Ministerio Secretaría General de la Presidencia

Gobierno de Chile

APRUEBA LA POLÍTICA DE ACCESO A LA INFORMACIÓN DEL MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA Y DEJA SIN EFECTO LA RESOLUCIÓN EXENTA Nº 313, DE 2021, DE ESTE ORIGEN.

RESOLUCIÓN EXENTA Nº 1028 /

SANTIAGO, 01 DIC 2022

V I S T O S:

La Ley Nº 18.993, que crea este Ministerio, y su Reglamento Orgánico, contenido en el Decreto Supremo Nº 7, de 1991, de esta Secretaría de Estado; 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 Nº 83, de 2004, que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; el Decreto Supremo Nº 12, de 2022, que designa a la Subsecretaria General de la Presidencia; la Resolución Exenta Nº 694, de 2021, que aprueba la Política General de Seguridad de la Información del Ministerio Secretaría General de la Presidencia; la Resolución Exenta Nº 313, de 2021, que aprobó la Política de Acceso a la Información de esta Secretaría de Estado, todas las anteriores de este origen; 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, según la Ley Nº 18.993, que crea el Ministerio Secretaría General de la Presidencia, establece que dicha Secretaría de Estado, estará encargada de realizar funciones de coordinación y de asesoría directa al Presidente de la República, al Ministerio del Interior y Seguridad Pública y a cada uno de los Ministros, especialmente en materias políticas, jurídicas y administrativas, referentes a las relaciones del Gobierno con el Congreso Nacional, los Partidos Políticos y otras organizaciones sociales e instituciones de la vida nacional, así como propender al logro de una efectiva coordinación programática general de la gestión de gobierno.

2. Que, lo indicado precedentemente implica la generación, envío, recepción, almacenamiento y distribución de multiples 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, en razón lo anterior, es necesario contar con una Política de Acceso a la Información de este Organismo, con el objeto de controlar, asignar, registrar, cancelar, eliminar o ajustar los privilegios de acceso a los sistemas de información, a sus bases de datos y servicios de información de esta Secretaría de Estado, obteniendo un mayor control al acceso de la información y a las instalaciones en la que se procesa dicha información, formando parte, además, del Sistema de Seguridad de la Información de este Ministerio, por lo cual se enmarca en el cumplimiento de la Norma Chilena ISO 27001:2013, cuyo objetivo principal es la protección de la información, permitiendo a la organización evaluar los riesgos de información a los que se encuentra expuesta, así como

a la aplicación de controles para mitigarlos, para alcanzar un sistema de información en el que se dé la confidencialidad, integridad y disponibilidad de los activos de información

4. Que, a través de Resolución Exenta Nº 313, de 30 de abril de 2021, de este origen, se aprobó la Politica de Acceso a la Información de esta Secretaría de Estado, la cual se encuentra en permanente evaluacion y revisión por parte del Encargado de Seguridad de la Información, quien en conformidad con el Comité de Seguridad de la Información de este Ministerio han aprobado realizar las actualizaciones correspondientes a la citada política.

5. Que, de acuerdo con lo expuesto, y teniendo presente el Memorándum Nº 355, de 13 de octubre de 2022, del Jefe de la División de Administración General, el presente acto administrativo viene en aprobar la nueva Política de Acceso a la Información del Ministerio Secretaría General de la Presidencia y dejar sin efecto la Resolución Exenta Nº 313, de 2021, de este Ministerio.

R E S U E L V O:

1º.- APRUÉBASE la Política de Acceso a la Información del Ministerio Secretaría General de la Presidencia, cuyo texto es el siguiente:

"POLÍTICA DE ACCESO A LA INFORMACIÓN
DEL
MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA

Controles NCH ISO 27001: 2013 Relacionados

Control	***Nombre***
A.09.01.01	*Política de Control de Acceso*
A.09.01.02	*Acceso a las Redes y 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.09.02.05	*Revisión de los Derechos de Acceso de Usuarios*
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 de 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*
A.10.01.02	*Gestión de Claves*

Nota de confidencialidad

La información contenida en este documento es de uso exclusivo de la Institución y su personal. Cualquier uso no autorizado por terceros, copia o distribución de la información está estrictamente prohibido.

