Ministerio Secretaría General de la Presidencia

Gobierno de Chile

APRUEBA PROCEDIMIENTO DE ACCESO A LA INFORMACIÓN DEL MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA Y DEJA SIN EFECTO LA RESOLUCIÓN EXENTA N° 397, DE 2020, DE ESTE ORIGEN.

RESOLUCIÓN EXENTA Nº 958 /

SANTIAGO, 24 OCT 2023

V I S T O S:

La ley Nº 18.993, que crea el Ministerio Secretaría General de la Presidencia; el Decreto Supremo Nº 7 de 1991, del Ministerio Secretaría General de la Presidencia, que aprueba su Reglamento Orgánico; el Decreto con Fuerza de Ley Nº 1/19.653 de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; el Decreto con Fuerza de Ley Nº 29 de 2004, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley Nº 18.834, sobre Estatuto Administrativo; el Decreto Supremo N° 83 de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba la norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; la Resolución Exenta Nº 397 de 2020, que aprueba el procedimiento de acceso a la información del Ministerio Secretaría General de la Presidencia; el Decreto Supremo Nº 12 de 2022, del Ministerio Secretaría General de la Presidencia, que designa a la Subsecretaria General de la Presidencia; y la Resolución Nº 7 de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.

C O N S I D E R A N D O:

1. Que, la ley N° 18.993, que crea al Ministerio Secretaría General de la Presidencia, establece que corresponde a dicha Secretaría de Estado realizar funciones de coordinación y asesoría directa al Presidente de la República, al Ministro del Interior y a cada uno de los Ministros, sin alterar sus atribuciones proveyéndoles, entre otros medios, de las informaciones y análisis político-técnicos necesarios para la adopción de las decisiones que procedan.

2. Que, el cumplimiento de dicha función implica la generación, envío, recepción, almacenamiento y distribución de múltiples y diversos activos de información que demandan requisitos de seguridad apropiados para garantizar los atributos esenciales de confidencialidad, integridad y disponibilidad de la misma.

3. Que, a raíz de lo anterior, se dictó la Resolución Exenta N° 397 de 2020 de este origen, mediante la cual se aprobó el procedimiento de acceso a la información del Ministerio Secretaría General de la Presidencia, con el objeto de resguardar la seguridad de los activos de información de esta Secretaría de Estado, siguiendo las directrices de la Norma Chilena ISO 27001:2013.

4. Que, dicho acto administrativo requiere ser actualizado incorporando, entre otros cambios, los siguientes subprocesos: (i) de autorización de creación o eliminación de red social institucional; (ii) de autorización de uso de red social en el portal institucional; (iii) de autorización de extracción de datos.

REPUBLICA DE CHILE - UNIDAD DE FISCALIA INTERNA - MINISTERIO SECRETARIA GENERAL DE LA PRESIDENCIA

5. Que, para dar cumplimiento a la actualización anteriormente señalada, se ha tenido presente el Memorándum N° 00252 de 2023, del Jefe de la División de Administración General.

6. Que, de acuerdo a lo expuesto, el presente acto administrativo viene en aprobar el nuevo procedimiento de acceso a la información del Ministerio Secretaría General de la Presidencia y, en consecuencia, dejar sin efecto el procedimiento contemplado en la Resolución Exenta N° 397, de 2020, de este origen.

R E S U E L V O:

1° APRUÉBASE el Procedimiento de Acceso a la Información del Ministerio Secretaría General de la Presidencia, cuyo texto es el siguiente:

"Controles NCH ISO 27001:2013 Relacionados

CONTROL	*NOMBRE*
A.09.01.02	Acceso a las Redes y a los Servicios de Red
A.09.02.01	Registro y Cancelación de Registro de Usuario
A.09.02.02	Asignación de Acceso de Usuario
A.09.02.03	Gestión de Derechos de Acceso Privilegiado
A.09.02.06	Eliminación o Ajuste de los Derechos de Acceso
A.09.03.01	Uso de Información de Autenticación Secreta
A.09.04.01	Restricción del Acceso a la Información
A.09.04.02	Procedimiento de Inicio de Sesión Seguro
A.09.04.03	Sistema de Gestión de Contraseñas
A.09.04.04	Uso de Programas Utilitarios Privilegiados
A.09.04.05	Control de Acceso al Código Fuente de los Programas

2023

Control de Versiones

Fecha	Versión	Responsables	Descripción
30-09-2019	1.0	Jorge Romero Vargas Solange Godoy Carrera	Elaboración de procedimiento.
17-04-2020	2.0	Jorge Romero Vargas Solange Godoy Carrera	Mejoras en formularios AIN-01 (pág.21), AIN-07 (pag.27), AIN-11 (pág.31). Creación de subprocesos: Solicitud de designación de propietario de carpeta compartida (pág.19). Solicitud de autorización de uso y publicación de contenido en plataformas digitales y redes sociales (pág.20).
15-06-2020	2.1	Jorge Romero Vargas	Mejoras en la redacción del documento.
21-12-2021	2.2	Jorge Romero Vargas	Actualización sección firmantes. Mejoras en formularios AIN-07 y AIN-09.

15-11-2022	2.3	Jorge Romero Vargas	Incorpora subprocesos de: (i) Autorización de creación o eliminación de red social Institucional. (ii) Autorización de uso de red social en portal institucional. (iii) Autorización de extracción de datos. Actualización sección firmantes. Incorpora formularios AIN-15, AIN-16 y AIN-17 para registros de subprocesos. Actualización formulario AIN-14.
11-08-2023	2.4	Jorge Romero Vargas	Actualiza Unidad de Tecnologías de la Información por Área de Tecnologías de la Información. Actualiza Jefe/a Unidad de Tecnologías de la Información por Encargado/a Área de Tecnologías de la Información.

1. Introducción

El Ministerio Secretaría General de la Presidencia, en adelante el "Ministerio" o "el servicio", dispone del presente procedimiento denominado "Procedimiento de Acceso a la Información", como parte integrante del Sistema de Seguridad de la Información. En específico, se enmarca en el cumplimiento de la Norma Chilena ISO 27001, cuyo objetivo principal es la protección de la información, que propone como requisito de control:

Control A.09.01.02 Accesos a las redes y a los servicios de red

"Los usuarios sólo deben tener acceso directo a la red y a los servicios de la red para los que han sido autorizados específicamente".
Requisito de control, A.09.01.02 NCH ISO 27001:2013

Control A.09.02.01 Registro y cancelación de registro de usuario

"Se debe implementar un proceso de registro y cancelación de registro de usuario para habilitar la asignación de derechos de acceso".
Requisito de control, A.09.02.01, NCH ISO 27001:2013

Control A.09.02.02 Asignación de acceso de usuario

"Debe existir un procedimiento formal de asignación de acceso de usuario para asignar o revocar los derechos de acceso para todos los tipos de usuarios, a todos los sistemas y servicios".
Requisito de control, A.09.02.02 NCH-ISO 27001:2013

Control A.09.02.03 Gestión de derechos de acceso privilegiados

"Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado".
Requisito de control A.09.02.03 NCH-ISO 27001:2013

Control A.09.02.06 Eliminación o ajuste de los derechos de acceso

"Se deben retirar los derechos de acceso de todo el personal y usuarios externos a la información y a las instalaciones de procesamiento de información, una vez que termine su relación laboral, contrato o acuerdo o se ajuste según el cambio".
Requisito de control A.09.02.06 NCH-ISO 27001:2013

Control A.09.03.01 Uso de información de autenticación secreta

"Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta".
Requisito de control A.09.03.01 NCH-ISO 27001:2013

Control A.09.04.01 Restricción de acceso a la información

"Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso".
Requisito de control A.09.04.01 NCH-ISO 27001:2013

Control A.09.04.02 Procedimiento de inicio de sesión seguro

"Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro".
Requisito de control A.09.04.02 NCH-ISO 27001:2013

Control A.09.04.03 Sistema de gestión de contraseñas

"Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad".
Requisito A.09.04.03 NCH-ISO 27001:2013

Control A.09.04.04 Uso de programas utilitarios privilegiados

"Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden estar en capacidad de anular el sistema y los controles de aplicación".
Requisito A.09.04.04 NCH-ISO 27001:2013

Control A.09.04.05 Control de acceso al código fuente de los programas

"Se debe restringir el acceso al código fuente de los programas".
Requisito A.09.04.05 NCH-ISO 27001:2013

2. Objetivo

Este procedimiento tiene por objeto el control, asignación, registro, cancelación, eliminación o ajuste a los privilegios del acceso a los sistemas de información del Ministerio, así como a las bases de datos y servicios de información con que éste cuente. Además, las/ los usuarios deben dar cumplimiento a lo establecido en el uso de la información de autenticación secreta, para el acceso de sesión seguro a los sistemas y aplicaciones. La definición del ámbito de los controles de acceso que sea necesario implementar, así como tener un mayor control al acceso de la información y a las instalaciones en la que se procesa la información restringiendo y controlando el uso de programas utilitarios y el acceso al código fuente.

3. Alcance

Este procedimiento debe aplicarse a todos los funcionarios/as y servidores/as públicos del Ministerio, o a cualquier tercero que pueda estar prestando servicios a éste, todos en conjunto denominados "usuario o usuarios", y que requieran la utilización de equipos tecnológicos para acceder a la información perteneciente al servicio, por cuanto se les deberá otorgar accesos privilegiados a la información y proveer de las claves de acceso necesarias para el desarrollo de sus funciones, así como la eliminación de los derechos de acceso, cuando sea requerido por la jefatura.

La División de Gobierno Digital podrá hacer uso de sus propios procedimientos adicionales o equivalentes como parte de los lineamientos internos definidos por su jefatura.

4. Roles y responsabilidades

Independiente del cargo/rol que se desempeñe, del nivel jerárquico del que se goce y de la modalidad bajo la cual se esté contratado, es responsabilidad de todo el personal de este Ministerio conocer y dar debido cumplimiento a este procedimiento, asimismo, es responsabilidad de:

- **Comité de Seguridad de la Información**, la revisión de este procedimiento, así como velar por su cumplimiento, actualización y difusión.
- **Encargado/a de Seguridad de la Información,** la difusión y mantención de revisiones periódicas del cumplimiento de esta norma en el Ministerio.

- **Encargado/a Área de Tecnologías de la Información,** asignar las credenciales de acuerdo con los requerimientos de las autoridades del Ministerio, así como la cancelación de estos accesos una vez terminado el contrato o el tiempo por el cual se solicitó acceso, resguardando las restricciones de los accesos físicos y lógicos del servicio.
- **Encargado/a Área de Soporte,** mantener el resguardo, control y asignación de las contraseñas de los sistemas, equipos o aplicaciones, así como el acceso a sistemas de redes con que cuente el Ministerio, y la eliminación o ajuste a dichos accesos por necesidad del servicio o petición de la jefatura.
- **Jefes/as de División, Comisión y Unidades,** difundir este procedimiento en las dependencias a su cargo, así como velar por el cumplimiento, difusión y supervisión del apego a esta norma del personal a su cargo.
- **Funcionarios/as/ Servidores/as,** actuar en base a lo establecido en esta norma, resguardando los recursos y la información contenida, disponiendo de usuario y clave de acceso, la cual es privada, personal e intransferible. Además, deberá velar por el resguardo de la información contenida en el equipo a su cargo.
- **Jefe/a Unidad de Gestión y Desarrollo de las Personas (Jefe/a UGDP),** autorizar solicitudes de subprocesos relacionadas con información de la Unidad.
- **Operador/a** realizar una operación específica determinada por el Encargado del Área de Tecnologías de la Información.
- **Solicitante**, iniciar un subproceso del procedimiento ante alguna necesidad específica.
- **Jefe/a Directo** del solicitante, autorizar formularios del/la solicitante, asociados a un subproceso específico por alguna necesidad.

