REPUBLICA DE CHILE
PROVINCIA DE LINARES
ILUSTRE MUNICIPALIDAD
RETIRO
Control Interno

DECRETO EXENTO N° 381 /
RETIRO, 30 de enero del 2024.

VISTOS:

1.- Lo dispuesto en el D.F.L N° 1-3063 Del Ministerio Del Interior, Las Facultades Que Me Confiere La Ley Orgánica Constitucional De Municipalidades N° 18.695 Y Sus Modificaciones Posteriores.

2.- La ley 19.880 que establece base del procedimiento administrativo que rigen los actos de los órganos de la administración del estado.

3. Manual de procedimiento de las siguientes materias pertenecientes al Unidad de Informática

4.- Las facultades que me confiere la Ley N° 18.695, Orgánica Constitucional de Municipalidades y sus modificaciones posteriores.

CONSIDERANDO:

1. Importante contar con manuales de procedimientos que contenga reglas y pautas conforme se indican de cómo se deben ejecutarse ciertos procesos administrativos. Este manual permitirá a la unidad de informática guiar y administrar sus operaciones, estrategias y flujos de trabajo hacia resultados óptimos, así como mantener estándares de eficiencia y eficacia.

DECRETO:

1. APRUEBESE, el manual de procedimiento de la dirección de informática, de la Ilustre Municipalidad de Retiro. -

2. COMUNIQUESE, a todo el personal del departamento administrativo de la Municipalidad De Retiro.

ANOTESE, COMUNIQUESE, NOTIFÍQUESE Y ARCHIVESE.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

GERARDO BAYER TORRES
SECRETARIO MUNICIPAL

I. MUNICIPALIDAD DE RETIRO
ALCALDE

RODRIGO RAMIREZ PARRA
ALCALDE

BFA/jsl-
DISTRIBUCIÓN:
Alcaldía.
- Juzgado De Policía Local
- Administrador Municipal.
- Secretaria Comunal de Planificaciones.
- Secretaria Municipal.
- Dirección Desarrollo Comunitario
- Dirección Administración y Finanzas.
- Departamento de Obras Municipales.
- Departamento de Tránsito y Transporte Público.
- Archivo Dirección de Control Interno/

Retiro
Tierra de Agricultores

MANUAL DE PROCEDIMIENTO

Soporte Informático

Ilustre Municipalidad de Retiro

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

INDICE

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

INTRODUCCIÓN

En atención a los riesgos y las amenazas que día a día pueden atacar el ámbito de la seguridad de los datos y la información, activos correspondientes a la Ilustre Municipalidad de Retiro, ha sido necesario tomar acciones necesarias para implementar un Sistema de Gestión de Seguridad de la Información que pretende minimizar los riesgos correspondientes al ámbito de la información y los datos que se procesan en el día a día laboral, es por eso que se ha documentado una serie de controles y procedimientos correspondientes a la Seguridad Informática y de la Información, tendiente a avanzar hacia la certificación de sus procesos y por ende consolidarse como una institución en donde la información que se procesa en el día a día, finalmente posea un valor significativo. Dado lo anterior se han documentado una serie de procedimientos, que sirven como un método de información para guiar al funcionario en el quehacer en materia de Seguridad de la Información, de tal modo que sea entendible y clara para tomar las acciones y medidas necesarias para que el Sistema de Gestión de Seguridad de la Información funcione de la forma más eficaz. Las tecnologías de la información y comunicación (TIC) contribuyen a optimizar y elevar los niveles de productividad y eficiencia, correspondiéndole al Departamento de Computación e Informática velar porque dichas tecnologías se integren a los procesos y actividades del servicio de manera tal de brindar al funcionario el máximo apoyo en cuanto a su gestión. Estos procedimientos están enfocados en el ámbito de resguardar la Confidencialidad, la Integridad y la Disponibilidad de todos los activos de información de la Ilustre Municipalidad de Retiro a tal modo de optimizar los recursos, evitando pérdidas de información y la difusión de documentos y contenidos confidenciales de la institución.

PROCESO	VERSION
Manual de procedimiento de soporte	1.0
PROPIETARIO	
Departamento de Informática	ENERO -24

OBJETIVO DEL MANUAL

El presente manual de procedimiento de atencion de usuarios es el documento que contiene la descripcion de los procesos y actividades que se deben seguir en la realizacion de servicios del departamento de Informática de la Ilustre Municipalidad de Retiro.

NORMATIVA

1.- Ley 19.223 Delitos Informacion
Identificacion de las normas: LEY-19223
Fecha de Publicacion:07.06.1993
Fecha de promulgacion: 28.05.1993
Organismo: MINISTERIO DE JUSTICIA

2.- Normas Chilenas oficial N.Ch2777 of.2003 ISO/IEC 27002:2013
INSTITUTO NACIONAL DE NORMALIZACION INN-CHILE
Tecnologia de la informacion-código de práctica para la gestión de seguridad.

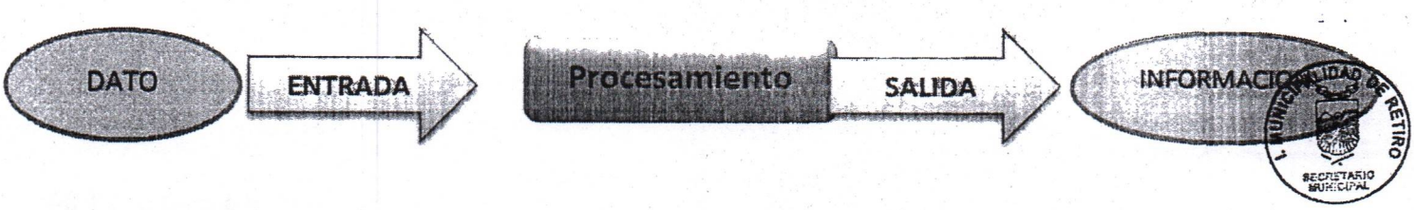
3.- Decreto supremo N° 83, normas tecnicas para los organos del estado sobre seguridad y confidencialidad de los documentos electronicos.
MINISTERIO SECRETARIA GENERAL DE LA RESIDENCIA
Marco base: Norma Chilena oficial N.Ch 2777

ALCANCE: Todos los usuarios de la Ilustre Mnicipalidad De Retiro que posean un equipo computacional unico o compartido, cuenta de dominio o correo institucional.

DEFINICIONES

¿Que Es La Informacion?

Según la Real Academia Española "es la comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada"
La información es un conjunto de datos acerca de algún suceso, hecho o fenómeno, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo".
A pesar que generalmente, los términos de datos e información se usan para describir lo mismo, para el profesional en tecnologías de información éstos términos significan diferentes cosas



¿Seguridad de la información?

La seguridad de la información es el conjunto de medidas y técnicas utilizadas para controlar y salvaguardar todos los datos que **se manejan dentro de la organización y asegurar que los datos no salgan del sistema** que ha establecido la organización. Es una pieza clave para que las instituciones puedan llevar a cabo sus operaciones, ya que los datos que maneja son esenciales para la actividad que desarrollan.
De forma mayoritaria, los sistemas de **las organizaciones se basan en las nuevas tecnologías**, no podemos confundir seguridad de la información y seguridad informática que, si bien están íntimamente relacionadas, no siendo el mismo concepto.
Es importante comprender que cualquier organización, independientemente de su tamaño, cuenta con dato confidenciales, bien de sus clientes, bien de sus trabajadores o bien de ambos, y que por ello tiene que **establecer las medidas de seguridad en protección de datos** necesarios para garantizar el correcto tratamiento de estos, algo que, con la entrada en vigor primero de LOPD y después de RGPD, no es una opción, sino una obligación.

Es por lo anteriormente expuesto que en el siguiente documento se establecen los procesos y políticas básicas de resguardo de la información del Municipio.

GLOSARIO DE TERMINOS

- **Correo electrónico:** bajo este epígrafe se agrupan una serie de tecnología que permiten la interconexión de ordenadores para el intercambio de mensajes, documentos, informaciones, etc. La conexión puede realizarse a través de una red o mediante módems y uso de líneas telefónicas. Las empresas utilizan este sistema a nivel comercial para facilitar el intercambio de información entre sus empleados.
- **Anexo telefónico:** los anexos permiten a las grandes compañías conectar a las personas que llaman con diversos departamentos y empleados. Existen varios atajos para ahorrar tiempo cuando llamas al anexo de una compañía. Gracias a los sistemas operativos sofisticados, podrás incluso programar teléfonos inteligentes a fin de que marquen anexos por ti.
- **Hardware:** el hardware es la parte física del dispositivo, esto es, sus accesorios, mientras que el software comprende el conjunto de códigos del sistema operativo.
- **Software:** oficial o soporte lógico al sistema formal de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hace posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados *hardware*. La interacción entre el software y el hardware hace operativo un ordenador (u otro dispositivo), es decir, el *software* envía instrucciones que el *hardware* ejecuta, haciendo posible su funcionamiento.
- **Cuentas de usuario de dominio:** Una cuenta de usuario de dominio permite al servicio sacar el máximo partido de las características de seguridad del servicio de Windows y Microsoft Active Directory Domain Services. El servicio tiene cualquier acceso local y de red que se conceda a la cuenta, o a cualquier grupo de los que la cuenta sea miembro.
- **Dominio:** es un grupo de trabajo de máquinas SMB que tienen un añadido: un servidor que actúa como controlador de dominio.
- **Login:** ingreso de usuario a un programa o sistema protegido bajo previa autenticación.
- **Mailing list:** Lista de correo o listas de distribución, establecen foros de discusión privados a través de correo electrónico. Las listas de correo están formadas por direcciones e-mail de los usuarios que la componen.
- **Microsoft Outlook:** cliente de correo desarrollado por la empresa Microsoft. Existen 2 versiones en este programa: la versión Outlook Express o Window Mail, que es gratuita y la versión de pago incluida en la suite office (Microsoft Word, Excel, Power Point y Outlook)
- **Modelo OSI:** El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) fue el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984

MUNICIPALIDAD DE RETIRO SECRETARIO MUNICIPAL

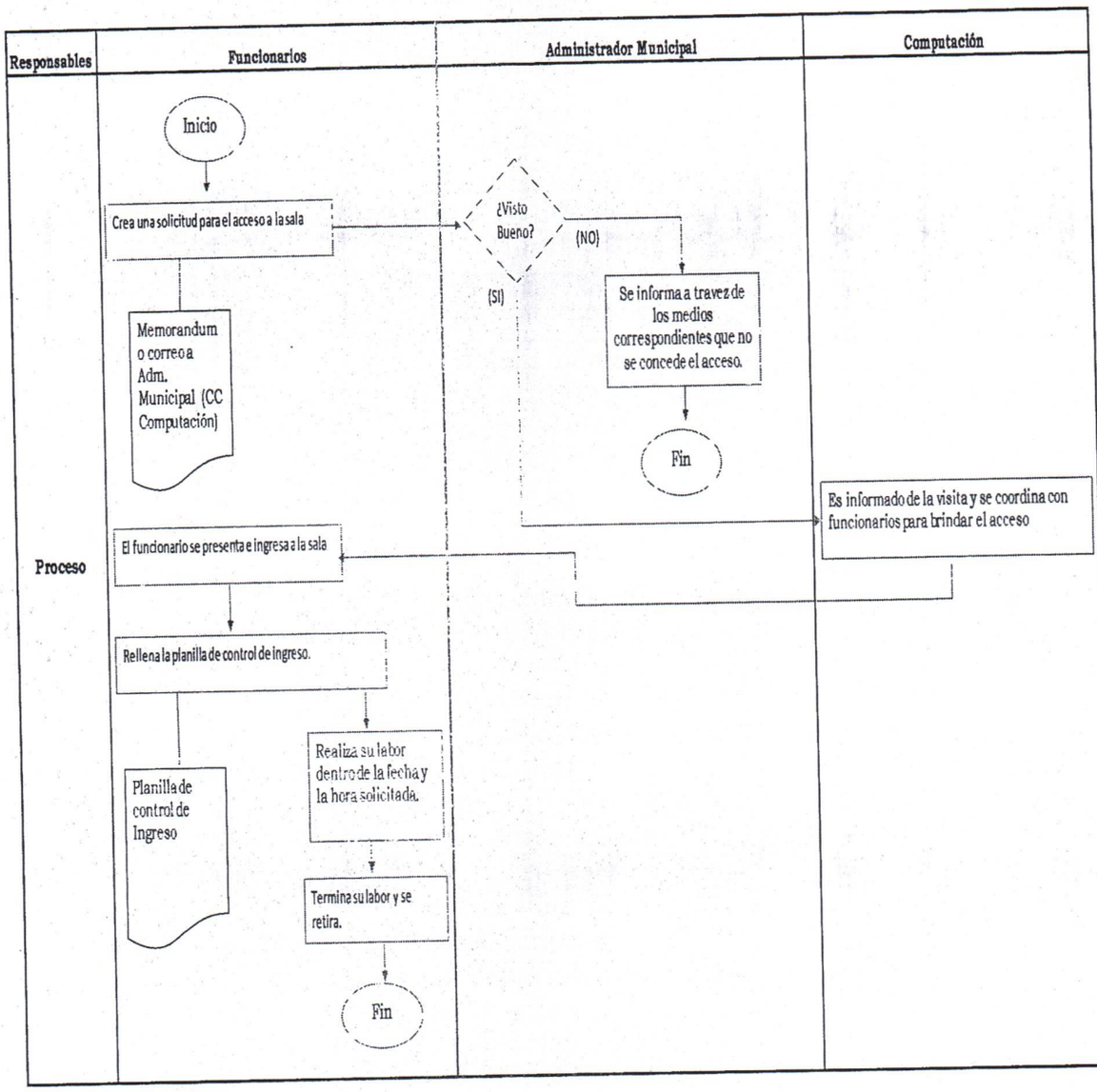
Es decir, fue un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

- **Password:** Se refiere al complemento del código de acceso, que es la parte secreta y que sólo el dueño del código de acceso la debe de conocer, también conocida como clave o password.
- **PST:** Extensión de archivo utilizado por Microsoft Outlook para almacenar los correos localmente.
- **Recursos de red:** Elementos disponibles para su uso a través de la red. Pueden ser impresoras, archivos, carpetas etc.
- **SMB: (Server Message Block)** es un Protocolo de red (que pertenece a la capa de aplicación en el modelo O.S.I.) que permite compartir archivos e impresoras (entre otras cosas) entre nodos de una red. Es utilizado principalmente en ordenadores con Microsoft Windows y DOS.
- **Spam o Spamming:** Una manera inapropiada de utilizar una Lista de Correo, algún otro tipo de comunicación en el Internet tal como si fuese un medio de emisión múltiple de mensajes (el cual no lo es) enviando el mismo mensaje a un gran número de personas aún y cuando no lo hayan solicitado.
- **Webmail:** (correo basado en web, correo electrónico de sitio web, correo web) Este es un servicio muy utilizado por los usuarios en Internet, en donde a través de una página pueden revisar sus correos, sin necesidad de tener que utilizar un cliente de correo.

