MUNICIPALIDAD DE TIL TIL

SECRETARIA MUNICIPAL

SANCIONA MANUAL DE PROCEDIMIENTOS SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION.

TIL TIL, 12 JUN. 2017

DECRETO N° 769 **/2017**

LA ALCALDÍA DECRETO HOY:

VISTOS:

1. FACULTADES QUE ME CONFIERE LA LEY 18.695, ORGÁNICA CONSTITUCIONAL DE MUNICIPALIDADES,
2. LEY Nº 19.880, DE BASES GENERALES DE PROCEDIMIENTOS ADMINISTRATIVOS DE LA ADMINISTRACIÓN DEL ESTADO.
3. LEY Nº 18.575, DE BASES GENERALES DE LA ADMINISTRACION DEL ESTADO

CONSIDERANDO:

1. NECESIDAD DE CONTAR CON PROCEDIMIENTOS INTERNOS QUE PROTEJAN LA INFORMACION INSTITUCIONAL Y USO DE PLATAFORMAS DIGITALES
2. APROBACION DE MANUAL DE PROCEDIMIENTOS POR PARTE DEL HONORABLE CONCEJO MUNICIPAL
3. INSTRUCCION DE CONTRALORIA GENERAL DE LA REPUBLICA RESPECTO DE ESTABLECER PROCEDIMIENTOS CLAROS TENDIENTES A LA PROTECCION, BUEN USO Y SEGURIDAD DE LA INFORMACION INSTITUCIONAL Y BUEN USO DE LOS SISTEMAS INFORMATICOS

DECRETO :

1. SANCIONECE CON ESTA FECHA MANUAL DE PROCEDIMIENTOS Y DOCUMENTACION "SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACION DE LA ILUSTRE MUNICIPALIDAD DE TIL TIL.
2. SANCIONA PROCEDIMIENTO Y POLITICA DE USO DE LOS CORREOS ELECTRONICOS INSTITUCIONALES
3. PONGASE EN CONOCIMIENTO DE LOS FUNCIONARIOS DE LA ILUSTRE MUNICIPALIDAD DE TIL TIL LOS MANUALES REFERIDOS, CON EL FIN DE QUE TOMEN CONOCIMIENTO

ILUSTRE MUNICIPALIDAD DE TIL TIL SECRETARIA MUNICIPAL

I. MUNICIPALIDAD DE TIL TIL ALCALDE

CLAUDIA PARRA CISTERNAS
SECRETARIA MUNICIPAL

NELSON ORELLANA URZUA
ALCALDE

DISTRIBUCION:
- CONTROL
- FINANZAS
- SECPLAC
- COMPUTACION
- ARCHIVO SECMUN

Políticas de la Seguridad de la Información

Índice

1. Introducción

La información es un recurso importante, que tiene valor para los procesos que realiza diariamente la Ilustre Municipalidad de TilTil y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, la operación de los equipos computacionales, a su vez, minimizando los riesgos de daño y hurto de información, además de contribuir y facilitar la gestión administrativa de la Municipalidad.

Para que estos principios escritos en esta Política de Seguridad de la Información sean efectivos, es necesario que este documento forme parte de la cultura organizacional de la Municipalidad, lo que implica que debe contarse con el compromiso de todos los funcionarios municipales para contribuir con la difusión, conocimiento e integración.

Como consecuencia a lo expuesto previamente, la Ilustre Municipalidad de TilTil integró, en una de sus tareas esenciales, la creación e implementación de Políticas de Seguridad de la Información, basándose en las características de varias fuentes de documentación al respecto, además, esta política se apoya de un Manual de Procedimientos en la cual se describen los pasos a seguir para ejecutar los lineamientos de esta política.

2. Palabras Claves y Definiciones

Esta sección describe todos los términos y definiciones que se usarán a lo largo de este documento por la cual tiene como objetivo facilitar la comprensión de este documento.

2.1. Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

- Confidencialidad: que la información se accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente se deberían considerar parte de esta preservación, los siguientes conceptos:

- Autenticidad: asegura la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- Duplicidad: consiste en asegurar que un traspaso de información se realice sólo una vez, a menos que se especifique lo contrario. Impide las múltiples copias que permiten que se duplique innecesariamente la información.
- Legalidad: referido a que la información se ajuste al marco de leyes, normas, reglamentaciones o disposiciones a las que está sujeto el municipio.
- Confiabilidad: que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

2.2. Información

Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, entre otras fuentes.

2.3. Sistema de Información

Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

2.4. Tecnologías de la Información y Comunicación (TIC)

Se refiere al hardware y software operados por los funcionarios públicos de esta organización, para llevar a cabo una función propia de la Municipalidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.5. Conceptos Técnicos

Wi-Fi: Wireless Fidelity, “Fidelidad Inalámbrica”, es un mecanismo a la cual dispositivos tecnológicos pueden conectarse a internet sin necesidad de algún cable, a eso se le llama internet inalámbrico.

Time Out: Periodos de tiempo en que la red se encuentra caída y no establece conexión a internet.

Hosting: es un sistema que almacena información, imágenes, vídeo, o cualquier contenido a través de internet y permite mostrar todo ese contenido vía páginas web (asociando este hosting a un “dominio”).

Dominio web: La parte principal de una dirección en la Web que indica la organización o compañía que administra dicha página o sitio web, básicamente es el identificador para acceder a dicha página web.

Sniffing: Proceso mediante el cual los datos que se trasmiten dentro de una red, son capturados o monitoreados por terceras personas.

Spoofing: en términos de seguridad de redes hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

Spyware: Software malicioso cuya función es monitorear las acciones del usuario de un computador y reportar estas acciones a un tercero, sin el consentimiento del propietario del computador o del usuario legítimo.

Adware: Cualquier paquete de software que automáticamente reproduce, muestra o descarga material publicitario en un computador después de que se instala un programa que contiene el material previamente mencionado.

Plug-in: Programa computacional que interactúa con una aplicación principal, a modo de ejemplo, un cliente de email o un browser, para proveer una función cuando sea demandada.

Rack: es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de distintos fabricantes. También son llamados bastidores, cabinas, gabinetes o armarios.

3. Políticas de Seguridad de la Información

3.1. Objetivos generales

A. Proteger los recursos de información de la Municipalidad y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los conceptos de confidencialidad, integridad y disponibilidad, partes claves de la seguridad de la información y la protección de datos.
B. Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
C. Mantener la Política de Seguridad del Municipio actualizado, para asegurar su vigencia y nivel de eficacia ante nuevas amenazas.

3.2. Sanciones por incumplimiento de la política

El incumplimiento de las disposiciones establecidas por las Políticas de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido como, por ejemplo, una sanción sería impartir un sumario administrativo y con ello, estableciendo las investigaciones necesarias para el o los casos que se observen.

4. Organización de la Seguridad

Son sus objetivos:

A. Administrar la seguridad de la información dentro del Municipio y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.
B. Fomentar la consulta y cooperación con otros Municipios especializados para la obtención de asesoría en materia de seguridad de la información.
C. Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros o de personal externo a la información de la Municipalidad.

4.1. Infraestructura de la Seguridad de la Información

4.1.1. Asignación de Responsabilidades

El Administrador Municipal de la Ilustre Municipalidad de TilTil asignó, en materia de Seguridad de la Información a Aníbal Alejandro Ramos González, nominado con el cargo de "Encargado de Seguridad de la Información", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Municipio, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política.

El Encargado de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades que surjan de los procesos de seguridad que se detallan a continuación:

a) Seguridad del Personal.
b) Seguridad Física y Ambiental.
c) Seguridad en las Comunicaciones y las Operaciones.
d) Control de Accesos.
e) Seguridad en el Desarrollo y Mantenimiento de Sistemas.
f) Planificación de la Continuidad Operativa.

Así mismo, el Encargado de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades de los propietarios de la información que correspondan, a su vez quienes serán los responsables de los departamentos a cargo del manejo de la misma.

4.1.2. Asesoramiento en Materia de Seguridad de la Información

El Encargado de Seguridad de la Información será el encargado de coordinar los conocimientos y las experiencias disponibles al Municipio, a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Municipios o asistir a capacitaciones para incrementar el conocimiento sobre esta materia.

4.1.3. Revisión de la Política de Seguridad de la Información

La Administración Municipal y el Encargado de Seguridad de la Información realizarán revisiones independientes sobre la vigencia e implementación de las Políticas de Seguridad

de la Información, esta política se revisará cada semestre (6 meses) a contar de su aprobación.

Estas revisiones aseguran que los puntos expuestos en la presente política cumplan con la vigencia correspondiente y establece planes de acción para realizar mejoras e integrar nuevas ideas.

4.2. Seguridad Frente al Acceso por Parte de Terceros

4.2.1. Identificación de Riesgos del Acceso de Personal Externo y Terceros

Cuando exista la necesidad de otorgar acceso a personal externo y a terceros, sobre la información del Municipio, el Encargado de Seguridad de la Información y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, los siguientes aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información (nivel de criticidad o importancia de la información).
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la seguridad de la información del Municipio.

En ningún caso se otorgará acceso a terceros a la información, a la sala de servidores u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un acuerdo previo para su ingreso.

4.2.2. Requerimientos de Seguridad en Contratos o Acuerdos con Terceros

Se revisarán los acuerdos existentes o se establecerá un análisis a los tratados que se efectúen con terceras entidades o personas, teniendo en cuenta la necesidad de aplicar los siguientes controles (el detalle de cada control se describe en las partes correspondientes de esta política):

A. Cumplimiento de la Política de Seguridad de la Información de la Municipalidad.
B. Protección de los activos de la Municipalidad, incluyendo:
    1. Procesos y Prácticas para proteger los bienes de la Municipalidad, abarcando los activos físicos, la información y el software.
    2. Procedimiento para determinar, investigar, monitorear y solucionar eventos que comprometan los bienes de información, por ejemplo, debido a pérdida o modificación de datos.
    3. Controles para garantizar la recuperación o destrucción de la información.
    4. Restricciones a la copia y divulgación de información.
C. Descripción de los servicios disponibles.
D. Nivel de servicio esperado y niveles de servicio aceptables.
E. Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
F. Existencia de Derechos de Propiedad Intelectual.

G. Definiciones relacionadas con la protección de datos.
H. Acuerdos de control de accesos que contemplen:
    1. Métodos de acceso permitidos, y el control y uso de identificadores únicos.
    2. Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
I. Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
J. Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
K. Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
L. Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
M. Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
N. Proceso claro y detallado de administración de cambios al software o sistemas.
O. Controles que garanticen la protección contra software malicioso.
P. Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

4.3. Subcontratación

4.3.1. Requerimientos de Seguridad referentes a la Subcontratación

Los contratos o acuerdos de contemplen una subcontratación total o parcial para la administración y control de sistemas de información y redes y/o de la Municipalidad, se contemplarán además de los puntos especificados en “Requerimientos de Seguridad en Contratos o Acuerdos con Terceros”, los siguientes aspectos:

A. Forma en que se cumplirán los requisitos legales aplicables.
B. Medios para garantizar que todas las partes involucradas en la subcontratación, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.
C. Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos del Municipio.
D. Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible del Municipio.
E. Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
F. Niveles de seguridad física que se asignarán al equipamiento de terceras personas.
G. Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

5. Clasificación y Control de Activos

Son sus objetivos:

A. Garantizar que los activos de información reciban un apropiado nivel de protección.
B. Clasificar la información para señalar su sensibilidad y criticidad.
C. Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Esta Política se aplica a toda la información administrada en la Municipalidad, cualquiera sea el soporte en que se encuentre (ya sea física o información virtual).
Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información, que realizarán con la información posteriormente en caso de destrucción y a su vez identificar los riesgos que esta información tenga.
El Encargado de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan, es decir, según el grado de importancia de los recursos de información, son las cuales obtendrán mayor prioridad, según la clasificación de riesgos.
Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplido de acuerdo a lo establecido en la presente Política.

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.

5.2. Clasificación de la información

Para clasificar un Activo de Información, de un equipo informático, se evaluarán las tres características de la información en las cuales se basa la seguridad:

- Confidencialidad.
- Integridad.
- Disponibilidad.

5.3. Rotulado de la Información

Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia.
- Almacenamiento.
- Transmisión por correo, fax, correo electrónico.
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

Este rotulado de la información se puede realizar bajo este esquema:

- Nombre del recurso.
- Tipo.

- Almacenamiento.
- Criticidad. (Medible bajo un análisis de criticidad descrito en el punto).
- Descripción Breve.

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.

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.

6. Seguridad del Personal

Son sus objetivos:

A. Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.
B. Explicitar las responsabilidades en materia de seguridad en la etapa de entrega de equipos computacionales al funcionario.
C. Garantizar que los funcionarios estén al día de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Municipalidad en el transcurso de sus tareas normales.
D. Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Esta Política se aplica a todo el personal del Municipio, en todos los grados y estamentos, y al personal externo que efectúe tareas dentro del ámbito de la Municipalidad.

El Encargado de Seguridad de la Información tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al personal municipal sobre las tendencias en cuanto a amenazas y riesgos que puedan afectar a los equipos informáticos del municipio.

Todo el personal del Municipio es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten, y debidamente deben de informar al Encargado de Seguridad de la Información sobre las posibles dudas o sospechas reales de amenazas.

6.1. Definición de Puestos de Trabajo y la Asignación de Recursos

6.1.1. Inducción de Seguridad de la información en los Puestos de Trabajo

Las funciones y responsabilidades en materia de seguridad serán dictaminadas una vez que se le entregue un equipo computacional al funcionario. Estas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de las Políticas de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

6.2. Capacitación del funcionario

6.2.1. Formación y Capacitación en Materia de Seguridad de la Información

Todos los funcionarios del Municipio y cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en el municipio, recibirán una capacitación y actualización periódica en materia de la política, normas y procedimientos de la Municipalidad. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de los recursos computacionales en general.

6.3. Respuesta a Incidentes y Anomalías en Materia de Seguridad

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.

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.

6.3.3. Comunicación de Anomalías del Software

La comunicación de anomalías de software y otros riesgos informáticos deben de ser de este modo para una respuesta más rápida frente a estos riesgos, la pauta es la siguiente:

A. Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
B. Alertar inmediatamente al Encargado de Seguridad de la Información referente al activo comprometido al cual se presenta la anomalía.
C. Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.

6.3.4. Aprendiendo de los Incidentes

Dentro del procedimiento de identificación de anomalías y evaluación de riesgos está un apartado en donde se registra el incidente ocurrido, 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.

