Gobierno de Chile

MINISTERIO DE SALUD
GABINETE DE LA MINISTRA
FGV.JVC / SML/ EAR/RGI/SZV

JEFE GABINETE V°B°

APRUEBA PROCEDIMIENTOS ESPECÍFICOS PARA LA SEGURIDAD DE LA INFORMACIÓN.

EXENTA N° 1566 /

SANTIAGO, 28 DIC. 2016

VISTOS: Lo dispuesto en la ley N° 19.880 que establece Bases de los Procedimientos Administrativos; en el D.F.L N°1, de 2005, del Ministerio de Salud, que fija el texto refundido, coordinado y sistematizado del decreto ley N° 2763, de 1979 y las leyes N° 18.933 y N°18.469; en el decreto supremo N° 136, de 2004, del Ministerio de Salud, que aprueba Reglamento Orgánico del Ministerio de Salud; en la ley N° 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; la ley 19.628 sobre protección a la vida privada; la ley 20.584 sobre derechos y deberes del paciente; el D.S N° 83, de 2004, del Ministerio Secretaria General de la Presidencia, que aprueba Norma Técnica para Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; en la ley N° 19.233 sobre delitos informáticos; en la Norma Chilena NCh-ISO 27001.0f2009 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos; en el Memorándum A22 N°10 de 16 de noviembre de 2016 de la Jefa de Departamento Gestión Sectorial de TIC; Resolución Exenta N°1161 de 04 de octubre de 2016, conjunta del Subsecretario de Salud Pública y Subsecretario de Redes Asistenciales que aprueba nuevo sistema de seguridad de la información, la Resolución Exenta N°1332 de 14 de noviembre de 2016 que aprueba la Política General de Seguridad de la Información, la Resolución N° 1.600, de 2008, de la Contraloría General de la República; y

CONSIDERANDO:

1°.- Que, las nuevas tecnologías de la información y de las comunicaciones (TIC) al ser incorporadas progresivamente a los procesos institucionales y al quehacer personal de los funcionarios al ejercer sus labores en el Ministerio de Salud, presentan una serie de beneficios, ventajas y oportunidades de diversa índole, pero conlleva también ciertos riesgos, que pueden afectar a los activos de información institucional.

2°.- Que, se oficializó la norma técnica sobre seguridad y confidencialidad del documento electrónico para los órganos de la Administración del Estado a través del Decreto Supremo N°83 de 2004, del Ministerio Secretaria General de la Presidencia.

3°.- Que, por consiguiente, gestionar la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental existente, tales como: Ley N° 19.799, 2002 sobre documentos electrónicos, firma electrónica y servicios de certificación de firma del Ministerio de economía Fomento y Reconstrucción, Ley N° 19.628, de 1999 sobre protección a la vida privada y datos personales del Ministerio Secretaría General de la Presidencia, Ley N° 19.223, de 1993 sobre delitos informáticos del Ministerio de Justicia, entre otras, con el firme propósito de lograr la protección de los activos relevantes de información y con ello la protección de los derechos de las personas.

4°.- Que, asimismo, el imperativo indicado en el numeral anterior, consiste básicamente o se traduce, entre otras cosas, en la realización de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine, basándose para ello en metodologías y técnicas estándares en estas materias, con el firme propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo, que permita lograr niveles de integridad, confidencialidad y disponibilidad, con todos sus activos de información relevantes para la institución, como un principio clave en la gestión de procesos.

5°.- Que la seguridad de la información es un tema de suma relevancia para el Ministerio, habida cuenta de la información personal sensible que maneja, existe la necesidad de contar con protocolos claros y exigentes dentro de la organización, que definan los lineamientos y prácticas que deben ser adoptado, siendo una prioridad ministerial, basada en los principios de confidencialidad, integridad y disponibilidad de la información.

6°.- Que internamente han existido procedimientos y políticas anteriores del Ministerio y que en su afán de mejora continua, es necesario modernizar y reemplazar.

7°.- Que, debido a la implementación del sistema de seguridad de la información en conjunto por la Subsecretaría de Redes se ha aprobado por Resolución Exenta N°1332 de 14 de noviembre de 2016 la Política General de Seguridad de la Información.