PROCEDIMIENTO PARA LA SALA ELÉCTRICA Y SERVIDOR	
Nombre	Procedimiento para Acceso a Sala Eléctrica y Servidor
Alcance y aplicación	Todos los Funcionarios Municipales y personal externo a la Municipalidad
Descripción	Se describe las acciones a realizar en caso de que un funcionario municipal o personal externo a la municipalidad, desea acceder a la sala eléctrica y de servidor del municipio.
Normativa	Punto 7 – Seguridad Física y Ambiental En la Ilustre Municipalidad de Retiro, la única área protegida total la cual se describe en esta política de seguridad de la información es a la Sala Eléctrica y de Servidores, ubicada en el patio de los naranjos de la Municipalidad. Punto 7.2 – Controles de Acceso Físico Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, la entrada a la sala de servidores, está ubicada en una sala en la cual ya posee acceso restringido, a su vez esta sala de servidores tiene señalética en su puerta que indica que sólo el personal autorizado por el Alcalde, Administrador Municipal, Encargado de Computación o Encargado de Seguridad de la Información pueden acceder. Esta concesión de acceso está definida por un procedimiento a la cual se debe considerar la solicitud de acceso, y registrar al personal que ingrese a la sala eléctrica y de servidores. En relación a los Racks estos estarán protegidos con llave que sólo el Encargado de Computación tiene en su poder.

I. MUNICIPALIDAD DE RETIRO

DIAGRAMA DE FLUJO DE PROCEDIMIENTO

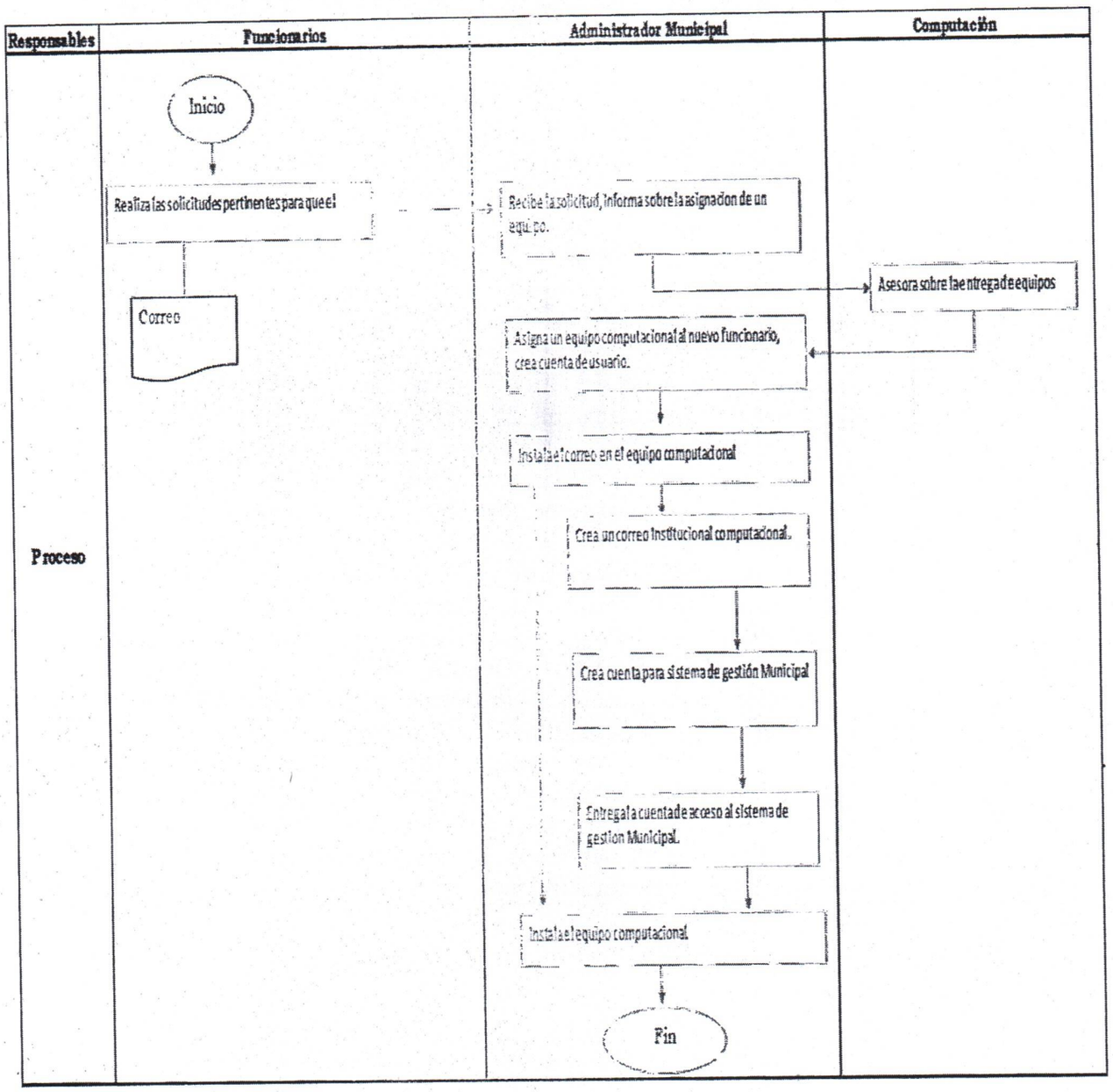


Nota	La solicitud de acceso a la sala eléctrica y de servidores debe llevar al menos los siguientes datos, en lo posible se exigirán los datos antes de que acceda el usuario, en este caso si es repentino, sólo basta con rellenar lo siguiente en una planilla de control de acceso (este estamento esta dictaminado para personal interno y externo a la municipalidad): a. Nombres y Apellidos. b. Organización, en el caso de que sea una persona interna puede mencionar el área de trabajo. c. Motivo de ingreso, importante para la concesión del acceso. d. Fecha de inicio y término de la visita, la fecha de término puede ser aproximado. e. Hora de inicio y término de la visita, la hora de término puede ser aproximado. La solicitud debe de ser enviada al Administrador Municipal para su visto bueno. El acceso debe de ser acompañado por un funcionario del área de Computación por motivos de control y registro de trabajo del usuario ingresado a esta zona.

ENTREGA DE ACCESO AL SISTEMA DE INFORMACIÓN	
Nombre	Entrega de Acceso a Sistemas de Información
Alcance y aplicación	Todos los Funcionarios Municipales
Descripción	Cada funcionario municipal que trabaja en oficina debe de contar con el acceso a los sistemas de información previamente autorizados por el Área de Computación
Normativa	Punto 9.2. Administración de Accesos de Usuarios Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información. Punto 9.2.1. Registración de Usuarios El Encargado de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, dependiendo de las necesidades a la cual se le concesione un acceso a un nuevo funcionario, además de tener claro cuales sistemas ocupaba un funcionario que es dado de baja. Punto 9.2.2. Administración de Privilegios Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Punto 9.2.3. Administración de Contraseñas de Usuario La asignación de contraseñas se realizará bajo ciertos patrones definidos por el Área de Computación. Punto 9.2.4. Administración de Contraseñas Críticas Existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de

	plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Encargado de Seguridad de la Información definirá procedimientos para la administración de dichas contraseñas críticas. Punto 9.2.5. Revisión de Derechos de Acceso de Usuarios A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate, llevará a cabo un proceso formal, a intervalos regulares de no más a 6 meses, a fin de revisar los derechos de acceso de los usuarios. Punto 9.3.1. Uso de Contraseñas Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. Los usuarios deben cumplir las directivas que se impartan a tal efecto. Punto 9.3.2. Equipos Desatendidos en Áreas de Usuarios Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

DIAGRAMA DE FLUJO



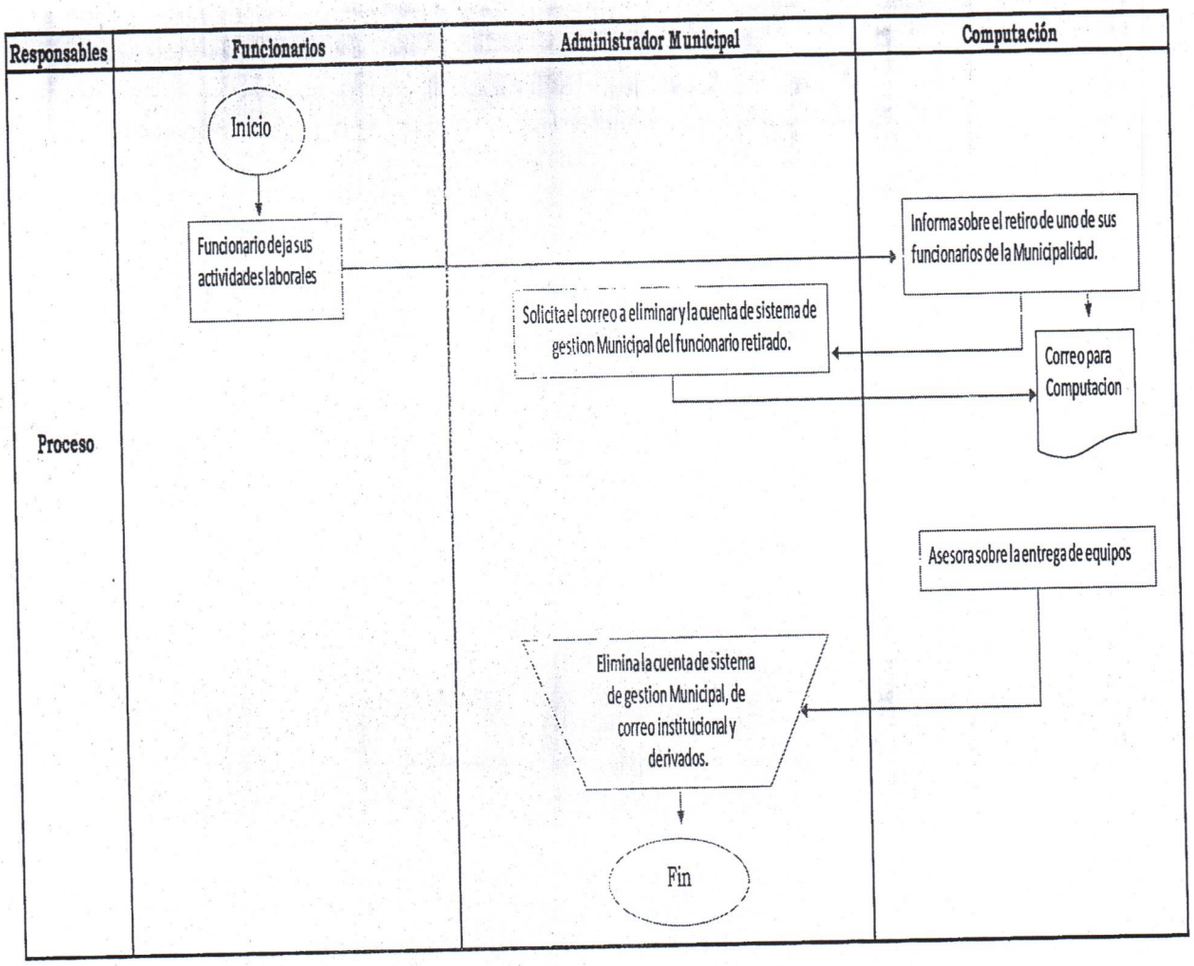
Nota	Las solicitudes deben de venir escritas por el jefe directo del nuevo funcionario. La creación de cuentas de acceso a los equipos computacionales se hace en base al servicio en la cual opera el nuevo funcionario, por ejemplo, si Pedro Pérez comienza sus labores en el servicio de Dibujante en la Dirección de Obras, la cuenta Windows, a la cual se le entrega el acceso al sistema de cómputo es "DibujanteDOM". La nueva cuenta de correo institucional se entrega con el siguiente formato: • Correo Electrónico: Inicial del nombre y apellido como identificador (ej: pperez@retiro.cl). • Todos los correos institucionales terminan con "@retiro.cl". • La clave del correo institucional debe de ser entregado por el jefe directo. Estos levantamientos de usuario quedarán registrados en un almacén de datos con todos los funcionarios operativos en la Ilustre Municipalidad de Retiro. La capacitación incluye, el uso del correo electrónico, los peligros y riesgos de seguridad de la información, los derechos y funciones referentes a esta materia, información de internet, de instalación de software, de uso de medios extraíbles, entre otros informativos de menor prioridad.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

REVOCACION DE ACCESO A SISTEMA DE NFORMACIÓN	
Nombre	Revocación De Acceso A Sistema De información
Alcance y aplicación	Funcionarios Municipales que dejan sus funciones.
Descripción	El objetivo de este procedimiento es cancelar el acceso a un funcionario que deja sus funciones en la Ilustre Municipalidad de Retiro, para evitar la filtración y el posterior mal uso de los servicios informáticos del municipio.
Normativa	Punto 9.2. Administración de Accesos de Usuarios Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información. Punto 9.2.1. Registración de Usuarios El Encargado de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, dependiendo de las necesidades a la cual se le concesione un acceso a un nuevo funcionario, además de tener claro cuales sistemas ocupaba un funcionario que es dado de baja. Punto 9.2.2. Administración de Privilegios Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Punto 9.2.3. Administración de Contraseñas de Usuario La asignación de contraseñas se realizará bajo ciertos patrones definidos por el Área de Computación.