7. Seguridad Física y Ambiental

Son sus objetivos:

A. Prevenir e impedir accesos no autorizados, daños e interferencia, y robo de información de la Municipalidad.
B. Proteger los equipos computacionales que contienen información crítica, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.
C. Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Municipio.
D. Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.
E. Brindar protección, en proporción a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la Municipalidad: instalaciones, equipamiento, cableado, medios de almacenamiento, etc.

El Encargado de Seguridad de la Información definirá junto con el Encargado de Computación y los Propietarios de la Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos, en función a un análisis de riesgos, y se realizará un seguimiento controlado de la información. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente Capítulo.

El Encargado de Seguridad de la Información asistirá al Encargado de Computación en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones de la Municipalidad.

Los Directivos de los departamentos municipales definirán los niveles de acceso físico del personal del municipio a las áreas restringidas bajo su responsabilidad. Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los funcionarios de la Municipalidad cuando lo crean conveniente.

Todos los funcionarios municipales son responsables del cumplimiento de las buenas prácticas correspondientes a pantallas y escritorios limpios, para la protección y el orden de la información relativa al trabajo diario en las oficinas.

En la Ilustre Municipalidad de Til-Til, 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 Zócalo (Subterráneo) de la Municipalidad.

Otras áreas parciales que están provistas de routers o switch para el uso y acceso a la red de internet son 2 cajas negras protegidas con llaves (técnicamente llamados Rack), ubicadas en los departamentos de DIDECO y SECPLAC.

7.1. Perímetro de Seguridad Física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físico alrededor del Municipio y de la sala de servidores municipal.

El Municipio utilizará perímetros de seguridad de acceso a la sala de servidor municipal, y proveerle a esta de suministro de:

- Electricidad.
- Aire Acondicionado.
- Luces de Emergencia.
- Extintores.
- Sensores que controlen el humo, humedad.
- Control que permita que no entre el agua.

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.

7.3. Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, agitación civil, y otras formas de desastres naturales o provocados por el hombre.

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.

7.5. Ubicación de los Medios de Almacenamiento de Respaldos

Los respaldos se realizarán en discos duros externos portátiles, designados para tal propósito, también se contará con una caja fuerte para almacenar el respaldo de las bases de datos históricas del servidor municipal. Esta caja fuerte estará ubicada en la Oficina de Computación.

7.6. Suministros de Energía

El equipamiento computacional con información más crítica, estará protegido contra posibles fallas en el suministro de energía y otras anomalías eléctricas que se podrían presentar. El suministro de energía alternativo estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo (en el caso de que el equipo computacional cuente con alguna batería) o en su defecto se instalará una UPS para evitar pérdidas de información por cortes energéticos.

También el municipio cuenta con un generador la cual se encargará de evitar la interrupción de los servicios que puedan comprometer la información, de todos los equipos computacionales y artefactos eléctricos del municipio.

7.7. Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, será ubicado en la parte posterior del equipo computacional, para evitar la intercepción del funcionario.

7.8. Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes, teniendo en cuenta a tal efecto:

A. La realización de tareas de mantenimiento físico al equipamiento, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsable del Área Informática.
B. Sólo el Área de Computación puede brindar mantenimiento y llevar a cabo reparaciones en los equipos computacionales.
C. La registración de todas las fallas “supuestas y/o reales” y de todo el mantenimiento preventivo y correctivo realizado.
D. La eliminación de toda información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

También se realizará un mantenimiento preventivo, la cual se revisarán aspectos previamente definidos por el Encargado de Seguridad de la Información, la periodicidad de las revisiones de mantenimiento preventivo es completamente aleatoria y será sin previo conocimiento del funcionario municipal.

7.9. Seguridad de los Equipos Fuera de las Instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la Municipalidad será autorizado por el Alcalde o Administrador Municipal. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la Municipalidad para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

7.10. Políticas de Escritorios y Pantallas Limpias

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en los equipos computacionales, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

7.11. Retiro de los Bienes

El equipamiento, la información y el software no serán retirados de la sede del Municipio sin autorización formal. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos del Municipio, añadido a la mantención preventiva.

8. Gestión de Operaciones en Aplicaciones y Cambios

Son sus objetivos:

A. Garantizar el funcionamiento correcto y seguro de la sala de servidores municipal, así como los equipos computacionales de los funcionarios municipales.
B. Establecer responsabilidades y procedimientos para la gestión operativa y la marcha de los sistemas municipales, incluyendo comportamientos técnicos, procedimiento para la respuesta a incidentes y separación de funciones ante esos incidentes.
C. Respaldar toda la información sensible (documentos, medios digitales, bases de datos, entre otros.), ante eventuales ataques e imprevistos.
D. Proteger a los equipos computacionales y a la información que procesan, entre ellos realizar mantención a la información, control de red y el procesamiento de medios extraíbles.

Además, se consideran la protección de redes y programas, la gestión operativa de los equipos computacionales, el intercambio de la información, el mantenimiento de la información digital, entre otros.

8.1. Control de Cambios y Separación de Funciones

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.

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.

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.

8.2. Planificación y Aprobación de Sistemas

8.2.1. Planificación de la Capacidad

El Encargado de Computación, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados.

Para ello tomará en cuenta además los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información de la Municipalidad para el período estipulado de vida útil de cada componente.

Asimismo, informará las necesidades detectadas a la Alcaldía para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

8.2.2. Aprobación del Sistema

El Encargado de Computación y el Encargado de Seguridad de la Información sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

8.3. Manejo de Software y Configuraciones Predeterminadas

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:
    - Para funcionarios: AVAST o Avira
    - Para equipos críticos: ESET NOD32
- WinRAR
- Google Chrome
- Microsoft Office (En el caso de Disponibilidad de Licencias, si no existe disponibilidad, se usa LibreOffice y Thunderbird para Correos)
- Yak!

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.

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.

8.4. Protección Contra Software Malicioso

8.4.1. Controles Contra Software Malicioso

El Encargado de Seguridad de la Información definirá controles de detección y prevención para la protección contra software malicioso. El Encargado de Computación, o el personal designado por éste, implementará dichos controles.

El Encargado de Seguridad de la Información entregará instructivos que formulen una conciencia y responsabilidad de los funcionarios en materia de seguridad de archivos, para los controles del acceso al sistema y para mejorar la administración de cambios.

8.5. Mantenimiento

8.5.1. Resguardo de la Información

El Encargado de Computación y el de Seguridad Informática junto a los Propietarios de la Información determinarán los requerimientos para resguardar cada software o driver de instalación según corresponda, el modo estándar se define que el Área de Computación, posea esos discos de instalación y respaldos.

8.5.2. Registro de Actividades del Personal Operativo

El Encargado de Computación asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

A. Errores del sistema y medidas correctivas tomadas.
B. Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas.
C. Ejecución de operaciones críticas.
D. Cambios a información crítica.

También se realizarán controles aleatorios de equipos municipales, a fin de detectar anomalías e infracciones que puedan incurrir los funcionarios sobre el uso de sus equipos, estos Check-list se deben hacer de forma aleatoria y el tiempo de revisión en un mes por departamento.

8.5.3. Registro de Fallas

El Encargado de Computación establecerá un modelo para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas, así como su registro.

8.6. Administración de la Red

8.6.1. 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.

8.7. Administración y Seguridad de los Medios de Almacenamiento

8.7.1. Eliminación de Medios de Información

Las eliminaciones de los medios constituyen en un formato o borrado de los archivos del mismo, este proceso consta de un formateo, a la cual debe de estar autorizado por el encargado de la información ante cualquier procedimiento que requiera el formato o el borrado de sus archivos.

8.7.2. Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se considerarán los recaudos para su protección, de almacenar la documentación del sistema en forma segura y restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

8.8. Respaldo de la Información

8.8.1. 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.

8.8.2. 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.

8.9. Intercambios de Información y Software

8.9.1. Acuerdos de Intercambio de Información y Software

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la Municipalidad y las consideraciones de seguridad sobre la misma.

8.9.2. Seguridad de los Medios en Transporte

El 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 o protección para el envío y la adopción de controles especiales, como revisión de números de serie, por ejemplo, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas.

8.9.3. Seguridad del Correo Electrónico Institucional

8.9.3.1. Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

A. La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.

B. La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
C. Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
D. La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.
E. El impacto de un cambio en el medio de comunicación en los procesos del Municipio.
F. Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
G. El uso inadecuado por parte del personal.

8.9.3.2. Política de Correo Electrónico

El Encargado de Seguridad de la Información define una política de correos electrónicos institucionales que trata respecto al uso del correo electrónico, esta política está separada de esta política general de seguridad de la información, esa política incluye los siguientes aspectos:

A. Protección contra ataques al correo electrónico, por ejemplo, virus, intercepción, etc.
B. Protección de archivos adjuntos de correo electrónico.
C. Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.
D. Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
E. Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del funcionario, etc.).
F. Definición de los alcances del uso del correo electrónico por parte del personal de la Municipalidad.

8.9.4. Sistemas de Acceso Público

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada.

Además, se integran los sistemas que son del Gobierno, estos sistemas y su uso están en exclusiva responsabilidad del funcionario en cuestión, y también el soporte que se le brinda a ese sistema, si un funcionario tiene una falla con un sistema del gobierno, el área de computación no se hace responsable por estas fallas.

9. Control de Accesos

Son sus objetivos:

A. Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
B. Implementar seguridad en los accesos de funcionarios por medio de técnicas de autenticación y autorización.
C. Controlar la seguridad en la conexión entre la red del Municipio y otras redes públicas o privadas.
D. Registrar y revisar eventos y actividades críticas llevadas a cabo por los funcionarios en los sistemas.
E. Concientizar a los funcionarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
F. Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

9.1. Administración de Accesos de Funcionarios

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.

9.1.1. Registro de nuevos Funcionarios

El Encargado de Seguridad de la Información definirá un procedimiento formal de registro de nuevos funcionarios para definir la concesión del acceso a todos los sistemas, bases de datos y servicios de información, dependiendo de las necesidades establecidas en el contrato, además de tener claro cuales sistemas ocupaba un funcionario que es dado de baja, para la revocación del acceso y su posterior eliminación.

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 que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal de parte de la Alcaldía.

9.1.3. Administración de Contraseñas de Funcionarios

La asignación de contraseñas se realizará bajo ciertos patrones secretos definidos por el Área de Computación, también el funcionario puede asignar sus propias contraseñas, debidamente escritas por comunicación interna, dependiendo del sistema que se le presente, también debe notificar al área de Computación cuando un funcionario desea cambiar la clave.

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 deben de estar protegidas por contraseñas con un mayor nivel de complejidad que el habitual, estas cuentas son superusuario, es decir, pueden cambiar a voluntad todos los parámetros de un sistema en concreto

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.

9.2. Responsabilidades del Usuario

9.2.1. Uso de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, existen dos buenas prácticas para el uso de las contraseñas que son las siguientes:

- La contraseña no debe ser menor a 6 caracteres
- Debe contener mayúsculas y minúsculas

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.

9.3. Control de Acceso a la Red

9.3.1. Política de Utilización de los Servicios de Red

Se controlará el acceso a los servicios de red tanto internos como externos. El Encargado de Computación tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de un Departamento que lo solicite para personal de su incumbencia.

9.3.2. Autenticación de Usuarios para Conexiones Externas

El Encargado de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

9.3.3. Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la Municipalidad. Por

consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas y verificadas.

9.3.4. 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.

9.3.5. 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 y por el Administrador Municipal. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

9.3.6. 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.

9.4. Control de Acceso al Sistema Operativo

9.4.1. Identificación Automática de Equipos

El Encargado de Seguridad de la Información junto con el Encargado de Computación realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo, esta evaluación de riesgos se define por lo siguiente:

9.4.2. Sistema de Administración de Contraseñas

El sistema de administración de contraseñas debe:

A. Imponer el uso de contraseñas individuales para determinar responsabilidades.
B. Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
C. Imponer una selección de contraseñas de calidad según lo señalado en el punto "Uso de Contraseñas".
D. Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto "Uso de Contraseñas".
E. Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
F. Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.

G. Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
H. Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
I. Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
J. Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo, claves de impresoras, hubs, routers, etc.).
K. Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

9.4.3. Uso de Utilitarios de Sistema

Existen programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Su uso será limitado y minuciosamente controlado.

9.4.4. Alarmas Silenciosas para la Protección de los Usuarios

Se considerará la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción. La decisión de suministrar una alarma de esta índole se basará en una evaluación de riesgos que realizará el Encargado de Seguridad de la Información junto con el Encargado de Computación.

9.4.5. Suspensión de equipos por Tiempo Muerto

El Encargado de Seguridad de la Información, junto con los Propietarios de la Información de que se trate definirán bajo qué tiempo desean que el equipo pase a estado de suspensión, la cual, el equipo queda protegido por contraseña. Las mismas se “apagarán” después de un periodo definido de inactividad.

Para los computadores, se implementará una contraseña, la cual la define el Propietario del equipo computacional y su información, con esto se evita el acceso no autorizado, pero no cierra las sesiones de aplicación o de red.

9.5. Control de Acceso a las Aplicaciones

9.5.1. Restricción del Acceso a la Información

Los usuarios de sistemas municipales, tendrán acceso a la información sensible de la Municipalidad como, por ejemplo, activos fijos, patentes municipales, tesorería, entre otros sistemas según corresponda la función del personal municipal y además esté conforme con las responsabilidades descritas en la Política de Control de Acceso.

Cualquier otro acceso a los sistemas municipales que no esté definido y previamente autorizado se considerará como intrusión a los sistemas municipales.

9.5.2. Aislamiento de los Sistemas Sensibles

El sistema sensible definido por la Municipalidad, es el servidor, ya que procesa todos los

datos que apoyan a los sistemas municipales a que cumplan sus funciones, este servidor se encuentra aislado de todo contacto humano no autorizado. Este servidor cuenta con un computador dedicado a las tareas de manejo de bases de datos y especificaciones para respaldos entre otros.

9.6. Monitoreo del Acceso y Uso de los Sistemas

9.6.1. Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, la fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema y un registro de intentos exitosos y fallidos de acceso a datos y otros recursos.

9.6.2. Monitoreo del Uso de los Sistemas

9.6.2.1. Procedimientos y Áreas de Riesgo

Se usarán programas y aplicaciones para monitorear el uso de los sistemas y equipos computacionales, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

9.6.2.2. Factores de Riesgo

Los Propietarios de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

10. Desarrollo y Mantenimiento de Sistemas

Son sus objetivos:

A. Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.
B. Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
C. Definir los métodos de protección de la información crítica o sensible.
D. Definir instructivos en la cual se pueda coordinar respuestas rápidas frente a incidentes.

