tendrá una vigencia indefinida, subsistiendo las obligaciones de confidencialidad incluso después de la terminación de la relación laboral o contractual del Servidor Público con el Municipio.

SÉPTIMA.

Para todo lo relacionado con la interpretación y cumplimiento del presente Convenio, las partes se someten a la jurisdicción de los tribunales competentes en el Estado de Nuevo León, renunciando a cualquier otro fuero que por razón de sus domicilios presentes o futuros pudiera corresponderles.

Leído que fue el presente Convenio y enteradas las partes de su contenido y alcance legal, lo firman por duplicado en la ciudad de San Pedro Garza García, Nuevo León, a los [DÍA] días del mes de [MES] de [AÑO].

POR EL MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN

[NOMBRE Y CARGO DEL REPRESENTANTE DEL MUNICIPIO]

EL SERVIDOR PÚBLICO

Nombre, número de empleado y firma

CONVENIO DE CONFIENCIALIDAD ANEXO DEL CONTRATO NÚMERO
(_____) QUE CELEBRAN POR UNA PARTE EL GOBIERNO DEL MUNICIPIO DE SAN PEDRO
GARZA GARCÍA, N.L. REPRESENTADA POR EN LO SUCESIVO “EL CLIENTE” Y POR LA
OTRA, _(nombre del proveedor) REPRESENTADA POR (nombre del representante), EN LO



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 128 de 150

SUCESIVO “EL PROVEEDOR”, AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS:

DECLARACIONES:

- I. Que es deseo de su mandante solicitar de “(nombre del proveedor)” la prestación de servicios para la realización del proyecto denominado “_____”.

En tal virtud y para tales efectos se le proporcionará a “(nombre del proveedor”, y también ésta entregará a “**EL CLIENTE**”, a partir de la fecha de firma del presente instrumento diversa información confidencial, de acuerdo con los términos y condiciones que se pacten en el presente convenio y conforme a lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y demás disposiciones aplicables.

- II. Declara “**EL PROVEEDOR**” por conducto de su apoderado:
- a) Que solicita y está de acuerdo en recibir y dar a “**EL CLIENTE**” cierta información confidencial para llevar a cabo la prestación de servicios, para la realización del proyecto denominado “_____”, de conformidad con los términos y condiciones que se pacten en este instrumento.

Expuesto lo anterior ambas partes se sujetan bajo los términos y condiciones a que este Convenio se refiere, de conformidad con las siguientes:

CLÁUSULAS:

PRIMERA. - Para efectos del presente convenio se considera como “**Información Confidencial**” toda aquella información verbal, escrita, digital o de cualquier otro tipo, relacionada con:

- Infraestructura tecnológica del Municipio.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 129 de 150

- Bases de datos, códigos fuente, contraseñas, accesos, configuraciones, reportes, incidencias, planes de contingencia.
- Información técnica, operativa o administrativa que sea propiedad del Municipio o que se encuentre bajo su resguardo.
- Datos personales y/o sensibles de usuarios o personal del Municipio.

Así como cualquier otra información identificada como confidencial conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Y en virtud del presente convenio, ambas partes se entregarán diversa información confidencial consistente en:

- a) **“EL CLIENTE”**, entregará a **“EL PROVEEDOR”** los permisos para acceder a las bases de datos que contienen la información comercial que forma parte integrante de este convenio para todos los efectos legales a que haya lugar, asimismo la información podrá ser entregada tanto en formato de papel como electrónicamente por medio de dispositivos USB.

En tal virtud **“LAS PARTES”**, recíprocamente se entregarán la referida información en forma enunciativa y no limitativa y que en lo sucesivo se le denominará la **“INFORMACIÓN”**.

SEGUNDA. - Asimismo, **“LAS PARTES”** se obligan a recibir, manejar, analizar y utilizar la **“INFORMACIÓN”** de manera estrictamente confidencial únicamente para los fines del contrato principal, así como para el uso y beneficio de las mismas; obligándose a lo siguiente:

- No revelar, divulgar, publicar, difundir o transmitir a cualquier tercero la **“INFORMACIÓN”** que reciban recíprocamente, para ningún objeto distinto al proyecto de
“_____”.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 130 de 150

- A su vez **“LAS PARTES”** se comprometen a no divulgar ni sacar provecho en forma directa o indirecta con terceras partes, sobre metodologías y herramientas de consultoría provenientes de las bases de datos y otras fuentes propiedad de **“EL CLIENTE”** y **“EL PROVEEDOR”**.