8°.- Que, en ese contexto se procede a actualizar los procedimientos para la gestión de los derechos de acceso y devolución de activos y el procedimiento monitoreo del uso de los medios de procesamiento de información, y teniendo presente lo anterior, se aprueba la siguiente,

RESOLUCIÓN:

1° APRUÉBENSE los siguientes procedimientos específicos de seguridad de la información de la Subsecretaría de Redes Asistenciales y de la Subsecretaría de Salud Pública, del Ministerio de Salud, cuyos textos se incorporan a la presente Resolución como anexos:

1. Procedimiento para la gestión de los derechos de acceso y devolución de activos.
2. Procedimiento monitoreo del uso de los medios de procesamiento de información

2° ESTABLÉSCAZE la obligación de la División de Tecnologías de la Información del Ministerio de Salud, de difundir la presente política y velar por su estricto cumplimiento.

3° INSTRÚYANSE al Jefe de la División de Tecnologías de Información y Comunicaciones y a los Encargados de Seguridad de la Información que realicen las acciones tendientes a la implementación de la presente Política, en materias de su competencia.

4° DÉJESE SIN EFECTO el procedimiento para la gestión de los derechos de acceso y devolución de activos, aprobado por Resolución 780 de 14 de octubre de 2014 y el procedimiento monitoreo del uso de los medios de procesamiento de información aprobado por Resolución 1124 de 22 de diciembre de 2014.

ANÓTESE Y COMUNÍQUESE.

MINISTERIO DE SALUD SUBSECRETARIA DE REDES ASISTENCIALES

DRA. GISELA ALARCÓN ROJAS
SUBSECRETARIA DE REDES ASISTENCIALES

REPUBLICA DE CHILE SUBSECRETARIA DE SALUD PUBLICA MINISTERIO DE SALUD

DR. JAIME BURROWS OYARZÚN
SUBSECRETARIO DE SALUD PÚBLICA

Distribución:
- Jefe de Gabinete Ministra.
- Gabinete Ministra de Salud.
- Jefe de Gabinete Subsecretaría de Redes Asistenciales.
- Jefe de Gabinete Subsecretaría de Salud Pública.
- Jefes de División Subsecretaría de Salud Pública.
- Jefes de División Subsecretaría de Redes Asistenciales.
- Secretarios Regionales Ministeriales de Salud.
- División Jurídica.
- Departamento de Tecnologías de Información y Comunicaciones.
- Oficina de partes.

Contenido

1 PROPÓSITO 1
2 ALCANCE 1
3 TERMINOLOGÍA 2
4 DOCUMENTOS APLICABLES 2
5 ROLES Y RESPONSABILIDADES 2
6 PROCEDIMIENTO 3
6.1 Registro de usuarios 3
6.2 Eliminación o ajuste de los derechos de acceso 7
6.3 Responsabilidades en la desvinculación o cambio de empleo 9
6.4 Gestión de derechos de acceso privilegiados 10
6.5 Revisión de los derechos de acceso de usuario 10
7 REGISTROS 10
8 DIFUSION 11
9 REVISION Y MEDICION 11
10 CONTROL DE VERSIONES 11

1 PROPÓSITO

Establecer las actividades necesarias para la gestión de derechos de accesos a la información por parte de los usuarios, a través de los sistemas, junto a la devolución de activos de la organización.

Administrar el ciclo de vida de los usuarios desde la creación de las cuentas, roles y permisos necesarios, hasta su inoperancia, todo ello a partir de los requerimientos reportados por el Departamento de Gestión de Personas y/o directamente de su Jefatura directa. Lo anterior para que el funcionario tenga acceso adecuado a los sistemas de información y recursos tecnológicos, validando su autenticación, perfiles, autorización y auditoría.

2 ALCANCE

Subsecretarías de Salud Pública y de Redes Asistenciales.

Este procedimiento es aplicable a todos los funcionarios[1] (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores a través del procedimiento de compra de servicios, etc.) que presten servicios para las Subsecretarías de Salud Pública y de Redes Asistenciales y que tengan derechos de acceso a la información que puedan afectar los activos de información del Ministerio de Salud.

