DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

RESOLUCION EXENTA Nº 2516

SANTIAGO, 31 AGO 2016

VISTOS:

Las facultades que me confieren el Decreto Supremo Nº 674/2014 del Ministerio del Interior y Seguridad Pública; el artículo 24 letra o) de la Ley Nº 19.175; el DFL N° 29 de 2004 del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.834, Estatuto Administrativo; la Ley N° 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado; lo dispuesto en la Ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma; el Decreto N° 181/2002 que aprueba el Reglamento de la Ley N° 19.799; el Decreto Supremo N° 83/2005 del Ministerio Secretaría General de la Presidencia sobre seguridad y confidencialidad de los documentos electrónicos; la Resolución N° 1.600 de 2008 de la Contraloría General de la República; y

CONSIDERANDO:

1.- Que, se hace necesario contar con una normativa adecuada en materia de seguridad de activos de información, la cual vele por su integridad, confidencialidad y disponibilidad,

2.- Que, es afán de este Gobierno Regional dar fiel cumplimiento a la legislación vigente referente a seguridad de la información,

3.- Que, considerando que esta normativa se encuentra en el marco del Indicador Transversal de Seguridad de la Información del Programa de Mejoramiento de la Gestión PMG, el cual nos permite lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucional considerados relevantes, asegurando la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios / clientes / beneficiarios.

4.- Que, se debe desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.

5.- Que, para lo anterior, se debe incluir los requisitos para administrar claves criptográficas incluidas la generación, el almacenamiento, el archivo, la recuperación, la distribución, el retiro y la destrucción de claves,

RESUELVO:

1.- **APRUÉBESE** el **PROCEDIMIENTO DE GESTIÓN DE CLAVES**, el cual se adjunta y es parte constitutiva de la presente Resolución:

2.- **PUBLÍQUESE** un ejemplar de la presente Resolución en la Intranet Institucional.

ANÓTESE, REGÍSTRESE Y COMUNÍQUESE.

INTENDENCIA REGION METROPOLITANA

INTENDENTE

CLAUDIO ORREGO LARRAIN
INTENDENTE
REGION METROPOLITANA DE SANTIAGO

FF/GEP/MRT/SGA/CHM/JGG

Distribución:
Administración Regional
División de Administración y Finanzas
División de Análisis y Control de Gestión
División de Planificación y Desarrollo
Departamento de Gestión Institucional
Departamento de Informática
Oficina de Partes.

15873029

Procedimiento
en
Gestión de Claves

1 INDICE

2 OBJETIVO

Establecer las actividades necesarias para la gestión de derechos de acceso a los sistemas de información.

3 ALCANCE

Gobierno Regional Metropolitano de Santiago y Parque Lo Errazuriz

Este procedimiento es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencias) personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para el Gobierno Regional Metropolitano o el Parque Lo Errazuriz.

4 DESARROLLO DEL PROCEDIMIENTO

4.1 Responsabilidades

Jefatura de Unidad, Departamento o División.	• Autorizar el Ingreso de Nuevos Funcionarios y notificar • Solicitar la creación o eliminación de los accesos a los sistemas de información. • Notificar cualquier desvinculación de funcionarios
Funcionario designado del Departamento de Gestión de Personas.	• Solicitar los accesos a los sistemas de información. • Notificar cualquier desvinculación de funcionarios. • Recopilar y revisar los antecedentes mínimos para el inicio de tramites de ingreso y asignación de derechos de accesos provisorios.
Departamento de Informática	• Crear los accesos básicos a los nuevos funcionarios • Revisar y gestionar los permiso de accesos a los sistemas de información • Eliminar los derechos de accesos de los funcionarios que se desvinculan.
Encargado de Seguridad de la información	• Coordinar la Revisión de derechos de acceso de usuario.
Funcionarios	• Las responsabilidades de los funcionarios se describen en el punto 4.3