TERCERA. - Las restricciones de uso o divulgación de la información establecidas en la presente cláusula, no serán aplicables en forma recíproca a cualquier información que se encuentre en las siguientes condiciones:

- Que sea desarrollada independientemente por **“LAS PARTES”** sin el uso o soporte de la información o que sea recibida libre de restricción de un tercero que tenga derecho o licencia para divulgar esa información; o
- Que posteriormente se convierta en información del dominio público sin que **“LAS PARTES”** hayan violado este Convenio, o
- Que, al momento de haberse divulgado, era conocida por **“LAS PARTES”** sin existir restricción de uso, según sea comprobado con documentación en posesión de la parte que así corresponda.

CUARTA. - La información estará sujeta a las siguientes restricciones:

- Si está por escrito o en otra forma tangible, únicamente si está marcada como PROPIEDAD, CONFIDENCIAL o PROPIEDAD de **“LAS PARTES”** al entregarse.
- El resultado de la información del servicio contratado estará supeditados a las restricciones establecidas por ambas de partes.

QUINTA. - Ninguna licencia de uso de marca registrada, patente, derecho de autor, secreto de empresa o cualquier otro derecho de propiedad intelectual, ni autorización de uso para un fin distinto al previsto en este Convenio, se entiende que ha sido otorgada, expresa o tácitamente, a cualquiera



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 131 de 150

de "LAS PARTES" por habérseles divulgado información. Ninguna parte de la información que se divulgue o intercambie, constituye una declaración, garantía, aseveración o interpretación de cualquier tipo, de "EL CLIENTE" a "EL PROVEEDOR", o de "EL PROVEEDOR" a "EL CLIENTE", con relación a derechos de terceros (marcas, patentes, derechos de autor o cualquier otro derecho de propiedad industrial).

SEXTA. - Ni este Convenio, ni la divulgación o recibo de información constituye o se interpreta como una promesa o compromiso de realizar una compraventa de productos o servicios por "LAS PARTES", con relación a la comercialización presente o futura de cualquier producto o servicio.

SÉPTIMA. - "EL PROVEEDOR" reconoce que toda la información además de la mencionada, así como aquellos documentos rotulados y preparados específicamente que sean resultado de las actividades de los proyectos y que estén relacionados con el mercado, producto o proceso productivo son propiedad de "EL CLIENTE", en todo momento, lugar y circunstancia, razón por la cual "EL PROVEEDOR" tratará como estrictamente confidencial y secreta la INFORMACIÓN que le revele o entregue "EL CLIENTE" a "EL PROVEEDOR"

OCTAVA. - "LAS PARTES" se obligan a guardar secreto y confidencialidad en forma recíproca respecto de toda la INFORMACIÓN que reciba una de otra, de manera permanente desde la firma del presente convenio, así como después de concluido éste.

NOVENA. - "LAS PARTES" por ningún motivo podrán ceder sus derechos y obligaciones contraídas en el presente Convenio a cualquier tercero.

Asimismo, este convenio constituye el acuerdo íntegro de las partes y ninguna modificación verbal o escrita tendrá efectos legales, excepto que se encuentre firmada por apoderado legal de cualquiera de las mismas.

DÉCIMA. - Ambas partes recíprocamente se obligan a responder, indemnizar y asumir toda responsabilidad, por cualquier divulgación o revelación que cualquiera de ellas haga de la INFORMACIÓN en contravención a lo dispuesto en el presente convenio, ya sea directamente o por conducto de sus funcionarios, trabajadores, empleados, agentes o representantes respectivamente.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 132 de 150

DÉCIMA PRIMERA.- Las partes manifiestan expresamente que no se encuentran vinculadas bajo ningún tipo de relación laboral, de modo que “EL CLIENTE” y “EL PROVEEDOR”, en forma independiente serán los únicos responsables en todo tiempo y lugar de sus relaciones laborales con los trabajadores y empleados a su servicio, asumiendo expresamente cada parte su exclusiva responsabilidad para el caso de cualquier conflicto individual y/o colectivo derivado de dicha relación, obligándose la parte que incumpla a esta obligación, a sacar en paz y a salvo a la otra, sin necesidad de juicio previo.