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollo propio o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por la Municipalidad en donde residan los desarrollos mencionados.

El Encargado de Seguridad de la Información junto con el Propietario de la Información, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Encargado de Seguridad de la Información, junto con el Propietario de la Información, definirán en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Encargado de Seguridad de la Información definirá junto con el Responsable del Área de Sistemas, los métodos de encriptación a ser utilizados.

10.1. Requerimientos de Seguridad de los Sistemas

10.1.1. Análisis y Especificaciones de los Requerimientos de Seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen. Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

10.2. Controles Criptográficos

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

10.2.1. Política de Utilización de Controles Criptográficos

Se utilizarán controles criptográficos en los siguientes casos:

1. Para la protección de claves de acceso a sistemas, datos y servicios.
2. Para la transmisión de información clasificada, fuera del ámbito del Municipio.
3. Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Encargado de Seguridad de la Información.

10.2.2. Cifrado

Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Encargado de Seguridad de la Información, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

10.2.3. Firma Digital

Se tomarán recaudos para proteger la confidencialidad de las claves privadas. Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

10.2.4. Servicios de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

10.3. Seguridad de los Procesos de Soporte

10.3.1. Revisión Técnica de los Cambios en el Sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

10.3.2. Restricción del Cambio de Paquetes de Software

La modificación de paquetes de software suministrados por proveedores, previa autorización del Encargado de Computación, deberá:

A. Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
B. Evaluar el impacto que se produce si el Municipio se hace cargo del mantenimiento.
C. Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

10.3.3. Canales Ocultos y Código Malicioso

Se evaluarán los siguientes aspectos para asegurar que ningún software posea algún código malicioso que pueda atacar a los distintos sistemas.

A. Adquirir programas a proveedores acreditados o productos ya evaluados.
B. Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
C. Controlar el acceso y las modificaciones al código instalado.
D. Utilizar herramientas para la protección contra la infección del software con código malicioso.

10.3.4. Desarrollo Externo de Software

Para el caso que se considere la subcontratación del desarrollo de software, se exigirán los siguientes puntos:

A. Acuerdos de licencias, propiedad de código y derechos conferidos.
B. Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
C. Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
D. Verificación del cumplimiento de las condiciones de seguridad contempladas en el punto 4.3.1. Requerimientos de Seguridad referentes a la Subcontratación.
E. Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

11. Administración de la Continuidad de las Actividades del Municipio

Son sus objetivos:

A. Minimizar los efectos de las posibles interrupciones de las actividades normales de la Municipalidad (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
B. Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
C. Maximizar la efectividad de las operaciones de contingencia del Municipio con el establecimiento de planes que incluyan al menos las siguientes etapas:
    a. Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.
    b. Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
    c. Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.
D. Asegurar la coordinación con el personal del Municipio y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.
E. El Encargado de Seguridad de la Información participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia. Los Propietarios de la Información y el Encargado de Seguridad de la Información cumplirán las siguientes funciones:
    - Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del Municipio.
    - Evaluar los riesgos para determinar el impacto de dichas interrupciones.
    - Identificar los controles preventivos.
    - Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Municipio.
    - Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del Municipio.

11.1. Continuidad de las Actividades y Análisis de los Impactos

Se establece la necesidad de contar con un Plan de Continuidad de las Actividades de la Municipalidad que contemple los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación.
- Identificar los controles preventivos.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los

procesos y recursos de información de que se trate y el Encargado de Seguridad de la Información, considerando todos los procesos de las actividades de la Municipalidad y no limitándose a los equipos computacionales municipales.

11.2. Elaboración e Implementación de los Planes de Continuidad de las Actividades del Municipio

Los propietarios de procesos y recursos de información, con la asistencia del Encargado de Seguridad de la Información, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Municipalidad.

11.3. Marco para la Planificación de la Continuidad de las Actividades del Municipio

Se mantendrá un solo marco para los planes de continuidad de las actividades del Municipio, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

12. Cumplimiento

Son sus objetivos:

A. Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la Municipalidad y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
B. Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la Municipalidad.
C. Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.
D. Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.
E. Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.
F. Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la Municipalidad.

12.1. Cumplimiento de Requisitos Legales

12.1.1. Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

12.1.2. Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

12.1.2.1. Derecho de Propiedad Intelectual del Software

El Encargado de Seguridad de la Información, con la asistencia del Área Legal, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

A. Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
B. Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
C. Mantener un adecuado registro de activos.
D. Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
E. Verificar que sólo se instalen productos con licencia y software autorizado.
F. Elaborar y divulgar un procedimiento para el mantenimiento de condiciones

adecuadas con respecto a las licencias.

G. Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
H. Utilizar herramientas de auditoría adecuadas.
I. Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

12.1.3. Protección de los Registros de la Municipalidad

Los registros críticos del Municipio se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la Municipalidad.

12.1.4. Protección de Datos y Privacidad de la Información Personal

Todos los funcionarios deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

12.1.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información del Municipio se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido. Todos los funcionarios deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

12.1.6. Regulación de Controles para el Uso de Criptografía

Al utilizar firmas digitales o electrónicas, se deberá considerar lo dispuesto por la Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma y su reglamento, el Decreto Supremo Nº181/2002, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

12.1.7. Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

12.2. Revisiones de la Política de Seguridad y la Compatibilidad Técnica

12.2.1. Cumplimiento de las Políticas de Seguridad

Cada directivo de departamento, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Encargado de Seguridad de la Información, realizará revisiones periódicas de todas las áreas del Municipio a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

A. Sistemas de información.
B. Proveedores de sistemas.
C. Propietarios de la Información.
D. Funcionarios Municipales.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

12.2.2. Verificación de la Compatibilidad Técnica

El Encargado de Seguridad de la Información verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados.

12.3. Consideraciones de Auditorías de Sistemas

12.3.1. Controles de Auditoría de Sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

12.3.2. Protección de los Elementos Utilizados por la Auditoría de Sistemas

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos. Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido. Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoría dispuestas por la Contraloría General de la República.

12.4. Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en las presente Políticas de Seguridad conforme a lo dispuesto por las normas estatutarias, escalafonarias y convencionales que rigen al personal municipal, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Municipios pertinentes.

Manual de Procedimientos y Documentación

Sistema de Gestión de Seguridad de la Información (SGSI)

Ilustre Municipalidad de Til-Til

Índice

Control de Versiones

Fecha	Responsable	Motivo	Versión
15-01-2015	Aníbal Ramos G.	Elaboración Inicial	1.0

Introducción

En atención a los riesgos y a 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 Til-Til, 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 Til-Til a tal modo de optimizar los recursos, evitando pérdidas de información y la difusión de documentos y contenidos confidenciales de la institución.

¿Qué es la información?

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”.

En la actualidad la información se ha convertido en uno de los bienes más importantes y preciados, es por esta razón que se invierte a nivel mundial gran cantidad de otros recursos (profesionales, tecnológicos, económicos, etc.) para protegerla, pero ¿es solo la protección de ella la que debe preocuparnos? La respuesta es no, existen otros factores igual de importantes que considerar como, por ejemplo: la oportunidad, integridad, validez o confiabilidad, de lo anterior surge la necesidad entonces de “Asegurar” el conjunto elementos que dan su valor.

¿Qué es la seguridad de la información?

La información es un bien que, como otros, tiene distinto valor para una organización y/o personas, consecuentemente, con ello, necesita ser protegida en forma apropiada. La seguridad debe entenderse como un conjunto de conductas, acciones, procedimientos, tecnologías y otros que buscan "asegurar" su buen uso, integridad, confidencialidad, confiabilidad y oportunidad, es por lo anterior que no podemos observar a la seguridad o sistemas como un agente externo o distinto a nosotros ya que somos parte activa de ella, ningún sistema de seguridad será lo suficientemente bueno como para evitar por ejemplo: que alguno de nosotros al salir a colación o a realizar algún trámite dejemos sobre nuestro escritorio el informe final de un caso, y que este pueda ser sustraído, copiado o adulterado, ningún sistema de control de acceso va a ser efectivo si permanentemente dejamos las puertas de acceso abiertas o colocamos trabas para facilitar nuestro transitar de un lado a otro, ningún sistema de auditaría va a servir si entregamos nuestras credenciales (nombre de usuario y contraseña).

Recordar también lo indicado en nuestra propia Ley orgánica la que nos impone el "deber de sigilo" o como lo define la Real Academia Española "Secreto que se guarda de una cosa o noticia".

La información puede existir de muchas formas, puede ser impresa, escrita, o almacenada o transmitida electrónicamente, mostrada en películas o hablada. Cualquier forma que tome la información, o los dispositivos por los cuales es compartida o almacenada, siempre deberán estar sujetos al mismo cuidado.

La seguridad de la información se caracteriza aquí como la preservación de:

a) Confidencialidad: asegurar que la información sea accesible sólo por aquellos usuarios autorizados para tener acceso;

b) Integridad: salvaguardar que la información y los métodos de procesamiento sean exactos y completos;

c) Disponibilidad: asegurar que los usuarios autorizados tengan acceso a la información y bienes asociados cuando lo requieran.

La seguridad de la información se logra mediante la implementación de un adecuado conjunto de controles, los que podrían ser políticas, prácticas, procedimientos, estructuras organizacionales y funciones.

Procedimientos

Simbología Utilizada

Inicio o Terminal

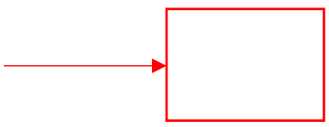
Proceso

Conector Flecha

Conector que se adjunta a un proceso

Documento

Método Alternativo



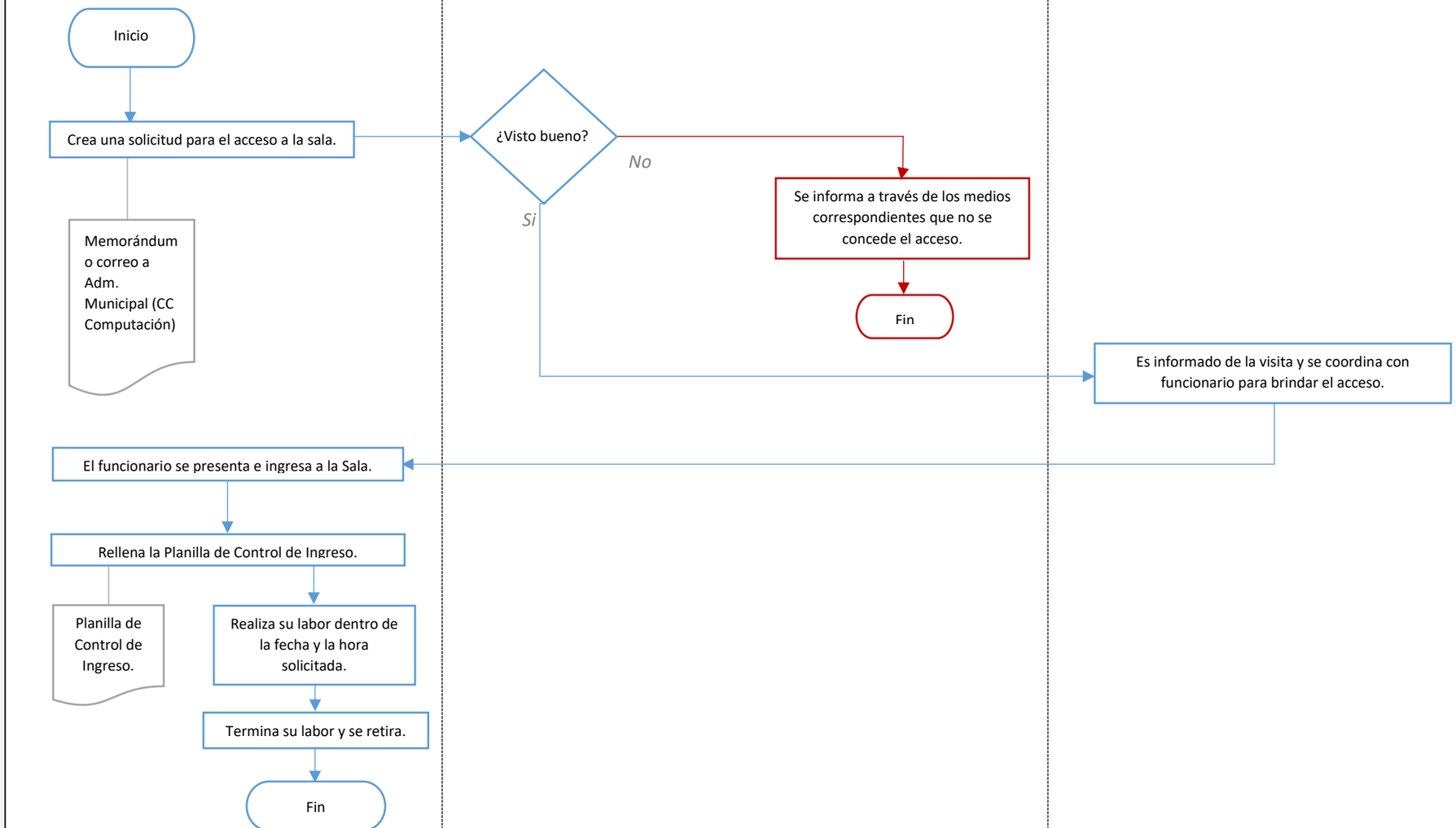
Negación (Color Rojo)

Almacenaje de Información

Procedimiento INF-001: Acceso a Sala Eléctrica y Servidor

INF-001	
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 Til-Til, 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 Zócalo (Subterráneo) 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.