Esta política abarca los siguientes controles definidos en la norma NCh-ISO 27001.Of2013:

- A.07.03.01 Responsabilidades en la desvinculación o cambio de empleo
- A.08.01.04 Devolución de activos
- A.09.02.01 Registro y cancelación de registro de usuario

[1] A lo largo del procedimiento cada vez que se mencione funcionario se refiere a: funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.).

- A.09.02.03 Gestión de derechos de acceso privilegiados
- A.09.02.04 Gestión de información secreta de autenticación de usuarios
- A.09.02.05 Revisión de los derechos de acceso de usuario
- A.09.02.06 Eliminación o ajuste de los derechos de acceso

3 TERMINOLOGÍA

MINSAL: Ministerio de Salud.
SGSI: Sistema de Gestión de Seguridad de Información.

4 DOCUMENTOS APLICABLES

- NCh-ISO27001.Of2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
- Ley 20.285 regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la Administración del Estado.
- Ley 19.628 de Protección de vida privada y datos.
- Ley 19.223 de Delitos informáticos.
- Ley 19.927 de Delitos de Pornografía Infantil.
- Política de seguridad en la identificación y autenticación de usuarios.
- Procedimiento de Eliminación Segura o Reutilización de Equipos.
- Procedimiento para la validación de requisitos de ingreso.
- Política de Seguridad para el control de acceso.
- Política de Seguridad para las relaciones con los proveedores.
- Política uso de internet.

5 ROLES Y 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 o cambio de funciones de funcionarios.
- Comunicar las responsabilidades asociadas al cumplimiento de políticas internas.

Coordinador Administrativo o funcionario designado
- Solicitar los accesos a los sistemas de información.
- Notificar cualquier desvinculación de funcionarios.
- Recopilar y revisar los antecedentes mínimos para el inicio de trámites de ingreso y asignación de derechos de acceso provisorios.

División TIC
- Crear los accesos básicos a los nuevos funcionarios.
- Revisar y gestionar los permisos de acceso a los sistemas de información.
- Eliminar los derechos de acceso de los funcionarios que se desvinculan.
- Recuperar los activos de información de los funcionarios que se desvinculan (ver 6.2.2 del presente procedimiento).

Departamento Administración y Servicios
- Recuperar los activos asignados a los funcionarios que se desvinculan (ver 6.2.2 del presente procedimiento).

Departamento de Gestión de Personas
- Enviar listado con personas ingresadas y desvinculadas al menos una vez al mes.

Encargado de Seguridad de la Información:
- Coordinar la Revisión de derechos de acceso de usuario y eliminación de cuentas administradas por el Departamento de Gestión de Tecnologías de Información.

Funcionarios:
- Mantener confidenciales y bajo su estricto control las claves secretas.
- Cumplir con lo establecido en las Políticas y Procedimientos del Sistema de Seguridad de la Información, en todo lo que sea de su competencia.
- No divulgar ni ceder a terceros la información pertinente al Ministerio de Salud.
- Entender la responsabilidad funcionaria, aún fuera de las dependencias de trabajo y fuera del horario normal de trabajo.
- Hacer traspaso de la información perteneciente al Ministerio toda vez cese sus funciones o estas cambien.
- Todos los funcionarios o terceros que tengan un usuario en cualquier plataforma tecnológica del MINSAL, deberán conocer y cumplir con los establecido en las Políticas de Seguridad de la Información del ministerio.