	Punto 9.2.4. Administración de Contraseñas Críticas Existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Encargado de Seguridad de la Información definirá procedimientos para la administración de dichas contraseñas críticas. Punto 9.2.5. Revisión de Derechos de Acceso de Usuarios A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate, llevará a cabo un proceso formal, a intervalos regulares de no más a 6 meses, a fin de revisar los derechos de acceso de los usuarios. Punto 9.3.1. Uso de Contraseñas Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. Los usuarios deben cumplir las directivas que se impartan a tal efecto. Punto 9.3.2. Equipos Desatendidos en Áreas de Usuarios Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

DIAGRAMA DE FLUJO



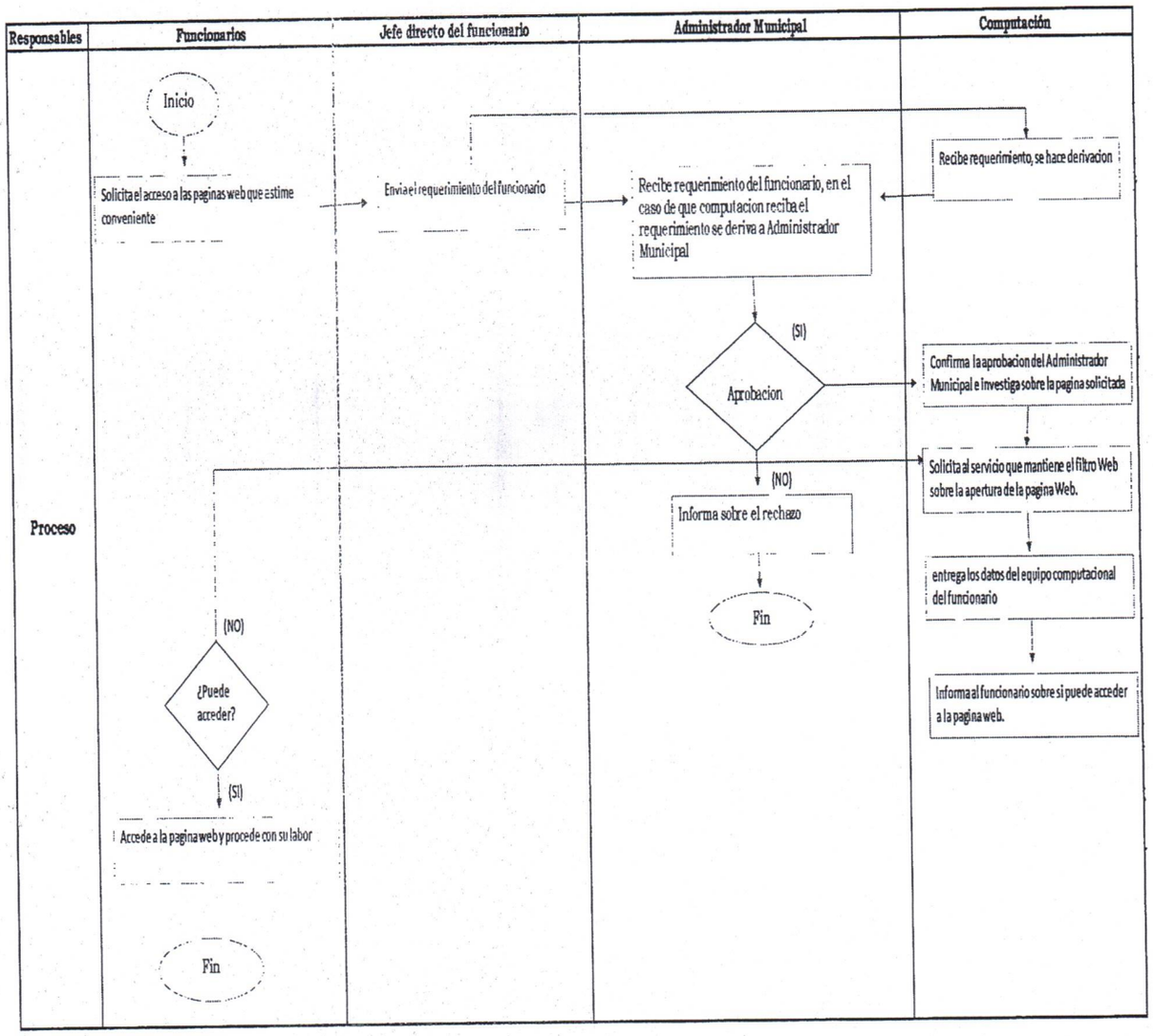
Notas	La eliminación de los registros del ex-funcionario contemplan lo siguiente: • Cuentas de Sistemas de Gestión Municipal (en el caso de que el funcionario ocupara estos sistemas). • Cuenta de Correo Electrónico. • Limpieza de clave de la cuenta de usuario. El computador en la cual el ex-funcionario realizaba sus funciones quedará a disposición de la alta dirección para la toma de decisión.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

SOLICITUD DE ACCESO A PAGINAS WEB FILTRADAS	
Nombre	Solicitud De Acceso A Páginas Web Filtradas
Alcance y aplicación	Todos los Funcionarios Municipales
Descripción	Conceder el acceso a páginas web que facilitan la labor del funcionario y que debido al cortafuegos del municipio no pueden acceder ya que el sitio web se encuentra filtrado en las categorías bloqueadas.
Normativa	Punto 8.5.1. Controles de Redes El Encargado de Seguridad de la Información definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes del Municipio, contra el acceso no autorizado, con controles que indiquen el monitoreo de red y su uso. El Encargado de Computación implementará dichos controles. Punto 9.4.6. Subdivisión de Redes Se definirán y documentarán los perímetros de seguridad que sean convenientes, que se implementarán mediante la instalación de "Gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado. Punto 9.4.7. Acceso a Internet El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El Encargado de Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente, por escrito, por el Director de cada Departamento Municipal, quien esté a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios. Punto 9.4.8. Control de Conexión a la Red Se podrán implementar controles para limitar la capacidad de conexión de los usuarios, de acuerdo a las políticas que se establecen a tal efecto. Dichos controles se podrán implementar en los "Gateways" que separan los diferentes dominios de la red. Punto 9.4.9. Control de Ruteo de Red Se incorporarán controles de ruteo, para asegurar que las conexiones

	informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino. Punto 9.4.10. Seguridad de los Servicios de Red El Encargado de Seguridad de la Información junto con el Encargado de Computación definirán las pautas para garantizar la seguridad de los servicios de red de la Municipalidad, tanto de los públicos como los privados.

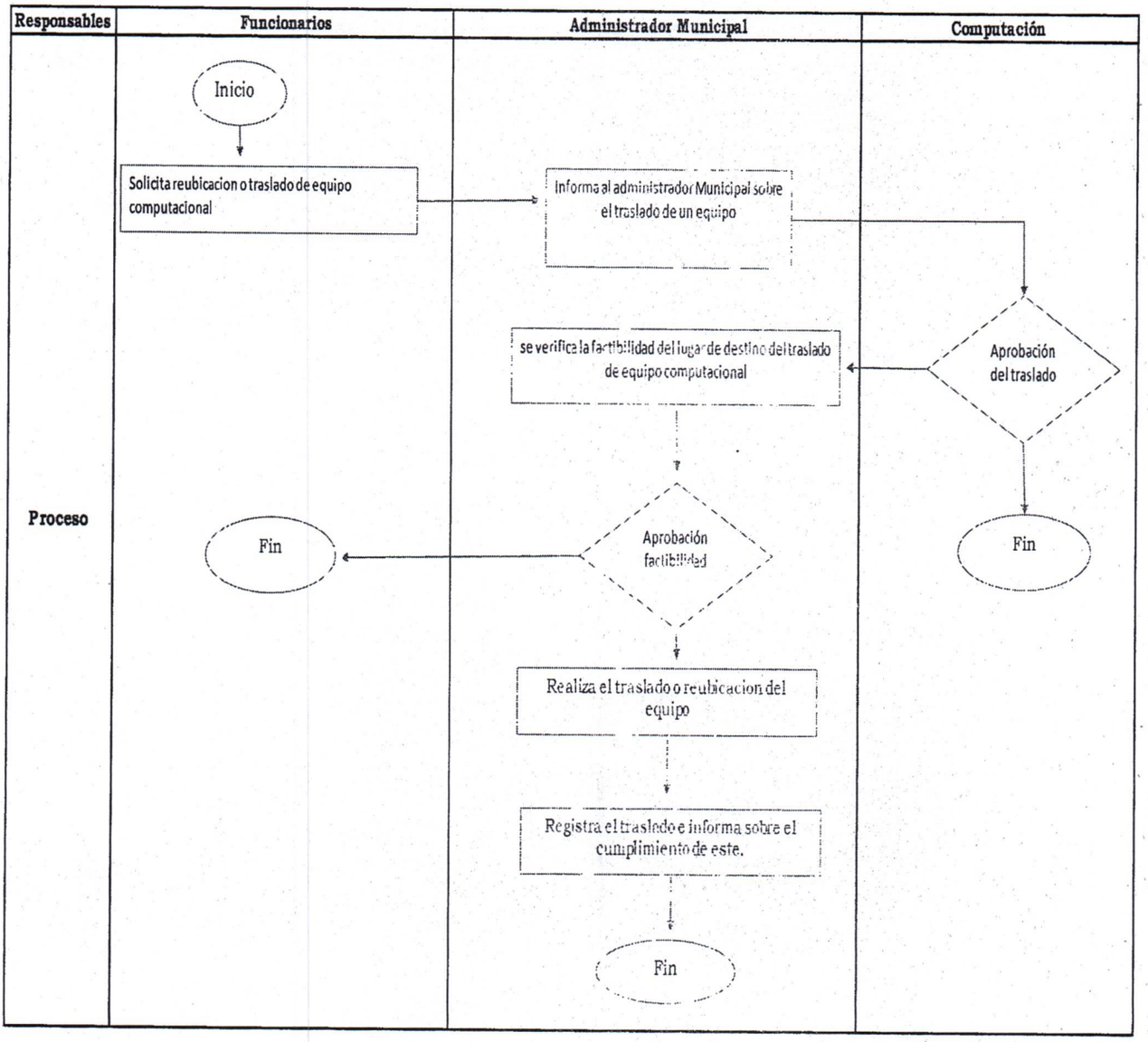
DIAGRAMA DE FLUJO



Notas	El funcionario debe de solicitar la apertura de la página web a su jefe directo y con la aprobación de la solicitud, el jefe directo del funcionario le realiza la solicitud al Administrador Municipal. En el caso de que Computación reciba la solicitud, se deriva la solicitud al Administrador Municipal. Si no se aprueba las páginas web solicitadas, se le informa al Jefe Directo del funcionario en cuestión que se denegó el acceso a la página web. Si se aprueba la o las páginas web, se realiza la solicitud al Administrador del Firewall, en este caso, la solicitud se realiza al servicio de internet contratado con la IP objetivo a la cual se le concede el acceso, esto se repite si aún el funcionario no puede acceder a la página web.

REUBICACION DE EQUIPOS MUNICIPALES	
Nombre	Reubicación de equipos Municipales.-
Alcance y aplicación	Todos los Funcionarios Municipales que requieran del cambio de su lugar de trabajo.
Descripción	Detallar el procedimiento para el traslado o reubicación de equipos municipales con el fin que estime conveniente el funcionario, encargado de un departamento o un directivo de la Ilustre Municipalidad de Retiro.
Normativa	Punto 8.8.2. Seguridad de los Medios en Tránsito Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar la utilización de medios de transporte o servicios de mensajería confiables, suficiente embalaje para el envío y la adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Punto 5.1. Inventario de activos Se identificarán los activos físicos que procesan datos e información, sus respectivos propietarios y su ubicación para luego elaborar un inventario con dicha información. El departamento encargado de elaborar el inventario y mantenerlo actualizado ante cualquier modificación de la información, es la Dirección de Administración y Finanzas de la Municipalidad. Punto 7.4. Ubicación y Protección del Equipamiento El equipamiento computacional y su cableado serán ubicados y protegidos, de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, a su vez para evitar riesgos para el funcionario.