5. Definiciones y modo de operación

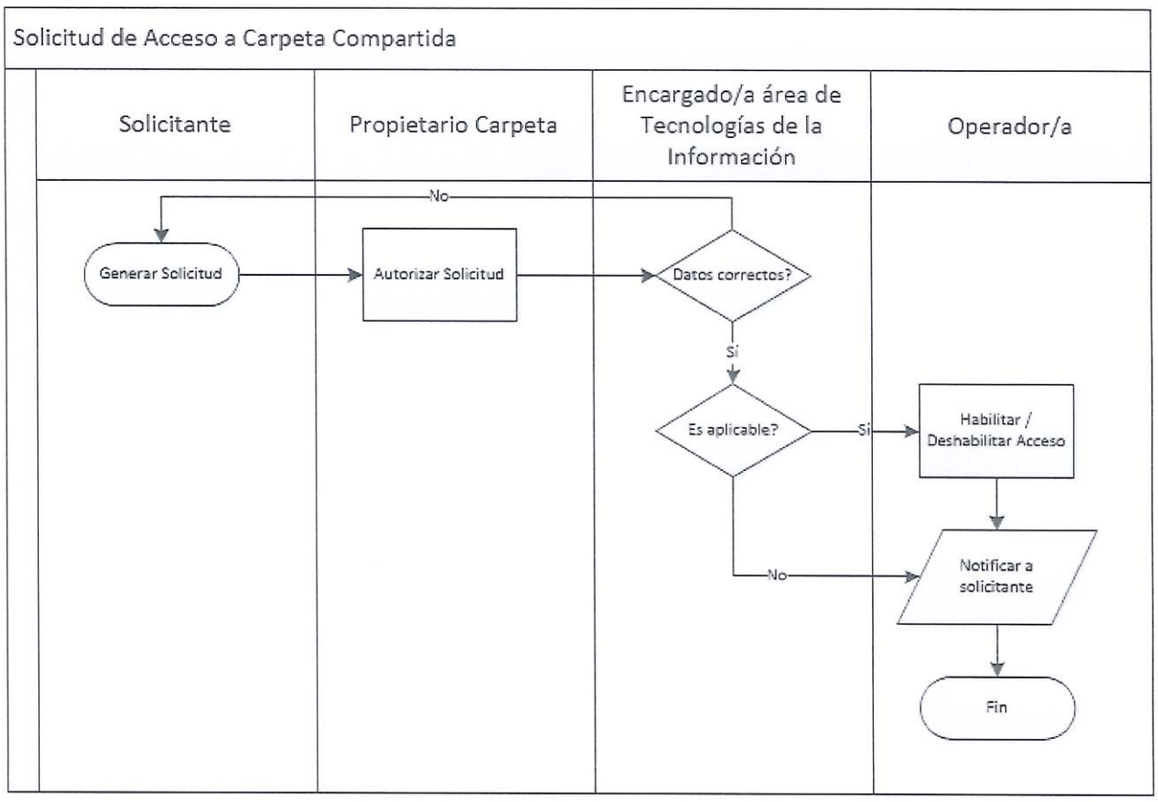
El Procedimiento de Acceso a la Información contempla los siguientes subprocesos:

- Solicitud de Acceso a Carpeta Compartida
- Solicitud de Acceso VPN
- Solicitud de Registro y Cancelación de Registro de Usuario
- Solicitud Habilitación/Deshabilitación de Acceso a Aplicaciones
- Solicitud Autorización de Derechos de Acceso Privilegiado
- Solicitud de Eliminación o Ajuste de Derechos de Acceso
- Solicitud de Creación y Cambio de Contraseña
- Solicitud Consulta Restricción de Acceso a la Información
- Solicitud Consulta Estado Inicio Sesión Seguro
- Solicitud Consulta Estado Sistema Gestión de Contraseñas
- Solicitud de Autorización Uso Programas Privilegiados
- Solicitud de Acceso a Código Fuente de Aplicación
- Solicitud de Designación de Propietario de Carpeta Compartida
- Solicitud de Autorización de Uso y Publicación de Contenido en Plataformas Digitales y Redes Sociales
- Solicitud de Autorización de Creación o Eliminación de Red Social Institucional
- Solicitud de Autorización de Uso de Red Social en Portal Institucional
- Solicitud de Autorización de Extracción de Datos

Subproceso: Solicitud de Acceso a Carpeta Compartida

Control: A.09.01.02 Acceso a las redes y a los servicios de red

El Área de Tecnologías de la Información, debe controlar los accesos físicos y lógicos, como las redes y sistemas del Ministerio, así como fuera de éste, impidiendo el acceso no autorizado a los sistemas de información, a través de la autenticación y autorización. Los usuarios deben tener presente la responsabilidad que tienen frente a la utilización de contraseñas en los equipos.

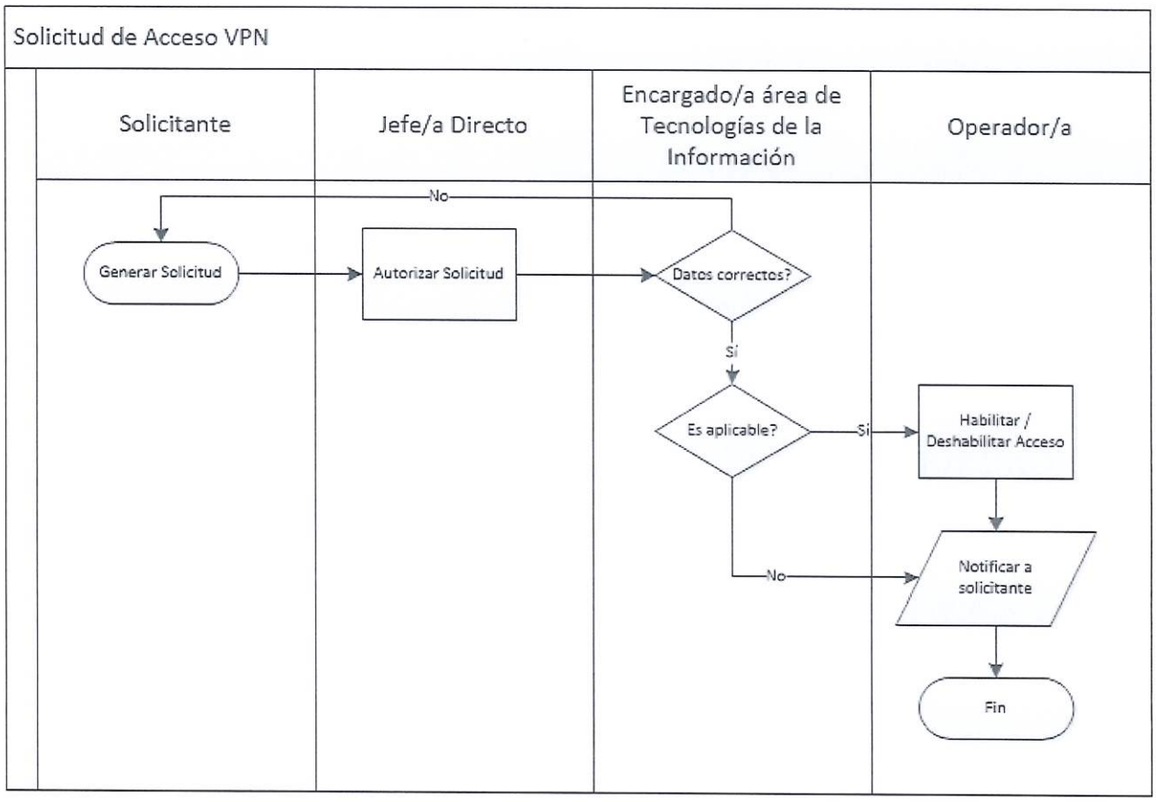


Descripción de actividades: El/la solicitante generará la solicitud de acceso a la carpeta compartida indicando la información requerida, la que debe ser autorizada por el propietario de la referida carpeta. Aprobada esta solicitud, es enviada al Encargado/a del Área de Tecnologías de la Información quien verificará los datos y, si es aplicable, solicitará al operador/a Habilitar/Deshabilitar el acceso y posteriormente notificar al solicitante. En caso de no ser aplicable la solicitud será rechazada y se notificará de igual forma al solicitante.

Subproceso: Solicitud de Acceso VPN

Control: A.09.01.02 Acceso a las redes y a los servicios de red

El acceso a las redes a través de VPN, Virtual Private Network, o red inalámbrica será por clave de acceso directo, para lo cual el usuario solicitante debe levantar el requerimiento a su jefatura la que posteriormente, enviará al Encargado/a del Área de Tecnologías de la Información, quién autorizará o rechazará para luego indicar al operador/a que esté a cargo realizar lo solicitado, así como también el acceso a las carpetas compartidas.



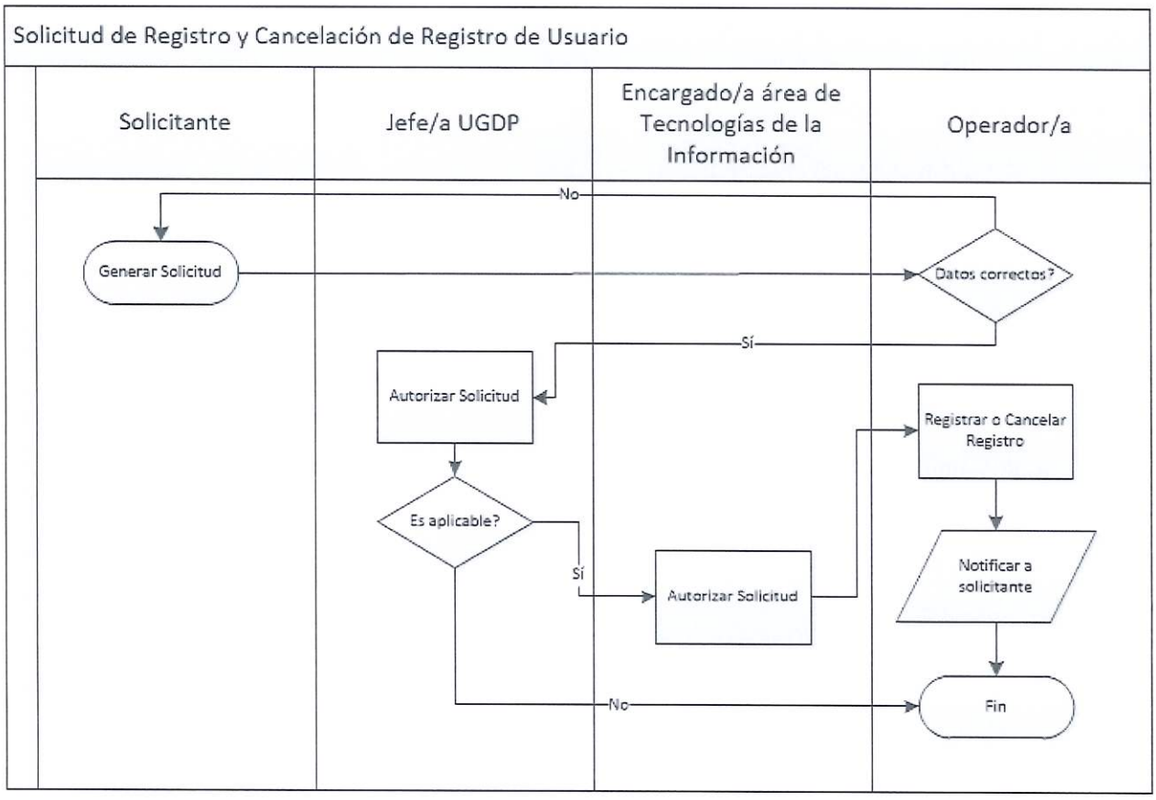
Descripción de actividades: El/la solicitante generará una solicitud de acceso VPN, la cual debe ser autorizada por la Jefatura Directa, para ser enviada al Encargado/a del Área de Tecnologías de la Información, quien verificará los datos y solicitará al operador/a Habilitar/Deshabilitar el acceso de ser aplicable, notificando, además al solicitante. En caso de no ser aplicable, también será notificado el solicitante.

Subproceso: Solicitud de Registro y Cancelación de Registro de Usuario

Control: A.09.02.01 Registro y cancelación de registro de usuario

Al ingreso de los usuarios a prestar servicios al Ministerio, el Área de Tecnologías de la Información entregará una identificación personal en el dominio de la institución, así como también una clave de acceso por la cual podrá acceder a los recursos y servicios, como correo electrónico, equipo computacional y todas las aplicaciones a las que esté autorizado. Cuando el usuario/a deje de prestar servicios a la institución dichas cuentas serán revocadas, así como todos los derechos de acceso a los servicios y aplicaciones del Ministerio.