2022

Control de versiones

Fecha	*Versión*	*Responsables*	*Descripción*
30-05-2019	*1.0*	*Jorge Romero Vargas* *Solange Godoy Carrera*	*Elaboración de Documento*
17-04-2020	*1.1*	*Jorge Romero Vargas* *Solange Godoy Carrera*	*Incorpora definición de uso de plataformas digitales y redes sociales dentro de la intuición en Acceso a redes y servicios de red.*
15-06-2020	*1.2*	*Jorge Romero Vargas*	*Mejoras en la redacción del documento*
30-04-2021	*1.3*	*Jorge Romero Vargas*	*Incorpora en el Control 09.01.02 el almacenamiento de los registros de información para uso de auditorías. Mejoras en la redacción del documento. Incorpora nueva dependencia de la institución. Incorpora lineamiento interno para el acceso a administración de servidores internos y alojados en infraestructura tecnológica en la nube.*
26-07-2022	*1.4*	*Jorge Romero Vargas*	*Actualización de sección firmantes. Regula la creación de redes sociales de uso institucional. Incorpora Control A.09.02.05 Revisión de los derechos de acceso de usuarios. Regula el proceso de extracción de datos y uso de repositorios externos gratuitos para el control de versiones de aplicaciones. Regula el proceso de creación y registro de dominios. Remueve dependencia de Laboratorio de Gobierno.*

Introducción

El Ministerio Secretaría General de la Presidencia, en adelante el "Ministerio", dispone del presente documento, denominado "Política de Acceso a la Información", como parte integrante del Sistema de Seguridad de la Información.

En específico, la presente política se enmarca en el cumplimiento de la Norma Chilena ISO 27001:2013, cuyo objetivo principal es la protección de la información, permitiendo a la organización evaluar los riesgos de información a los que se encuentra expuesta, así como a la aplicación de controles para mitigarlos, para alcanzar un sistema de información en el que se dé la confidencialidad, integridad y disponibilidad de los activos de información. Dichos controles son los siguientes:

Control A.09.01.01 Política de Control de Acceso

"Se debe establecer, documentar y revisar una política de control de acceso basadas en los requisitos del negocio y de seguridad de la información".

- *Requisito de control, A.09.01.01, NCH ISO 27001:2013*

Control A.09.01.02 Acceso a las Redes y Servicios de Red

"Los usuarios solo 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 Privilegiado

"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.09.02.05 Revisión de los derechos de acceso de usuarios

"Los propietarios de activos deberán revisar los derechos de acceso de los usuarios a intervalos regulares".

- *Requisito de control, A.09.02.05, 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 todos los empleados 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 de control 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 de control 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 de control A.09.04.05, NCH ISO 27001:2013*

Control A.10.01.02 Gestión de Claves

"Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante toda su vida útil".

- *Requisito de control A.10.01.02, NCH ISO 27001:2013*

1. Alcance

Esta política debe aplicarse a todos los funcionarios/as y servidores/as públicos del Ministerio o a cualquier tercero que pueda estar prestando servicios, todos en conjunto denominados "usuario o usuarios", y que requieran la utilización de equipos tecnológicos para acceder a la información perteneciente al servicio.

2. Objetivo

Esta política tiene por objetivo controlar el acceso a la información de la institución, el acceso a redes y servicios de red, el registro y cancelación del registro de usuario, la asignación de acceso a usuarios, la gestión de derechos de acceso privilegiado, la eliminación o ajuste de los derechos de acceso, el uso de la información de autenticación secreta, las restricciones de acceso a la información, los procedimientos de inicio de sesión seguro, el control de uso de programas utilitarios privilegiados, el control de acceso al código fuente de los programas y la gestión de contraseñas y claves.

3. 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 el debido cumplimiento a esta política. Asimismo, es responsabilidad:

- ***Del Comité de Seguridad de la Información**, la revisión de este documento, velar por el cumplimiento, actualización y difusión de la política.*

- ***Del encargado de Seguridad de la Información**, la aplicación de esta política, así como de su difusión y mantener revisiones periódicas del cumplimiento de esta norma en el Ministerio.*
- ***Del Jefe de la Oficina de Computación, en adelante "Unidad de Tecnologías de la Información"**, mantener en condiciones aceptables los dispositivos instalados para el control de los accesos físicos, redes, servicios de red, creando y asignando credenciales de acuerdo al requerimiento 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 físico y lógico del servicio.*
- ***Del Área de soporte**, mantener el resguardo, control y asignación de las contraseñas de los sistemas, equipos o aplicaciones, el acceso a sistemas de redes con que cuente el Ministerio, así como, la eliminación o ajuste a dichos accesos por necesidad del servicio o petición de la jefatura.*
- ***De los/las Jefes/as de División, Comisión, Unidad**, la aplicación de esta política en las dependencias a su cargo, así también, el cumplimiento, difusión y supervisión del apego de esta norma del personal a su cargo.*
- ***De los Usuarios**, actuar en base a lo establecido en esta norma. Resguardando los recursos y la información contenida, disponiendo de usuario y clave de acceso que es privada, personal e intransferible. Además, del resguardo de la información contenida en el equipo a su cargo.*