DIAGRAMA DE FLUJO



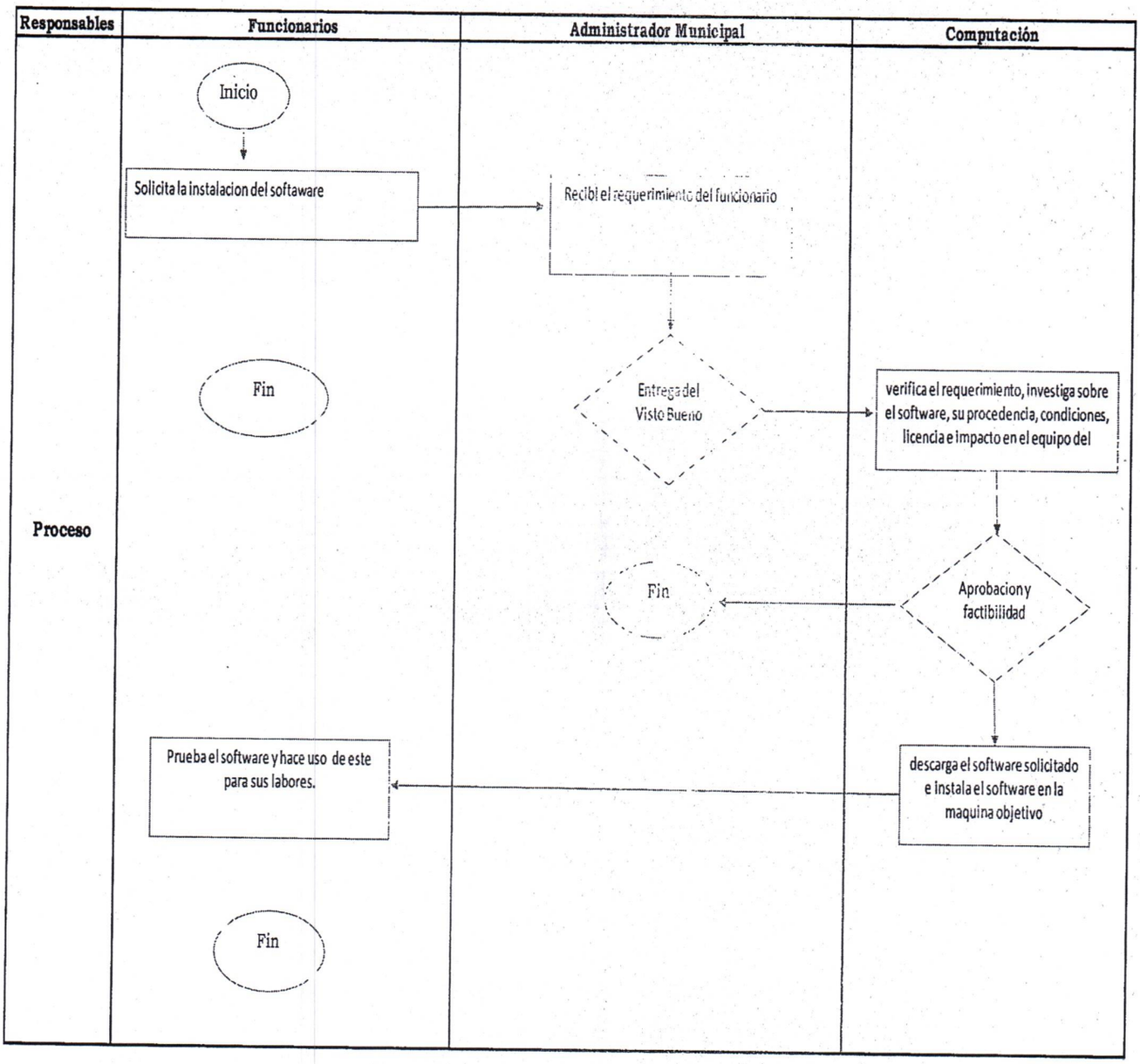
I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

Nota	El traslado o reubicación de equipos debe de ser aprobado previamente por Computación bajo el análisis de factibilidad técnica, y aprobado por el Administrador Municipal. Si la factibilidad técnica es viable, se procede a la validación de las partes antes mencionadas. Luego de esas validaciones, se procede al traslado del equipo según el requerimiento del funcionario.

INSTALACION DE SOFTWARE Y APLICACIONES	
Nombre	Instalación de Software y aplicaciones
Alcance y aplicación	Todos los Funcionarios Municipales que soliciten una nueva instalación de algún software que deseen.
Descripción	Este procedimiento tiene como objetivo describir los pasos a seguir para instalar un nuevo software en un equipo computacional de un funcionario, verificar y evaluar el software a instalar, con previo visto bueno de su Jefe Directo y además se evalúa si el software es compatible con el equipo computacional.
Normativa	Punto 8.3.1. Instalación Estándar de los Equipos Computacionales Cada vez que se formatea un equipo computacional, se deben de tomarse en cuenta las siguientes consideraciones: • Windows Instalado: Windows 7 Profesional (debido al programa de Actualización, se considera también la actualización directa a Windows 10 Pro) • Configuración Regional con los siguientes cambios: • Símbolo Decimal: "." • Símbolo de Separación de Miles: "," • Separador de Listas: ";" • Hora Corta: HH:mm • Hora Larga: HH:mm:ss • Símbolo a.m.: AM • Símbolo p.m.: PM • Fecha Corta: dd/MM/aaaa • Primer día de la Semana: lunes • Fondo Fijo de pantalla indicando el logo de la Municipalidad La instalación del software estándar municipal es el siguiente: • Lector de PDF • Antivirus: o Para funcionarios: AVAST o Avira o Para equipos críticos: ESET NOD32 • WinRAR • Google Chrome Microsoft office (Licenciado), Windows (licenciado) y antivirus (licenciado) • Yak! Punto. 8.3.2. Instalación de Software que no es estándar Para instalar un software que sea específico y que sea el funcionario debe realizar una solicitud por escrito, a

	Computación con la Autorización de su Jefe Directo, una vez que se ha aprobado, se procede a verificar que el equipo cumpla con los requisitos, para después empezar la instalación. Punto 8.3.3. Sanciones por Incumplimiento de Procedimiento Si el funcionario instala el software sin autorización, la próxima vez que se realice un control aleatorio de equipos, se desinstalará de su computador sin previo aviso. Además, si aún sigue instalando software, se expone a que se revoquen los accesos a los sistemas informáticos.

DIAGRAMA DE FLUJO



(*.mp3 y similares) y archivos de video que no estén relacionados con las funciones municipales.
Punto 8.7.2. Periodicidad de Respaldos Se hará un respaldo diario en un disco duro externo, la cual se realizará a las 18:30 hrs. de cada jornada laboral, y este disco duro externo se almacenará fuera de las dependencias del municipio cuando no se esté cursando la jornada laboral. También se genera un respaldo en el servidor, de acuerdo al plan de mantenimiento programado por el servidor SQL, este

PROCESO	VERSION
Manual de procedimiento de soporte	1.0
PROPIETARIO	
Departamento de Informática	ENERO -24

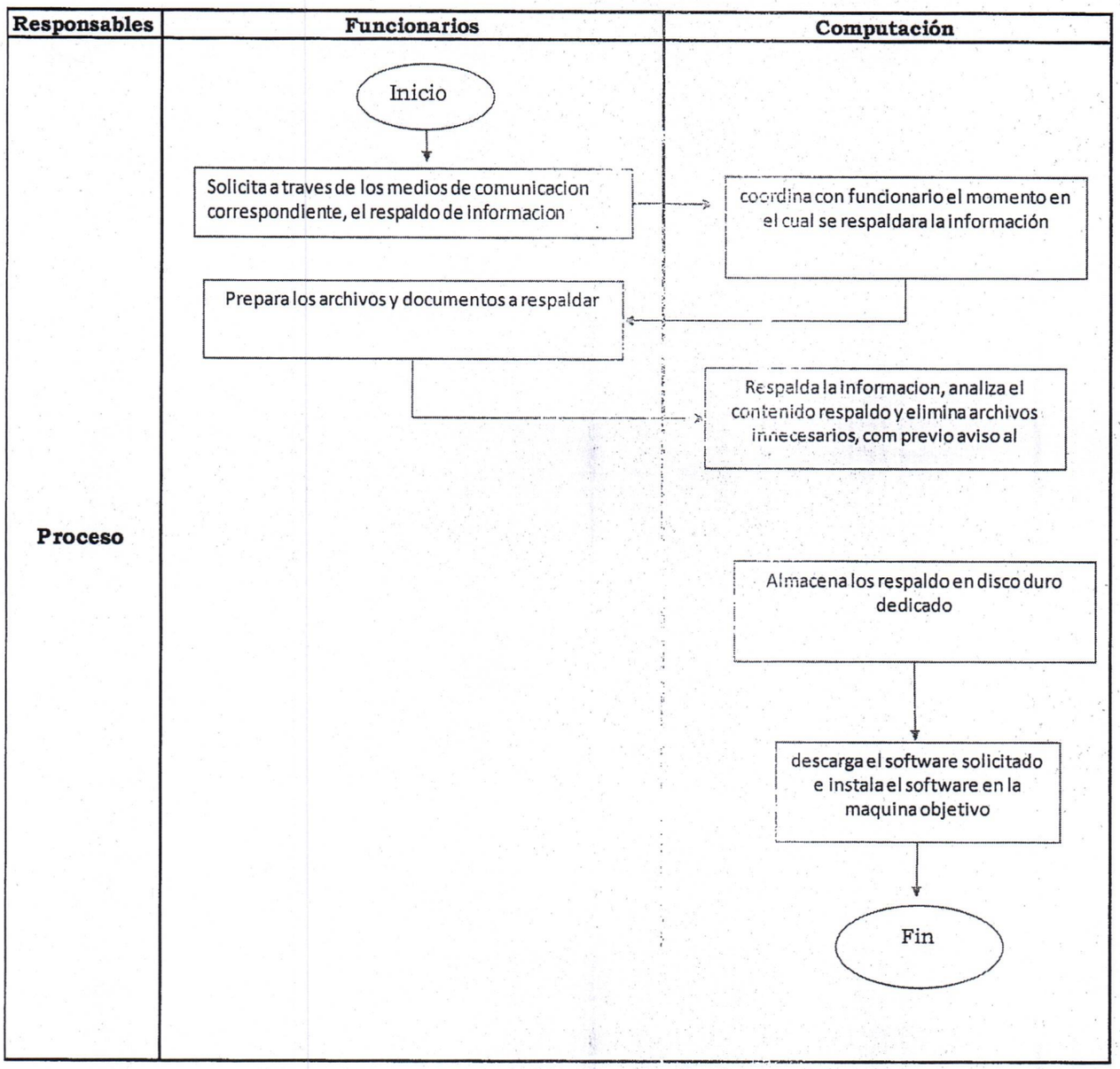
Notas	El software debe de ser aprobado previo a su instalación por el departamento de informática, si no cumple con las condiciones necesarias o bien presenta un riesgo para la seguridad informática del municipio, se denega el acceso. La solicitud del funcionario referente a software debe de contener un motivo, ese motivo es fundamental que contenga detalles que permitan conocer si el software a instalar cumple con las funciones municipales que se le confiere al funcionario.

PROCESO	VERSION
Manual de procedimiento de soporte	1.0
PROPIETARIO	
Departamento de Informática	ENERO -24

	de las capacidades del HDD del servidor, en promedio este HDD puede almacenar 7 días de respaldos. El Respaldo de las bases de datos históricas del servidor se hará de forma mensual y ese medio de almacenamiento a la cual recaerá esa información se encontrará protegido en una caja fuerte. El respaldo al funcionario, es cuando solicite que se le respalde la información en casos que le estime conveniente.

PROCESO	VERSION
Manual de procedimiento de soporte	1.0
PROPIETARIO	
Departamento de Informática	ENERO -24

DIAGRAMA DE FLUJO



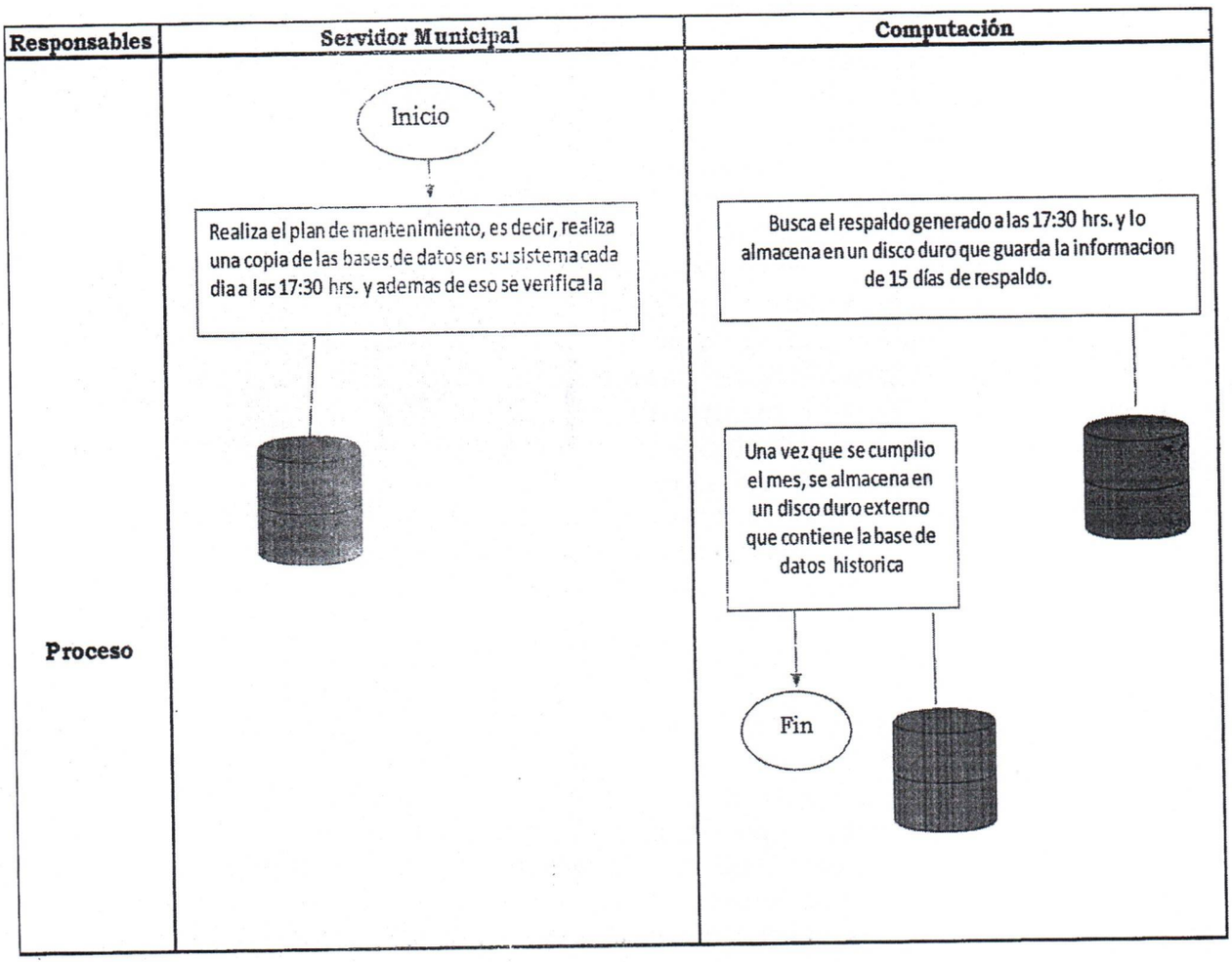
Notas	El respaldo de la información de un funcionario contempla los archivos y documentos relevantes para la Municipalidad, es decir, si se detectan archivos que no cumplen con este requisito, el departamento de informática se reserva el derecho de eliminar estos archivos. Los archivos que no son relevantes para el proceso de respaldo son: • Música (formatos mp3, wma, acc, entre otros). Imágenes que no tienen relevancia con el municipio (imágenes personales del funcionario).