La autorización para la creación y cambio de la contraseña debe ser requerida por el/la solicitante con la autorización de su jefatura directa, y el operador/a que esté cargo dará curso a lo solicitado.

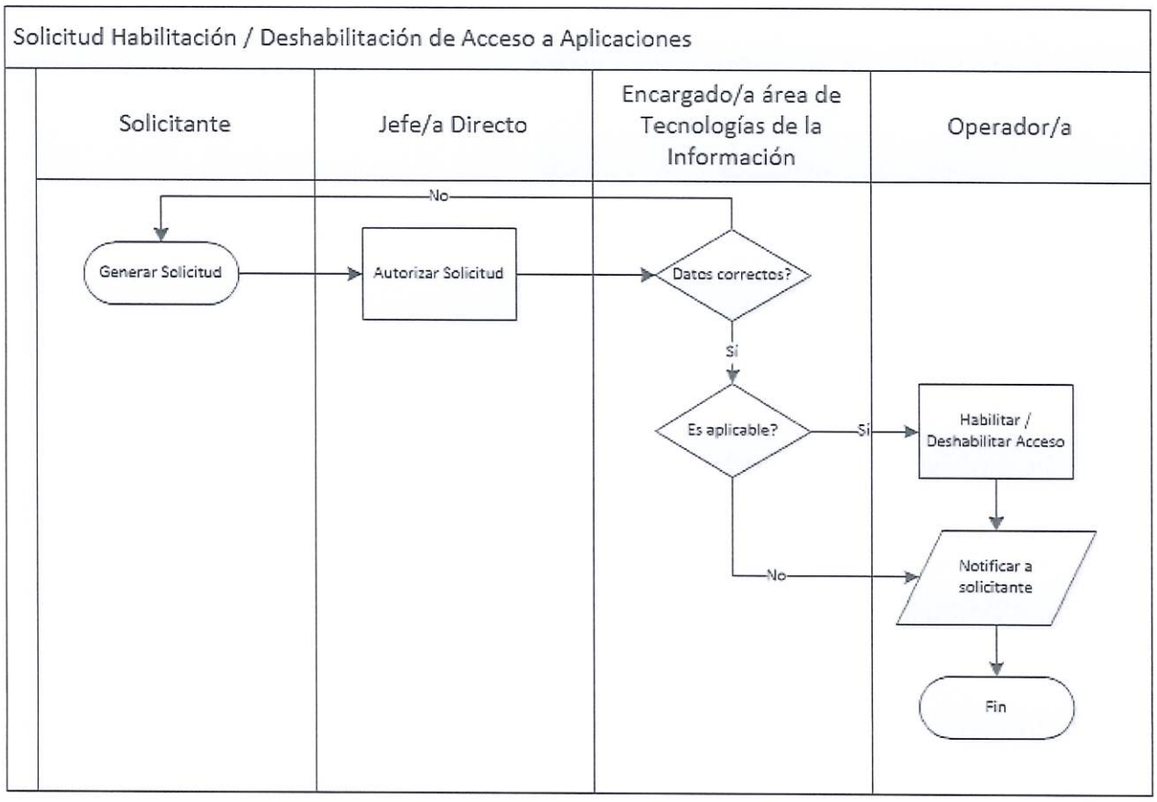


Descripción de actividades: El/la solicitante generará una solicitud de registro o cancelación de registro de usuario/a, para que luego el operador/a valide que los datos se encuentren correctamente ingresados para solicitar autorización de la Jefatura UGDP. Si es aplicable, se requerirá de la autorización del Encargado/a del Área de Tecnologías de las Información para que, posteriormente, el operador/a lleve a cabo el registro o cancelación de usuario, notificando finalmente al solicitante. En caso de que la Jefatura UGDP determine que no es aplicable, finalizará el proceso.

Subproceso: Solicitud Habilitación/Deshabilitación de Acceso a Aplicaciones

Control: A.09.02.02 Asignación de acceso a usuario

Para tener acceso a las aplicaciones de la institución, el usuario/a solicitante debe levantar el requerimiento a su jefatura, la que, posteriormente, la enviará al Encargado/a del Área de Tecnologías de la Información, quién autorizará o rechazará, para luego indicar al operador/a encargado de realizar lo solicitado. Cada funcionario/a contará con un usuario único y un rol asignado en la aplicación requerida. Se deberá señalar una fecha de inicio y término de uso junto con la acción de habilitar o deshabilitar.



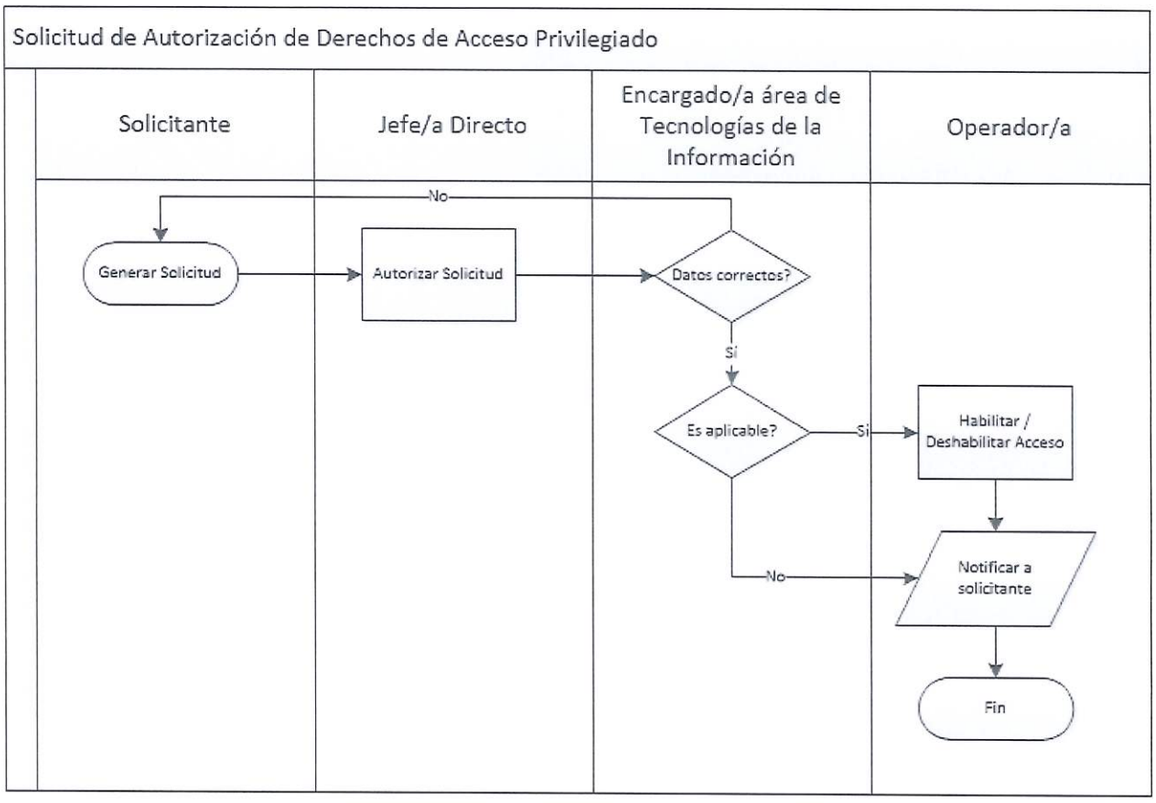
Descripción de actividades: El/la solicitante generará una solicitud de habilitación/deshabilitación de acceso a las aplicaciones, que deberá ser autorizada por la jefatura directa. Posteriormente, el Encargado/a del Área de Tecnologías de la Información validará que los datos se encuentren correctos y evaluará si es aplicable. En caso de ser aplicable, se solicitará al operador/a habilitar/deshabilitar el acceso quien posteriormente notificará al solicitante. En caso de no ser aplicable, el operador/a notificará al solicitante de igual forma.

Subproceso: Solicitud Autorización de Derechos de Acceso Privilegiado

Control: A.09.02.03 Gestión de derechos de acceso privilegiado

El acceso de los usuarios/as a la red y los servicios de red será con autorización. Dicho acceso será restringido y controlado, tanto en lo relativo a la asignación como el uso de los derechos de acceso privilegiado.

Para la asignación de acceso privilegiado el/la solicitante debe contar con la autorización de su jefatura directa y ser enviada al Encargado/a del Área de Tecnologías de la Información, quien autorizará o rechazará la solicitud.



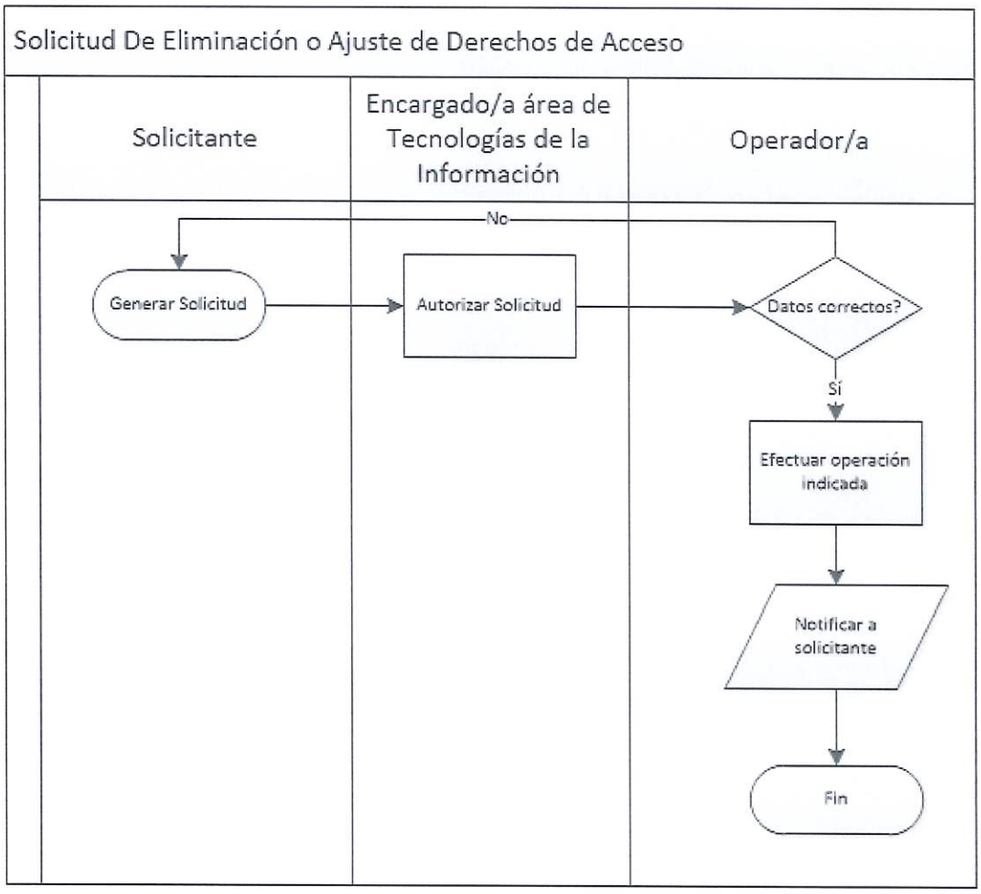
Descripción de actividades: El/la solicitante generará una solicitud de autorización de derechos de acceso privilegiado, que deberá ser autorizada por su jefatura directa. Esta solicitud deberá ser enviada al Encargado/a del Área de Tecnologías de la Información, quien verificará los datos y evaluará si es aplicable. En caso de ser aplicable, solicitará al operador/a habilitar/deshabilitar el acceso, debiendo, posteriormente, notificar al solicitante. En caso de no ser aplicable el operador/a de igual forma notificará al solicitante.

Subproceso: Solicitud de Eliminación o Ajuste de Derechos de Acceso

Control: A.09.02.06 Eliminación o ajuste de los derechos de acceso

El Área de Tecnologías de la Información debe controlar y restringir los derechos de acceso de las y los usuarios, el que será dado sólo con autorización formal, con indicación de los derechos de acceso, eliminación o ajuste cuando la relación laboral, contrato o acuerdo termine. Se deben retirar todos los derechos de las personas a correo electrónico, carpetas compartidas, sistemas o plataformas tecnológicas, entre otras.