4.2 Registro de usuarios

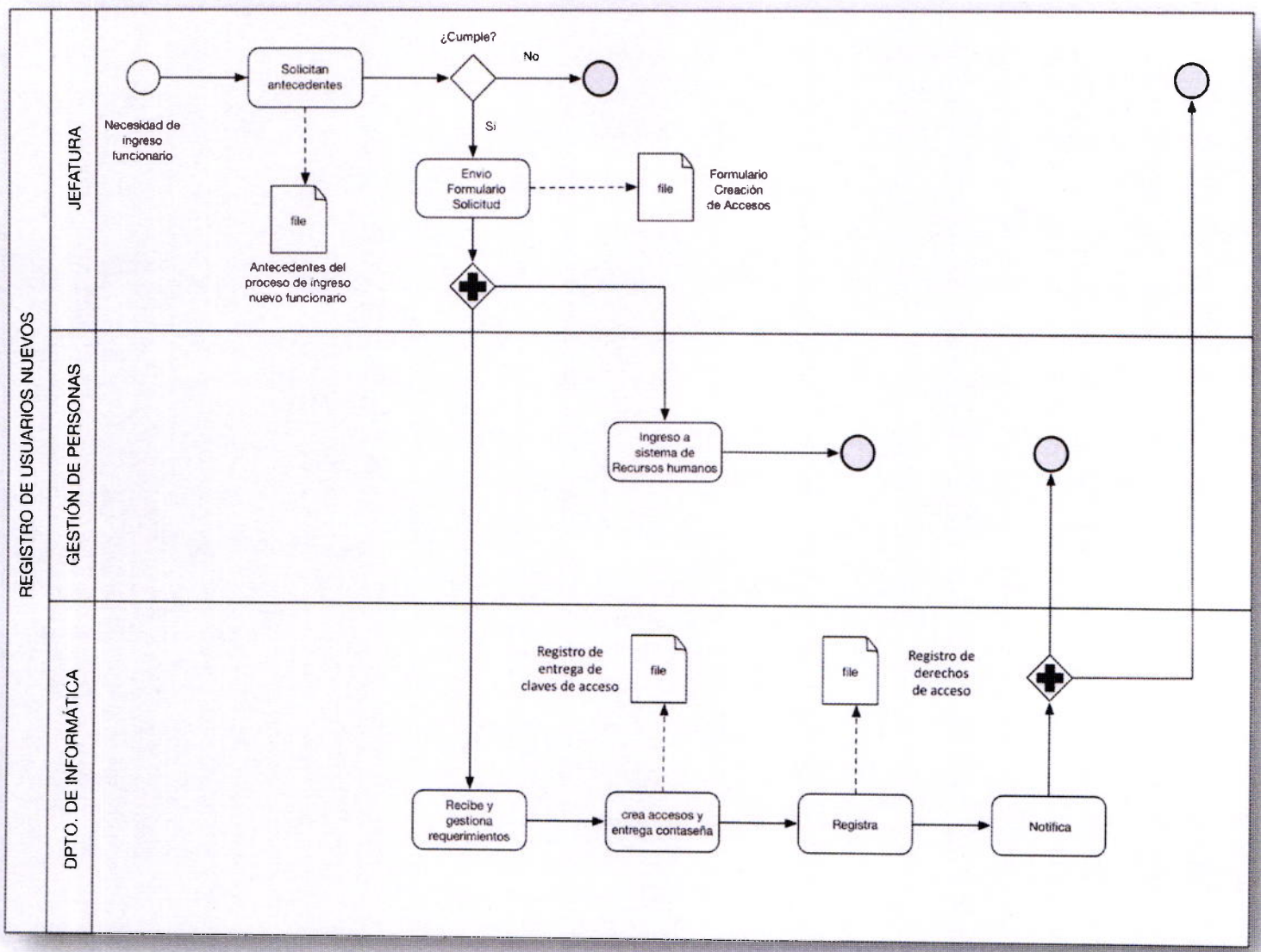
4.2.1 Consideraciones generales

En cualquier registro de usuarios se deben utilizar IDs únicos para permitir a los usuarios vincularse y ser responsables de sus acciones.

Es responsabilidad de los Administradores de Sistemas mantener un registro formal de todas las personas registradas para usar el servicio.