RESPALDO A BASE DE DATO DEL SERVIDOR	
Nombre	Respaldo a base de dato del servidor
Alcance y aplicación	Computación
Descripción	Resguardar los datos de los sistemas municipales, para evitar cualquier pérdida ante cualquier imprevisto, físico o ataques informáticos, entre otros riesgos. Se respaldan las bases de datos de los sistemas CAS-CHILE en 3 niveles.
Normativa	Punto 8.7.1. Selección de Respaldos Se establecerá un procedimiento especial para las bases de datos de los servidores, asimismo se realizarán respaldos a los archivos que solicite el Propietario de la Información, también se llevará un registro de los respaldos históricos de base de datos. Se ha definido que los respaldos de la información se harán en estos casos: 1. Respaldos a la Base de Datos Municipal. 2.Respaldos al funcionario en caso de que se realice un cambio de equipo por reparación o mantenimiento. 3.Respaldos en caso de que un funcionario lo solicite. Bajo este estamento, se respaldarán en un disco duro externo definido por el Área de Computación, también se indica que no se respaldan archivos de música (*.mp3 y similares) y archivos de video que no estén relacionados con las funciones municipales. 8.7.2. Periodicidad de Respaldos Se hará un respaldo diario en un disco duro externo, la cual se realizará a las 18:00 hrs. de cada jornada laboral, y este disco duro externo se almacenará fuera de las dependencias del municipio cuando no se esté cursando la jornada laboral. También se genera un respaldo en el servidor, de acuerdo al plan de mantenimiento programado por el servidor SQL, este respaldo estará almacenando varios días dependiendo de las capacidades del HDD del servidor, en promedio este HDD puede almacenar 7 días de respaldos. El Respaldo de las bases de datos históricas del servidor se hará de forma mensual y ese medio de almacenamiento a la cual recaerá esa información se encontrará protegido en una caja fuerte. El respaldo al funcionario, es cuando solicite

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

	que se le respalde la información en casos que le estime conveniente.

DIAGRAMA DE FLUJO

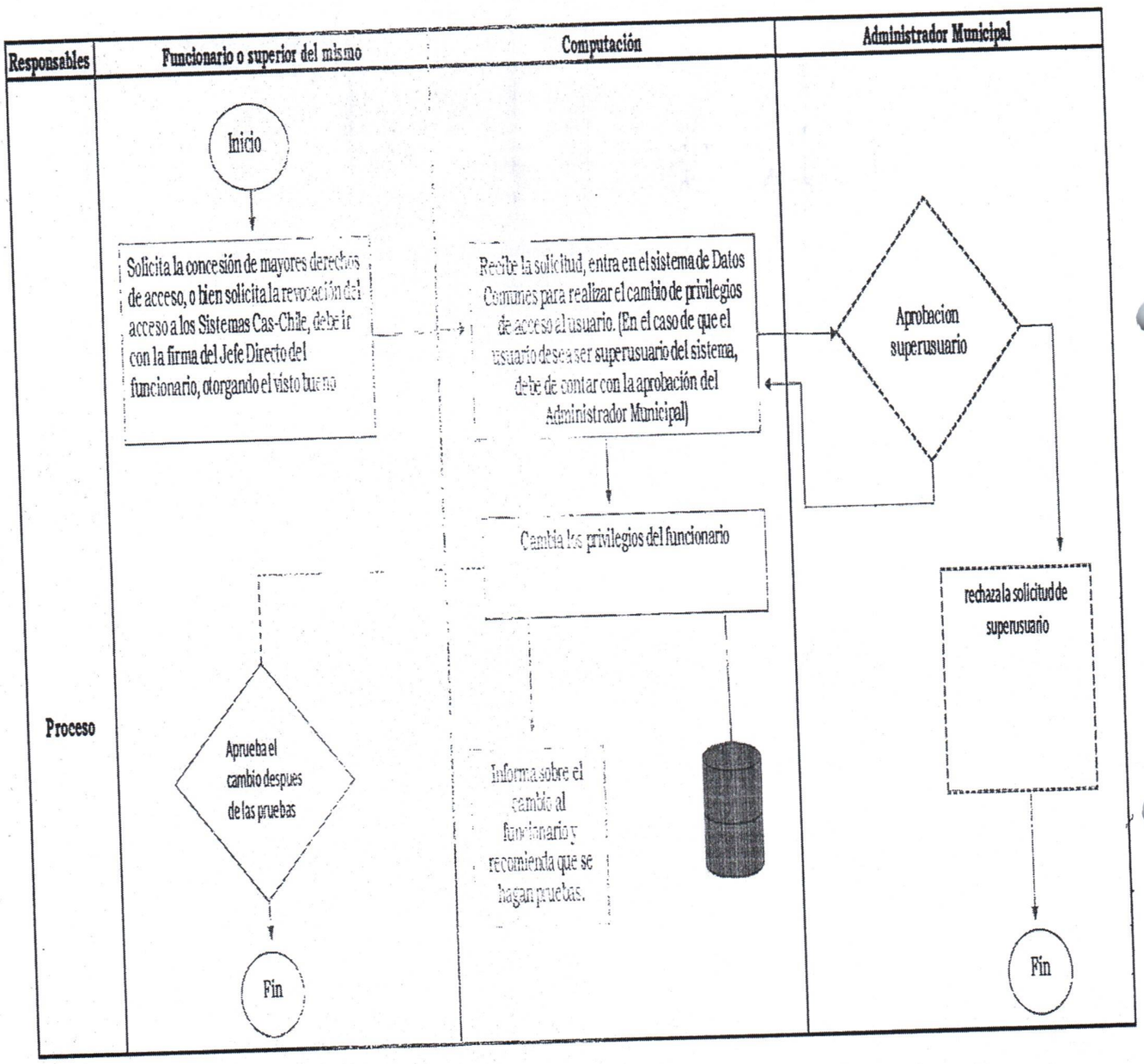


Notas	El respaldo de la información del servidor de las bases de datos, contempla 3 fases de respaldo: 1. Respalda la información diaria en el servidor (La capacidad varía por el tamaño del disco duro del servidor, en promedio puede guardar hasta 10 días de respaldos). 2. Se respalda la información diaria en un disco duro externo, la cual es trasladado fuera de la municipalidad una vez terminado el respaldo. 3. Respaldo de la información histórica, que contempla todos los meses de respaldos a la base de datos, este respaldo es cada mes. Antes de realizar el plan de mantenimiento, se ejecuta una verificación de integridad, y una vez que la base de datos sea compatible en un 80%, se ejecuta el plan de mantenimiento a la base de datos, que incluye estos respaldos

Modificación de derechos de acceso a Sistemas de Información	
Nombre	Modificación de derechos de acceso a sistema de Información
Alcance y aplicación	Funcionario que utiliza los sistemas de CAS-CHILE
Descripción	Este procedimiento tiene como objetivo modificar los derechos de acceso a los sistemas de Cas-Chile, para que el funcionario que los solicite tenga o mayor nivel de acceso para modificar parámetros que antes no tenía, o para revocar accesos en caso de que un jefe directo de él lo solicite o por la cuenta propia del funcionario.
Normativa	Punto 9.1.1. Registración de Usuarios El Encargado de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, dependiendo de las necesidades a la cual se le concesione un acceso a un nuevo funcionario, además de tener claro cuales sistemas ocupaba un funcionario que es dado de baja. Punto 9.1.2. Administración de Privilegios Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Punto 9.1.3. Administración de Contraseñas de Usuario La asignación de contraseñas se realizará bajo ciertos patrones definidos por el Área de Computación.

	Punto 9.1.4. Administración de Contraseñas Críticas Existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Encargado de Seguridad de la Información definirá procedimientos para la administración de dichas contraseñas críticas. Punto 9.1.5. Revisión de Derechos de Acceso de Usuarios A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Encargado de Computación de que se trate, llevará a cabo un proceso formal, a intervalos regulares de no más a 6 meses, a fin de revisar los derechos de acceso de los usuarios.

ORGANIGRAMA DE FLUJO



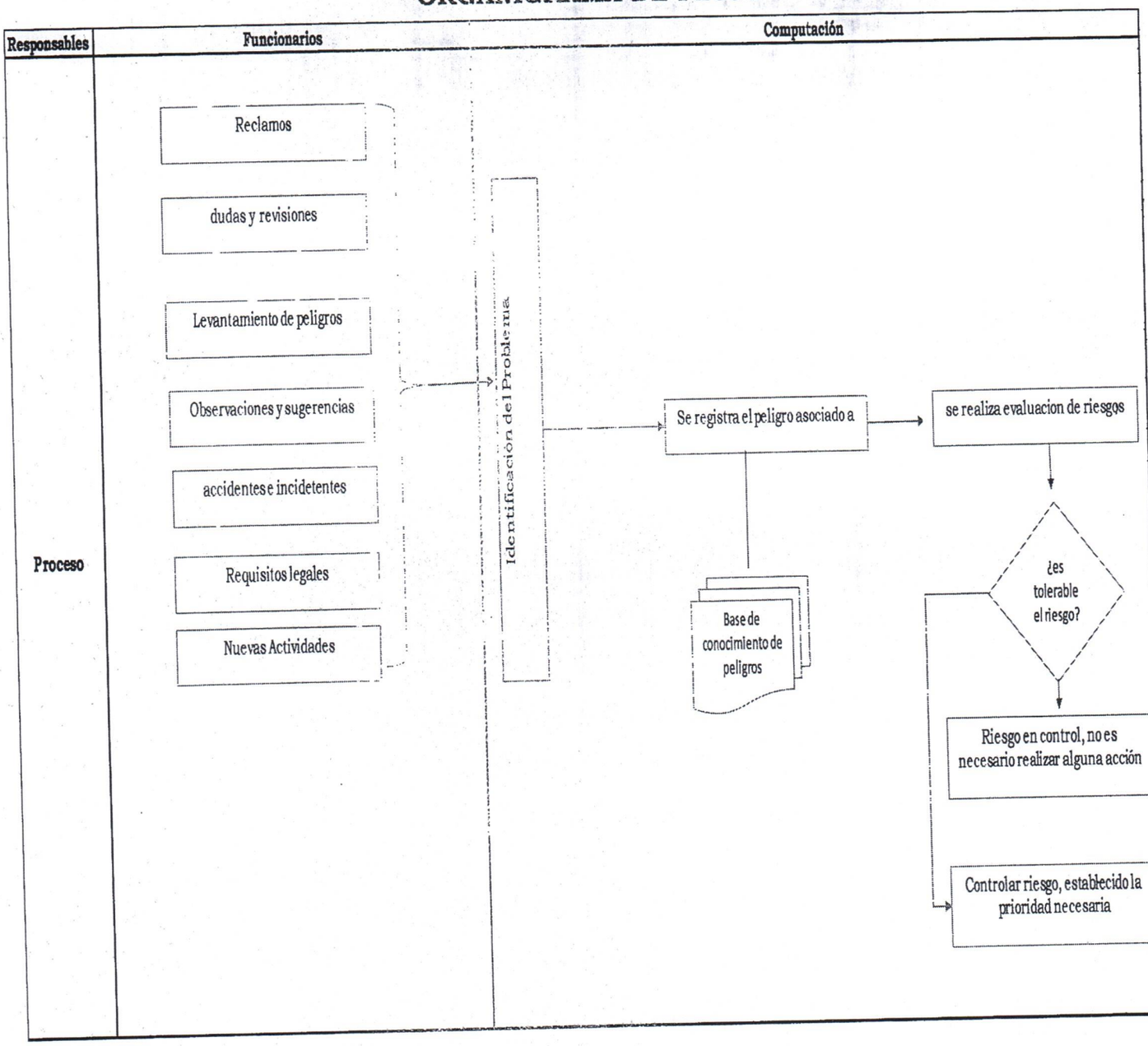
Notas	El funcionario, para determinadas actividades específicas requerirá el cambio de privilegios de alguno de los sistemas de CAS-CHILE para modificar algunos aspectos adicionales a los que ya tiene en su poder. Sólo si el funcionario desea tener en su poder una cuenta de superusuario de los Sistemas, debe de contar con la firma del Administrador Municipal. Una vez que tenga la firma, se procede al cambio de privilegios a superusuario. Después del proceso de cambio, si el usuario aún no puede hacer su trabajo, se modifican de nuevo los niveles de derechos de acceso.