Para la eliminación o ajuste, el requirente debe enviar la solicitud al Encargado/a del Área de Tecnologías de la Información, quien autorizará o rechazará dicha solicitud. Si esta es autorizada el operador/a encargado debe realizar la función.



Descripción de actividades: El/La solicitante generará una solicitud de eliminación o ajuste de derechos de acceso. Esta deberá ser autorizada por el Encargado/a del Área de Tecnologías de la Información, quien posteriormente solicitará al operador verificar que los datos se encuentren correctos y, en base a esto, efectuar la operación indicada. Finalmente se notificará al solicitante.

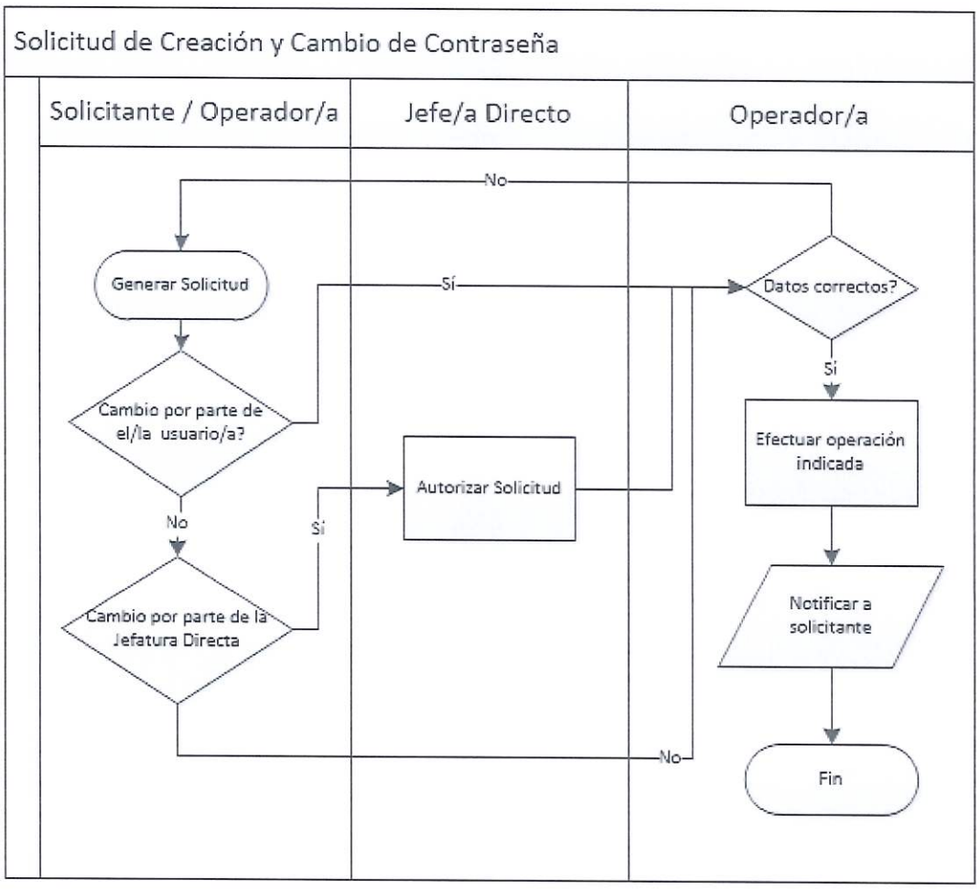
Subproceso: Solicitud de Creación y Cambio de Contraseña

Control: A.09.03.01 Uso de información de autenticación secreta

Los usuarios/as deben cumplir las normas de uso de la información de autenticación secreta, ingresando el nombre de usuario/a y contraseña, la que se validará con el registro de usuarios/as en la base de datos del sistema, de lo contrario, automáticamente se enviará un mensaje que dará cuenta que existe un error, el que si supera los cuatro intentos acarreará el bloqueo de la cuenta.

La contraseña de acceso debe contar con un mínimo de 6 caracteres y un máximo de 15, la que debe ser difícil de copiar.

El/La solicitante de creación o cambio de contraseña debe enviar al Encargado/a del Área de Tecnologías de la Información el requerimiento, quien indicará al operador/a responsable de realizar la función.



Descripción de actividades: El/la solicitante y operador/a podrán generar una solicitud de creación y cambio de contraseña que deberá ser autorizada por la jefatura directa cuando no sea solicitada por el usuario/a directamente. El operador/a podrá generar de igual forma esta solicitud en el caso de creación de contraseñas. En ambos casos, la información será validada por el operador/a, quien realizará la tarea indicada, notificando posteriormente al solicitante.

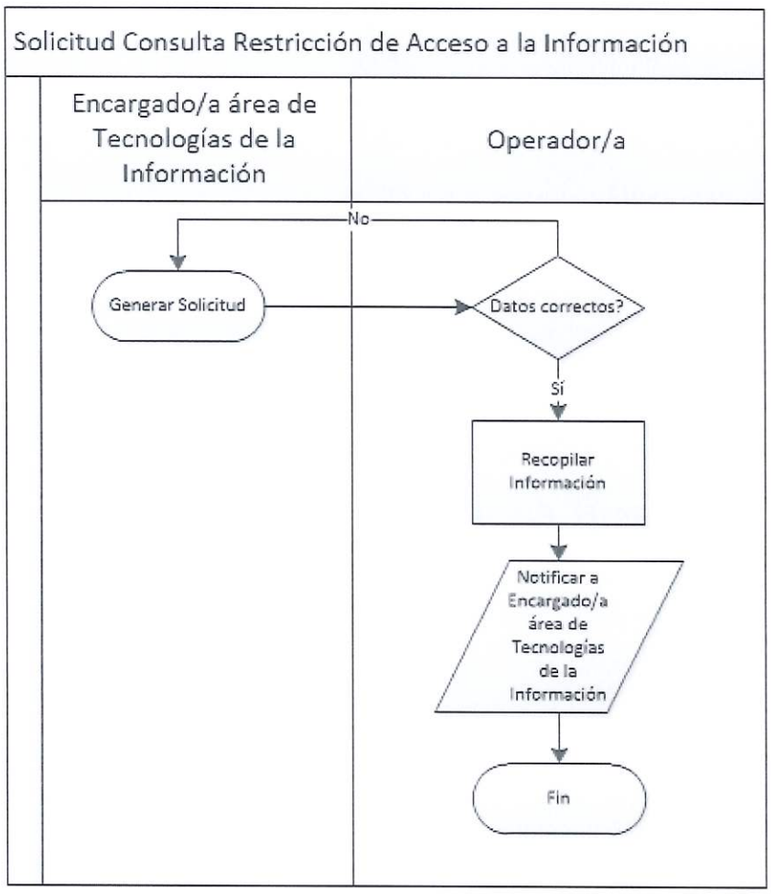
Subproceso: Solicitud Consulta Restricción de Acceso a la Información

Control: A.09.04.01 Restricción de acceso a la información

Todo acceso físico y lógico debe tener restricción de acceso a la información y a las funciones del sistema de aplicaciones. Estas restricciones tienen como finalidad el resguardo a la información depositada en los sistemas operativos y dispositivos móviles que han sido asignados por el Ministerio.

El Área de Tecnologías de la Información debe tener el control de los accesos a las funciones de los aplicativos.

El Encargado/a del Área de Tecnologías de la Información consultará al operador/a o encargado/a de los datos de los usuarios/as a los cuales se ha restringido acceso a la información.



Descripción de actividades: El Encargado/a del Área de Tecnologías de la Información generará una solicitud de consulta restricción de acceso a la información, la cual será enviada al operador/a quien validará los datos y realizará la recopilación de información notificando posteriormente al Encargado/a del Área de Tecnologías de la Información.

Subproceso: Solicitud Consulta Estado Inicio Sesión Seguro

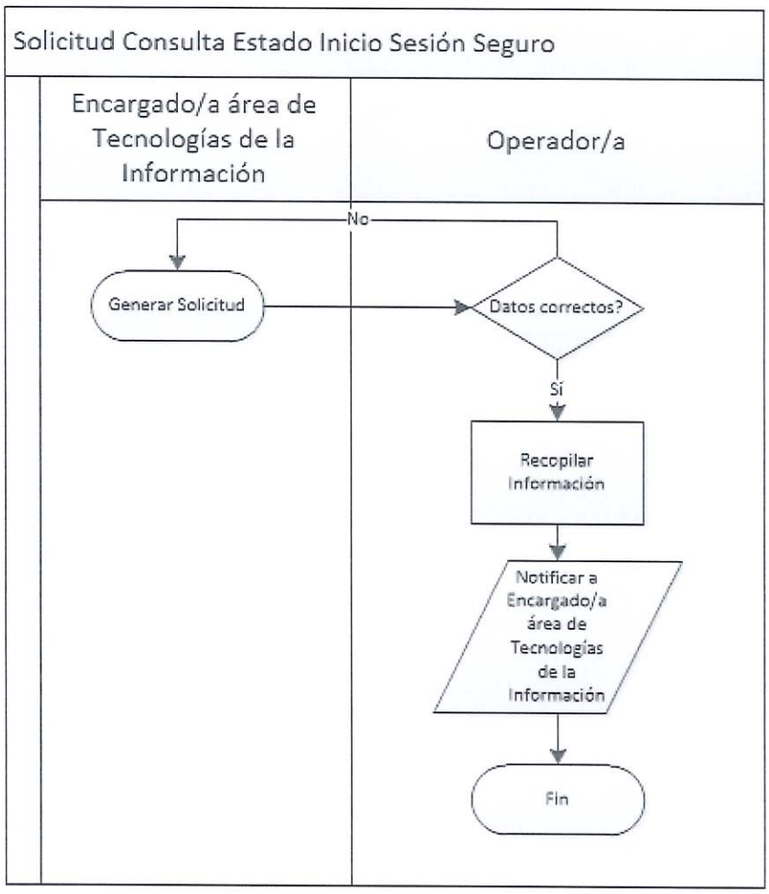
Control: A.09.04.02 Procedimiento de inicio de sesión seguro

El Área de Tecnologías de la Información debe contar con un plan o guía que indique el acceso a los sistemas operativos que deben estar protegidos por el inicio de sesión seguro en las aplicaciones y sistemas de credenciales de acceso de usuario/a y contraseña.

El inicio de sesión tiene cuatro intentos, la que en caso de fallar en todos ellos se bloqueará.

La contraseña no se debe visualizar en texto al ingreso y cuando el equipo no esté siendo usado, se bloqueará de forma automática.

El Encargado/a del Área de Tecnologías de la Información solicitará al operador/a indicar la verificación del cumplimiento de inicio de sesión seguro, sesión de dominio y de aplicación.



Descripción de actividades: El Encargado/a del Área de Tecnologías de la Información generará una solicitud de consulta de estado inicio sesión segura, la cual será enviada al operador/a quien validará los datos y realizará la recopilación de información, notificando posteriormente al Encargado/a del Área de Tecnologías de la Información.