4.2.2 Registro de usuarios nuevos

La creación de los accesos de nuevos funcionarios (correo electrónico, active directory, estaciones de trabajo, acceso a sistemas), se debe realizar de acuerdo al siguiente flujo.



La Jefatura de la Unidad, Departamento o División es responsable de solicitar los accesos básicos para los nuevos funcionarios mediante el **Formulario de solicitud para creación / eliminación de accesos**[1]

La Unidad de Soporte del Departamento de Informática es responsable de la creación de los accesos básicos de ingreso, que incluye:

- Creación de correo Electrónico.
- Creación de usuario en Active directory
- Creación de usuario en sistemas necesarios
- Habilitación de estación de trabajo

La entrega de las contraseñas temporales de ingreso se realiza mediante el **Registro de entrega de claves de acceso**[2], que es firmado por el funcionario que recepciona, quedando una copia en poder de soporte y otra en poder del funcionario.

En el registro de entrega de claves de acceso se proporciona un enunciado con las responsabilidades implicadas en el uso de los sistemas de información del Gobierno regional Metropolitano[3].

Las condiciones de uso incluyen:

- Mantener confidenciales las claves secretas.
- Cumplir con lo establecido en las Políticas y Procedimientos del Sistema de Seguridad de la Información, en lodo lo que sea de su competencia.
- No divulgar información pertinente al Gobierno Regional Metropolitano.
- Entender la responsabilidad funcionaria , aún fuera de las dependencias de trabajo y fuera del horario normal de trabajo.

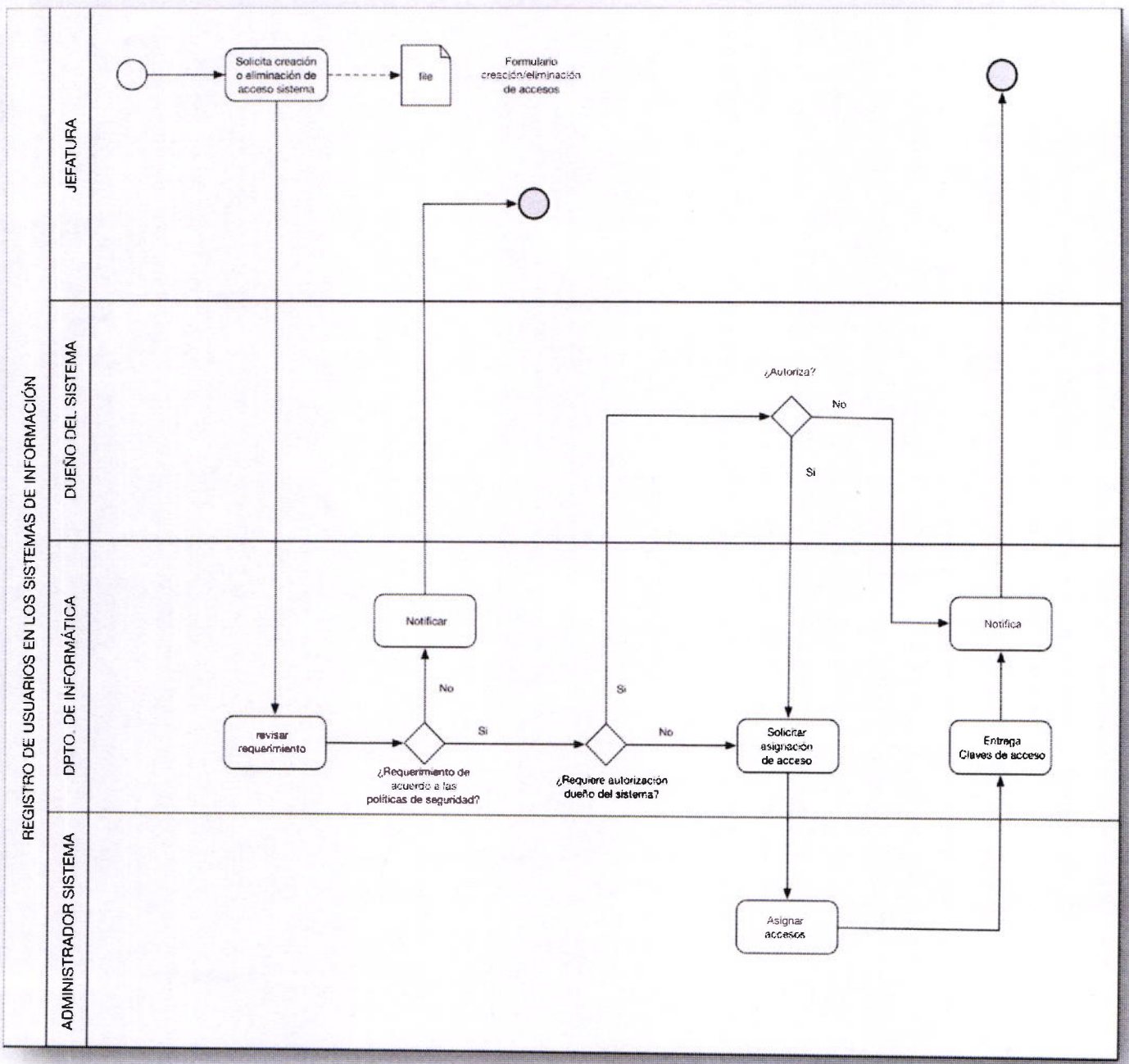
La creación de accesos se registra en la Planilla de **Registro de Derechos de Acceso**[4].