4. Mecanismo de difusión

Es responsabilidad del Comité de Seguridad de la Información la difusión de este documento, el que se enviará por correo electrónico a los usuarios y deberá permanecer en la intranet institucional a disposición de todo el personal del Ministerio.

5. Evaluación y revisión

El tiempo de evaluación y revisión estándar para este documento, será cada dos años. No obstante, podrá revisarse cuando la situación lo amerite o la autoridad lo disponga.

El Encargado de Seguridad de la Información propondrá en sesión del Comité de Seguridad de la Información los cambios y/o actualizaciones que sean necesarios para la presente política, quien los revisará, observará y aprobará para su correspondiente envió al Jefe de Servicio.

6. Definiciones

a) Control A.09.01.01 Control de acceso

Se debe tener control del acceso para el personal de la institución y las personas externas a este, siendo necesario que cada usuario mantenga el resguardo del acceso físico y lógico, teniendo claro que el no respetarlo pone en riesgo la seguridad de la información del Ministerio.

Asimismo, se debe controlar el acceso a la sala de servidores y todas las estaciones de trabajo en que se encuentre almacenada información sensible o crítica.

Por su parte, se debe establecer un control de acceso que tenga como objetivo impedir el acceso no autorizado a los sistemas de información, implementando mecanismos de seguridad, autenticación y autorización en los accesos de los usuarios y otras personas ajenas al servicio, además de concientizar al personal de la responsabilidad que tienen frente a la utilización de las contraseñas y equipos informáticos.

Se deberá resguardar el acceso de las personas no autorizadas por el servicio a todo tipo de información y redes del Ministerio. Los usuarios deberán tener asignado un nombre de usuario y contraseña para acceder al dominio del servicio, la que automáticamente solicitará la actualización cada 3 meses.

El usuario no está autorizado para acceder a la red ministerial desde el exterior. Si se requiere dicho acceso deberá realizarlo a través de acceso seguro mediante VPN, que deberá ser solicitado a la Unidad de Tecnologías de la Información.

El acceso a la red ministerial inalámbrica será mediante usuario y contraseña. Deberán existir redes inalámbricas separadas que permitan controlar y aplicar filtros de contenido de forma independiente, ya sea para funcionarios/as y colaboradores/as de cada una de las dependencias como también para visitas, quienes podrán hacer uso del servicio exclusivamente para navegación hacia internet.

Para el acceso físico se deberá definir y utilizar perímetros de seguridad para la protección de las áreas que contengan información sensible o crítica, además de las instalaciones de procesamiento de información.

El Ministerio, tiene dependencias ubicadas en Santiago y Valparaíso, por lo que estos espacios deberán tener un resguardo para el acceso a personas no autorizadas y mantener el control sobre el perímetro de acceso. Las dependencias del servicio son:

- *Palacio de La Moneda.*
- *Edificio Moneda 1160, entre piso, pisos 1-2-3-4-5 y 6.*
- *Edificio Moneda Bicentenario, piso 9.*
- *Congreso Nacional, Cámara de Diputados, piso 2.*
- *Congreso Nacional, Senado de la República, piso 4.*

Las áreas seguras deberán estar protegidas por controles que garanticen el acceso a las personas autorizadas, para lo cual, se deberán definir restricciones como:

- *Puertas con acceso restringido*
- *Conserjería externa en el caso de los edificios de Moneda Nº 1160, Edificio Moneda Bicentenario y control de acceso en el Congreso Nacional.*
- *Video vigilancia en todas las dependencias del Ministerio.*
- *Credenciales de acceso en Palacio de La Moneda y Moneda Bicentenario.*
- *En la oficina de la Unidad de Tecnologías de la Información se deberá controlar el acceso:*
  - *El registro de ingreso a dicha Unidad será mediante huella digital para los usuarios del Ministerio y datos como nombre y Rut para las personas externas al servicio.*
  - *Video vigilancia mediante cámaras de seguridad ubicadas en el interior y exterior de dicha Unidad, así como en la puerta de acceso de la sala de servidores.*
  - *Doble puerta de entrada en la citada Unidad.*

b) Control A.09.01.02 Acceso a redes y servicios de red

El Ministerio deberá adoptar líneas de control para el acceso físico y lógico a los recursos tecnológicos de la institución.