PROCEDIMIENTO DE IDENTIFICACION DE PELIGROS Y EVALUACION DE RIESGOS.	
Nombre	Procedimiento de Identificación de Peligros y Evaluación de Riesgos
Alcance y aplicación	Todos los Funcionarios Municipales.
Descripción	Este procedimiento tiene como objetivo recabar y realizar análisis con el fin de determinar causas de riesgo a los sistemas informáticos y a si información que contienen, además de eso registra en una base de conocimientos sobre futuros incidentes similares.
Normativa	Punto 6.3.1. Comunicación de Incidentes Relativos a la Seguridad Los incidentes relativos a la seguridad serán comunicados a través de canales apropiados tan pronto como sea posible. Se establecerá un procedimiento de comunicación y de respuesta a incidentes, indicando la acción que debe de emprenderse al recibir un informe sobre incidentes. Dicho procedimiento deberá contemplar que, ante la detección de un supuesto incidente o violación de la seguridad, el Encargado de Seguridad de la Información sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Punto 6.3.2. Comunicación de Debilidades en Materia de Seguridad Los funcionarios que posean equipos informáticos municipales, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Encargado de Seguridad de la Información. Punto 6.3.3. Comunicación de Anomalías del Software Se establecerá un procedimiento para la comunicación de anomalías de software, los cuales deberán contemplar: A. Registrar los síntomas del problema y los mensajes que aparecen en pantalla. B. Establecer las medidas de aplicación inmediata ante la presencia de una anomalía. C. Alertar inmediatamente al Encargado de Seguridad de la Información referente al activo comprometido al cual se presenta la anomalía. Punto 6.3.4. Aprendiendo de los Incidentes Se definirá un procedimiento que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para responder rápidamente ante incidentes recurrentes y a su vez establecer un registro estadístico de cómo actuar,

	identificar más rápidamente las causas de la anomalía y tener identificada la información, los costos asociados a ello y los métodos de recuperación, así como sus soluciones.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

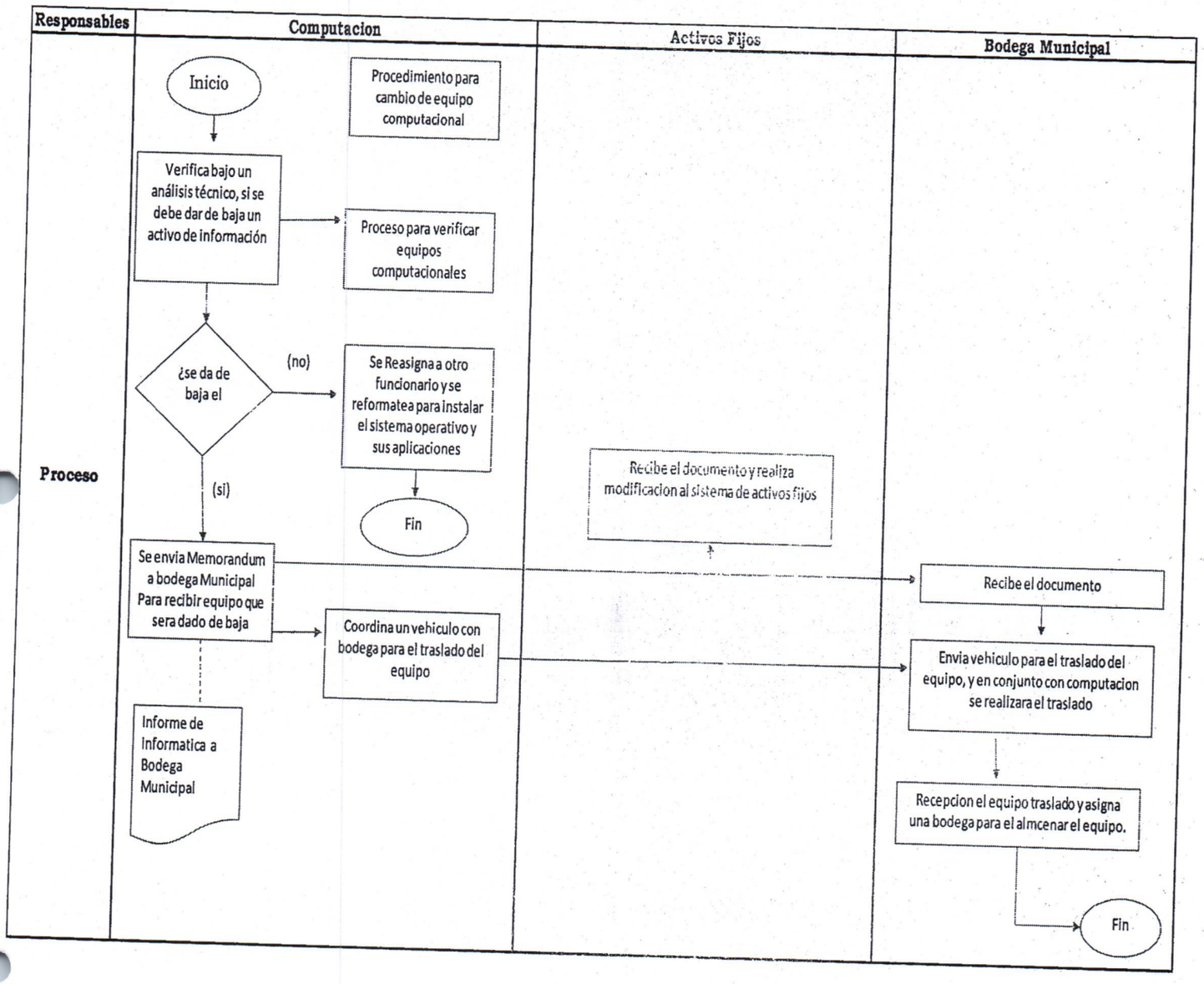
ORGANIGRAMA DE FLUJO



Notas	La identificación de un riesgo pasa por observaciones o actividades que realizan los funcionarios municipales, en este contexto, si el funcionario percibe que su información está siendo comprometida, da aviso a Computación. Ellos identifican el problema y bajo una matriz de riesgos, evalúan si es un riesgo potencial o no ofrece riesgo la actividad en cuestión.

DAR DE BAJA A ACTIVOS FIJOS QUE CONTIENEN INFORMACIÓN.	
Nombre	Dar de Baja a Activos Fijos que contienen información
Alcance y aplicación	Equipos Informáticos Municipales que contengan información. Funcionarios Municipales que requieren un cambio de equipo, dada las necesidades de la administración.
Descripción	Este procedimiento tiene como objetivo explicar el proceso necesario para desatender equipos informáticos, y con ello dar de baja el activo fijo físico informático, a su vez explica el proceso de traslado desde las dependencias municipales a la Bodega Municipal.
Normativa	Punto 5.4. Desatención de Equipos Informáticos Todo equipo computacional que no sea validado por el área de Computación (en cuanto a características técnicas se refiere), será dado de baja y desatendido, previo a eso se realizará un respaldo para asegurar los datos. Todos los equipos desatendidos deben de ser transferidos a la Bodega Municipal, para su almacenaje, así como también, se debe de dar el aviso a la Dirección de Administración y Finanzas, para que realice el cambio en el Activo Fijo Municipal

ORGANIGRAMA DE FLUJO



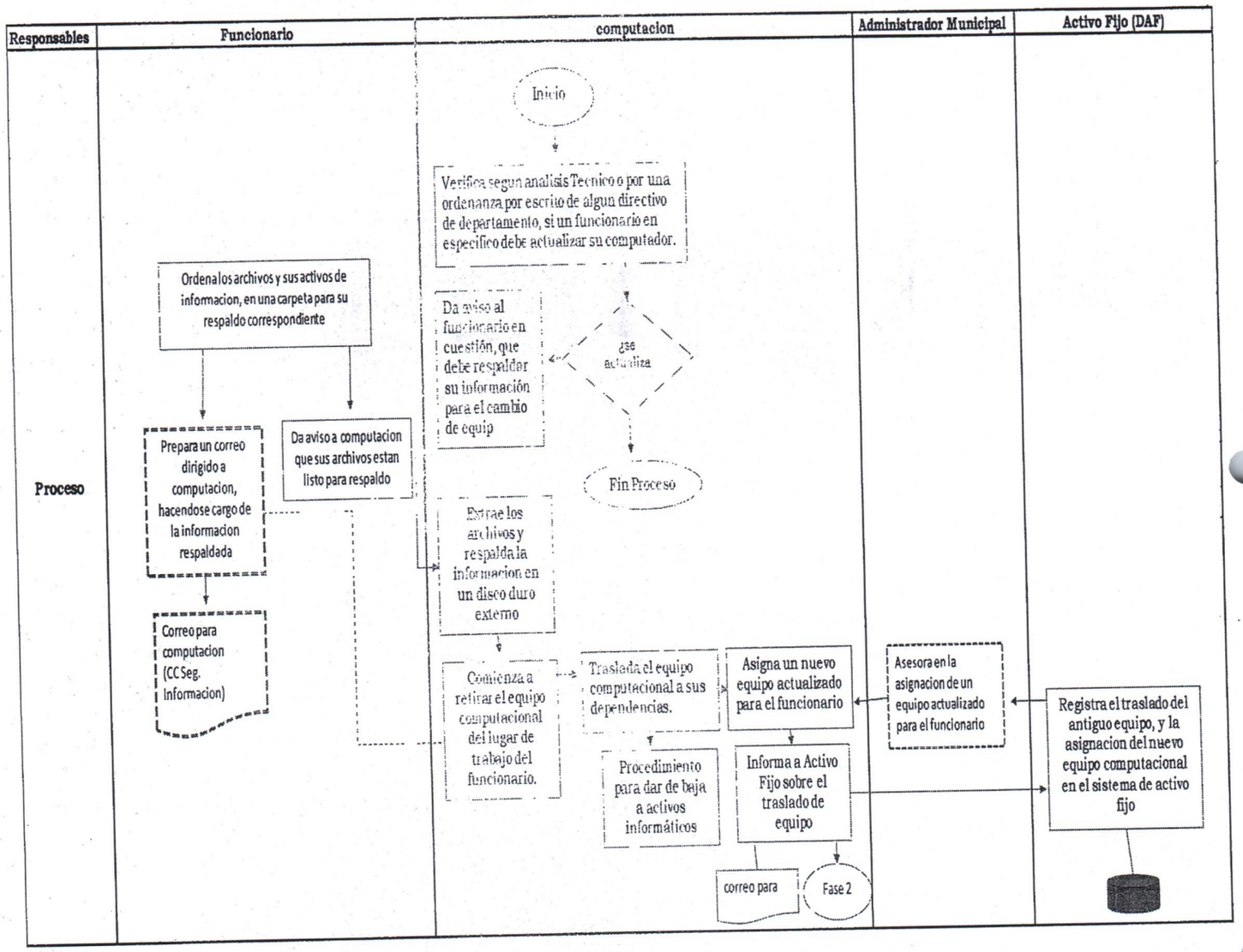
I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

PROCESO	VERSION
Manual de procedimiento de soporte	1.0
PROPIETARIO	
Departamento de Informática	ENERO -24

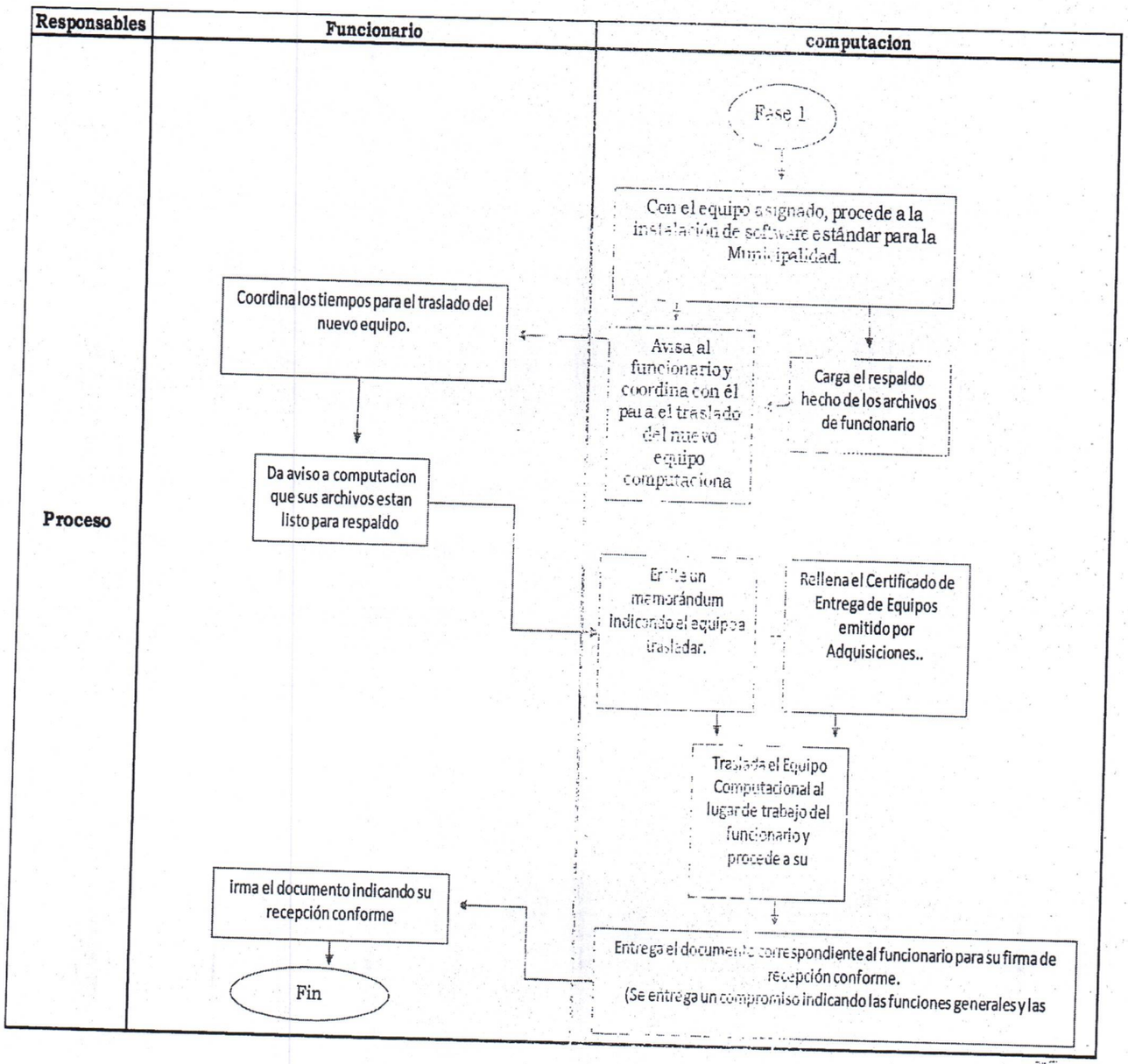
Notas	Antes de dar de baja el equipo computacional, se realiza un procedimiento, la cual contempla el cambio de equipo de un funcionario. Acto siguiente, se verifica a través de un proceso aparte, que el equipo no esté desactualizado a tal punto de que necesita ser desatendido. Una vez que el equipo no es válido para seguir en funcionamiento, se anotan los siguientes datos: • Tipo • Marca • Modelo • Número de Serie. Esos datos van contenidos en un memorándum enviado al Encargado de la Bodega Municipal, con copia a Activo Fijo, o en su defecto al Director de Administración y Finanzas. Una vez que ya se envió el documento, pueden ocurrir dos situaciones: • Que el Área de Computación coordine el vehículo para el traslado. • Que Bodega Municipal envíe el vehículo para el traslado. Se realiza el traslado y Bodega asigna una de sus plazas para almacenar el equipo