6 PROCEDIMIENTO

6.1 Registro de usuarios

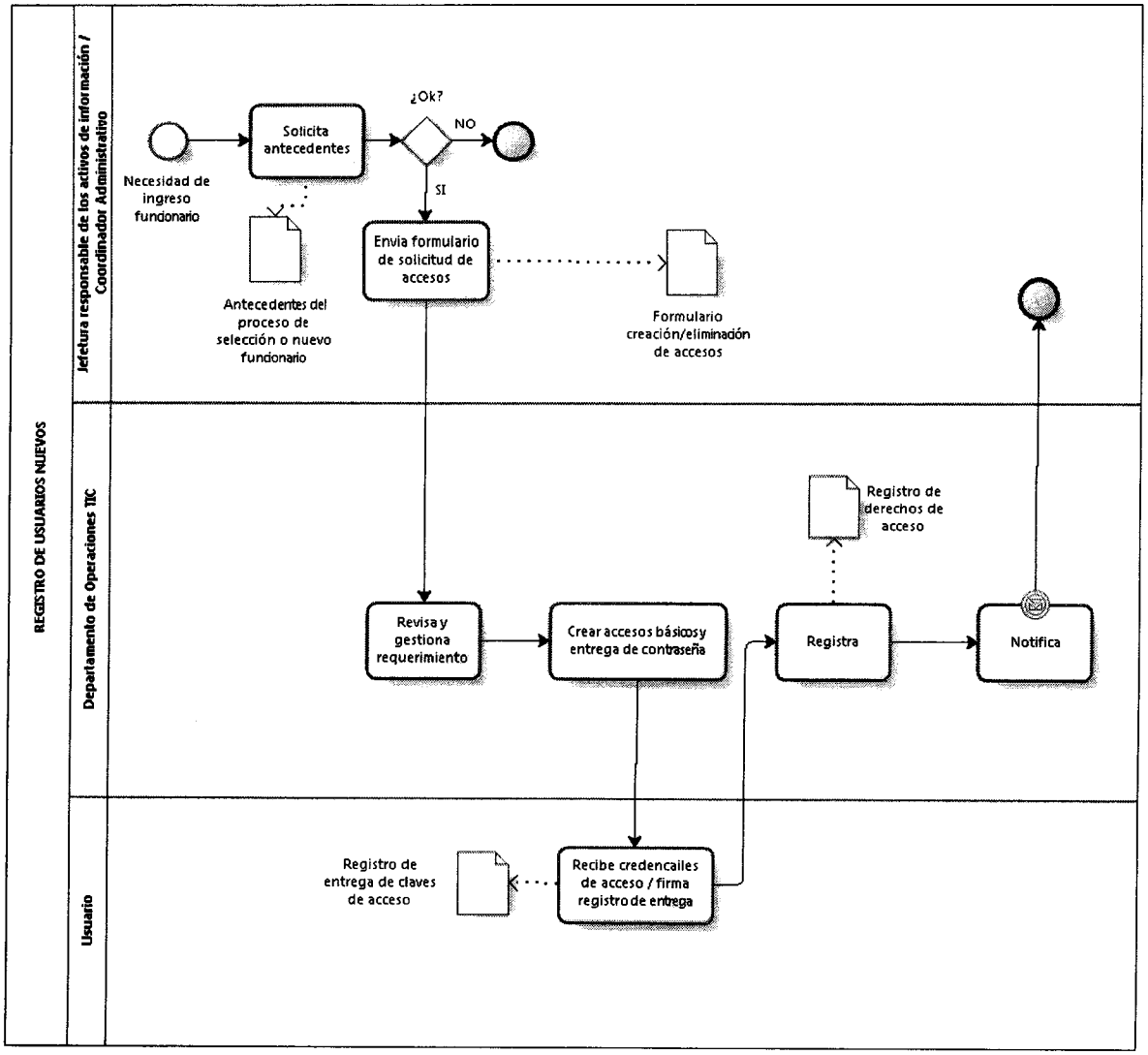
6.1.1 Consideraciones generales

En cualquier registro de usuarios se debe utilizar IDs únicos para permitir a los usuarios vincularse y ser responsables de sus acciones (ver Política de seguridad en la identificación y autenticación de usuarios).

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

6.1.2 Registro de usuarios

La creación de los accesos de nuevos funcionarios (correo electrónico, active Directory, estación de trabajo), se debe realizar de acuerdo al siguiente flujo:



La Jefatura de la Unidad, Departamento o División que sea responsable de los activos de información de su dependencia es responsable de solicitar mediante correo electrónico los accesos básicos para los nuevos funcionarios, mediante el *Formulario de solicitud para creación/eliminación de accesos*.

El área de Soporte de la División TIC es responsable de la creación de los accesos básicos de ingreso, que incluye:

- Creación de correo electrónico.
- Creación de usuario en Active Directory.
- Habilitación de estación de trabajo.

La entrega de las contraseñas temporales de ingreso se realiza mediante el *Registro de Entrega de Claves de Acceso*, 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 Ministerio[2].