El control de acceso se basa en los requisitos del negocio y de la seguridad de la información y su objetivo es impedir el acceso no autorizado a los sistemas de información, implementando la seguridad a través de herramientas de autenticación y autorización, concientizando a los usuarios de su responsabilidad frente a la utilización responsable de contraseñas en sus equipos.

La Unidad de Tecnologías de la Información estará a cargo del monitoreo del uso de los servicios de red en el Ministerio.

No se podrá acceder a la red interna del Ministerio, a sus bases de datos y a los servidores de aplicaciones en todos sus ambientes, desde el exterior.

Sin perjuicio de lo anterior, en casos excepcionales se podrá acceder a la red interna del Ministerio, para lo cual los usuarios deberán realizarlo a través de una conexión segura mediante VPN, la cual será actualizada cada 3 meses. Para lo anterior, las cuentas de acceso mediante VPN serán constantemente monitoreadas, deshabilitando las que no se encuentren en uso.

Se encuentra prohibido hacer uso de este recurso hacia la institución mediante conexiones Wifi-abiertas, proporcionadas de forma gratuita en lugares públicos. Así, el acceso informático a la infraestructura digital del Ministerio deberá hacerse mediante redes privadas con modalidad de cifrado de forma mínima en WPA2-PSK y WPA/WPA2-PSK. El dispositivo que accede deberá poseer un antivirus actualizado de forma obligatoria, certificado por la institución. Además, se deberá privilegiar el trabajo conectado directamente a su computador institucional mediante VPN haciendo uso de su computador personal sólo como terminal, evitando mantener información de carácter institucional en un computador personal.

El acceso a servidores alojados en la infraestructura tecnológica en la nube deberá ser realizado exclusivamente desde la red interna de la institución, para ello, se deberán realizar configuraciones especiales o VPN Sitio a Sitio en la cual se genere una relación de confianza entre la red interna institucional y la infraestructura tecnológica en la nube.

La administración de los servidores alojados en la infraestructura tecnológica en la nube deberá ser realizada en base a un servidor de salto o "Jump Server" el cual tendrá acceso exclusivo a cada uno de ellos, con el fin de aumentar la seguridad en el acceso.

Por su parte, podrán utilizarse otros mecanismos de seguridad excepcionales que la Unidad de Tecnologías de la Información considere adecuados de implementar, siempre con el objeto de resguardar la integridad y seguridad de la información institucional.

La autenticación para la administración de infraestructura tecnológica en la nube deberá considerar obligatoriamente un doble factor de autenticación y se deberá llevar un control señalando quiénes están autorizados a acceder, cómo deberán acceder, desde dónde y en qué circunstancias.

Toda publicación de contenido en plataformas digitales de internet y redes sociales con recursos de la institución se encuentra regulado. Las áreas de comunicaciones del Gabinete de Ministro/a y Subsecretario/a, por la naturaleza de sus funciones, se encontrarán autorizados para realizar estas actividades de forma directa. No obstante, la institución deberá mantener un registro de actividades histórico del Corta Fuego Institucional, identificando el usuario que accede al recurso. Esta información deberá ser monitoreada, analizada y protegida por un tiempo determinado. Podrá ser utilizada en auditorías de la Institución.

No obstante, deberán existir autorizaciones especiales para el personal que para el ejercicio de sus funciones deben acceder a ellas y publicar contenido, el que deberá estar siempre relacionado exclusivamente a la institución.

Por su parte, la Unidad o persona encargada de la cuenta genérica de la institución en redes sociales, deberá comunicar a la Unidad de Tecnologías de la Información los respectivos usuarios y contraseñas de acceso, para responder a posibles imprevistos como continuidad operacional dentro de la institución.

La cuenta oficial del Ministro/a y Subsecretario/a deberá ser administrada por ellos o quienes designen.

Todo lo anterior, con el fin de asegurar el cumplimiento de la normativa vigente y evitar actos que contravienen especialmente el principio de la probidad administrativa.

La creación de redes sociales con información relacionada a la institución deberá ser autorizada por el Gabinete del Ministro/a, quienes aprobarán su uso y publicación en portales oficiales. Deberá existir un catálogo de redes sociales asociadas a la institución, señalando además el responsable de la administración del contenido y en los portales institucionales en las que se encuentra embebido.