DÉCIMA SEGUNDA. - Al término del contrato principal, por cualquier causa, ambas partes se obligan a eliminar, destruir y abstenerse de conservar cualquier tipo de información confidencial o datos personales proporcionados mutuamente durante la relación contractual, por lo que esto deberá ser:

1. Eliminar de manera definitiva, total e irreversible toda la INFORMACIÓN confidencial o datos personales a los que haya tenido accesos, resguardo o tratamiento durante la vigencia del contrato, sin conservar copias físicas ni electrónicas, salvo que exista disposición legal expresa que los obligue a conservarlos.
2. Para información en soportes electrónicos o digitales, la eliminación deberá realizarse mediante técnicas de borrado seguro (wiping) o destrucción de bajo nivel (low-level formatting), conforme a los estándares internacionales de seguridad de la información, que impidan su recuperación o reconstrucción posterior.
3. Para documentos en formato físico o papel, la destrucción deberá realizarse mediante triturado, incineración o cualquier otro método que garantice la destrucción total e ilegible de la INFORMACIÓN.
4. “LAS PARTES” deberán entregarse recíprocamente en un plazo no mayor a 10 días hábiles posteriores a la terminación del contrato principal, un acta o constancia de destrucción o eliminación, firmada por su representante legal y responsable de seguridad de la información, en la que se detalle:



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 133 de 150

- El tipo de información eliminada (digital/física).
 - El medio o técnica utilizada para su destrucción.
 - La fecha en que se llevó a cabo la eliminación.
 - El personal responsable del proceso.
5. En caso de que alguna de "LAS PARTES" lo requiera, podrá realizar una verificación directa o solicitar evidencia técnica adicional que demuestre la destrucción efectiva.
6. El incumplimiento de esta obligación será considerado una falta grave y dará lugar a las acciones legales correspondientes, incluyendo la exigencia de responsabilidades civiles, administrativas o penales, según el caso.

DÉCIMA TERCERA.- El incumplimiento de lo dispuesto en este Convenio dará lugar a la aplicación de las sanciones legales, civiles, administrativas o penales que correspondan, conforme a las leyes aplicables, incluyendo la posibilidad de rescisión del contrato y/o exigencia de daños y perjuicios.

DÉCIMA CUARTA.- Para la interpretación y cumplimiento del presente Convenio, las partes se someten a la jurisdicción de los tribunales competentes, renunciando a cualquier otra que pudiera corresponderles con motivo de sus domicilios presentes o futuros.

Enteradas las partes de los efectos y alcances legales que implica la celebración del presente Convenio de Confidencialidad, lo firman de común acuerdo, por duplicado y ante la presencia de dos testigos, a los _____ días del mes de _____ del año _____.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 134 de 150

“EL CLIENTE”

“EL PROVEEDOR”

MUNICIPIO DE SAN PEDRO GARZA
GARCÍA, N.L.

Representado por:

(NOMBRE DEL PROVEEDOR)
Representada por:

TESTIGOS:



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 135 de 150

SAIA-DT-MPP-01-FORM-06-V3

REPORTE DE DIAGNÓSTICO DE EQUIPO DE CÓMPUTO



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 136 de 150

Número de oficio: _____

Dirigido a: _____
Puesto: _____
Área: _____

PRESENTE.-

Asunto: Diagnóstico de equipo de cómputo.

A través de este conducto le informamos que en la revisión del equipo de cómputo siguiente:

Descripción: _____
Marca: _____
Modelo: _____
Número de serie: _____ Número de Patrimonio: _____
Resguardante: _____

El Personal de Soporte Técnico de la Dirección de Tecnologías ha determinado:

- Dar de baja por reparación incosteable.
- Equipo obsoleto-funcional, sin opciones de actualización o reparación.
- Equipo reparable, leer observaciones.

Observaciones:

Sin más por el momento, agradeciendo de antemano su atención a la presente, me despido de Ud.
Reiterándole mi disposición para cualquier duda o aclaración del diagnóstico.

Atentamente:

Nombre, número de nómina y firma.