Las condiciones de uso incluyen:

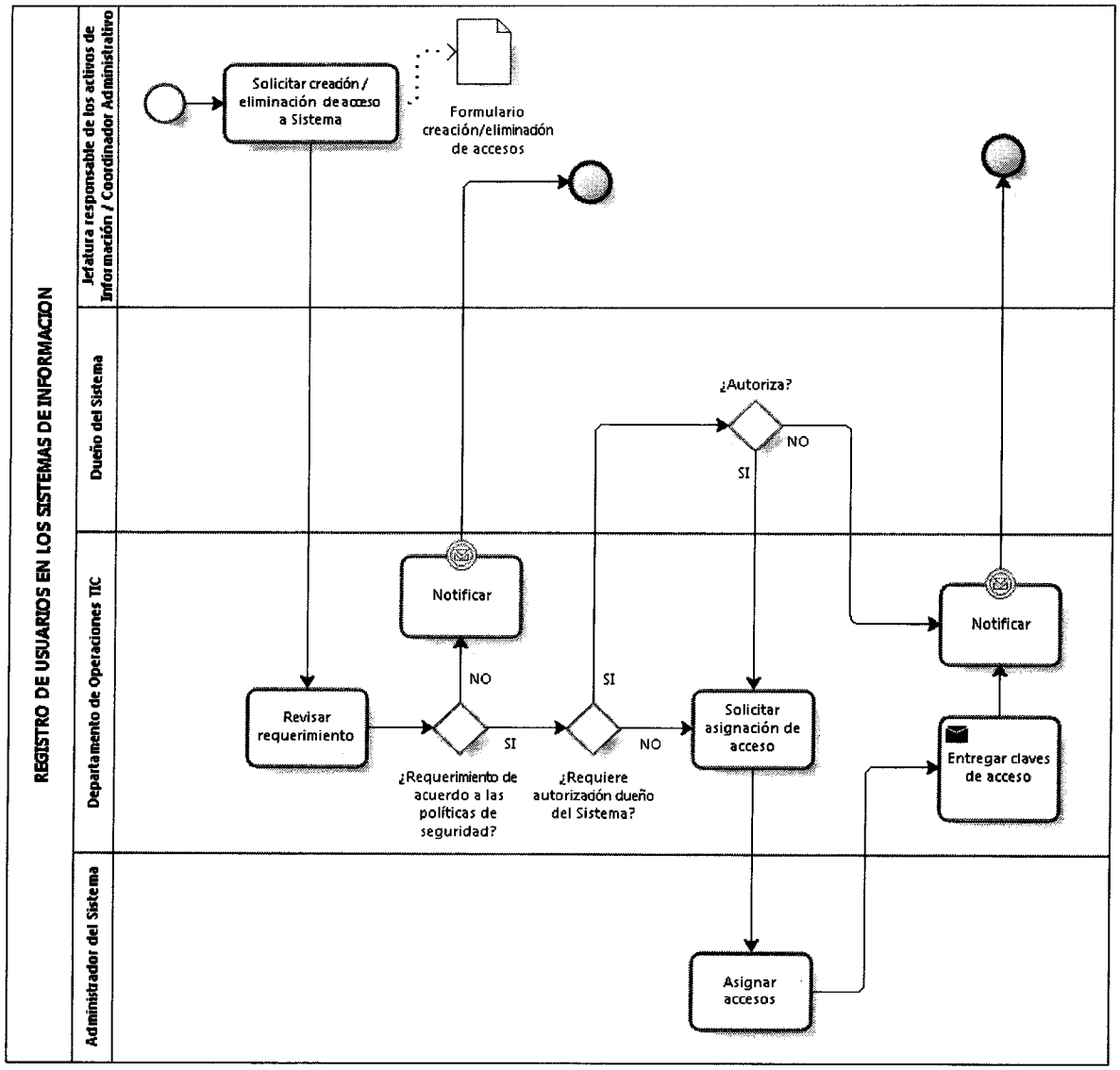
- Mantener confidenciales y el estricto control de las claves secretas.
- Cumplir con lo establecido en las Políticas y Procedimientos del Sistema de Seguridad de la Información, en todo lo que sea de su competencia.
- No divulgar información pertinente al Ministerio de Salud.
- Entender la responsabilidad 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*.

6.1.3 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:

[2] Los requerimientos de seguridad para el uso de correo electrónico y la gestión de contraseñas, están definidos en la política de protección de mensajes electrónicos y la Política de Seguridad en la identificación y autenticación de usuarios.