---

[1] Ver anexo 1 con formato de registro.
[2] Ver anexo 2 con formato de registro.
[3] Los requerimientos de seguridad para el uso de correo electrónico y la gestión de contraseñas, están definidos en la Norma de Uso Correo Electrónico, Norma de uso identificación y autentificación y la Norma de seguridad informática.
[4] Ver anexo 3 con formato de registro.

4.2.3 Registro de usuarios en los sistemas de información

La creación o eliminación de accesos a los sistemas de información se debe realizar de acuerdo al siguiente flujo:



La Jefatura de la Unidad, Departamento o División es responsable de solicitar la creación o eliminación de los accesos a los sistemas de Información mediante el **Formulario de solicitud de creación/eliminación de accesos** firmado.

El Departamento de Informática es responsable de chequear que el nivel de acceso solicitado es apropiado para el propósito institucional y que sea consistente con la Política(s) de Seguridad de la Organización.

En caso de ser necesario se debe solicitar la autorización de acceso del usuario a los sistemas, al propietario para su uso y/o acceso.

Las claves secretas temporales deben ser proporcionadas a los usuarios de una manera segura (ver 4.3).

4.3 Gestión de contraseñas del usuario

Es responsabilidad de todos los funcionarios cumplir con los siguientes requerimientos:

4.3.1 Características de contraseñas[5]

- Las contraseñas temporales deben ser proporcionadas a los usuarios de una manera segura, no se deben utilizar mensajes de correo electrónico de terceros o no protegidos (sin texto).
- Las contraseñas de acceso creadas por el usuario deben ser difíciles de adivinar por terceros y ser sólo de su conocimiento personal, quedando prohibida su divulgación, así como mantener anotada su clave de acceso en un lugar visible.
- Los sistemas de información deben validar la robustez de las contraseñas de tos usuarios.
- Las contraseñas de acceso de los usuarios deben contar con un archivo histórico, debidamente encriptado, con el objetivo de no permitir reutilizar una clave de acceso utilizada recientemente.
- Las contraseñas nunca deberían ser almacenadas de una forma desprotegida (ej. Contraseñas almacenadas en el navegador, post-it, cuadernos, etc.).
- Toda contraseña predeterminada por el vendedor debe ser cambiada después de la instalación de los sistemas o software.

4.3.2 Cambio de las contraseñas

- La contraseña temporal de una cuenta de usuario, se creará expirada, de modo de obligar su cambio durante el primer acceso.