Diagrama de Flujo

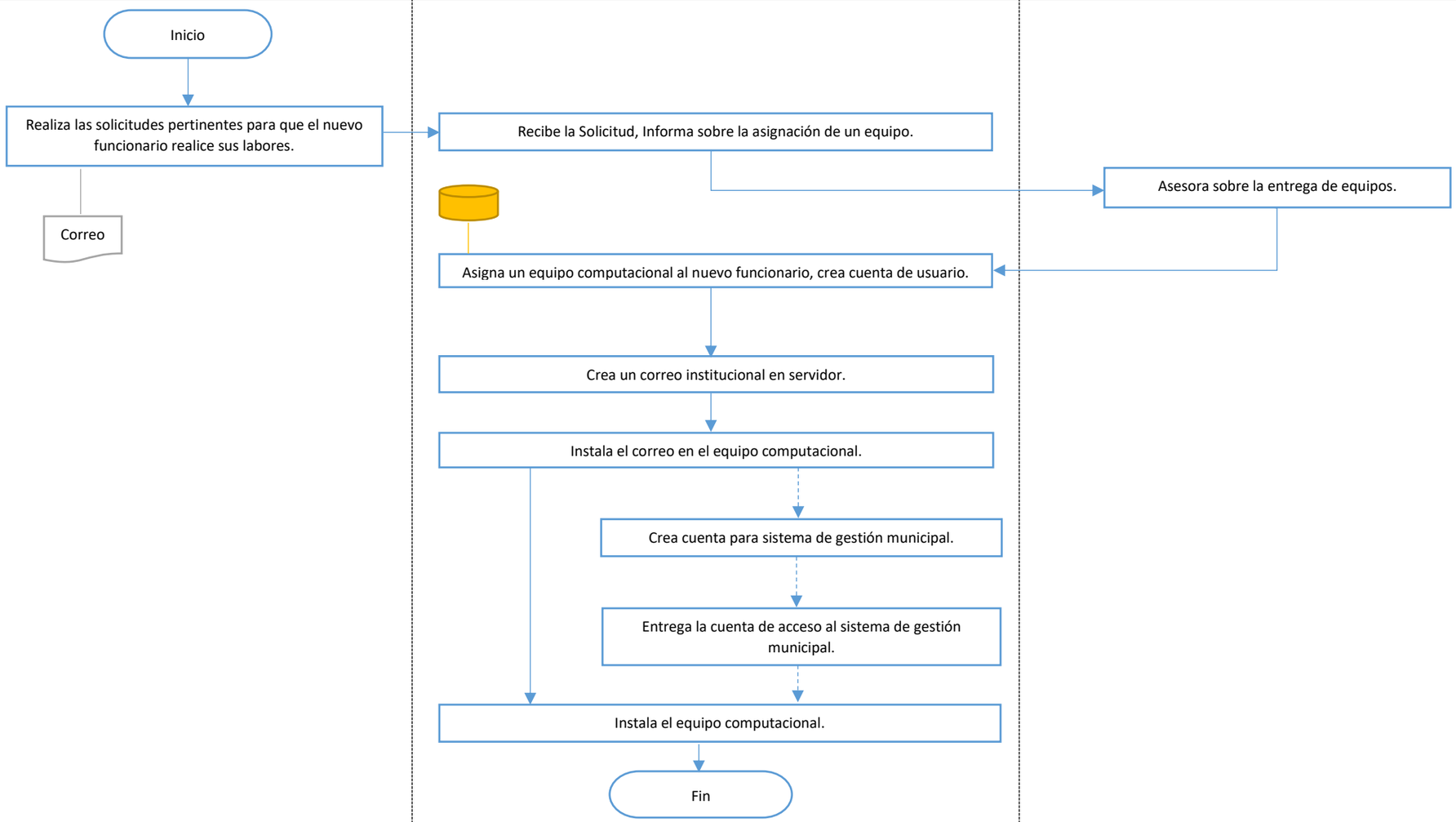
Responsables	Funcionario	Administrador Municipal	Computación
Proceso			

Notas	La solicitud de acceso a la sala eléctrica y de servidores debe llevar al menos los siguientes datos, en lo posible se exigiran 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.

Procedimiento INF-002: Entrega de Acceso a Sistemas de Información

INF-002	
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

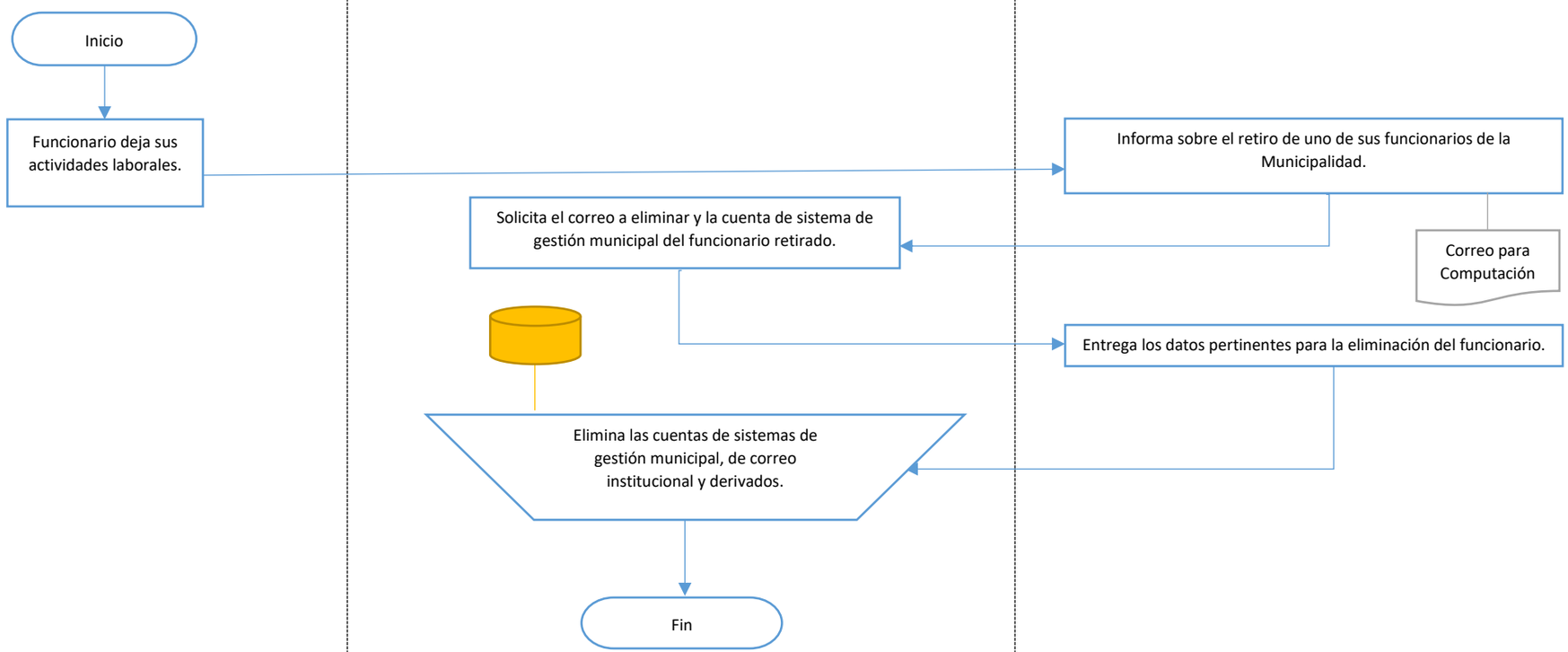
Responsables	Funcionario	Computación	Administrador Municipal
Proceso			

Notas	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@tiltil.cl). • Todos los correos institucionales terminan con “@tiltil.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 Til-Til. 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 extraibles, entre otros informativos de menor prioridad.

Procedimiento INF-003: Revocación de Acceso a Sistemas de Información

INF-003	
Nombre	Revocación de Acceso a Sistemas 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 Til-Til, 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

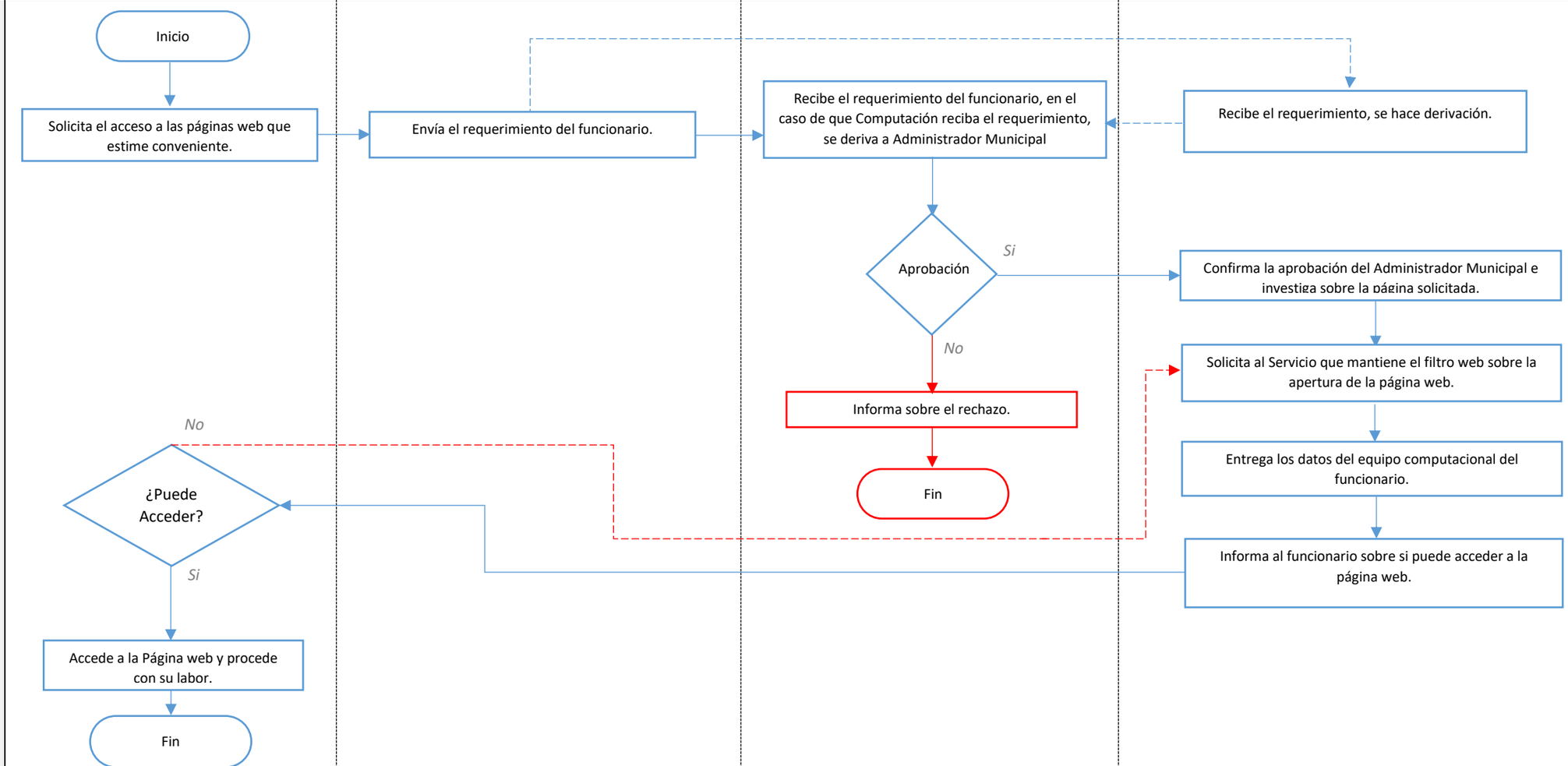
Responsables	Funcionario Retirado	Computación	Jefe Directo Funcionario Retirado
Proceso			

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.

Procedimiento INF-004: Solicitud de Acceso a Páginas Web filtradas

INF-004	
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

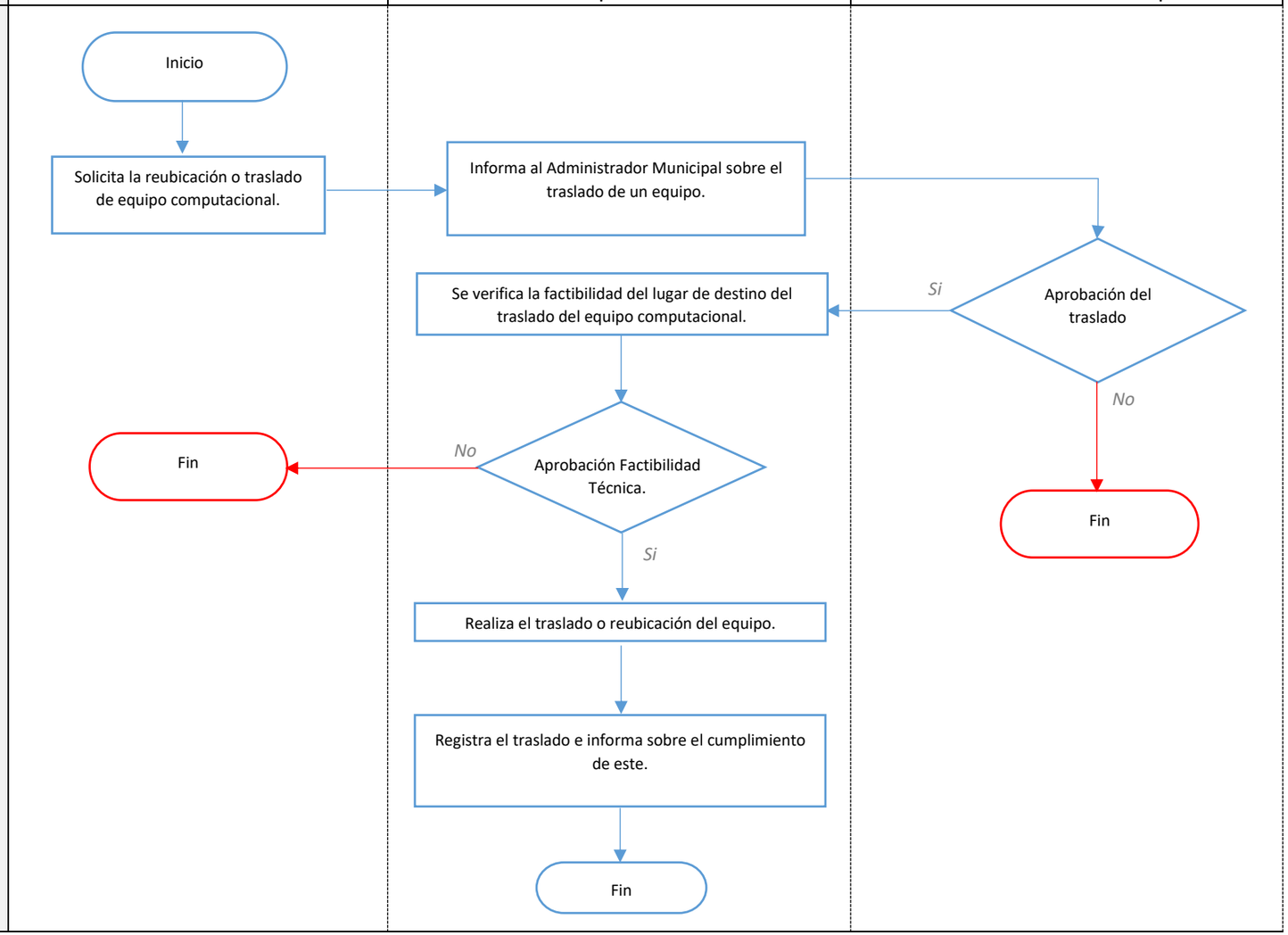


Notas	El funcionario debe de solicitar la apertura de la página web a su jefe directo y con la aprobación de la solicitud, el jefe directo del funcionario le realiza la solicitud al Administrador Municipal. En el caso de que Computación reciba la solicitud, se deriva la solicitud al Administrador Municipal. 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.