DIRECCIÓN DE TECNOLOGÍAS

Página 1/1



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 137 de 150

SAIA-DT-MPP-01-FORM-07-V3

REGISTRO DE RESPALDOS



[illegible]Página:

	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 139 de 150

SAIA-DT-MPP-01-FORM-08-V3

PLAN PARA RESPALDO DE INFORMACIÓN EN EQUIPOS DE USUARIOS (DISASTER RECOVERY PLAN, DRP)



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 140 de 150

PLAN PARA RESPALDO DE INFORMACIÓN EN EQUIPOS DE CÓMPUTO:

Para la información electrónica generada por los usuarios (sin considerar los datos capturados en los sistemas de información que residen en el Centro de Datos Municipal); resultado de sus funciones laborales dentro de la Administración Pública Municipal, se recomienda seguir los siguientes pasos para prevenir un desastre en la pérdida de información de relevancia e impacto para su departamento.

Pasos iniciales del Plan de Recuperación:

- I. Identificar el sitio; equipo de cómputo de trabajo, en la que se encuentra su información a respaldar.

Se recomienda identificar la ubicación física del equipo de cómputo; así como, el número de identificación de patrimonio. Es importante contar con un registro de los respaldos realizados, esto nos permitirá llevar un mejor control sobre los respaldos realizados. En los anexos se sugiere un formato ejemplo para el control de respaldos – ver anexo – Formato para Registro de Respaldos.

- II. Identificar el o los folders en donde se ubica la información.

Identificar la ubicación de los folders en donde se encuentra almacenada la información electrónica a ser respaldada.

- III. Valorar la información, determinando cuál es la de mayor criticidad e impacto en su departamento, si se tuviera una pérdida de la misma.

Esta clasificación queda a total consideración del usuario. En lo que el usuario puede determinar qué información es realmente importante, de relevancia e impacto, bajo el esquema de continuidad en el servicio o valor histórico para la Administración Pública Municipal.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 141 de 150

IV. Establecer el tiempo para el Punto de Recuperación Objetivo, PRO (Recovery Point Objective) y el Tiempo de Recuperación Objetivo, RTO (Recovery time Objective).

El Punto de Recuperación Objetivo, PRO (Recovery Point Objective) es la capacidad de recuperar la información en el punto anterior. Es decir, cuántos datos puede perder el área antes de que se paralice su funcionamiento de trabajo. Por ejemplo, si ocurre un desastre y quiere recuperar una hora de datos, entonces el PRO recomendado es de una hora.

El Tiempo de Recuperación Objetivo, RTO (Recovery Time Objective), es el tiempo que se tarda en volver el servicio. Es decir, cuánto tiempo tiene el usuario para volver a contar con la información en el sistema después de una pérdida de información.

El Punto de Desastre, es el momento en que, por alguna situación, la información o datos no puede ser leída, accesada, extraviada o simplemente no se encuentra en el equipo de cómputo de trabajo.

Como parte del plan de continuidad del servicio, el usuario debe examinar cuánto tiempo puede permitirse de no tener disponible los datos antes de que falle el servicio. La respuesta es crucial para la eficiente continuidad del servicio.

La unidad de medición, tanto en el PRO como en el TRO, es el tiempo, con valores que abarcan desde segundos, minutos, horas, hasta días o semanas. Los valores cambian dependiendo de cada necesidad y de la actividad que realice el área administrativa a la que pertenece el usuario.

Cuanto más se acerquen los varios PRO y TRO a cero, mayor será la dependencia del departamento, en el proceso de continuidad del servicio y; por consiguiente, mayor prioridad tendrá a la hora de recuperar los datos, en caso de interrupción o pérdida.

V. Respaldar la información de mayor criticidad.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 142 de 150

El usuario realiza los respaldos en dispositivos de almacenamiento masivo. Los dispositivos más comunes que se pueden utilizar son el USB, DVD, disco externo, etc.

El usuario también podrá considerar realizar un respaldo adicional en el mismo equipo de cómputo y otro equipo de la Administración Pública Municipal.

La Dirección de Tecnologías también ofrece el servicio de disponer espacio en algún servidor del Centro de Datos. Este servicio estará condicionado a las capacidades de espacio disponibles en el momento del servicio y a la determinación del tiempo en que permanecerá la información en estos servidores. El usuario podrá solicitar el servicio a la Dirección de Tecnologías, usando el Formato de Soporte Técnico – ver anexo.

- VI. Mantener la periodicidad de respaldos de acuerdo al PRO establecido, así como realizar pruebas de verificación.