- Los usuarios deben cambiar su contraseña de acceso con la frecuencia establecida por la Unidad de Soporte, como mínimo.
- Las contraseñas deben ser únicas para cada funcionario y deben cumplir, a lo menos, con los siguientes requisitos:
  - Debe contener 8 caracteres como mínimo.
  - No debe contener: los nombres o apellidos del funcionario, el user name o nombre de usuario, el nombre de la institución o unidad funcional.
  - No debe contener palabras completas.
  - Contener al menos un carácter de las siguientes categorías.

Categoría	Ejemplo
Letras Mayúsculas	A, B, C
Letras Minúsculas	A, b, c
Números	0,1,2,3,4,5,6,7,8,9
Símbolos	", -, %, $, ¡, ¿.....

Ejemplo de Contraseña segura: **"J0Ab77c3**

4.3.3 Intentos Fallidos

- El número de intentos erróneos de acceso a una cuenta, debe estar limitado según se indique en el estándar definido por la Unidad de Soporte del Departamento de Informática.
- De cumplirse el número de intentos fallidos definido, la cuenta debe quedar bloqueada, siendo los únicos autorizados para su desbloqueo la Unidad de Soporte del Departamento de Informática.
- Toda reasignación de contraseña debe ser solicitada por el Jefe directo del usuario titular de la cuenta mediante correo electrónico.

4.4 Revisión de derechos de acceso de usuarios5

La administración de los perfiles radica en los Usuarios Encargados de los sistemas de información y las jefaturas de División correspondiente.

Para administrar los accesos a los sistemas de información se definirán perfiles de acceso asignables a grupos de usuarios que, por su responsabilidad en la organización, presenten necesidades de accesos equivalentes.

- El Encargado de Seguridad de la información es responsable de que se efectúe la revisión de los derechos de acceso de acuerdo a los siguientes lineamientos:
- Se debe revisar los derechos de acceso de los usuarios cada seis meses.
- Las autorizaciones para derechos de acceso con privilegios especiales se deben revisar a intervalos de tres meses.
- Se debe chequear la asignación de privilegios para asegurar que no se hayan obtenido privilegios no autorizados.
- Chequeo de IDs de usuario y cuentas redundantes.
- Revisión después de cualquier cambio, como un ascenso, democión o termino de contrato.

Los Usuarios Encargados de alguna aplicación deben revisar en forma periódica los perfiles de usuarios del personal vigente y solicitar al Jefe del Departamento de Informática la actualización de éstos cada vez que ocurra un cambio en la definición de funciones.

[5]Los requerimientos de seguridad para la gestión de derechos de acceso, están definidos en Norma de acceso físico y el Instructivo de Autorización y Control para Instalaciones.

4.5 Eliminación de derechos

La Jefatura del Área involucrada es responsable de informar cualquier desvinculación de funcionarios mediante el Formulario de solicitud para creación/eliminación de accesos.

Esta notificación debe ser enviada en simultáneamente a:

- Departamento de Gestión de Personas.
- Departamento de Informática.

Ante el informe de desvinculación de algún funcionario, el Departamento de Informática es responsable de gestionar la recuperación de los activos asignados al funcionario. Entre otros, se encuentran:

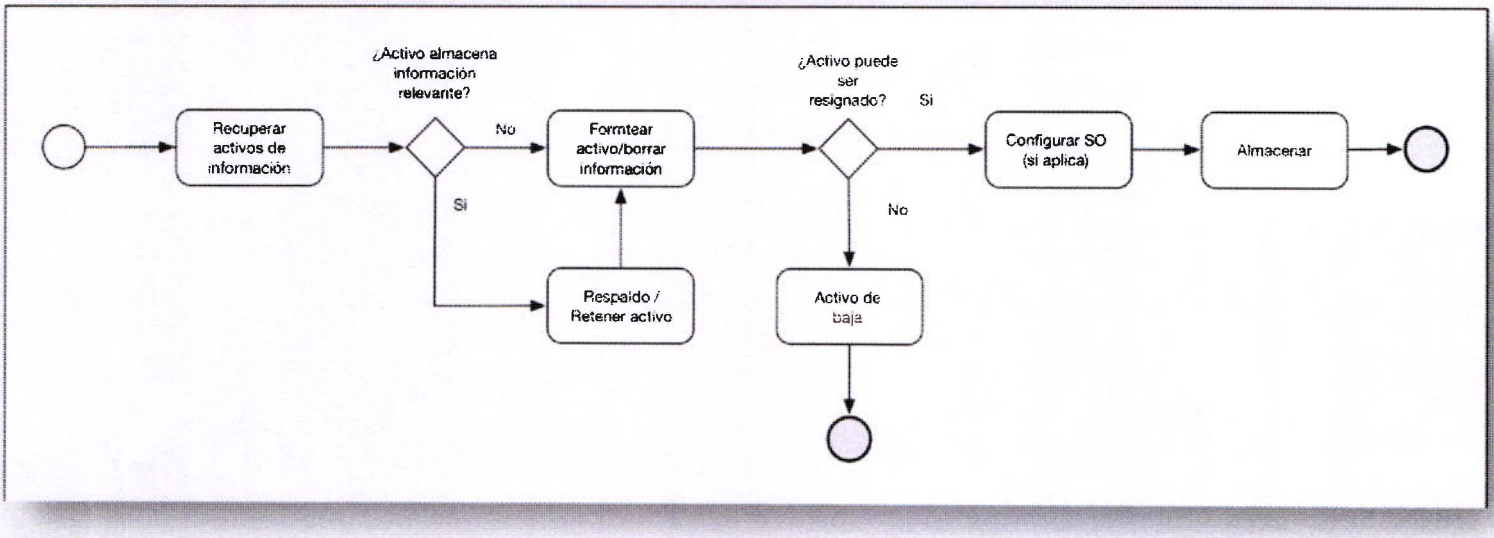
- Equipamiento
- Teléfonos móviles
- Tablets
- Pendrives
- Notebook
- Tarjetas de Acceso

Los activos recuperados deben ser informados a la Unidad de Inventario del Departamento de Servicios Generales.

El Departamento de Informática es responsable de eliminar los derechos de acceso a los sistemas de información (cambio de contraseñas , eliminación de usuario según sea requerido). junto con recuperar los activos de información asignados al funcionario . Entre otros, se encuentran:

- Discos Duros.
- CD - DVD de respaldos .
- Software.
- Manuales.
- Cualquier Información almacenada en medios electrónicos.

La recuperación de activos de información se realizara de acuerdo al siguiente modelo:



5 DOCUMENTOS APLICABLES O RELACIONADOS[6]

- Norma de Eliminación, reutilización y devolución de activos de información.
- Norma de Escritorio Limpio
- Norma de Uso para los Equipos Tecnológicos Portátiles
- Normas de seguridad informática

[6] Las normas o procedimientos referenciados pueden ser consultadas en la intranet institucional https://intranet.gobiernosantiago.cl

6 CONTROL DE REGISTRO

Identificación	Almacenamiento	Protección	Recuperación	Retención	Disposición
Formulario de solicitud para creación/eliminación de accesos	\\10.13.10.91\SSI	Carpeta con segregación de privilegios	Fecha	5 años	Destrucción
Registro de entrega de claves de acceso	\\10.13.10.91\SSI	Carpeta con segregación de privilegios	Fecha	5 años	Destrucción
Registro de derechos de acceso	\\10.13.10.91\SSI	Carpeta con segregación de privilegios	Fecha	5 años	Destrucción

7 INDICADORES

Formula de Calculo	Periodo de cálculo del indicador	Evidencia	Supuestos	Notas
(Nº de contrataciones personal nuevo con acceso correctamente concedido / Nº total de contrataciones en el periodo_t)*100	1 mes	Procedimiento Gestión de claves Registro de ingreso Departamento de Gestión de personas Registro de derechos de acceso	Que existan contrataciones en el periodo	En el registro de derechos de acceso se deben registrar los accesos correctamente concedidos
(Nº de desvinculaciones con control aplicado / Nº total de desvinculaciones del periodo_t)*100	1 mes	Procedimiento Gestión de claves Registro de ingreso Departamento de Gestión de personas Registro de derechos de acceso	Que existan desvinculaciones en el periodo	En el registro de derechos de acceso se deben registrar los accesos correctamente eliminados

8 REVISIÓN

El siguiente Procedimiento será revisado, evaluado y/o actualizado según corresponda una vez al año por el Comité de Seguridad de la Información, en cuanto a su funcionamiento y correcta aplicación en la Institución.