Procedimiento INF-005: Reubicación de Equipos Municipales

INF-005	
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 Til-Til.
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

Responsables	Funcionario	Computación	Administrador Municipal
Proceso			

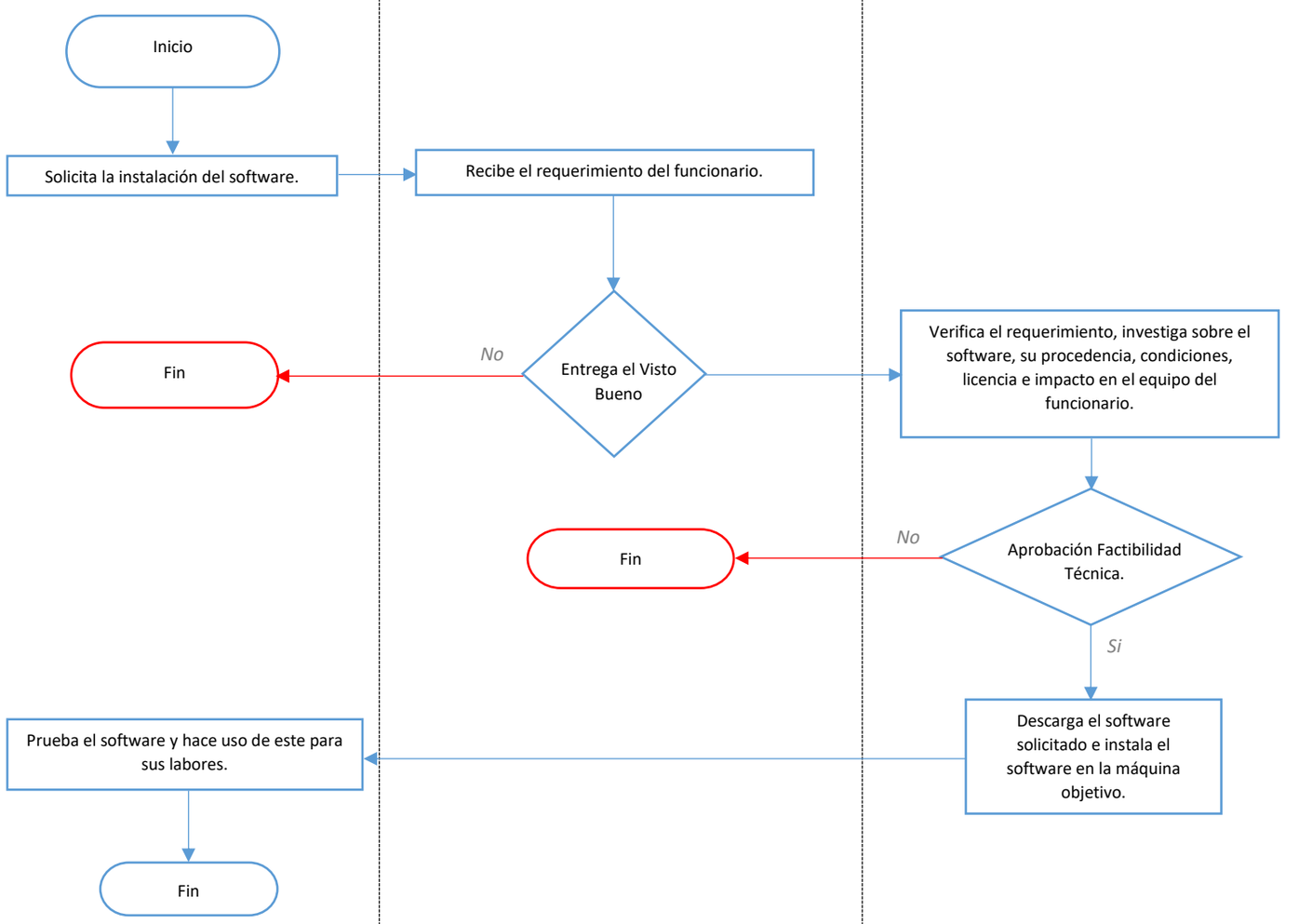
Notas	El traslado o reubicación de equipos debe de ser aprobado previamente por Computación bajo el análisis de factibilidad técnica,y aprobado por el Administrador Municipal. Si la factibilidad técnica es viable, se procede a la validación de las partes antes mencionadas. Luego de esas validaciones,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

Procedimiento INF-006: Instalación de Software y aplicaciones

INF-006	
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:
	  ○ Para funcionarios: AVAST o Avira
	  ○ Para equipos críticos: ESET NOD32
	• WinRAR
	• Google Chrome
	• Microsoft Office (En el caso de Disponibilidad de Licencias, si no existe disponibilidad, se usa LibreOffice y Thunderbird para Correos)
	• 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.

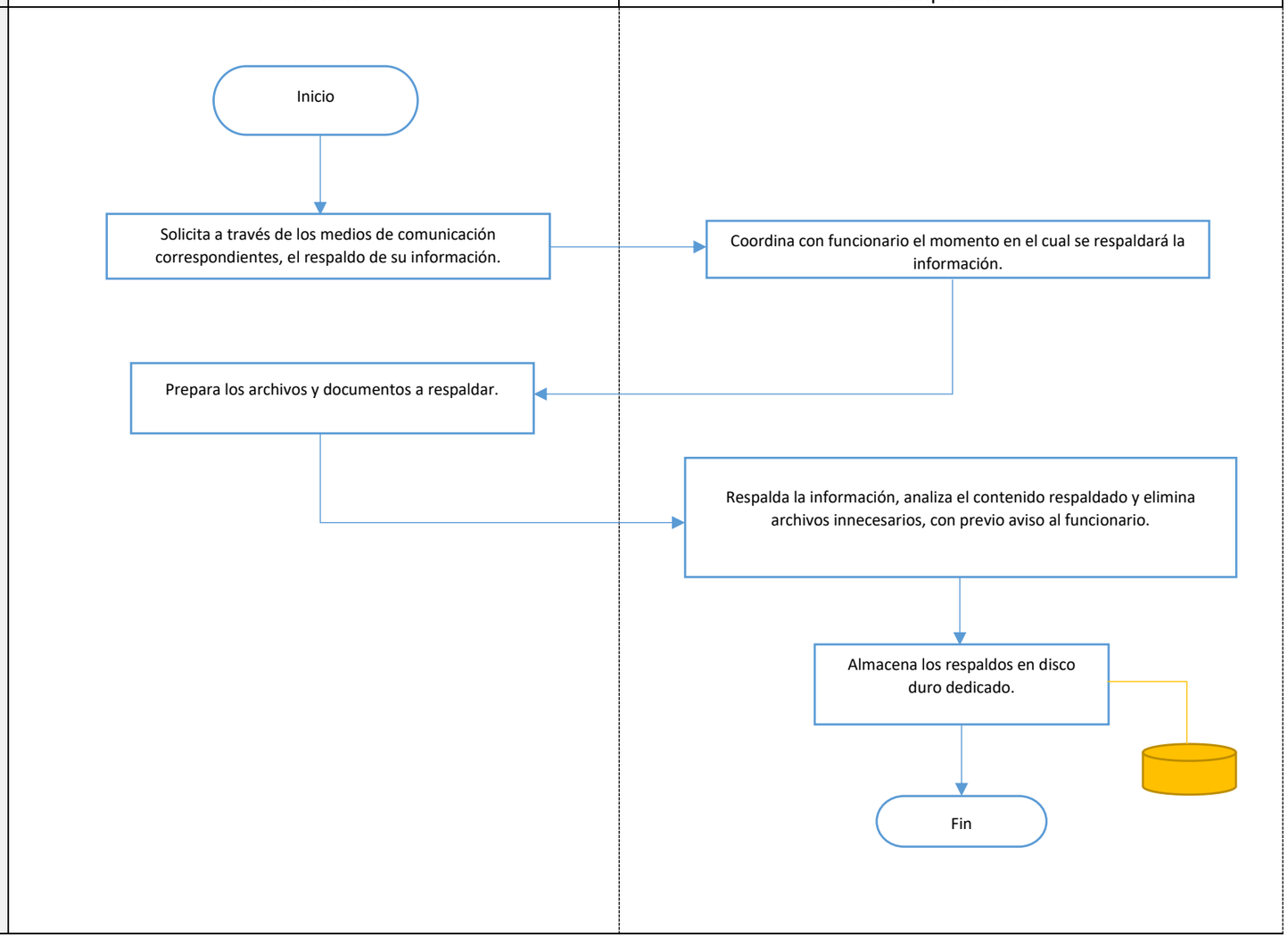
Diagrama de Flujo

Responsables	Funcionario	Jefe Directo Funcionario	Computación
Proceso			

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.

Procedimiento INF-007: Solicitud de Respaldo Especial de Información de un Funcionario

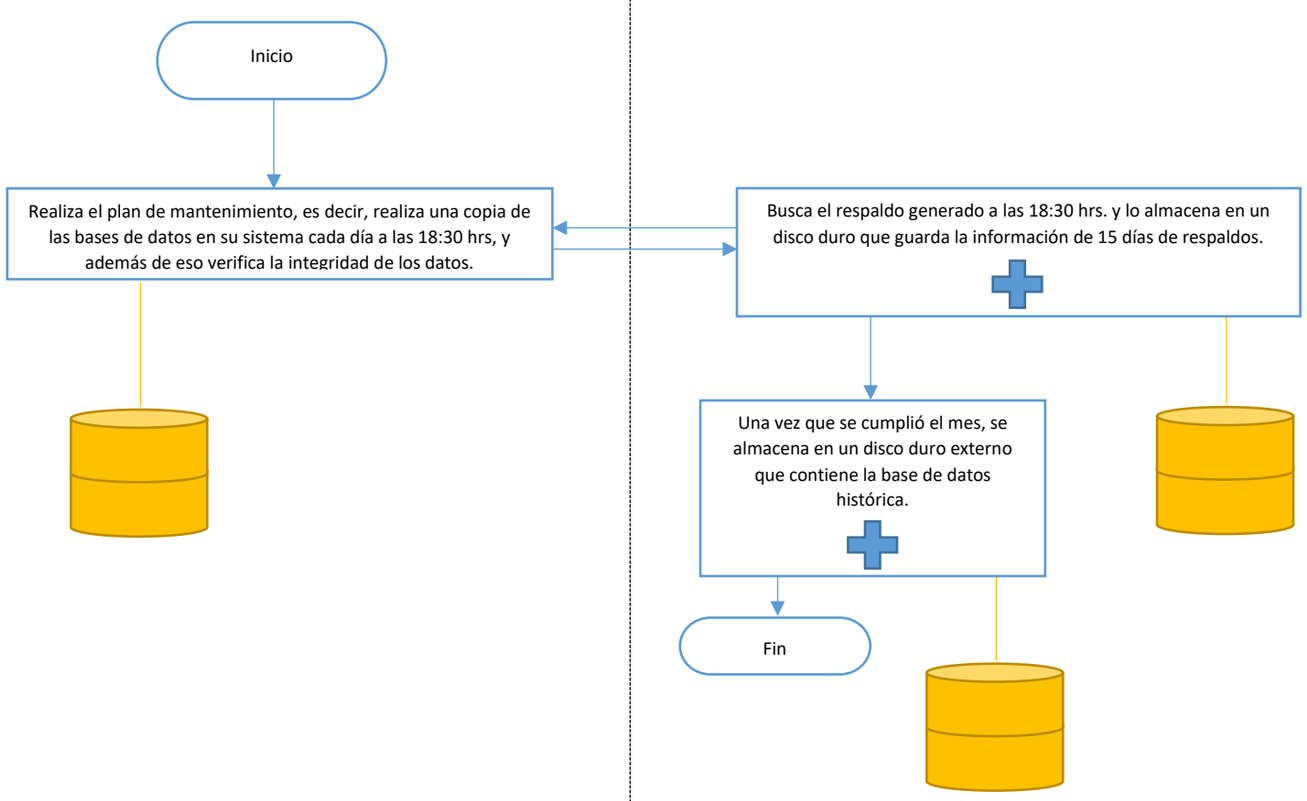
INF-007	
Nombre	Solicitud de Respaldo Especial de Información de un Funcionario.
Alcance y Aplicación	Todos los Funcionarios Municipales.
Descripción	Resguardar los datos de los Funcionarios Municipales a fin de evitar la pérdida de datos sensibles, en caso de cualquier falla de los equipos informáticos o bien para evitar la pérdida involuntaria de archivos en caso de formateo.
Normativa	Punto 8.4.1. Resguardo de la Información El Encargado de Computación y el de Seguridad Informática junto a los Propietarios de la Información determinarán los requerimientos para resguardar cada software o driver de instalación según corresponda, el modo estándar se define que el Área de Computación, posea esos discos de instalación y respaldos. 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.

Diagrama de Flujo		
Responsables	Funcionario	Computación
Proceso		

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).

Procedimiento INF-008: Respaldo a Bases de Datos del Servidor

INF-008	
Nombre	Respaldo a Bases de Datos 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 18:30 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.