La Jefatura de la Unidad, Departamento o División que sea responsable de los activos de información de su dependencia es responsable de solicitar mediante correo electrónico la creación o eliminación de los accesos a los sistemas de información[3] mediante el *Formulario de solicitud de creación/eliminación de accesos*, firmado.

En el formulario se deberá indicar:

- Usuario a asignar accesos (nombre.apellido).
- Rut.
- Detallar el o los sistemas a los cuales el funcionario deberá tener acceso.
- Detalle del perfil de usuario con el que debe contar el funcionario para cada uno de los sistemas a los cuales se solicita acceso.

[3] Para el caso de los Sistemas y/o software que no cuente con licenciamiento, la solicitud debe ser acompañada con los recursos necesarios para la compra y/o licenciamiento.

El área de Operaciones de la División TIC 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.

6.2 Eliminación o ajuste de los derechos de acceso

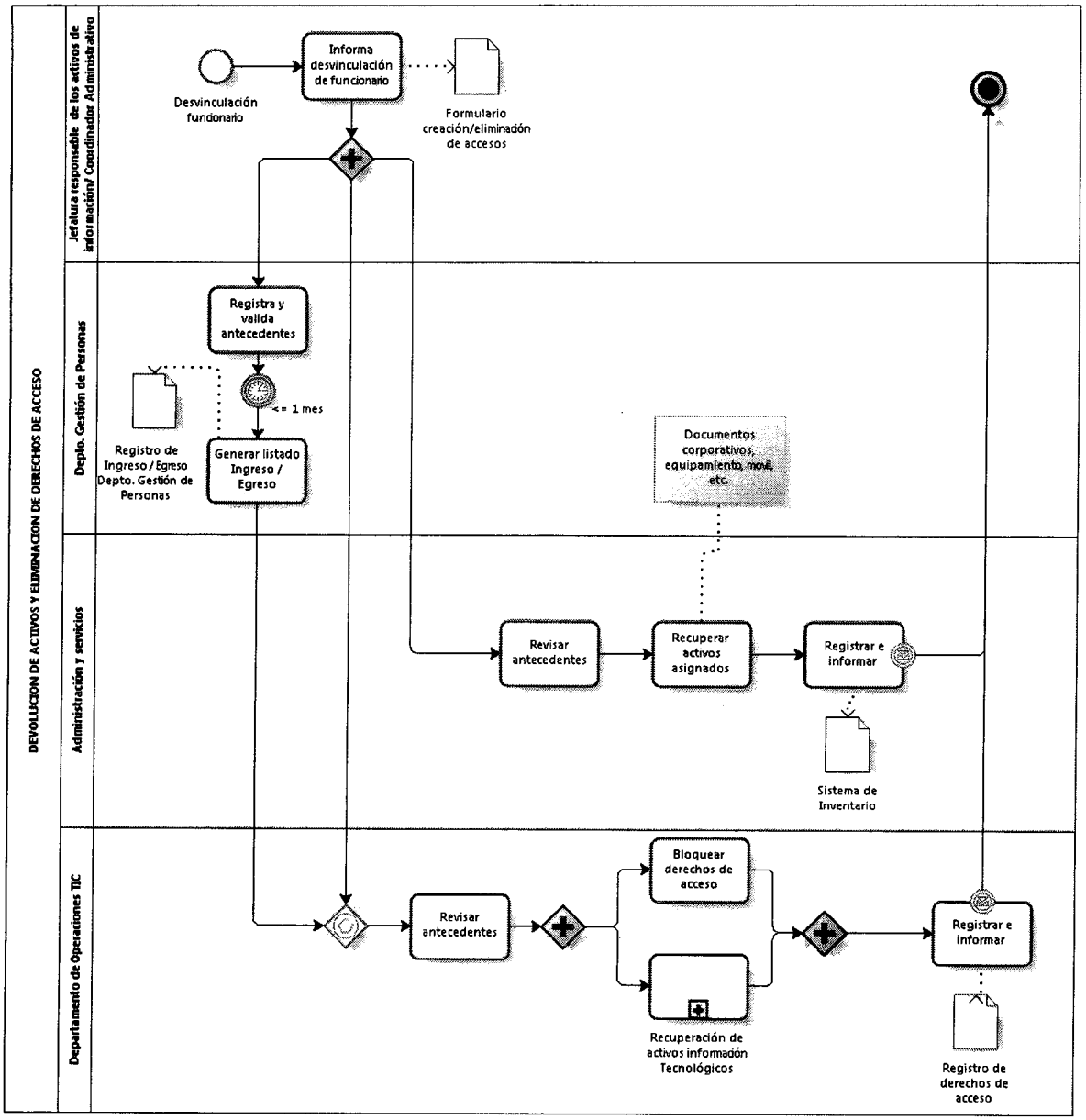
6.2.1 Consideraciones generales

Todo funcionario es responsable de devolver todos los activos pertenecientes a la organización que estén en su poder como consecuencia de la finalización de su relación laboral, contrato o acuerdo.

Equipos personales: en los casos en que un funcionario utilice equipos propios, tiene la obligación de transferir toda la información pertinente a Minsal y eliminarla de cualquier soporte que posea. de ser necesario, la División TIC podrá tener acceso a los equipos para asegurar la transferencia de información.