Subproceso: Solicitud Consulta Estado Sistema Gestión de Contraseñas

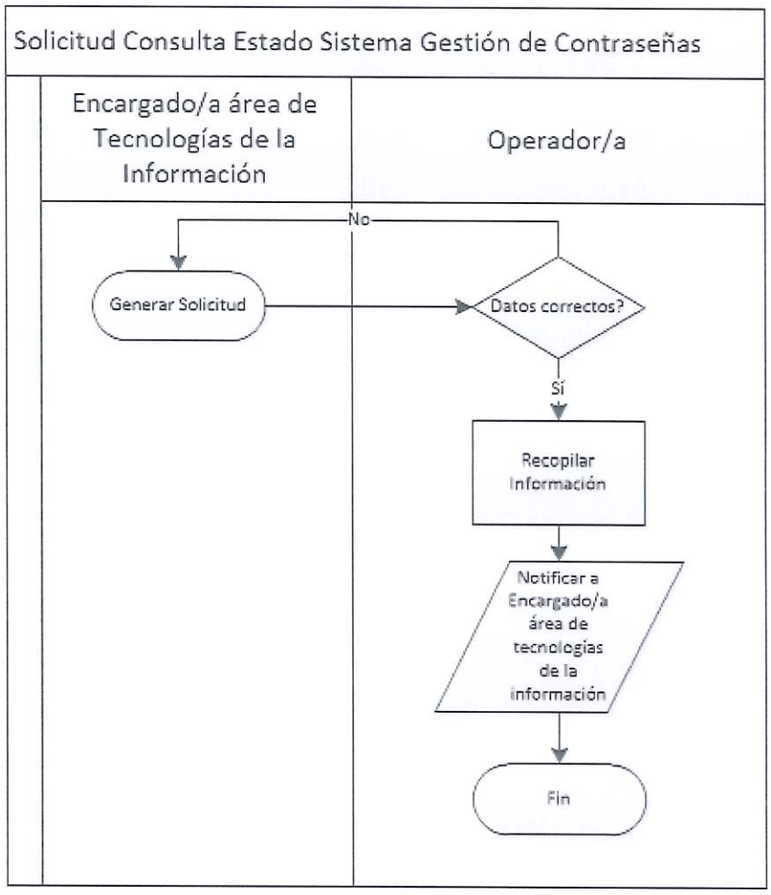
Control: A.09.04.03 Sistema de gestión de contraseñas

A cada usuario/a se le asignará una clave de acceso, la que debe ser personal, y que deberá cambiar por una clave privada.

Será responsabilidad de los usuarios/as no divulgar o entregar la contraseña a un tercero.

La clave tendrá una duración de 3 meses, la que debe ser cambiada al finalizar el periodo. Asimismo, debe tener un mínimo de 6 caracteres y un máximo de 15, sin permitir el uso de claves similares a las usadas previamente.

El Encargado/a del Área de Tecnologías de la Información solicitará al operador/a la verificación del estado de cumplimiento de la aplicabilidad de las contraseñas de dominio y de aplicación.

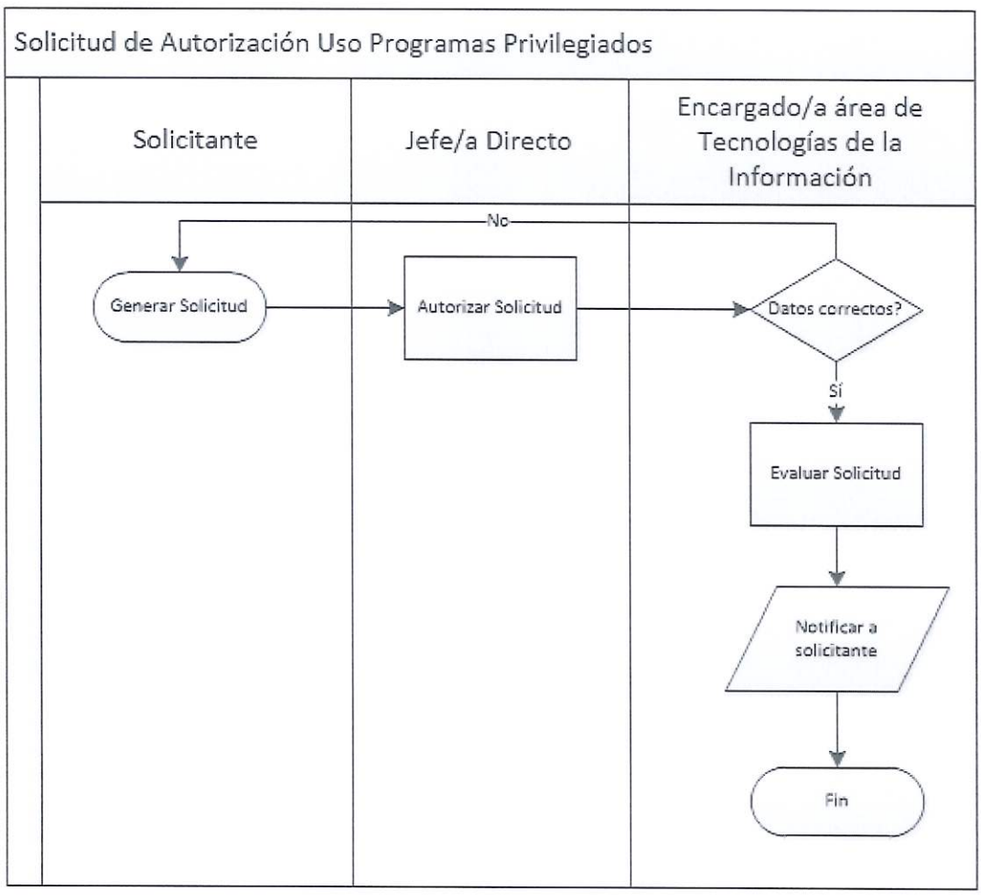


Descripción de actividades: El Encargado/a del Área de Tecnologías de la Información generará una solicitud consulta de estado sistema gestión de contraseñas, la cual será enviada al operador/a quien validará los datos y realizará la recopilación de información notificando posteriormente al Encargado/a del Área de Tecnologías de la Información.

Subproceso: Solicitud de Autorización Uso Programas Privilegiados

Control: A.09.04.04 Uso de programas utilitarios privilegiados

El Área de Tecnologías de la Información ejerce un control estricto sobre los programas utilitarios privilegiados, estableciendo límites y restricciones en su uso, ya que estos pueden afectar los controles de los sistemas. Por lo tanto, es imperativo definir con precisión las personas autorizadas para acceder y utilizar estas aplicaciones. Para solicitar acceso a los programas, el solicitante, previa autorización de su jefatura directa, deberá dirigirse al Encargado del Área de Tecnologías de la Información. Este último evaluará y, posteriormente, aprobará o denegará la solicitud de uso de programas utilitarios privilegiados.



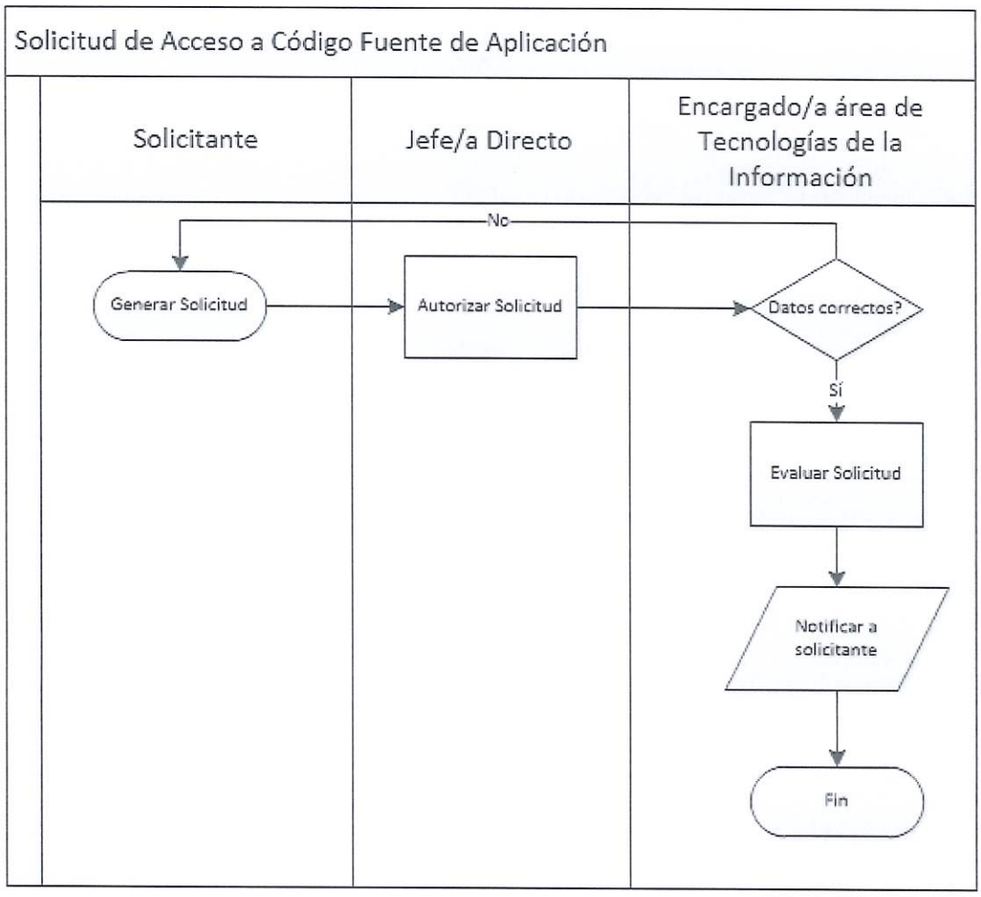
Descripción de actividades: El/la solicitante generará una solicitud de autorización de uso programas privilegiados la cual deberá ser autorizada por su jefatura directa. Esta solicitud deberá ser enviada al Encargado/a del Área de Tecnologías de la Información, quien verificará los datos y evaluará. Posteriormente, notificará al solicitante.

Subproceso: Solicitud de Acceso a Código Fuente de Aplicación

Control: 09.04.05 Control de acceso al código fuente de los programas

El Área de Tecnologías de la Información, debe tener el control de los accesos al código fuente de los programas y aplicaciones del Ministerio.

Para tener acceso al código fuente de los programas, se debe solicitar autorización a la jefatura directa, la cual tiene que pedir autorización al Encargado/a del Área de Tecnologías de la Información e indicar si el acceso es a la aplicación, servidor, carpeta. Además, deberá precisar si el privilegio es de lectura o escritura, y quien podrá autorizar o rechazar la solicitud.



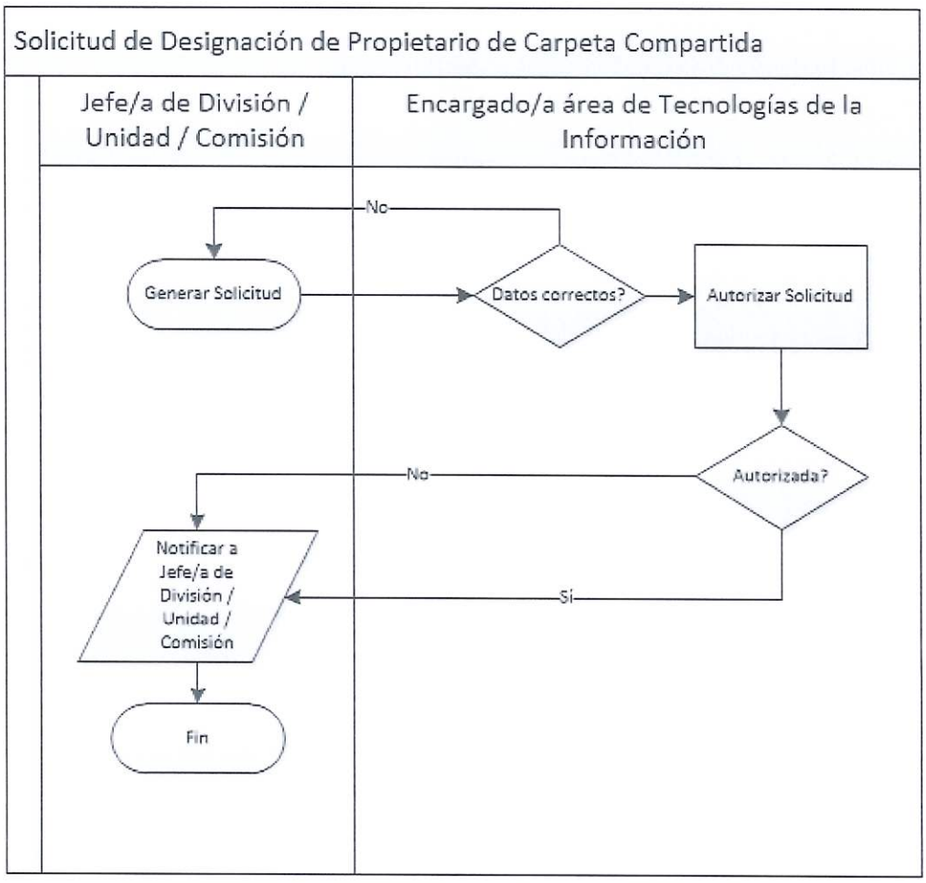
Descripción de actividades: El/la solicitante generará una solicitud de acceso a código fuente de aplicación la cual deberá ser autorizada por su jefatura directa. Esta solicitud deberá ser enviada al Encargado/a del Área de Tecnologías de la Información, quien verificará los datos y evaluará. Posteriormente, notificará al/la solicitante.