CAMBIO O ACTUALIZACIÓN DE EQUIPO COMPUTACIONAL	
Nombre	Procedimiento para Cambio o Actualización de Equipo Computacional
Alcance y aplicación	Equipos informáticos de funcionarios municipales que necesitan de una actualización de Hardware.
Descripción	Este procedimiento abarca la necesidad de que el funcionario cuente siempre con el equipo computacional actualizado y le permita realizar sus labores, además de brindar mayor seguridad a la información ante imprevistos. Se explica el proceso de cambio de equipo computacional, basándose bajo un análisis previo (que puede ser a simple vista del Área de Computación o por ordenanza escrita, con la consecuencia de que el cambio sea forzado), incluyendo los respaldos de datos de los funcionarios y la posibilidad de dar de baja un equipo la cual está ya desactualizado y no puede seguir las tendencias actuales
Normativa	Punto 5.5. Cambio o Actualización de Equipo Computacional Se explica el proceso de cambio de equipo computacional, basándose bajo un análisis previo (que puede ser a simple vista del Área de Computación o por ordenanza escrita, con la consecuencia de que el cambio sea forzado), incluyendo los respaldos de datos de los funcionarios y la posibilidad de dar de baja un equipo la cual está ya desactualizado y no puede seguir las tendencias actuales. Los respaldos de la información del funcionario tienen dos casos: • Computación realiza el respaldo. • El funcionario realiza el respaldo (debe de declarar por escrito que la información que respalde está bajo su responsabilidad). Una vez retirado el equipo computacional, el Administrador Municipal puede asesorar a Computación sobre qué equipo puede entregar al nuevo funcionario, este asesoramiento es opcional, siempre y cuando el nuevo equipo computacional sea bajo ordenanza del Administrador Municipal o que la ordenanza escrita del directivo del área correspondiente al funcionario contenga la firma del Administrador Municipal. Dentro de este mismo círculo del proceso, se puede verificar que el activo puede ser dado de baja o no, gatillando un nuevo procedimiento. El certificado de entrega de equipos computacionales, pueden ser 2 opciones: • A través de un memorándum indicando especificaciones mínimas del equipo computacional a entregar, tales como marca, modelo y número de serie. • A través de un certificado emitido por adquisiciones, indicando los mismos datos. Una vez instalado el equipo computacional, se da aviso al funcionario, indicando las responsabilidades del equipo computacional entregado, así como sus responsabilidades y funciones.

ORGANIGRAMA DE FLUJO



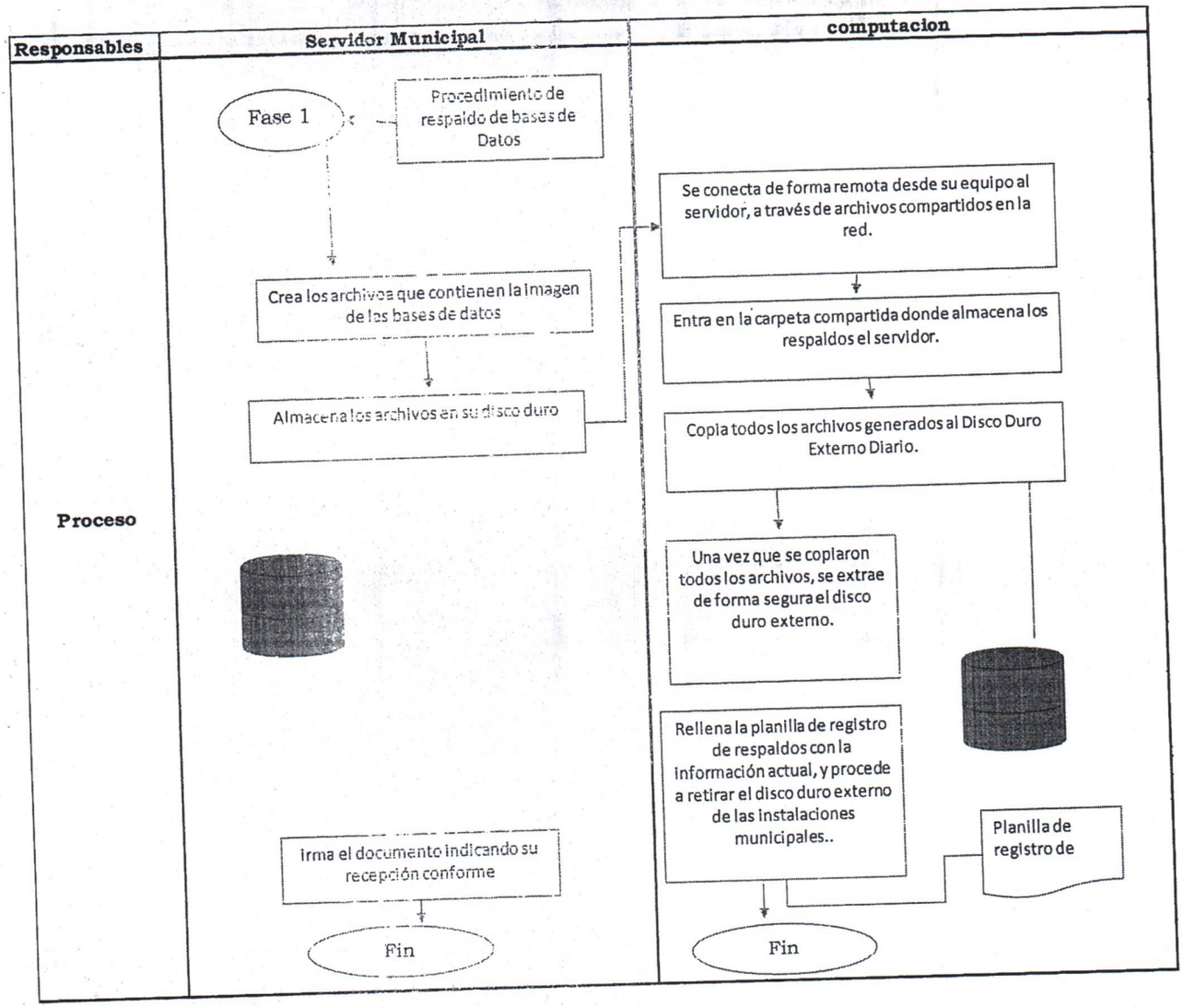
ORGANIGRAMA DE FLUJO (FASE 2)



Notas	Se verifica bajo un análisis técnico a simple vista del Área de Computación si se necesita una actualización del equipo, también este procedimiento puede ser gatillado por una ordenanza escrita de un directivo de la Municipalidad. Los respaldos de la información del funcionario tienen dos casos: • Computación realiza el respaldo. • El funcionario realiza el respaldo (debe de declarar por escrito que la información que respalde está bajo su responsabilidad). Una vez retirado el equipo computacional, el Administrador Municipal puede asesorar a Computación sobre qué equipo puede entregar al nuevo funcionario, este asesoramiento es opcional, siempre y cuando el nuevo equipo computacional sea bajo ordenanza del Administrador Municipal o que la ordenanza escrita del directivo del área correspondiente al funcionario contenga la firma del Administrador Municipal. Dentro de este mismo círculo del proceso, se puede verificar que el activo puede ser dado de baja o no, gatillando un nuevo procedimiento. El certificado de entrega de equipos computacionales, pueden ser 2 opciones: • A través de un memorándum indicando especificaciones mínimas del equipo computacional a entregar, tales como marca, modelo y número de serie. • A través de un certificado emitido por adquisiciones, indicando los mismos datos. Una vez instalado el equipo computacional, se da aviso al funcionario, indicando las responsabilidades del equipo computacional entregado, así como sus responsabilidades y funciones.

RESPALDO DIARIO A LAS BASES DE DATOS DEL SERVIDOR	
Nombre	Respaldo diario a las bases de datos del servidor
Alcance y aplicación	Servidor Municipal, el que ejecuta el plan de mantenimiento para almacenar todos los respaldos de sus bases de datos. Computación, quien administra los respaldos en discos duros externos.
Descripción	Este procedimiento cumple la función de describir y exponer los pasos a seguir para el tratamiento y aseguración de las bases de datos del servidor, de forma diaria y después del horario laboral.
Normativa	Punto 8.7.1. Selección de Respaldos Se establecerá un procedimiento especial para las bases de datos de los servidores, asimismo se realizarán respaldos a los archivos que solicite el Propietario de la Información, también se llevará un registro de los respaldos históricos de base de datos. Se ha definido que los respaldos de la información se harán en estos casos: 1. Respaldos a la Base de Datos Municipal. 2. Respaldos al funcionario en caso de que se realice un cambio de equipo por reparación o mantenimiento. 3. Respaldos en caso de que un funcionario lo solicite. Bajo este estamento, se respaldarán en un disco duro externo definido por el Área de Computación, también se indica que no se respaldan archivos de música (*.mp3 y similares) y archivos de video que no estén relacionados con las funciones municipales. 8.7.2. Periodicidad de Respaldos Se hará un respaldo diario en un disco duro externo, la cual se realizará a las 18:30 hrs. de cada jornada laboral, y este disco duro externo se almacenará fuera de las dependencias del municipio cuando no se esté cursando la jornada laboral. También se genera un respaldo en el servidor, de acuerdo al plan de mantenimiento programado por el servidor SQL, este respaldo estará almacenando varios días dependiendo de las capacidades del HDD del servidor, en promedio este HDD puede almacenar 7 días de respaldos. El Respaldo de las bases de datos históricas del servidor se hará de forma mensual y ese medio de almacenamiento a la cual recaerá esa información se encontrará protegido en una caja fuerte. El respaldo al funcionario, es cuando solicite que se le respalde la información en casos que le estime conveniente.