Si un funcionario posee conocimiento que es importante para las operaciones en curso, es su responsabilidad documentar dicha información y transferirla al Servicio.

6.2.2 Recuperación de activos y eliminación de derechos de accesos



La Jefatura de la Unidad, Departamento o División que sea responsable de los activos de información de su dependencia, es responsable de informar mediante correo electrónico cualquier desvinculación de funcionarios mediante el *Formulario de solicitud para creación/eliminación de accesos*[4]. Esta notificación debe ser enviada en simultáneamente a:

- Departamento de RRHH.
- Departamento de Administración y Servicios.
- División TIC.

[4] Para el caso de los cambios de en la funciones o dependencias, la Jefatura debe informar dichos cambios al Departamento de RRHH quién a su vez informará a la División TIC la revisión de los derechos de acceso de los usuarios.

Ante el informe de desvinculación de algún funcionario, el Departamento de Administración y Servicios[5] es responsable de gestionar la recuperación de los activos asignados al funcionario. Entre otros, se encuentran:

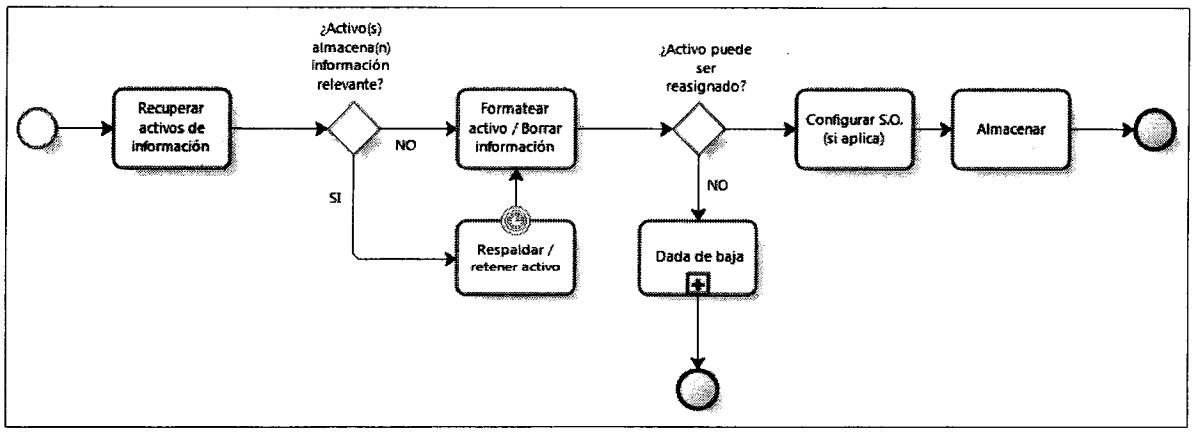
- Documentos corporativos
- Equipamiento
- Teléfonos móviles
- Tarjetas de acceso
- Manuales

Los activos recuperados deben ser registrados en el Sistema de Inventario.