Subproceso: Solicitud de Designación de Propietario de Carpeta Compartida

Control: A.09.01.02 Acceso a las redes y a los servicios de red

El Área de Tecnologías de la Información, deberá mantener la designación de propietarios de carpetas compartidas con el fin de validar los accesos requeridos.

La designación de propietario/a de carpeta deberá ser solicitada por cada Jefatura de División/Unidad/ Comisión, lo cual permitirá facultar a un funcionario/a o colaborar/a para realizar cualquier incorporación y/o eliminación de accesos de otros usuarios/as; realizar modificación de estructura y/o eliminación de contenido de carpetas compartidas que sean especificadas.



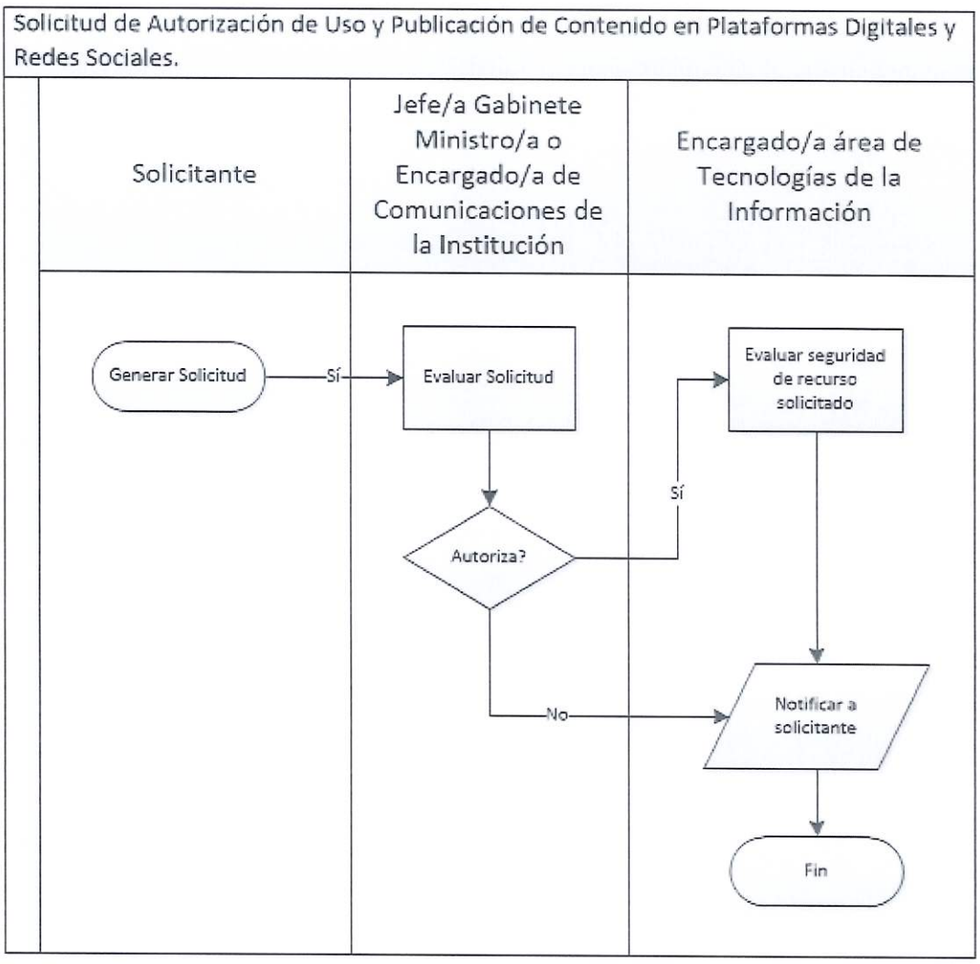
Descripción de actividades: La Jefatura de División/Unidad/Comisión generará una solicitud de designación de propietario/a de carpeta compartida, especificando en detalle el nombre de cada carpeta. Esta solicitud será enviada al Encargado/a del Área de Tecnologías de la Información, quien verificará los datos y evaluará. Posteriormente, notificará al solicitante.

Subproceso: Solicitud de Autorización de Uso y Publicación de Contenido en Plataformas Digitales y Redes Sociales.

Control: A.09.01.02 Acceso a las redes y a los servicios de red

El Área de Tecnologías de la Información, deberá gestionar la autorización de uso y publicación de contenido en plataformas digitales y redes sociales dentro de la institución.

Para tener acceso al uso y publicación de contenido en plataformas digitales y redes sociales el/la solicitante con la autorización de la jefatura directa deberá solicitar autorización al/la jefe/a de Gabinete del Ministro/a o Encargado/a de Comunicaciones de la Institución. Posteriormente el Área de Tecnologías de la Información evaluará la seguridad del recurso al que desea acceder.

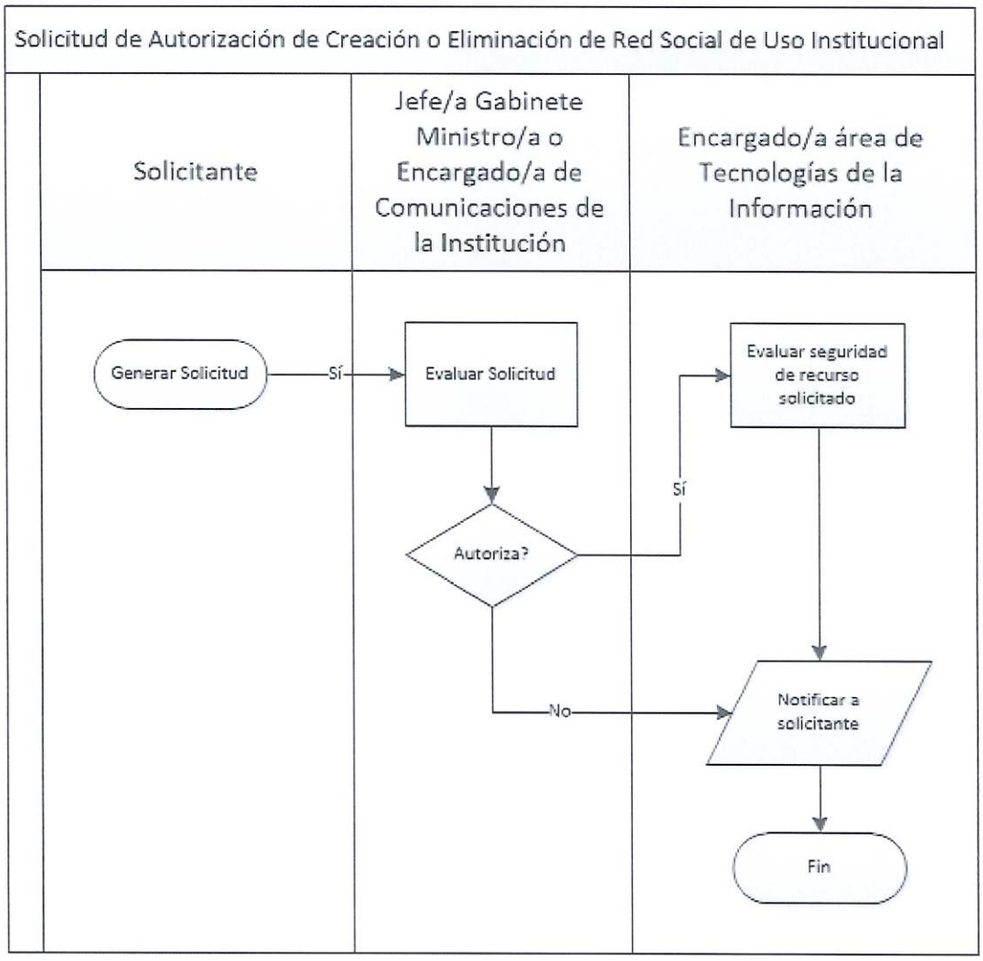


Descripción de actividades: El/la solicitante generará una solicitud de autorización de uso y publicación de contenido en plataformas digitales y redes sociales la cual deberá ser autorizada por su jefatura directa. Esta solicitud deberá ser enviada a la Jefatura del Gabinete del Ministro/a o Encargado/a de Comunicaciones de la Institución, quien estimará y, posteriormente, solicitará evaluar la seguridad del recurso solicitado. Posteriormente notificará al solicitante.

Subproceso: Solicitud de Autorización de Creación o Eliminación de Red Social Institucional
Control: A.09.01.02 Acceso a las redes y a los servicios de red

Cada centro de responsabilidad deberá gestionar con el Gabinete del Ministro/a la autorización de creación o eliminación de redes sociales de uso institucional.

Para crear o eliminar una red social de uso institucional el jefe/a del centro de responsabilidad solicitante deberá hacer llegar esta solicitud de autorización al Jefe/a de Gabinete del Ministro/a o Encargado/a de Comunicaciones de la Institución. Deberá señalar el motivo y responsable de la red social.

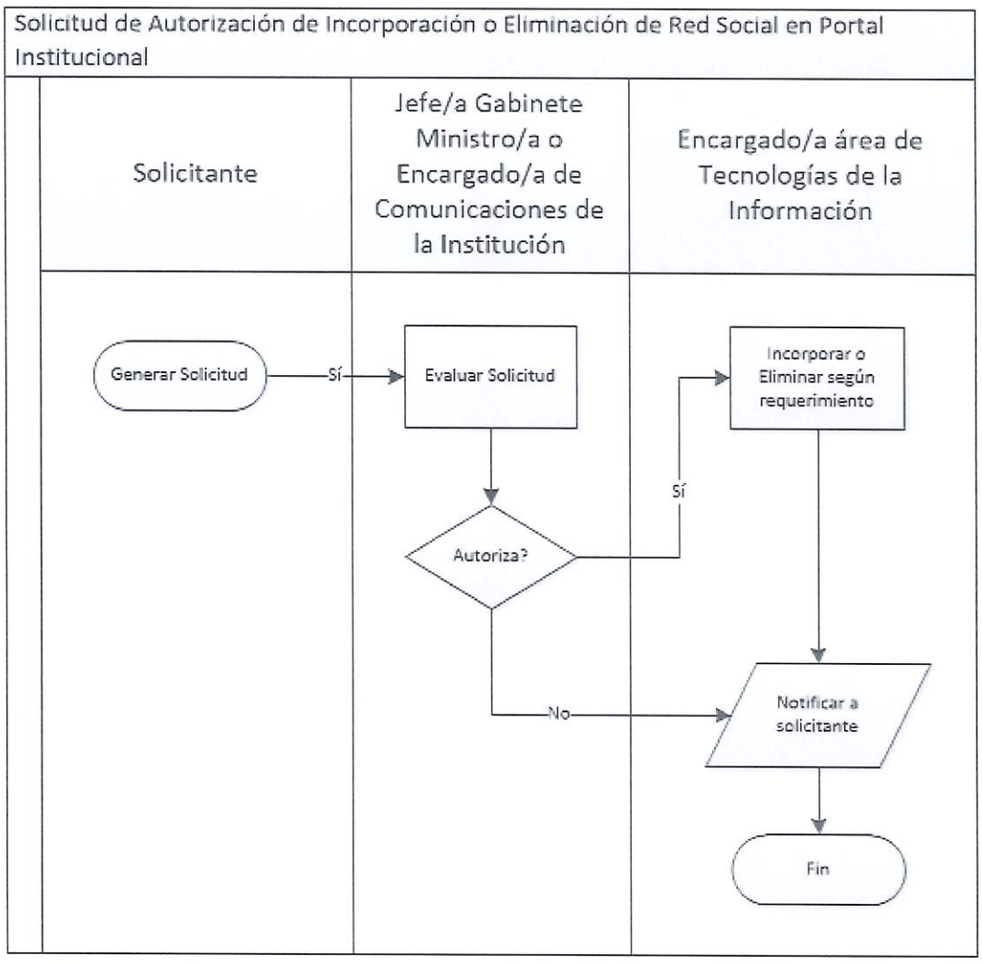


Descripción de Actividades: El/la solicitante generará una solicitud de creación o eliminación de Red Social Institucional la cual deberá ser autorizada por el Jefe/a del Centro de Responsabilidad. Esta solicitud deberá ser enviada al Jefe/a de Gabinete del Ministro/a o Encargado/a de Comunicaciones de la Institución, quien evaluará el requerimiento y solicitará al Encargado/a del área de tecnologías de la información, evaluar la seguridad del recurso solicitado. Posteriormente notificará al/la solicitante.