9 DIFUSIÓN

El presente documento será difundido a través de correo electrónico a todo el personal del Servicio, así como también una copia de éste será publicada en la intranet Institucional.

10 APROBACIÓN

Elaborado por	Revisado por	Aprobado por
Carlos Hernández A. Analista Departamento de Informática	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI	Presidente Comité de Seguridad
	Paulo Mendoza R. Encargado Unidad de Soporte	
	Carolina Hidalgo M. Jefa Departamento de Gestión Institucional	

11 ANEXOS

ANEXO 1: Formulario de solicitud para la creación de accesos

Formulario de Solicitud para creación/eliminación de accesos

1.- Tipo de Solicitud

Creación de Usuario	
Acceso de Sistemas	
Eliminación de accesos	

Fecha Solicitud	

2.- Jefatura que solicita:

Nombre Completo	
Depto. o Unidad	
Correo Electronico	

3.- Identificación del Funcionario

Nombre Completo	
RUT	
División y Departamento	
Calidad Jurídica	
Fecha de Ingreso a la Institución	

4.- Sistema(s) a los que se solicita acceso / eliminación

1	
2	
3	
4	

_____

Firma Jefatura que solicita

ANEXO 2: Registro de entrega de claves de acceso:

Entrega de Claves de acceso a Sistemas

Santiago XX de XXXX de 20XX se hace entrega de claves de acceso a los sistemas de Active Directory, Correo Electrónico y Sistemas de Información del Gobierno Regional Metropolitano al Usuario XXXX XXXX XXXX XXXX.

1.- Active Directory.

Usuario	
Password	

Esta clave será transitoria y después de instalado el equipo, el usuario **deberá cambiarla** mediante la solicitud que se le generara en el primer inicio de sesión.

2.- Correo Electrónico

Se encuentra habilitado el servicio de webmail http://mail.gobiernosantiago.cl

Usuario	jperez@gobiernosantiago.cl
Password	**3TYj8k47**

Esta podrá ser cambiada por el usuario desde el wabmail, esta clave funciona en directa relación con configuraciones de Equipos Celulares, Tablets, Notebooks, Outlook. **Si cambia la contraseña deberá cambiarla también en los respectivos dispositivos en que la tenga configurada.**

3.- Seguridad en el uso de los sistemas

Las condiciones de uso del equipamiento y sistemas de información implican las siguientes responsabilidades:

- Mantener confidenciales las claves secretas.
- Cumplir con lo establecido en las Políticas y procedimientos del Sistema de Segundad de la Información, en todo lo que sea de su competencia.
- No divulgar información pertinente al Gobierno Regional Metropolitano.
- Entender la responsabilidad funcionaria aún fuera de los dependencias de trabajo y fuera del horario normal de trabajo.

En la Intranet institucional se encuentran disponibles, las políticas, normas y procedimientos de seguridad en el uso de estos Sistemas de Información. http://intranet.gobiernosantiago.cl

Solicitado por XXXXXXX XXXXXXXX

Técnico: XXXXXXX XXXXXXX XXXXX

Fecha de Instalación: xx/xx/xxxx

ANEXO 3: Registro de derechos de acceso:

Tipo Acceso	Solicitado por	funcionario	Fecha	Sistema o carpeta	Usuario	Nivel de acceso	Grupo de acceso	Ip usuario	Técnico autoriza
carpeta	Juan Pérez	Matias Hernández	13/07/2016	RRHH	mhernandez	administrador	administradores	172.16.0.16	pmendoza
sistema	Roberto Olea	Pablo Espinoza	16/07/2016	\\172.16.0.20\tesoreria	pespinoza	lectura	Tesorería_lectura	172.16.067	cramirez