La División TIC es responsable de Bloquear los derechos de acceso a los sistemas de información (cambio de contraseñas, eliminación de usuario según sea requerido, correos electrónicos), junto con recuperar los activos tecnológicos 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 realiza de acuerdo al siguiente modelo:



Una vez transcurridos 60 días desde el bloqueo de los derechos de acceso, estos deben ser eliminados.

En caso que no se devuelvan todos los equipos asignados o sean devueltos con desperfectos, se debe informar al Departamento de Administración y Servicios, para que se tomen las medidas correspondientes.

6.3 Responsabilidades en la desvinculación o cambio de empleo

Personal externo:

[5] En los casos de equipos asignados directamente por la División o Departamento, el Coordinador Administrativo o la Jefatura correspondiente debe gestionar la recuperación de los activos.

Según lo definido en la política de seguridad para las relaciones con los proveedores, todo personal externo que desarrolle labores para MINSAL deberá tomar parte en el desarrollo de la Política General de Seguridad de la Información, disponible en el sitio web de MINSAL, observando sus directrices y colaborando en su aplicación dentro de su ámbito de acción, resguardando la confidencialidad de toda la información a la que tenga acceso, todas estas obligaciones y las definidas en el Sistema de Gestión de Seguridad de la Información continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para MINSAL.

Personal a honorarios:

Según lo definido en las cláusulas de confidencialidad en contratos de honorarios deberán dar cumplimiento a las políticas de Seguridad de la Información del Minsal, resguardando la confidencialidad de toda la información a la que tenga acceso todas estas obligaciones y las definidas en el Sistema de Gestión de Seguridad de la Información continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para MINSAL.

Funcionarios (Planta, contrata, reemplazos y suplencia):

Todas las obligaciones de protección de datos y confidencialidad de la información, definidas en el Sistema de Gestión de Seguridad de la Información de Minsal, continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para MINSAL.

6.4 Gestión de derechos de acceso privilegiados

Los derechos de acceso privilegiados, es decir con acceso a: sistemas de información, sistema operativo, sistema de administración de base de datos; será controlado por el División TIC, a través del Departamento de Operaciones.

Estos permisos serán asignados a los usuarios en base a su necesidad de uso y en base a la Política de control de acceso, es decir, en base al requisito mínimo para sus roles o funciones.

6.5 Revisión de los derechos de acceso de usuario[6]

El Departamento de Operaciones de la división TIC, es responsable de gestionar 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.
- 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.

Los dueños de los activos de Información deben revisar en forma periódica (a lo menos una vez al año), los perfiles de usuarios y accesos del personal vigente y solicitar a Jefe Depto. Sectorial TIC la actualización de éstos cada vez que ocurra un cambio en las funciones.

7 REGISTROS

- Formulario de solicitud para creación de accesos
- Registro de entrega de claves de acceso
- Registro de derechos de acceso

El período de mantención de los registros será de dos años.

[6] Los requerimientos de seguridad para la gestión de derechos de acceso, están definidos en la política de control de Acceso.

8 DIFUSION

La comunicación del presente procedimiento, se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Publicación en la página web de MINSAL http://web.minsal.cl/seguridad_de_la_informacion
- Publicación en la intranet de Minsal http://isalud.minsal.cl/
- Correo informativo.

9 REVISION Y MEDICION

El presente procedimiento deberá ser revisado a lo menos cada dos años o cuando ocurran cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

10 CONTROL DE VERSIONES

Versión	Fecha de Aprobación	Motivo del cambio	Secciones modificadas
01	Diciembre 2013	Creación del documento	Todo el documento
02	Julio 2014	Actualización de los flujos del proceso	Registro de usuarios Eliminación de derechos de acceso
03	Noviembre 2016	Actualización a normativa 2013 de la NCh-ISO 27001	Se actualizan los flujos del proceso, se eliminó la sección de gestión de contraseñas (se incluyen en la política de identificación de usuarios. Se incluye el control: A.07.03.01 Responsabilidades en la desvinculación o cambio de empleo

ELABORADO POR	Rodrigo Vidal / Control de Gestión TIC
REVISADO POR	José Villa / Control de Gestión TIC Leonardo Cisterna / Departamento de Recursos Humanos Claudio Barra / Departamento de Operaciones División TIC
APROBADO POR	Soledad Muñoz / Presidenta Comité de Seguridad de la Información