Subproceso: Solicitud de Autorización de Incorporación o Eliminación de Red Social en Portal Institucional
Control: A.09.01.02 Acceso a las redes y a los servicios de red

Cada centro de responsabilidad deberá gestionar con el Gabinete del Ministro/a la autorización de incorporación o eliminación de redes sociales en portal institucional.

Para incorporar o eliminar una red social en un portal institucional, el Jefe/a del Centro de Responsabilidad deberá hacer llegar esta solicitud de autorización al Jefe/a de Gabinete del Ministro/a o Encargado/a de Comunicaciones de la Institución, indicando el motivo, responsable de la red social y el portal institucional involucrado.

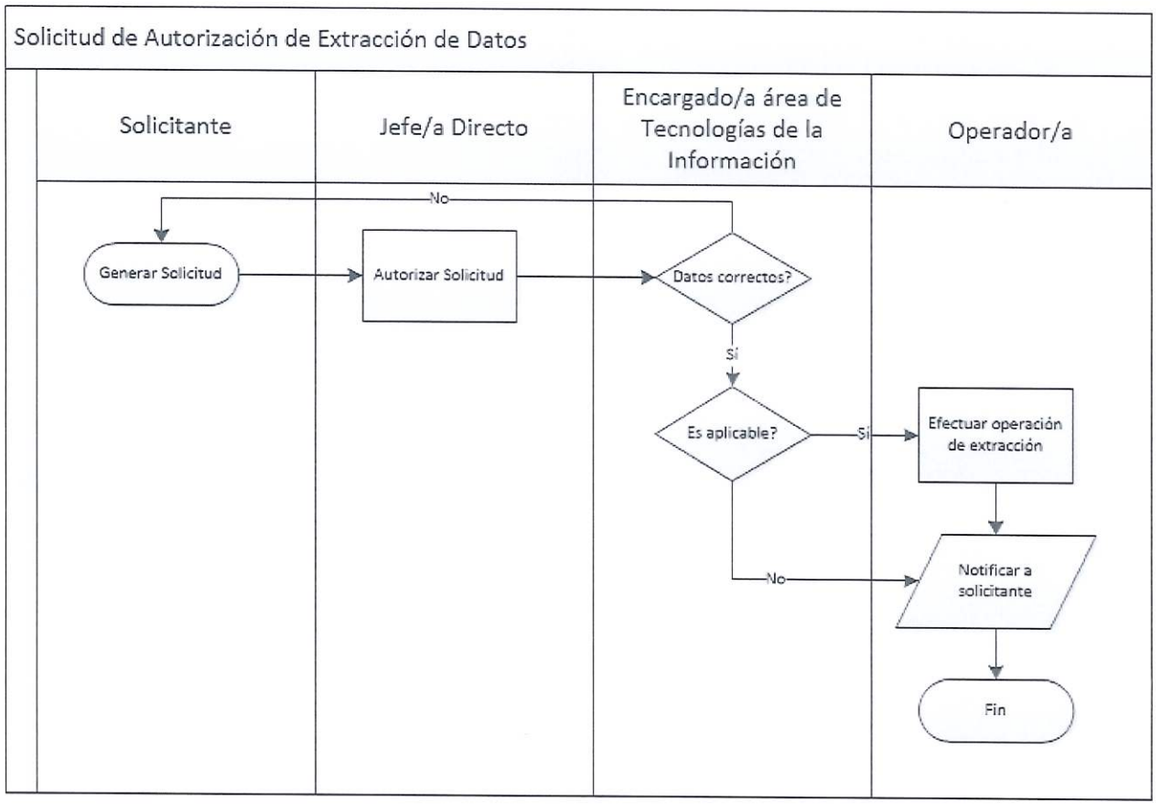


Descripción de Actividades: El/la solicitante generará una solicitud de incorporación o eliminación de red social en el portal institucional la cual deberá ser autorizada por el Jefe/a del Centro de Responsabilidad. Esta solicitud deberá ser enviada al Jefe/a de Gabinete del Ministro/a o Encargado/a de Comunicaciones de la institución, quien evaluará el requerimiento y solicitará al Encargado/a del área de tecnologías de la información, evaluar la seguridad del recurso solicitado. Posteriormente notificará al/la solicitante.

Subproceso: Solicitud de Autorización de Extracción de Datos

Control: A.09.04.01 Restricción de acceso a la información

La extracción de datos de sistemas, aplicaciones o portales se encuentra regulado y se requerirá una formalidad que autorice esta operación. Cada centro de responsabilidad deberá solicitar al propietario/a o encargado/a del sistema, aplicación o portal una autorización de extracción de datos. En esta solicitud se deberá señalar el motivo, detalle de la extracción, periodo y medio de entrega. Una vez autorizada la solicitud está será enviada al Encargado/a del Área de Tecnologías de la Información, quien autorizará o rechazará dicha solicitud. Si esta es autorizada el operador/a que esté a cargo debe realizar la función.



Descripción de Actividades: El/la solicitante generará una solicitud de extracción de datos. Esta deberá ser autorizada por el propietario/a o encargado/a del sistema, aplicación o portal. Autorizado esto el Encargado/a del Área de Tecnologías de la Información evaluará la solicitud, quien posteriormente solicitará al operador verificar que los datos se encuentren correctos y en base a esto efectuar la operación indicada. Finalmente notificará al solicitante.

6. Registros de Operación

Subproceso: Solicitud de Acceso a Carpeta Compartida
Control: A.09.01.02 Acceso a las redes y a los servicios de red
Formulario: *AIN-01*

AIN-01
Área de Tecnologías de la Información

Solicitud de acceso a carpetas compartidas

A.09.01.02

Fecha:

Solicitante

Nombre:

RUT:

Autorizado por Propietario/a de carpeta:

Nombre:

RUT:

Justificación:

Nombre de carpeta compartida: R | W

Fecha desde:

Fecha hasta:

Firma

Creación de Carpeta y Configuración de permiso

Nombre:

RUT:

Firma

Instalación de acceso directo

Nombre:

RUT:

Firma

Autorizado Encargado/a Área de Tecnologías de la Información

Nombre:

RUT:

Firma

Subproceso: *Solicitud de Acceso VPN*
Control: *A.09.01.02 Acceso a las redes y a los servicios de red*
Formulario: *AIN-02*

AIN-02
Área de Tecnologías de la Información
Solicitud de acceso VPN

A.09.01.02

Solicitante

Fecha: ☐

Habilitar: ☐ Fecha desde: ☐

Deshabilitar: ☐ Fecha hasta: ☐

Nombre: ☐

RUT: ☐

Correo: ☐

Justificación:

☐

Jefe/a directo

Nombre: ☐

RUT: ☐

_____
Firma

Operado por

Nombre: ☐

RUT: ☐

_____
Firma

Encargado/a Área de Tecnologías de la Información

Autorizado: ☐ Nombre: ☐

Rechazado: ☐ RUT: ☐

Observación: ☐

_____
Firma

Subproceso: *Solicitud de Registro y Cancelación de Registro de Usuario*
Control: *A.09.02.01 Registro y cancelación de registro de usuario*
Formulario: *AIN-03*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-03
Área de Tecnologías de la Información

Solicitud de registro y cancelación de registro de usuarios

A.09.02.01

Fecha: _____

Solicitante

Nombre: _____

RUT: _____ Fecha desde: _____

Fecha hasta: _____

☐ Registro

☐ Cancelación de registro

_____
Firma

Usuario/a

Nombre: _____

RUT: _____ Identificación: _____

Jefe/a (UGDP)

Autorizado: ☐ Nombre: _____

Rechazado: ☐ RUT: _____

Observaciones:

_____

_____
Firma

Encargado/a Área de Tecnologías de la Información

Autorizado: ☐ Nombre: _____

Rechazado: ☐ RUT: _____

_____
Firma

Observaciones:

_____

Operado por

Nombre: _____

RUT: _____

_____
Firma

Subproceso: *Solicitud Habilitación/Deshabilitación de Acceso a Aplicaciones*
Control: *A.09.02.02 Asignación de acceso de usuario*
Formulario: *AIN-04*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-04
Área de Tecnologías de la Información
Solicitud de habilitación/deshabilitación de acceso aplicaciones
A.09.02.02

Fecha:

Solicitante

Nombre:

RUT:

Justificación:

Aplicación	Perfil	Fecha desde	Fecha hasta	Habilitar	Deshabilitar

Autorización Jefe/a Directo o Propietario/a de Aplicación

Nombre:

RUT:

Firma

Operado por

Nombre:

RUT:

Firma

Encargado/a Área de Tecnologías de la Información

Nombre:

RUT:

Firma

Subproceso: *Solicitud Autorización de Derechos de Acceso Privilegiado*
Control: *A.09.02.03 Gestión de derechos de acceso privilegiado*
Formulario: *AIN-05*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-05
Área de Tecnologías de la Información
Solicitud de autorización de derechos de acceso privilegiado
A.09.02.03

Fecha: _____

Solicitante

Nombre: _____

RUT: _____ Identificación de usuario/a: _____

Aplicación o sistema: _____

Justificación:

_____

Fecha desde: _____ Fecha hasta: _____

- El uso inadecuado de los privilegios de administración del sistema (cualquier función o instalación de un sistema de información que permite al usuario/a anular los controles del sistema o la aplicación) es un factor importante que contribuye a los incumplimientos de los sistemas.

_____
Firma

Autoriza Jefe/a directo:

Nombre: _____

RUT: _____

_____
Firma

Encargado/a Área de Tecnologías de la Información

Autorizado: ☐ Nombre: _____

Rechazado: ☐ RUT: _____

Observaciones:

_____

_____
Firma

Operado por

Nombre: _____

RUT: _____

_____
Firma

Subproceso: *Solicitud de Eliminación o Ajuste de Derechos de Acceso*
Control: *A.09.02.06 Eliminación o ajuste de los derechos de acceso*
Formulario: *AIN-06*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-06
Área de Tecnologías de la Información

Solicitud de eliminación o ajuste de derechos de acceso

A.09.02.06

Fecha: ☐

Solicitante Jefe/a Directo

Nombre: ☐

RUT: ☐

Funcionario/a: ☐

Cese de funciones realizado por:
☐ Funcionario/a
☐ Jefe/a Directo

Verificar: ☐ Eliminación ☐ Ajuste de Acceso

- ☐ Carpetas compartidas
- ☐ Dependencias de la institución
- ☐ Datacenter
- ☐ Local a servidor
- ☐ Local administración de dispositivos de red
- ☐ Local administración de aplicaciones externas cloud u otros
- ☐ Autenticación de dominio de la institución
- ☐ Correo electrónico institucional

Observaciones:

☐

Firma

Encargado/a Área de Tecnologías de la Información

Autorizado: ☐ Nombre: ☐

Rechazado: ☐ RUT: ☐

Observaciones:

☐

Firma

Operado por

Nombre: ☐

RUT: ☐

Firma

Subproceso: *Solicitud de Creación y Cambio de Contraseña*
Control: *A.09.03.01 Uso de información de autenticación secreta*
Formulario: *AIN-07*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-07
Área de Tecnologías de la Información
Solicitud creación y cambio de contraseña

A.09.03.01

☐ Creación de contraseña.
☐ Cambio de contraseña por parte del usuario/a.
☐ Cambio de contraseña por parte del jefe/a directo.
☐ Cambio de contraseña por baja de usuario/a o cese de funciones.