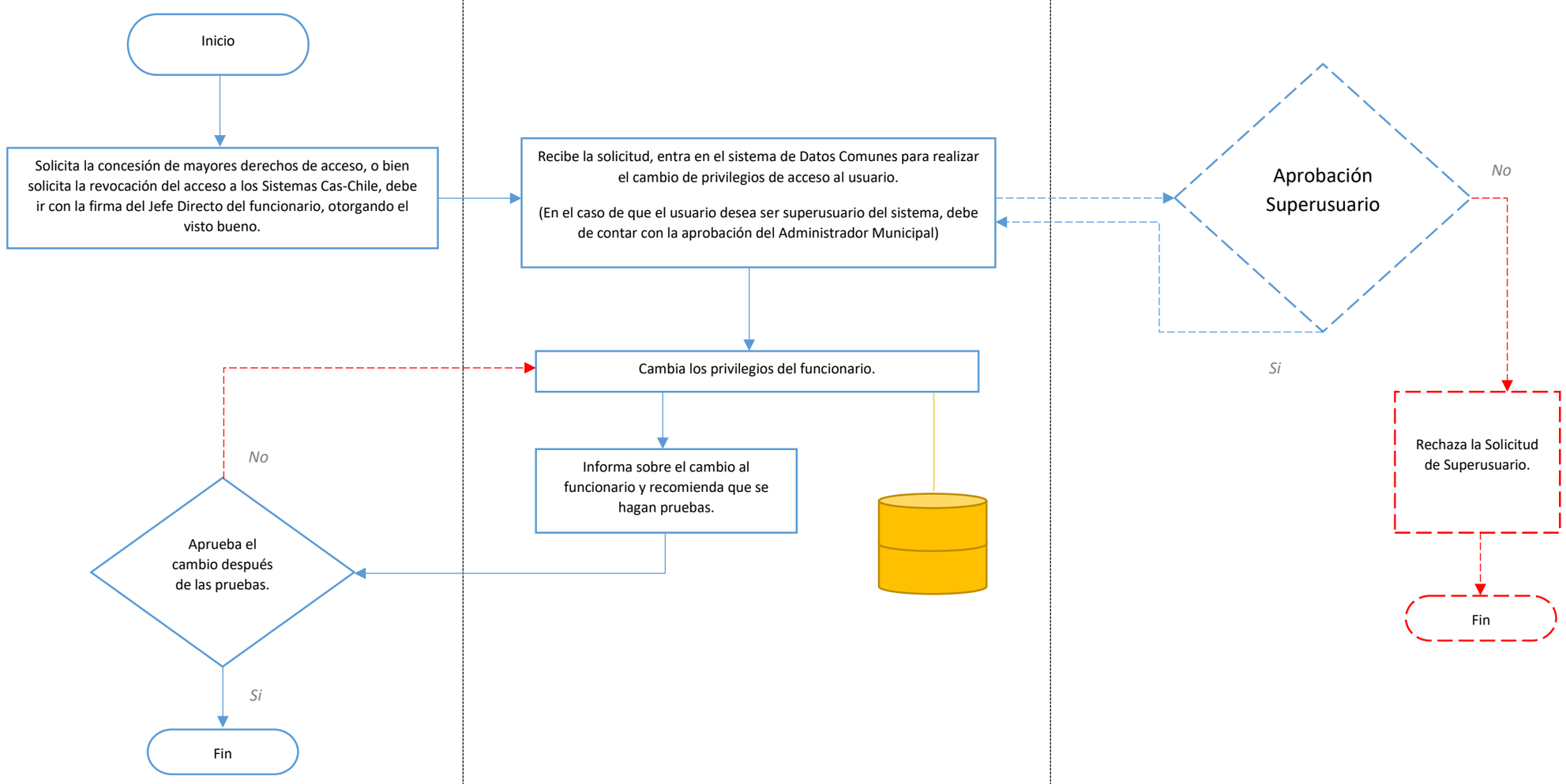
Diagrama de Flujo		
Responsables	Servidor Municipal	Computación
Proceso		

Notas	El respaldo de la información del servidor de las bases de datos, contempla 3 fases de respaldo: 1. Respalda la infomación 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.

Procedimiento INF-009: Modificación de derechos de acceso a Sistemas de Información

INF-009	
Nombre	Modificación de derechos de acceso a Sistemas 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.

Diagrama de Flujo

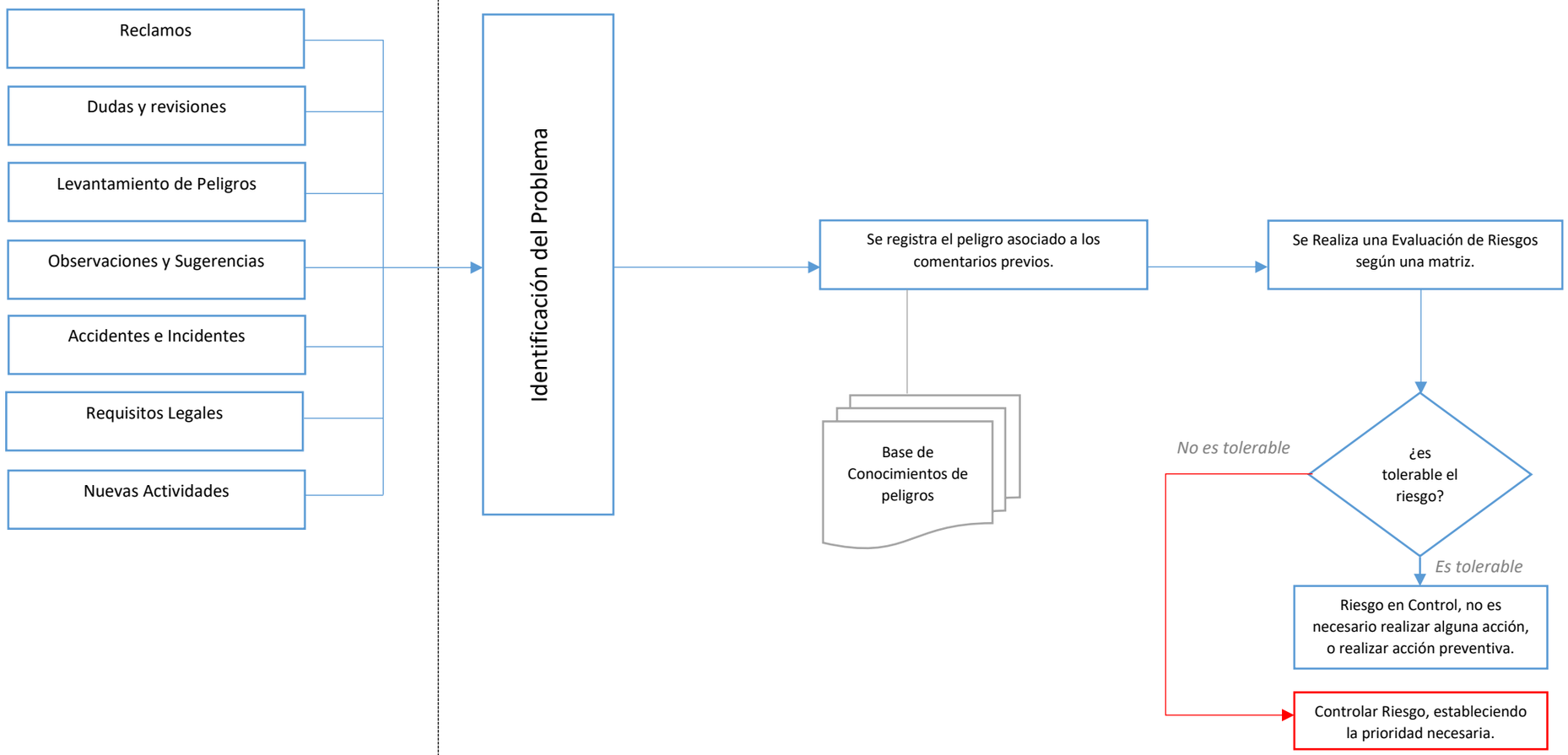
Responsables	Funcionario o Superior del mismo	Computación	Administrador Municipal
Proceso			

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. Despues del proceso de cambio, si el usuario aún no puede hacer su trabajo, se modifican de nuevo los niveles de derechos de acceso.

Procedimiento INF-010: Identificación de Peligros y Evaluación de Riesgos

INF-010	
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.

Diagrama de Flujo

Responsables	Funcionarios	Computación
Proceso		

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, evaluan si es un riesgo potencial o no ofrece riesgo la actividad en cuestión.

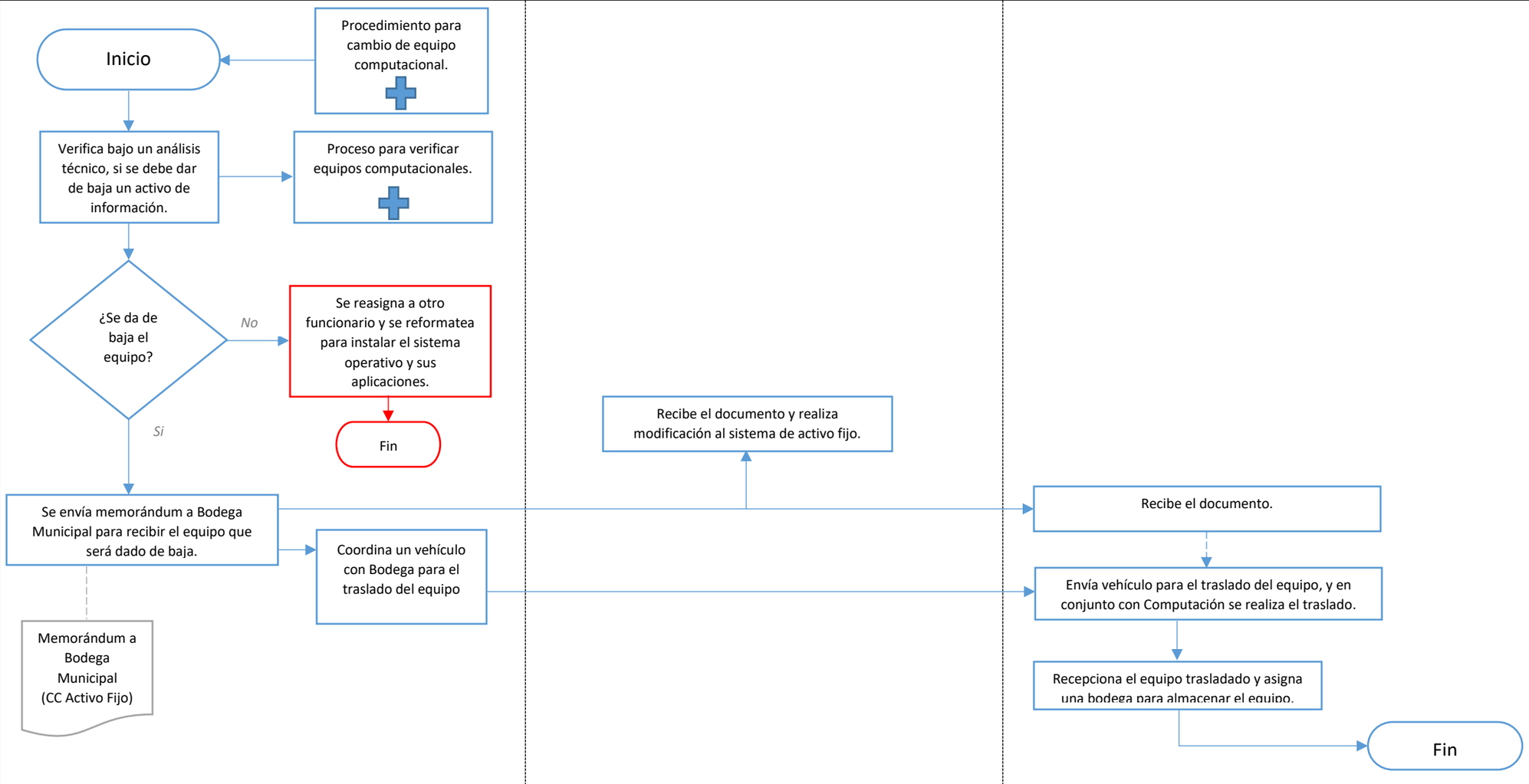
Procedimiento INF-011: Dar de Baja a Activos Fijos que contienen información

INF-011	
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.

Diagrama de Flujo

Responsables	Computación	Activo Fijo (DAF)	Bodega Municipal

Proceso



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 vehiculo para el traslado. • Que Bodega Municipal envíe el vehiculo para el traslado. Se realiza el traslado y Bodega asigna una de sus plazas para almacenar el equipo.

Procedimiento INF-012: Cambio o Actualización de Equipo Computacional

INF-012	
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.

Diagrama de Flujo (Fase 1 – Retiro de Equipo Computacional y Asignación de Nuevo Equipo)

Responsables	Funcionario	Computación	Administrador Municipal	Activo Fijo (DAF)
Proceso (Fase 1)				