ORGANIGRAMA DE FLUJO

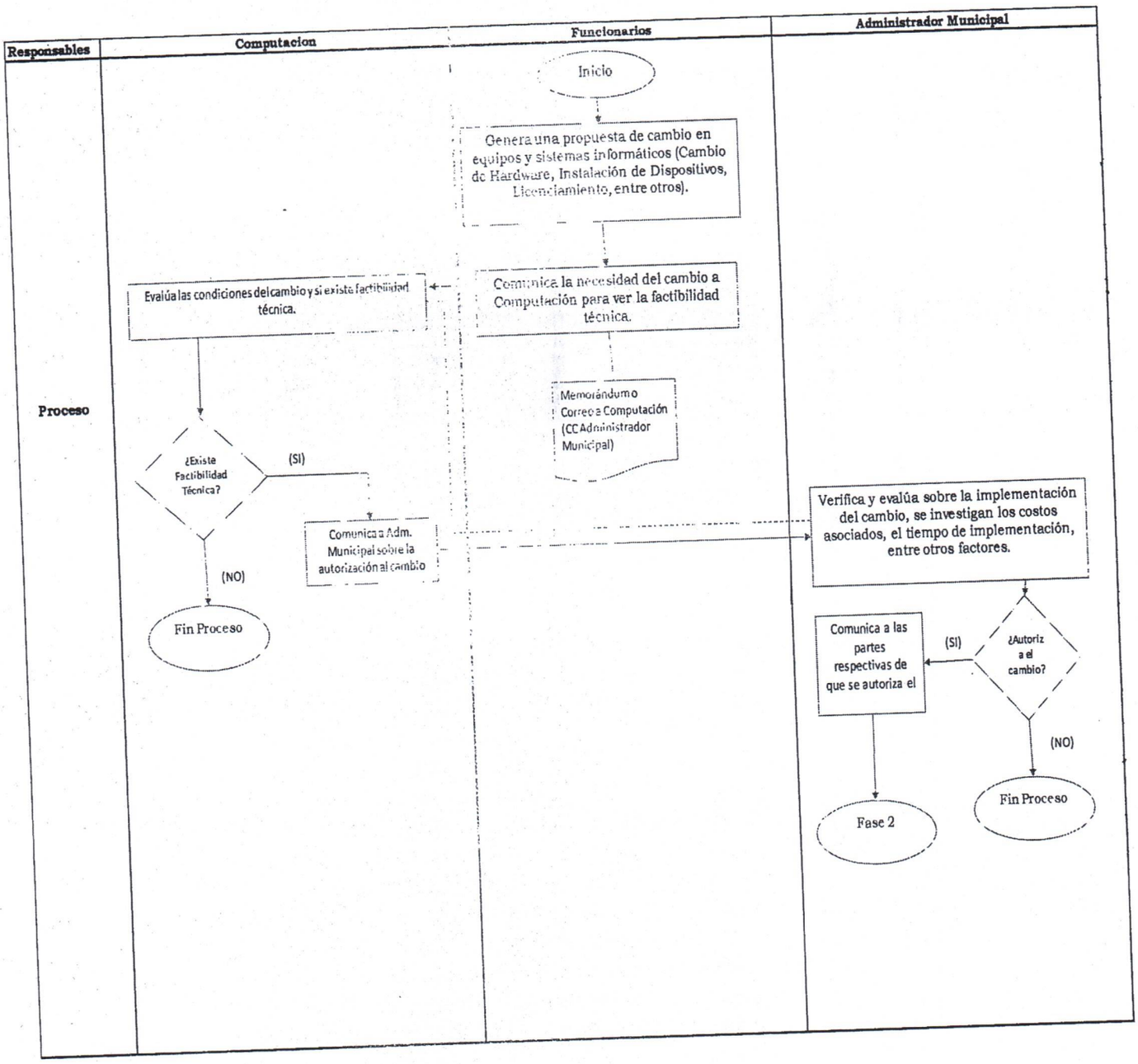


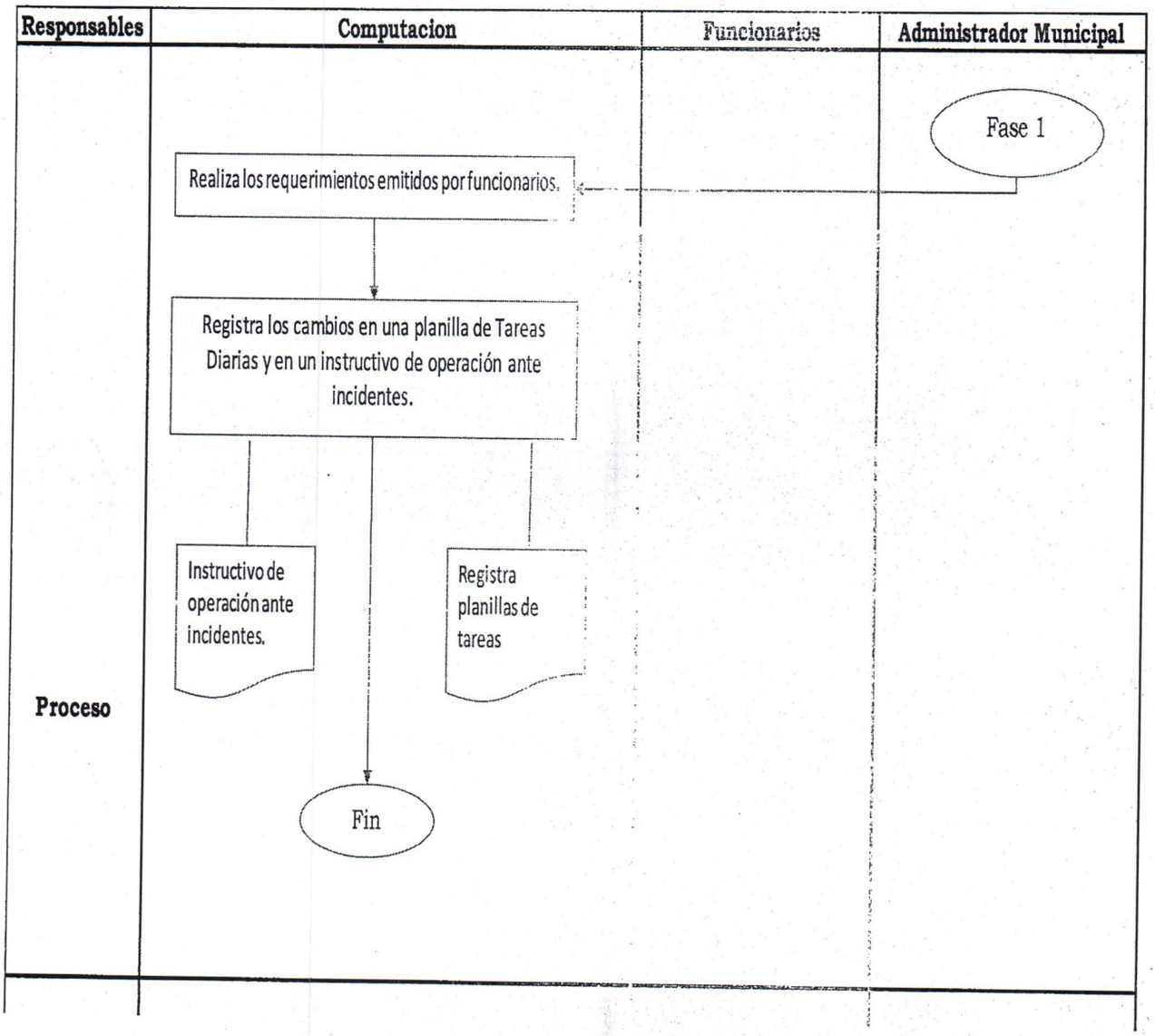
Notas	El servidor municipal realiza estos respaldos a las 18:00 hrs, cuando el plan de mantenimiento del servidor se cumple en un 80%. Se copian estos archivos generados por el servidor en un disco duro externo. Una vez que termina el respaldo diario, se registra en la planilla de registro de respaldos y se procede al retiro del disco duro de las instalaciones municipales, para resguardos ante cualquier incidente (ya sea de forma natural, intencional o humana).

Notas	Este tipo de respaldo se hace de forma mensual, guardando los 3 últimos días de cada mes, en un archivo comprimido para ahorrar espacio y guardado con un código que es: • (número de mes)bkp_(mes)(año).rar Después de la copia, el disco duro externo se ingresa a una caja fuerte que está ubicada en el área de Computación. Luego se registra en la planilla de registro de respaldos la operación realizada.

GESTIÓN RELACIONADA AL CONTROL DE CAMBIOS DE SISTEMAS INFORMÁTICOS.	
Nombre	Gestión relacionada al Control de Cambios de Sistemas Informáticos.
Alcance y aplicación	Todos los Sistemas informáticos que son sujetos a evaluación de cambios. Todos los funcionarios municipales que estén involucrados en un proceso de cambio ordenada por la Dirección Municipal.
Descripción	Este procedimiento es de carácter adaptable y tiene como objetivo, establecer un estándar en la gestión de Cambios en Equipos y Sistemas Informáticos, llevar un control del antes y después de la modificación asignada a los equipos, registrar las posibles fallas que se adquieran durante el proceso de cambio, integrar una base de conocimientos incluyendo lo antes mencionado, para una rápida respuesta ante incidentes dentro del proceso.
Normativa	Punto 8.1.1. Control de Cambios en las Operaciones Se definirá un procedimiento para el control de los cambios en el ambiente operativo, programas licenciados y sistemas municipales. Todo cambio a los sistemas debe de ser registrado según: • Tipo del cambio (menor, mayor). • Que recursos afecta. • Versión. • Compatibilidad con otros programas, entre otros aspectos específicos. El Encargado de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Encargado de Computación evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación. Punto 8.1.2. Procedimientos de Manejo de Incidentes Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a resguardar la información, además se documentarán todos los incidentes que sean pertinentes, para su rápida respuesta y coordinación posterior, además de llevar un registro estadístico indicando cuáles son las fallas más comunes, los costos asociados a tiempo, y el conocimiento previo de esa situación. Punto 8.1.3. Separación de Funciones Se contemplará la separación de la gestión o ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas. En los casos en los que este método de control no se pudiera cumplirse, se implementarán controles tales como el monitoreo de las actividades y/o la elaboración de registros de auditoría y control periódico de los mismos.

ORGANIGRAMA DE FLUJO





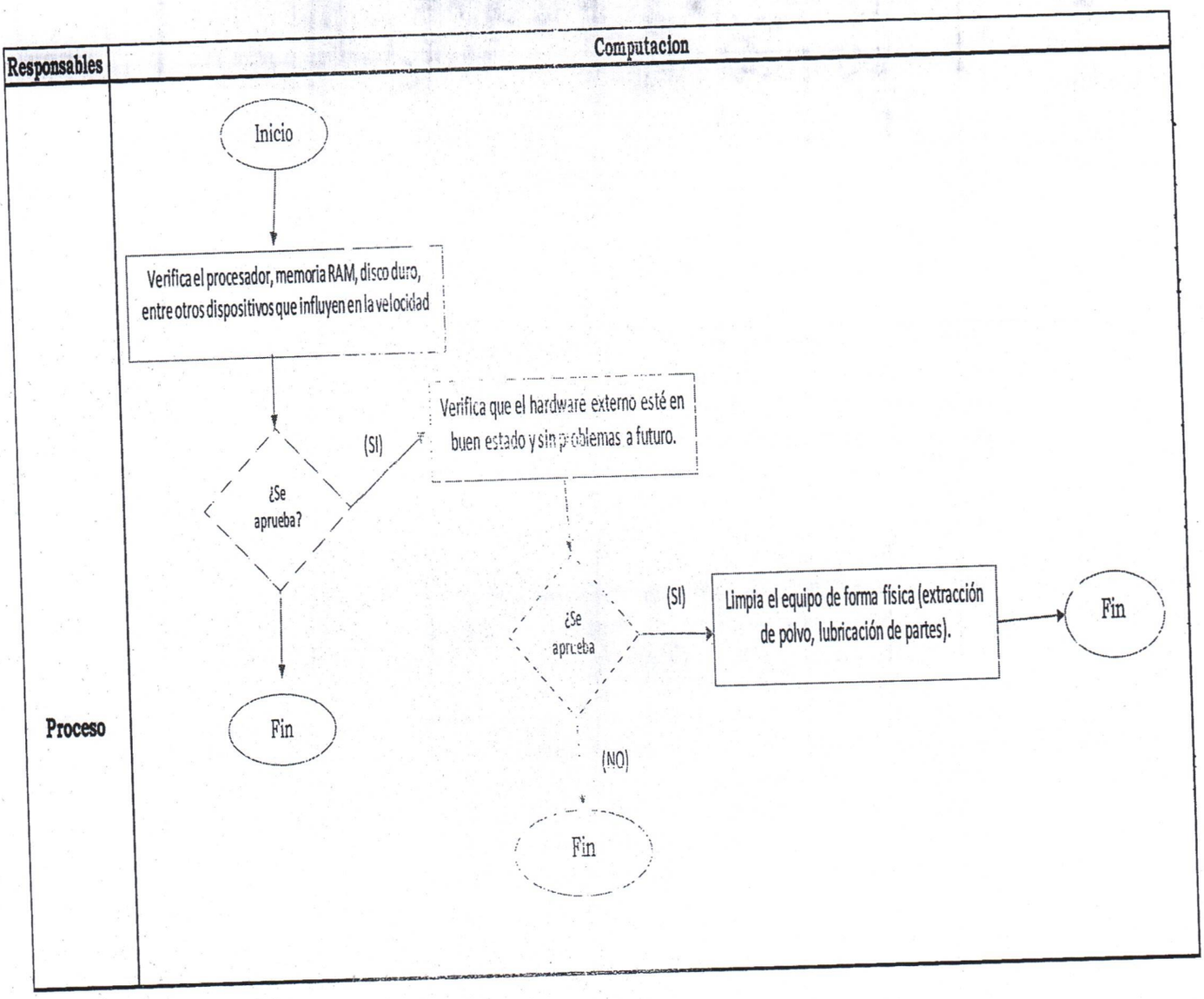
I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

Notas	Un Funcionario o el Administrador Municipal según sea el caso, puede enviar un requerimiento al Área de Computación indicando una propuesta de un cambio. Dentro de los Cambios que se generan en los sistemas informáticos se incluye lo siguiente: • Actualizaciones de Programas. • Adquirir Software Original. • Cambio o traslado de equipos. • Solicitudes de Acceso a Internet. • Respaldos de Información. • Entre otros cambios más. Estos cambios deben de ser aprobados por el Administrador Municipal, para que el Área de Computación reciba la orden de que implemente los cambios que sean necesarios. Estos cambios son a nivel de Computación, lo que son las demás materias, el Área de Computación no se hace responsable de ello. Una vez que los cambios han sido implementados, se registra en una planilla de Tareas Diarias que indica el cambio que se realizó y si está pendiente o solucionado. También en casos especiales, se realizarán instructivos sobre cómo afrontar casos más complicados y que llevan tiempo en arreglarse

VERIFICACIÓN TÉCNICA DE EQUIPO INFORMÁTICO	
Nombre	Verificación Técnica de Equipo Informático
Alcance y aplicación	Computadores que están incluidos en un proceso de cambio. Computación, quién verifica esos computadores.
Descripción	Este procedimiento cumple la función de exponer los detalles referentes a como se verifican los equipos para determinar si el equipo puede ser dado de baja o sigue en condiciones para funcionar correctamente.
Normativa	Punto 5.5. Cambio o Actualización de Equipo Computacional Se explica el proceso de cambio de equipo computacional, basándose bajo un análisis previo (que puede ser a simple vista del Área de Computación o por ordenanza escrita, con la consecuencia de que el cambio sea forzado), incluyendo los respaldos de datos de los funcionarios y la posibilidad de dar de baja un equipo la cual está ya desactualizado y no puede seguir las tendencias actuales. Los respaldos de la información del funcionario tienen dos casos: • Computación realiza el respaldo. • El funcionario realiza el respaldo (debe de declarar por escrito que la información que respalde está bajo su responsabilidad). Una vez retirado el equipo computacional, el Administrador Municipal puede asesorar a Computación sobre qué equipo puede entregar al nuevo funcionario, este asesoramiento es opcional, siempre y cuando el nuevo equipo computacional sea bajo ordenanza del Administrador Municipal o que la ordenanza escrita del directivo del área correspondiente al funcionario contenga la firma del Administrador Municipal. Dentro de este mismo círculo del proceso, se puede verificar que el activo puede ser dado de baja o no, gatillando un nuevo procedimiento. El certificado de entrega de equipos computacionales, pueden ser 2 opciones: • A través de un memorándum indicando especificaciones mínimas del equipo computacional a entregar, tales como marca, modelo y número de serie. • A través de un certificado emitido por adquisiciones, indicando los mismos datos. Una vez instalado el equipo computacional, se da aviso al funcionario, indicando las responsabilidades del equipo computacional entregado, así como sus responsabilidades y funciones.

PROCESO	VERSION
Manual de procedimiento de soporte	1.0
PROPIETARIO	
Departamento de Informática	ENERO -24

ORGANIGRAMA DE FLUJO



Notas	Comenzando el proceso, se verifica que el equipo cumpla con las exigencias de velocidad, investigando velocidades del procesador, cantidad de memoria RAM, espacio en disco duro. Luego se verifica la parte física del computador (Hardware). Después de que todo se encuentra aprobado para seguir funcionando, se da comienzo a la limpieza y posterior mantenimiento del equipo computacional.