Fecha: _____

Debo:

1. Resguardar la información de autenticación como confidencial, evitando su divulgación incluso a personas con autoridad.
2. Evitar registrar la información de autenticación en formatos tangibles (como papel) o digitales, a menos que se garantice un almacenamiento seguro y dicho método cuente con la aprobación correspondiente, como una bóveda de contraseñas.
3. Modificar la información de autenticación si hay indicios de un posible compromiso.
4. Al utilizar contraseñas como método de autenticación, elijir aquellas que cumplan con las siguientes características:
   I. Sean fáciles de recordar, pero a la vez seguras.
   II. No esten basadas en datos personales que puedan ser fácilmente inferidos o conocidos.
   III. Esten diseñadas para resistir ataques comunes, como los de tipo diccionario.
   IV. Evite secuencias de caracteres idénticos y no se limiten solo a números o letras.
   V. En caso de recibir una contraseña temporal, cámbiela en su primer uso.
5. La información de autenticación de un usuario/a no debe ser compartida.
6. Garantice una protección adecuada de las contraseñas al emplearlas en procedimientos automáticos de inicio de sesión y en su almacenamiento.
7. Evitar usar la misma información de autenticación para propósitos comerciales y no comerciales.

Usuario/a (Sólo cambio de contraseña por parte del usuario/a)

Nombre: _____

RUT: _____

_____
Firma

Autorizado por Jefe/a directo (Sólo cambio de contraseña por parte del jefe/a directo)

Nombre: _____

RUT: _____

Justificación: _____

_____
Firma

Operado por

Nombre: _____

RUT: _____

_____
Firma

***Por su seguridad su contraseña debe ser cambiada en el próximo inicio de sesión.**

REPÚBLICA DE CHILE · UNIDAD DE FISCALÍA INTERNA · MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA

Subproceso: *Solicitud Consulta Restricción de Acceso a la Información*
Control: *A.09.04.01 Restricción del acceso a la información*
Formulario: *AIN-08*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-08
Área de Tecnologías de la Información
Solicitud consulta restricción de acceso a la información

A.09.04.01

Fecha:

Solicitante Encargado/a Área de Tecnologías de la Información

Nombre:

RUT:

Nombre carpeta compartida: _____

_____
Firma

Operado por

Nombre:

RUT:

Usuario/a	Lectura	Escritura	Eliminación

_____
Firma

Subproceso: *Solicitud Consulta Estado Inicio Sesión Seguro*
Control: *A.09.04.02 Procedimiento de inicio de sesión seguro*
Formulario: *AIN-09*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-09
Área de Tecnologías de la Información
Consulta estado inicio sesión seguro

A.09.04.02

Fecha: _____

Solicitante Encargado/a Área de Tecnologías de la Información

Nombre: _____

RUT: _____

Verificación cumplimiento de:

☐ Proteger contra los intentos de inicio de sesión forzados.

☐ Terminar las sesiones inactivas después de un periodo de inactividad.

☐ No mostrar una contraseña que se ingrese.

Aplicable para: ☐ Sesión de Dominio

☐ Sesión de Aplicación

Nombre aplicación: _____

_____

Firma

Operado por

Nombre: _____

RUT: _____

Resultado: ☐ Cumple

☐ No cumple

Observaciones: _____

_____

Firma

Subproceso: *Solicitud Consulta Estado Sistema Gestión de Contraseñas*
Control: *A.09.04.03 Sistema de gestión de contraseñas*
Formulario: *AIN-10*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-10
Área de Tecnologías de la Información

Consulta estado sistema gestión de contraseñas

A.09.04.03

Fecha: _____

Solicitante Encargado/a Área de Tecnologías de la Información

Nombre: _____

RUT: _____

Verificación cumplimiento de:

- ☐ Forzar el uso de IDs de usuario/a y contraseñas individuales para mantener la responsabilidad
- ☐ Permitir a los usuarios/as seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para permitir los errores de entrada
- ☐ Imponer la selección de contraseñas de calidad
- ☐ Obligar a los usuarios/as a cambiar sus contraseñas al primer Inicio de sesión
- ☐ Imponer cambios regulares de contraseñas según sea necesario
- ☐ Mantener un registro de las contraseñas utilizadas anteriomente y evitar su nuevo uso
- ☐ No mostrar contraseñas en la pantalla mientras se ingresan
- ☐ Almacenar archivos de contraseñas de manera separada de los datos del sistema de aplicación
- ☐ Almacenar y transmitir contraseñas en forma protegida

Aplicabilidad para: ☐ Contraseña de dominio ☐ Contraseña de aplicaciones

_____
Firma

Operador por

Nombre: _____

RUT: _____

_____
Firma

Subproceso: *Solicitud de Autorización Uso Programas Privilegiados*
Control: *A.09.04.04 Uso de programas utilitarios privilegiados*
Formulario: *AIN-11*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-11
Área de Tecnologías de la Información
Solicitud de autorización de uso de programas privilegiados
A.09.04.04

Fecha: ☐

Solicitante

Nombre: ☐

RUT: ☐

Justificación:

☐

Programa:

_____
_____
_____
_____
_____
_____
_____

Autorización Jefe/a Directo o Propietario/a de Aplicación

Nombre: ☐

RUT: ☐

_____
Firma

Encargado/a Área de Tecnologías de la Información

Autorizado: ☐ Nombre: ☐

Rechazado: ☐ RUT: ☐

Justificación:

☐

_____
Firma

Subproceso: *Solicitud de Acceso a Código Fuente de Aplicación*
Control: *A.09.04.05 Control de acceso al código fuente de los programas*
Formulario: *AIN-12*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-12
Área de Tecnologías de la Información

Solicitud de acceso código fuente de aplicación

A.09.04.05

Fecha: _____

Solicitante

Nombre: _____

RUT: _____

Justificación:

Aplicación	Servidor	Carpeta	Fecha desde	Fecha hasta	Privilegio de Lectura	Privilegio Escritura

Autorización Jefe/a directo

Nombre: _____

RUT: _____

_____
Firma

Encargado/a Área de Tecnologías de la Información

Autorizado: ☐ Nombre: _____

Rechazado: ☐ RUT: _____

Observación:

_____
Firma

Subproceso: *Solicitud de Designación de Propietario de Carpeta Compartida*
Control: *A.09.01.02 Acceso a las redes y a los servicios de red*
Formulario: *AIN-13*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-13
Área de Tecnologías de la Información

Solicitud de Designación de Propietario de Carpeta Compartida

A.09.01.02

Jefe/a de División / Unidad / Comisión **Fecha:**

Nombre:

RUT:

Propietario/a Designado/a

Nombre:

RUT:

La designación de un propietario/a de carpeta compartida permitirá informar y solicitar autorización para la incorporación, modificación y/o eliminación de accesos de carpetas compartidas, posee por defecto permisos de lectura y escritura lo que da una capacidad para realizar cualquier tipo de modificación, eliminación de contenido y cambios en la estructura.

Nombre de la Carpeta

Firma

Encargado/a Área de Tecnologías de la Información

Autorizado: ☐ Nombre:

Rechazado: ☐ RUT:

Firma

Subproceso: *Solicitud de Autorización de Uso y Publicación de Contenido en Plataformas Digitales y Redes Sociales.*
Control: *A.09.01.02 Acceso a las redes y a los servicios de red*
Formulario: *AIN-14*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-14
Área de Tecnologías de la Información

Solicitud de Autorización de Uso y Publicación de Contenido en Plataformas Digitales y Redes Sociales
A.09.01.02

Solicitante
Nombre:

RUT:

Fecha:

Autoriza Jefe/a Directo
Nombre:

RUT:

Justificación:

Toda publicación de contenido en plataformas digitales de internet y redes sociales con recursos de la institución se encuentra regulado, por lo que la autorización de uso y publicación de contenido permite al funcionario/a o colaborador/a que por el rol de sus funciones, se encuentre habilitado para acceder a ellas y publicar contenido relacionado exclusivamente a la institución.

Identifique qué plataformas digitales o redes sociales requiere acceder con fines institucionales:

Firma

Jefe/a Gabinete Ministro/a o Encargado/a de Comunicaciones de la Institución

Autorizado: ☐ Nombre:

Rechazado: ☐ RUT:

Firma

Encargado/a Área de Tecnologías de la Información

Autorizado: ☐ Nombre:

Rechazado: ☐ RUT:

Firma

Subproceso: *Solicitud de Autorización de Creación o Eliminación de Red Social Institucional*
Control: *A.09.01.02 Acceso a las redes y a los servicios de red*
Formulario: *AIN-15*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-15
Área de Tecnologías de la Información

Solicitud de Autorización de Creación o Eliminación de Red Social Institucional

A.09.01.02

Fecha: _____

Solicitante

Nombre: _____

RUT: _____

Identifique qué plataformas digitales o redes sociales requiere crear o eliminar con fines institucionales:

Red Social	Crear	Eliminar

Justificación:

_____

_____
Firma

Jefe/a Gabinete Ministro/a o Encargado/a de Comunicaciones de la Institución

Autorizado: ☐ Nombre: _____

Rechazado: ☐ RUT: _____

_____
Firma

Encargado/a Área de Tecnologías de la Información

Autorizado: ☐ Nombre: _____

Rechazado: ☐ RUT: _____

Observaciones:

_____

_____
Firma

Subproceso: *Solicitud de Autorización de Incorporación o Eliminación de Red Social en Portal Institucional*
Control: *A.09.01.02 Acceso a las redes y a los servicios de red*
Formulario: *AIN-16*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-16
Área de Tecnologías de la Información

Solicitud de Autorización de Incorporación o Eliminación de Red Social en Portal Institucional

A.09.01.02

Solicitante **Fecha:**

Nombre:

RUT:

Portal Institucional:

Identifique qué plataformas digitales o redes sociales requiere incorporar o eliminar en el portal institucional señalado:

Red Social	Incorporar	Eliminar

Justificación:

Firma

Jefe/a Gabinete Ministro/a o Encargado/a de Comunicaciones de la Institución

Autorizado: ☐ Nombre:

Rechazado: ☐ RUT:

Firma

Encargado/a Área de Tecnologías de la Información

Autorizado: ☐ Nombre:

Rechazado: ☐ RUT:

Observaciones:

Firma

Subproceso: *Solicitud de Autorización de Extracción de Datos*
Control: *A.09.04.01 Restricción de acceso a la información*
Formulario: *AIN-17*

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

AIN-17
Área de Tecnologías de la Información
Solicitud de Autorizaciòn de Extracciòn de Datos

A.09.01.02

Solicitante Fecha: ☐

Nombre: ☐

Rut: ☐

Requerimiento de Información	Motivo	Destino
☐	☐	☐

Activo: _____ _____
Firma

Autorización Propietario/a del activo de Información

Autorizado: ☐ Nombre: ☐

Rechazado: ☐ Rut: ☐

Medio de almacenamiento

☐ Servicio en la nube de la institución

☐ Disco Duro Externo ☐ Pendrive ☐ Correo Electrónico

☐ Otro: _____ _____
Firma

Encargado/a Área de Tecnologías de la Información

Autorizado: ☐ Nombre: ☐

Rechazado: ☐ Rut: ☐

Observaciones:

☐ _____
Firma

Operado por

Nombre: ☐

Rut: ☐ _____
Firma

7. Documentos relacionados

Este procedimiento está relacionado directamente con controles contenidos en la Política de Acceso a la Información, documento vigente, del Ministerio Secretaría General de la Presidencia.

8. Indicador

El indicador mide la ejecución del procedimiento y subprocesos en base a las solicitudes que se ingresan y son atendidas en general.

Meta anual: *80%*
Fórmula de cálculo:

*(N° de solicitudes realizadas / N° de solicitud recibidas) *100*

Plazo de ejecución: *< 24 horas de recibida la solicitud*

9. Control"

Constan las firmas de los integrantes del Comité de Seguridad de la Información y del Oficial de Seguridad de la Información, ambos del Ministerio Secretaría General de la Presidencia.

2° DÉJASE sin efecto la Resolución Exenta N° 397, 15 de junio de 2020, dictada por el Ministerio Secretaría General de la Presidencia.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

REPÚBLICA DE CHILE MINISTERIO SECRETARIA GENERAL DE LA PRESIDENCIA

MACARENA LOBOS PALACIOS
Subsecretaria General de la Presidencia

RSA/CPS/STG/IRV
DISTRIBUCIÓN:
1. MINSEGPRES (Gabinete Subsecretaria)
2. MINSEGPRES (Unidad de Fiscalía Interna)
3. MINSEGPRES (División de Administración General:
   - Área de Tecnología de la Información)
4. MINSEGPRES (Oficina de Partes)