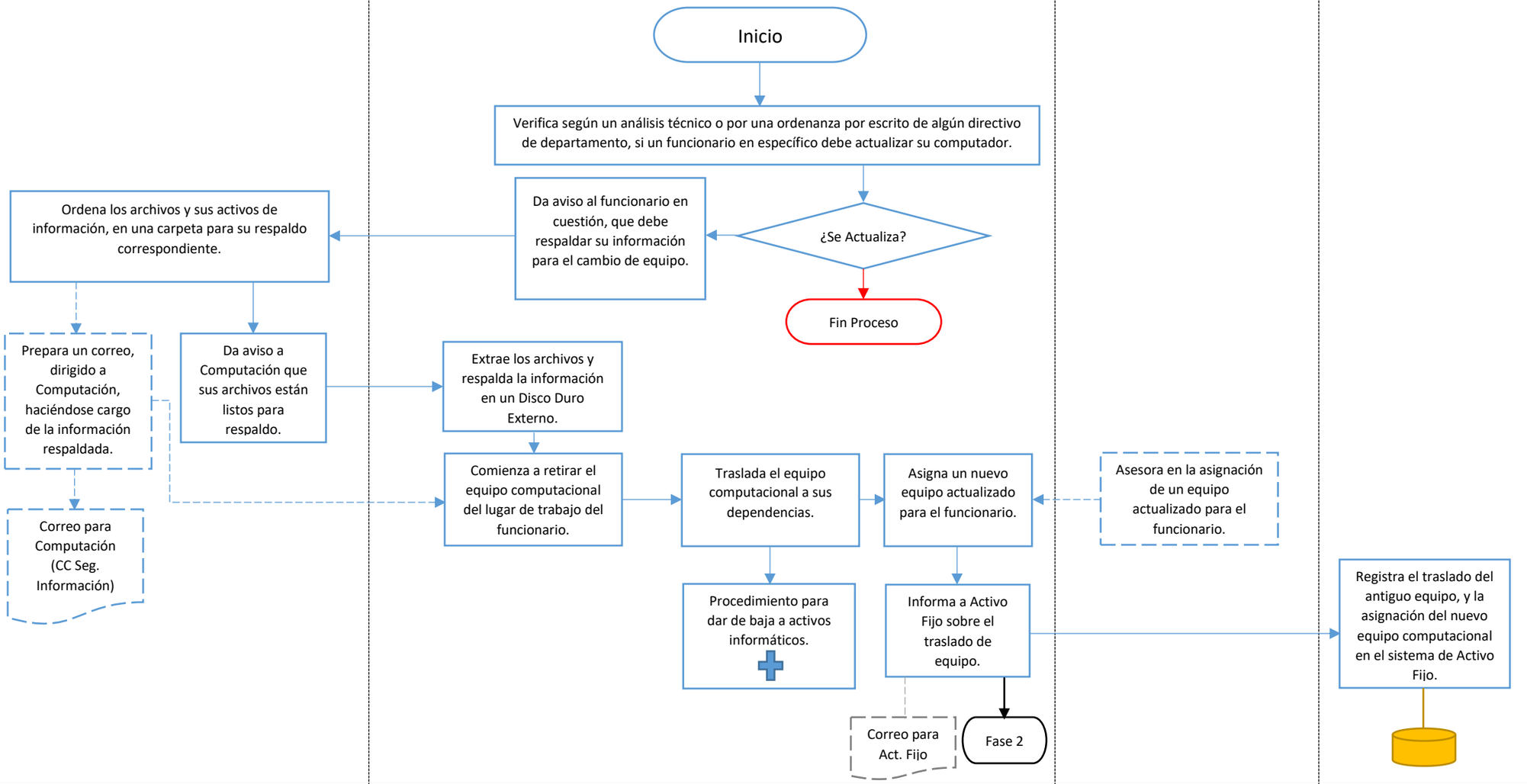
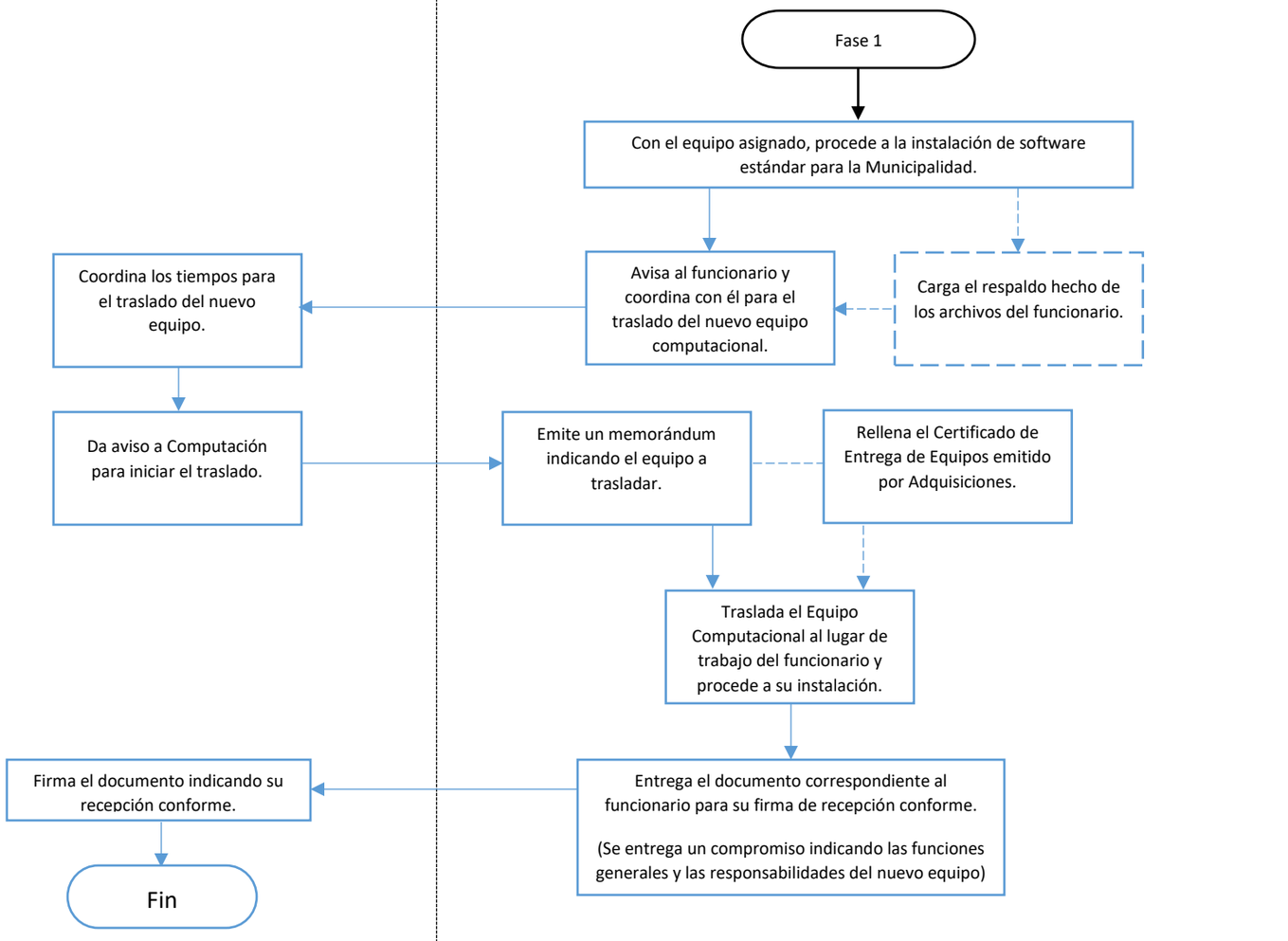


Diagrama de Flujo (Fase 2 – Instalación de Nuevo Equipo Computacional)

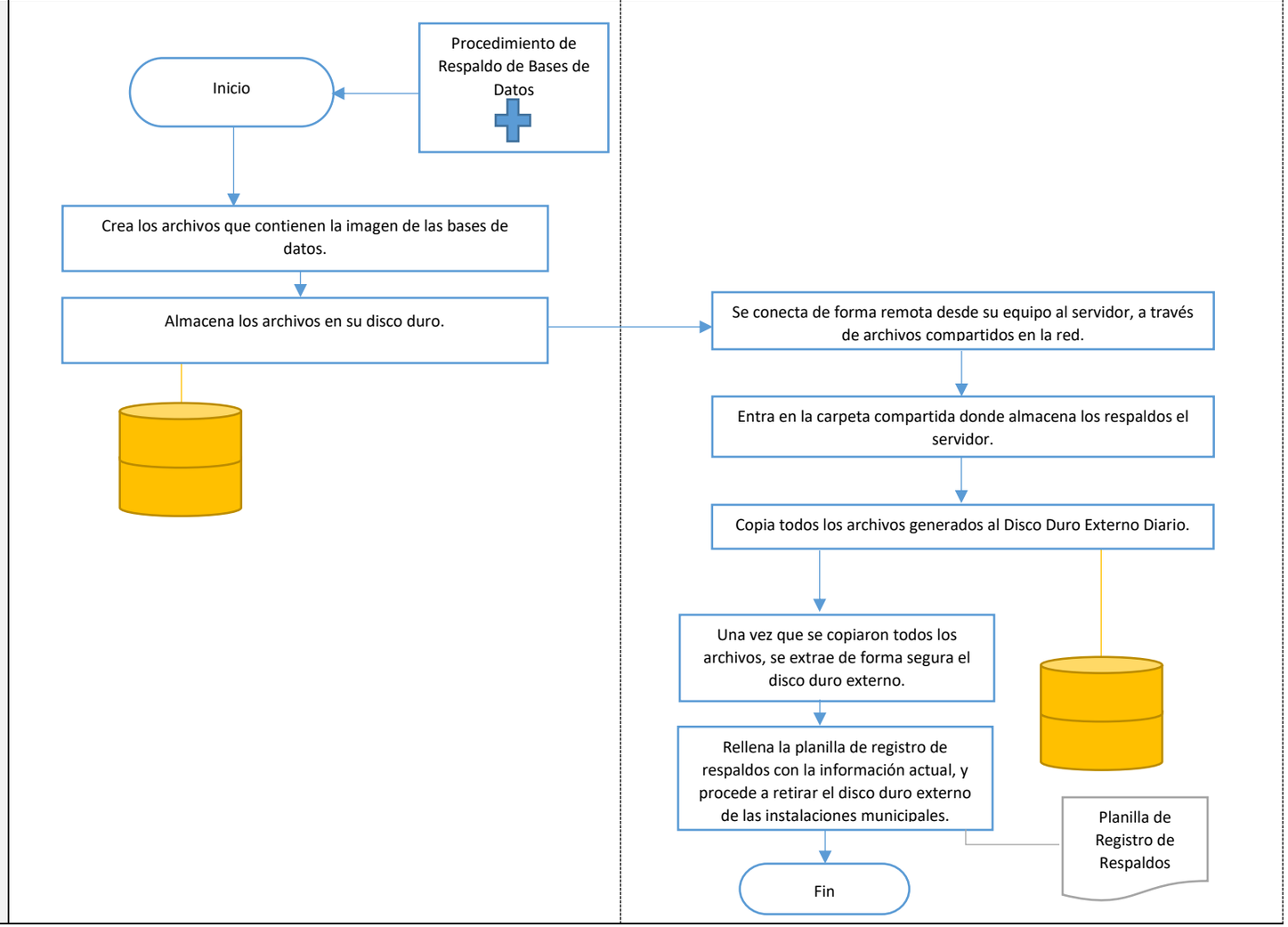
Responsables	Funcionario	Computación
Proceso (Fase 2)		



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 esta 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, asi como sus responsabilidades y funciones.

Procedimiento INF-013: Respaldo Diario a las Bases de Datos del Servidor

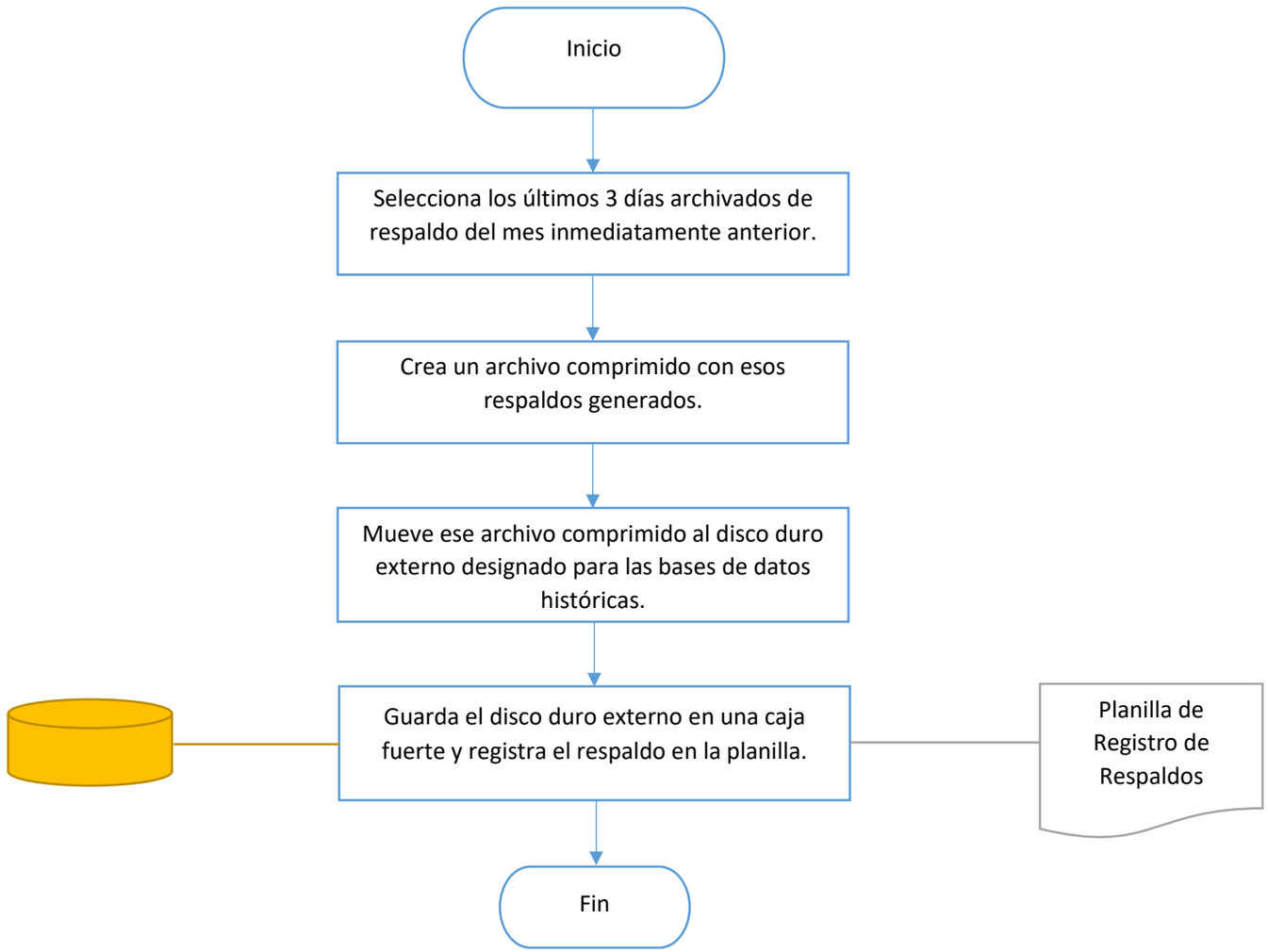
INF-013	
Nombre	Respaldo Diario a las Bases de Datos del Servidor
Alcance y Aplicación	Servidor Municipal, el que ejecuta el plan de mantenimiento para almacenar todos los respaldos de sus bases de datos. Computación, quien administra los respaldos en discos duros externos.
Descripción	Este procedimiento 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.

Diagrama de Flujo		
Responsables	Servidor Municipal (18:30 – 19:00 hrs.)	Computación
Proceso		

Notas	El servidor municipal realiza estos respaldos a las 18:30 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).

Procedimiento INF-014: Respaldo Histórico a las Bases de Datos del Servidor

INF-014	
Nombre	Respaldo Histórico 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 histórica y guardando un registro desde una fecha muy antigua a la actualidad, realizando registros mensuales de esta.
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.

Diagrama de Flujo	
Responsables	Computación
Proceso	

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 Despues 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.

Procedimiento INF-015: Gestión relacionada al Control de Cambios de Sistemas Informáticos

INF-015	
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.