De manera aleatoria el usuario deberá de realizar pruebas de la información respaldada, para que así constate que la información respaldada está totalmente disponible.

Una vez concluido el plan, el usuario mantendrá activo el plan con la tarea de respaldar (paso 5), de manera que lleva a cabo los respaldos con la periodicidad establecida en los pasos anteriores.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 143 de 150

SAIA-DT-MPP-01-FORM-09-V3

PLAN DE RESPALDOS DE INFORMACIÓN DEL CENTRO DE DATOS (DISASTER RECOVERY PLAN, DRP)



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 144 de 150

Plan de respaldos de información del Centro de Datos (Disaster Recovery Plan, DRP):

Para los sistemas de información que están ubicados en el centro de cómputo de la Dirección de Tecnologías y que, a través de la red municipal, son operados por los usuarios a los que se tiene acceso debidamente autorizado; la Dirección de Tecnologías deberá ejecutar acciones de un plan de respaldos y recuperación ante un posible desastre de pérdida de información de estos sistemas de información.

En este Plan de Respalos y Recuperación ante Desastres, indicamos que ante lo que pudiera ocasionar la pérdida de información en magnitud e impacto de los servicios, el respaldo de la información cumpla con los estándares de seguridad probados en el mercado. De tal manera que, ante un evento de pérdida de información, se debe ejecutar el Plan de Recuperación con un porcentaje de recuperación bastante alto. La Dirección de Tecnologías ha considerado que el esquema de respaldos en la nube (on cloud) ofrecen estándares suficientemente altos para resguardo y recuperación.

Pasos del DRP para los sistemas de información en la nube:

- Identificar los sitios.

Se identificarán los servidores en donde se encuentran los sistemas de información a respaldar.

- Identificar los sistemas de información.

Elaborar un inventario de los sistemas de información en cada uno de los servidores, indicando entre otros aspectos, la ubicación de los folders en donde se ubican los sistemas de información.

- Evaluación de la criticidad de los sistemas de información



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 145 de 150

Clasificar los sistemas de mayor impacto. En esta clasificación se podrán tomar diferentes parámetros como la cantidad de usuarios operativos, cantidad de servicios o transacciones, etc.

- Determinar los tiempos estimados en que debemos de recuperar los servicios.

Para ello determinamos los siguientes parámetros de tiempo para cada uno de los sistemas de información.

Punto de Recuperación Objetivo, PRO (Recovery Point Objective).- Capacidad de recuperar la información en el punto anterior. Es decir, cuántos datos puede perder el área antes de que se paralice su funcionamiento de trabajo. Por ejemplo, si ocurre un desastre y quiere recuperar una hora de datos, entonces el PRO recomendado es de una hora.

Tiempo de Recuperación de Trabajo, TRT (Work Recovery Time).- Tiempo que se necesita para verificar el sistema, la integridad de los datos, comprobar las bases de datos y asegurarse de que las aplicaciones o servicios se están ejecutando bien. Cuando los sistemas o datos afectados por el desastre son verificados, se reanuda de nuevo el servicio.

Tiempo Máximo Sin Servicio, TMSS (Maximum Tolerable Downtime).- Tiempo Máximo Tolerable fuera de servicio para cada proceso en cada instalación, con el fin de ayudar en la definición de las estrategias de recuperación.

En la siguiente gráfica se aprecian los conceptos antes citados. También se indican los distintos eventos ocurridos durante el proceso de respaldo y recuperación.

Etapas indicadas en el gráfico anterior, indicando un escenario en que ocurre un evento de pérdida de información.

Etapas 1.- Etapa en operación normal.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 146 de 150

En esta etapa todos los sistemas están trabajando con normalidad, respaldos realizados con normalidad.

Etapa 2.- Ocurre un paro de servicio.

Se presenta un paro en el servicio, se inicia el procedimiento del plan de recuperación. En este punto, el Punto de Recuperación, PRO, determina la máxima cantidad de datos perdidos aceptable en el tiempo.

Etapa 3.- Etapa de recuperación.

En esta etapa los sistemas son restaurados, pero no están listos para ponerse en producción aún. El Tiempo de Recuperación Objetivo, RTO, determina la máxima cantidad de tiempo tolerable necesario para llevar de regreso todos los sistemas. Esto cubre, por ejemplo, restaurar los datos de los respaldos o corregir alguna falla. En muchos casos ésta parte es llevada por el administrador del sistema, el administrador de la red, el administrador de respaldos, etc.