La creación de dominios de gobierno y registros de dominios públicos deberá contar con la autorización del Gabinete del Ministro/a, los cuales deberán ser inscritos a nombre de la institución.

Los dominios externos asociados a la institución deberán ser administrados por la Unidad de Tecnologías de la Información, quienes solicitarán e informarán su renovación antes de su periodo de expiración.

c) Control A.09.02.01 Registro y cancelación del registro de usuario

Cada nuevo usuario poseerá una identificación única en el dominio de la institución. Con esta identificación junto con una clave de acceso podrá acceder a los recursos y servicios, tales como correo electrónico, computador personal y otras aplicaciones internas.

Una vez que el usuario cese en sus funciones dentro de la institución, la cuenta será revocada, junto con los derechos de acceso a servicios y aplicaciones.

d) Control A.09.02.02 Asignación de acceso de usuario

A los usuarios se les asignará nombre de usuario y contraseña única para acceder al dominio que le corresponda, ejemplo [inicialnombre][apellido]@minsegpres.gob.cl

La asignación de acceso mediante VPN requerirá de la autorización de la Jefatura directa del funcionario/a o trabajador/a de la institución.

Para el acceso a la red inalámbrica, será mediante contraseña y a un espacio de navegación restringido. Para usuarios de la institución, existirán redes con acceso a internet y en algunos casos con acceso a recursos internos del Ministerio, lo cual será regulado por la Unidad de Tecnologías de la Información, realizando la configuración de acceso directamente. En el caso de visitas, solo tendrán acceso a internet y no podrán acceder a los recursos internos de la institución.

Se deberá llevar una definición y control de "niveles de acceso" o "roles" para cada sistema o plataforma, la cual deberá ser validada de forma periódica.

e) Control A.09.02.03 Gestión de derechos de acceso privilegiado

Para el acceso a las redes y a los servicios, los usuarios deberán tener acceso directo y servicios de red para los que han sido autorizados.

Se deberá restringir y controlar la asignación y uso de los derechos de accesos privilegiados. Esta asignación de derechos de acceso deberá contar con la autorización formal de la jefatura directa del personal, de acuerdo con las funciones, rol o cargo que desempeñe en el servicio, para lo que se deberán identificar los derechos de acceso. La jefatura de la Unidad de Tecnologías de la Información evaluará dicha solicitud y deberá considerar la pertinencia de los accesos privilegiados.

f) Control A.09.02.05 Revisión de los derechos de acceso de usuarios

La Unidad de Tecnologías de la Información, verificará mensualmente los derechos de acceso de usuario en cada uno de los activos de administración que administre. Para ello en base a la nómina de altas y bajas de usuario provista por la Unidad de Gestión y Desarrollo de las Personas corroborará la actualización de accesos y efectuará directamente la revocación de estos en caso de que corresponda. Cabe destacar que será responsabilidad de cada División/Unidad informar cualquier cambio de acceso relacionado a un funcionario/a o colaborador/a, debido al cambio de funciones que este presente. Se deberá contar con una nómina de accesos a portales y aplicaciones que será compartida a cada responsable del activo de información institucional para que pueda corroborar y certificar cada funcionario/a o colaborador/a existente y en el rol asignado.

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

La Unidad de Tecnologías de la Información, deberá verificar los controles de acceso a los sistemas, con la finalidad de revisar que los usuarios tengan el acceso a aquellos recursos de red y servicios de las plataformas tecnológicas para los que fueron autorizados y realizar la mantención correspondiente de estos privilegios.

La asignación y el uso de los derechos de acceso deberá ser restringido y controlado, sólo se dará por medio de una autorización formal en la que se debe identificar los derechos de accesos, eliminación o ajuste de estos derechos.

Una vez terminada la relación laboral, contrato o acuerdo, se deberán retirar todos los derechos de acceso, correo electrónico, carpetas compartidas, sistemas o plataformas tecnológicas, entre otras, de todos los colaboradores y usuarios externos (proveedores) a la información y también a las instalaciones de procesamiento de información, una vez que termine la relación laboral, servicio o acuerdo con el Ministerio, y así proteger y mitigar cualquier riesgo de la información y las instalaciones de procesamiento.

h) Control A.09.03.01 Uso de información de autenticación secreta

Los usuarios del Ministerio deben dar estricto cumplimiento de las prácticas de la organización en uso de la información de autenticación secreta.