Diagrama de Flujo (Fase 1 – Autorización del Cambio)

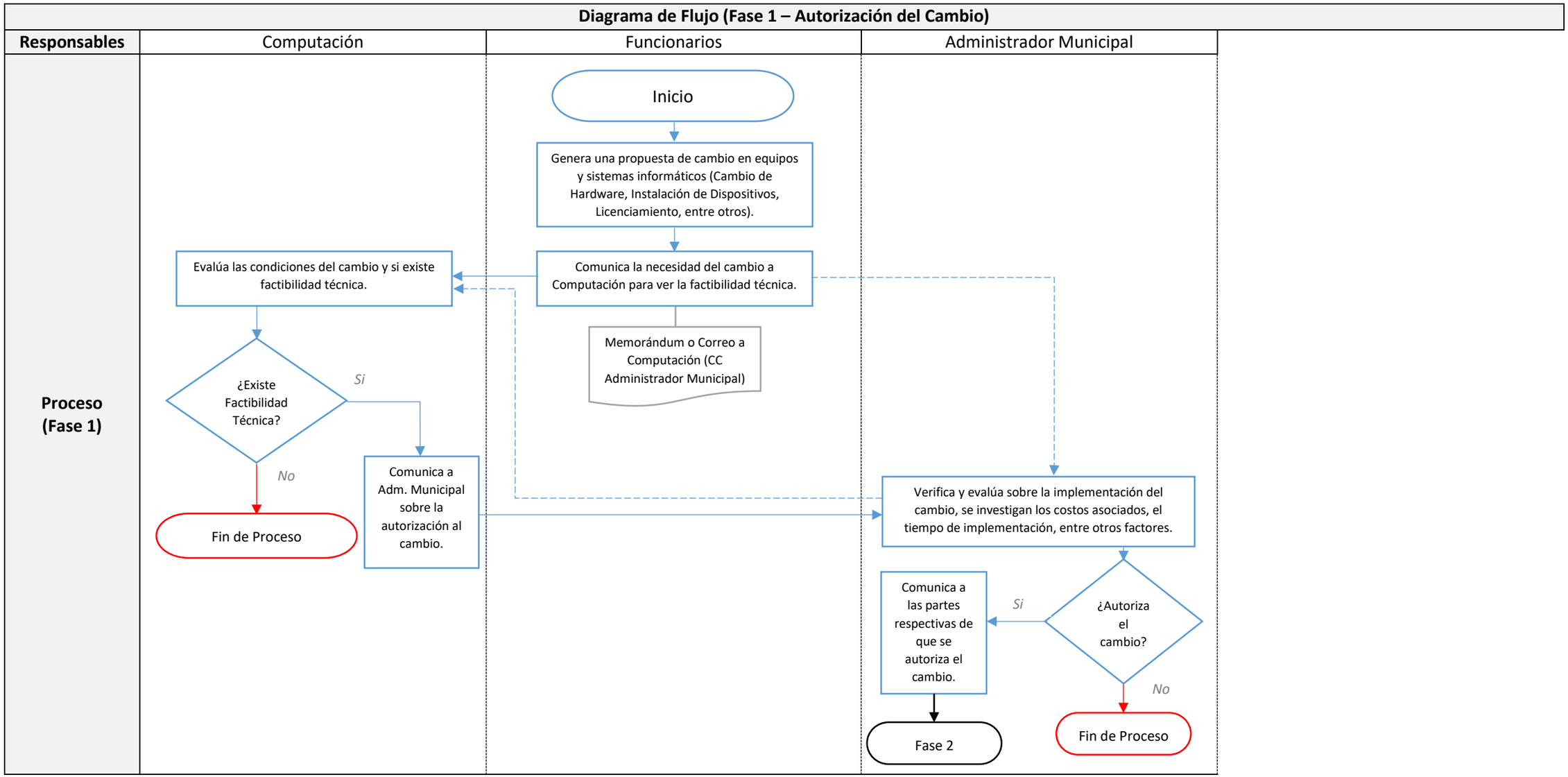
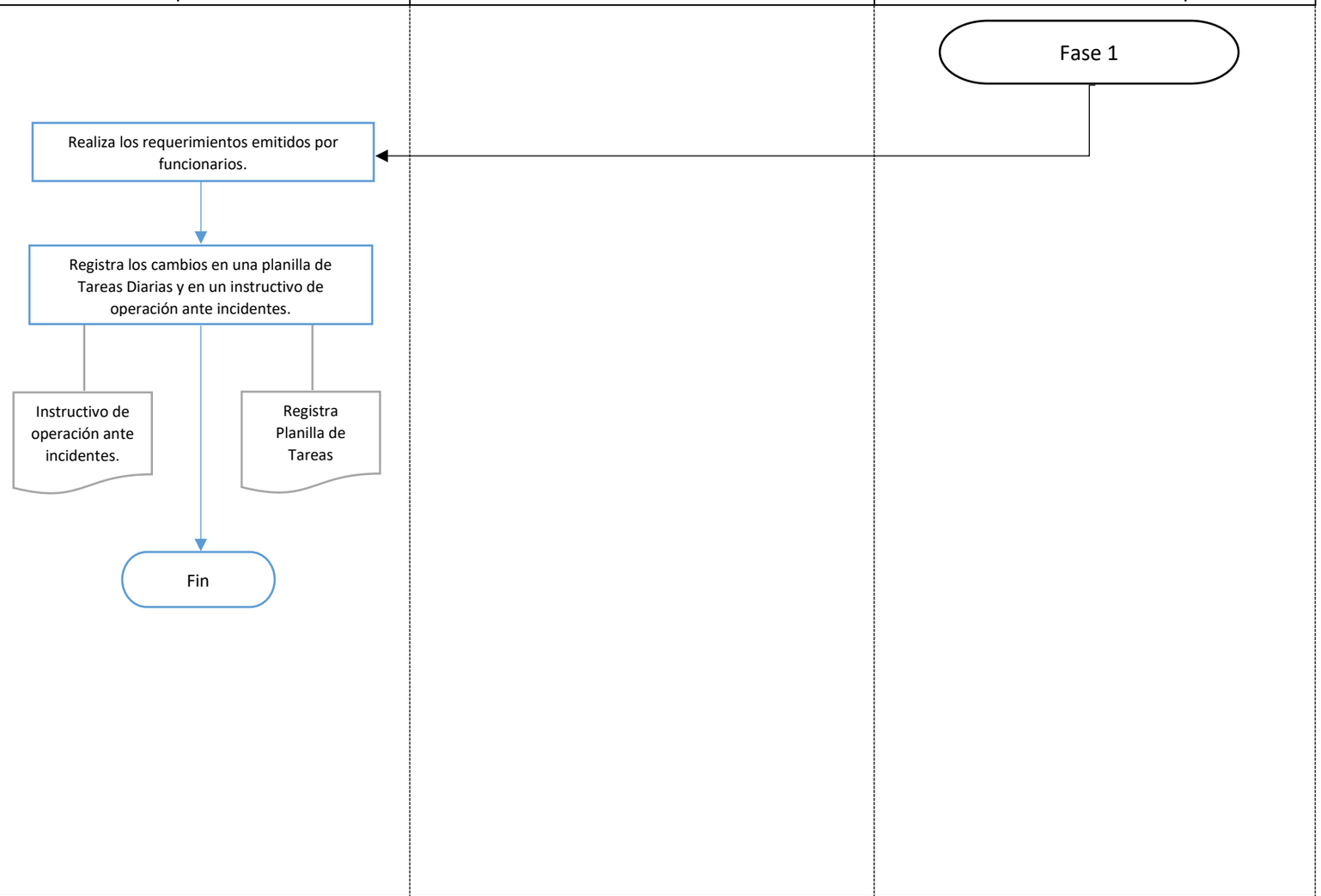


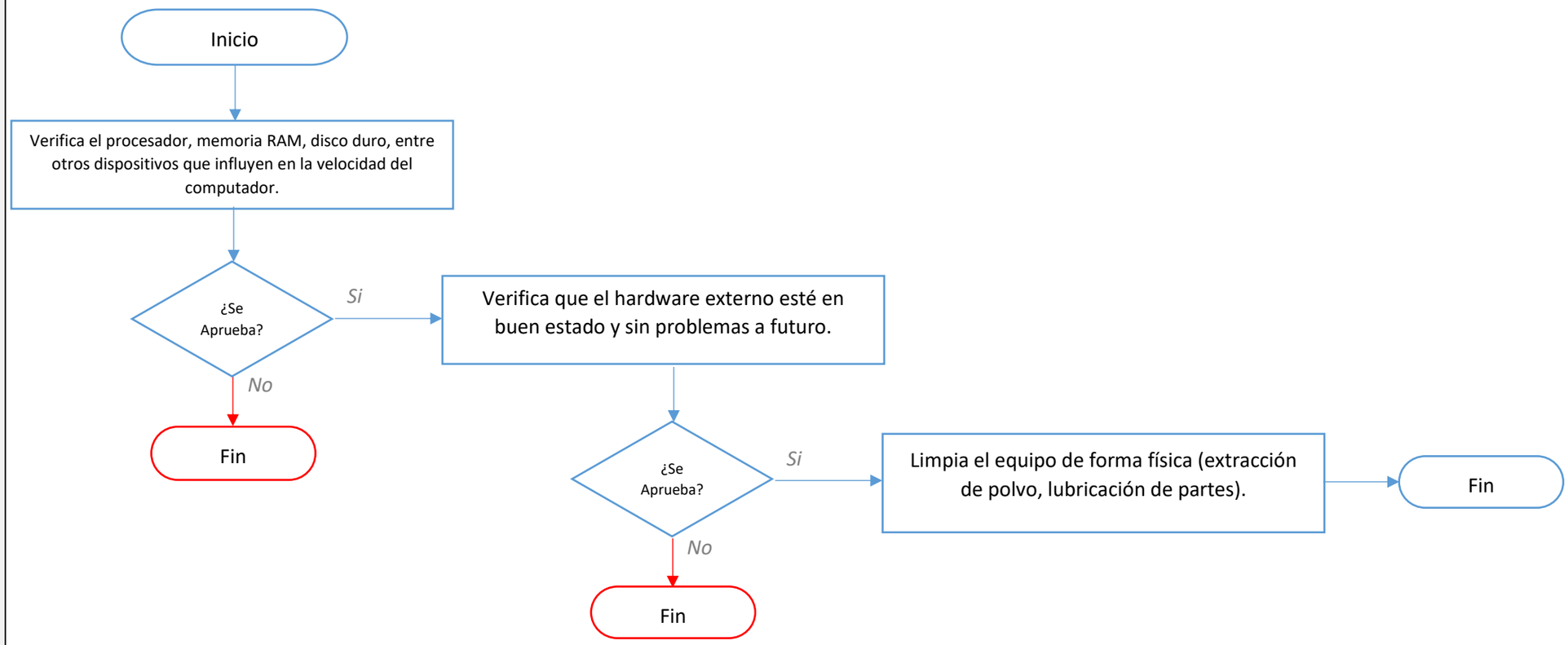
Diagrama de Flujo (Fase 2 – Implementación del Cambio)

Responsables	Computación	Funcionarios	Administrador Municipal
Proceso (Fase 2)			

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. Tambien en casos especiales, se realizarán instructivos sobre como afrontar casos más complicados y que llevan tiempo en arreglarse.

Procedimiento INF-016: Verificación Técnica de Equipo Informático

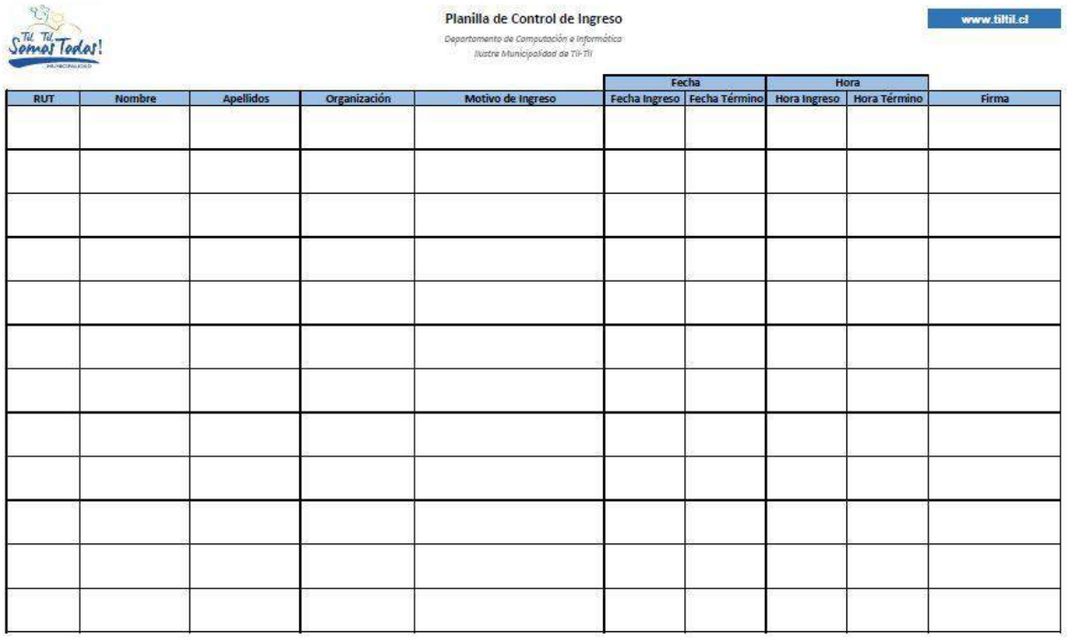
INF-016	
Nombre	Verificación Técnica de Equipo Informático
Alcance y Aplicación	Computadores que están incluidos en un proceso de cambio. Computación, quién verifica esos computadores.
Descripción	Este procedimiento cumple la función de exponer los detalles referentes a como se verifican los equipos 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.

Diagrama de Flujo	
Responsables	Computación
Proceso	

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). Despues de que todo se encuentra aprobado para seguir funcionando, se da emiezo a la limpieza y posterior mantenimiento del equipo computacional.

Anexos

Anexo 1: Planilla de Control de Ingreso



Planilla de Control de Ingreso

Departamento de Computación e Informática
Ilustre Municipalidad de Til-Til

www.tiltil.cl

RUT	Nombre	Apellidos	Organización	Motivo de Ingreso	Fecha		Hora		Firma
					Fecha Ingreso	Fecha Término	Hora Ingreso	Hora Término	

**: Cuenta con una versión digital mantenida por el Encargado de Seguridad de la Información.*

Anexo 2: Planilla de Registro de Respaldos

Planilla de Registro de Respaldos hechos al Servidor					
			Disco Duro de Respaldo		
Fecha	Tipo de Respaldo	Tablas de Base de Datos Respaldadas	N° Serie	Marca	Modelo

**: Planilla digital proporcionada para el Departamento de Computación*

Anexo 3: Planilla de Tareas Diarias

Planilla de Tareas Diarias				
Fecha	**Funcionario**	**Área**	**Cambio Realizado**	**Validación de Solución**

**: Planilla digital proporcionada para el Departamento de Computación*