Etapa 4.- Se recupera la producción de los sistemas.

En esta etapa todos los sistemas recuperados, la integridad o los datos son verificados y los sistemas críticos pueden llevar a las operaciones normales. El Tiempo de Recuperación del Trabajo, TRT, determina el máximo tiempo tolerable que es necesario verificar el sistema y/o la integridad de los datos. Esto puede ser, por ejemplo, checar las bases de datos y los "logs", asegurarse que las aplicaciones o servicios estén corriendo y estén disponibles. En muchos casos estas tareas son ejecutadas por el administrador de la aplicación, el administrador de las bases de datos, etc. Cuando todos los sistemas son verificados y/o recuperados, el medio ambiente está listo para reiniciar los servicios nuevamente.

La suma de TRO y TRT está definida como el Tiempo Máximo Tolerable Sin Servicio, TMSS (Maximum Tolerable Downtime) el cual define el total de tiempo que los servicios del departamento pueden estar indisponibles sin causar alguna consecuencia inaceptable.



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 147 de 150

SAIA-DGT-MPP-01-FORMATO-10-V3

SOLICITUD DE PRÉSTAMO TEMPORAL DE EQUIPO DE CÓMPUTO

www.sanpedro.gob.mx

SAIA-DT-MPP-01-V3



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 148 de 150

		###/###/###	####
1. INFORMACIÓN DEL USUARIO.			
Nombre del usuario solicitante. Haga clic o pulse aquí para escribir texto.		Nómina y puesto Haga clic o pulse aquí para escribir texto.	
Secretaría Haga clic o pulse aquí para escribir texto.	Departamento / Oficina Haga clic o pulse aquí para escribir texto.	Teléfono / Extensión Haga clic o pulse aquí para escribir texto.	
2. SERVICIOS.			
☒ Solicitud de préstamo temporal de equipo de cómputo (A.11.8)	☐ Servicio de Instalación. (A.11.3)	☐ Otros. (Describir en la sección 4)	
3. EQUIPO PRÉSTAMO.			
Capture la cantidad de equipos requeridos (verificar disponibilidad).			
Laptop(s): #	Impresora(s) a blanco y negro: #	Antena(s): #	
Tableta(s): #	Proyector(es): #		
4. INFORMACIÓN DEL EVENTO O REQUERIMIENTO.			
Describa el evento y/o requerimiento. Teclee aquí.		Horario (fecha y hora). De ____/____/____ ____ hrs. A ____/____/____ ____ hrs.	
5. FIRMA DE SOLICITUD.			
_____		____/____/____	
firma del usuario solicitante		Fecha firma	
6. AREA EXCLUSIVA DE LA Dirección de Tecnologías.			
Entrega del equipo			



	SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL DIRECCIÓN DE TECNOLOGÍAS MANUAL DE POLÍTICAS Y PROCEDIMIENTOS	Codificación: SAIA-DT-MPP-01-V3
		Versión: 3
		Emisión: 01 de agosto de 2018
		Actualización: 10 de agosto de 2026
		Página: 149 de 150

Fecha de Préstamo: ____/____/____ Hora de Préstamo: ____:____
hrs.

Dirección de Tecnologías	
Departamento entrega	Departamento recibe
Nombre y Firma	Nombre y Firma

Detalle equipo

No	Cantidad	Equipo	Número Identificador (Serie/Patrimonio/Tecnologías)

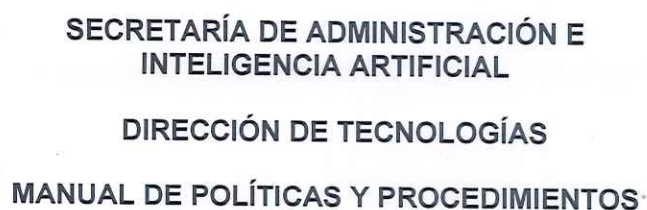
Equipo programado para devolverse en:

Fecha de devolución: ____/____/____ Hora de devolución: ____:____
hrs.

Devolución del equipo.

Fecha de devolución: ____/____/____ Hora de devolución: ____:____
hrs.





Página: 150 de 150

[]

Departamento entrega

Nombre y Firma