El personal deberá ingresar el nombre de usuario y contraseña, que se validará con el registro de usuarios en la base de datos del sistema; si no se valida se deberá enviar un mensaje automático dando cuenta de error. Si se valida se deberá registrar un acceso correcto a la autenticación. Si los accesos erróneos al sistema supera cuatro intentos, la cuenta de acceso será deshabilitada o bloqueada automáticamente.

Si existiera una sesión activa se deberá realizar la expiración de ambas sesiones, se deberá cambiar aleatoriamente la contraseña y deberá ser enviado al usuario por correo electrónico.

La contraseña deberá contar con un mínimo de 10 caracteres, que sea lo suficientemente difícil de copiar y lo suficientemente fácil de recordar, además, se deberá recomendar la no utilización de esta contraseña para fines comerciales.

i) Control A.09.04.01 Restricción de acceso a la información

La restricción del acceso a la información y a todas las funciones del sistema de aplicaciones será, de acuerdo con el control de acceso tanto, físico como lógico, contenido en esta norma.

Para obtener accesos a sistemas de información, se deberá solicitar autorización de la jefatura, con el fin de resguardar y restringir los accesos, tanto en los sistemas operativos como en los dispositivos móviles asignados por el servicio, para lo que, el personal deberá tomar los resguardos, criterio y responsabilidad para evitar la fuga o pérdida de información. La Unidad de Tecnologías de la Información deberá tener el control de los accesos a todas las funciones de los aplicativos, con el fin, de controlar los datos a los que puedan acceder los usuarios previa autorización, resguardando los accesos a la información y aplicaciones sensibles o críticas de la institución.

El proceso de extracción de datos para cualquier aplicación o portal administrado por la Unidad de Tecnologías de la Información en un ambiente productivo se encontrará regulado. Toda entrega de información de ambientes productivos ya sea total o parcial, deberá ser autorizada por el responsable del activo de información. Se deberán tomar los resguardos necesarios para la transferencia de información, deberá considerar el uso de autenticación de usuario, claves de acceso o códigos de autorización con tiempos de expiración específicos. En caso de proveedores externos, deberá considerar un acuerdo de confidencialidad de la información y responsabilidad de uso. En caso de existir transferencias de información mediante procesos automatizados, deberá existir un convenio de colaboración entre las entidades relacionadas, el cual deberá ser autorizado por el Jefe de Servicio.

j) Control A.09.04.02 Procedimiento de inicio de sesión seguro

El Ministerio, deberá contar en sus aplicaciones y sistemas con credenciales de acceso mediante usuario y contraseña.

Se deberá contar con un plan, guía o procedimiento que dé cuenta del acceso a los sistemas operativos, los que deberán estar protegidos mediante inicio de sesión seguro, validando los datos de entrada a los sistemas a los que puedan acceder los usuarios.

El sistema deberá contar con tres intentos para iniciar sesión. Al cuarto intento fallido el sistema se bloqueará, para lo cual, el usuario deberá tomar contacto con la Unidad de Tecnologías de la Información o deberá esperar 10 minutos para poder nuevamente ingresar a su equipo.

Las contraseñas no se mostrarán en texto al ser ingresadas, para evitar que sean copiadas y así mitigar riesgos de ingreso no autorizado.

El sistema no deberá mostrar ningún tipo de información mientras el proceso de inicio esté completo.

Cuando el equipo computacional esté inactivo deberá contar con 10 minutos antes de ser bloqueado automáticamente, teniendo que reingresar las credenciales para seguir con sus funciones.

k) Control A.09.04.04 Uso de programas utilitarios privilegiados

El uso de programas utilitarios privilegiados en el Ministerio, se encuentran restringidos y controlados por la Unidad de Tecnologías de la Información.

Se deberá limitar el uso de programas de utilidad que puedan tener impacto en los controles de sistemas, por lo que se deberá definir estrictamente a los usuarios que podrían tener acceso y uso de estas aplicaciones promoviendo limitar el uso a equipos de administración de sistemas.

La jefatura directa deberá solicitar los permisos correspondientes para su personal, durante el tiempo que sea necesario, directamente a la Jefatura de la Unidad de Tecnologías de la Información o al Área de Soporte, el que otorgará las credenciales solicitadas.

La Unidad de Tecnologías de la Información deberá eliminar o deshabilitar y controlar las credenciales a los programas que no sean necesarios tener acceso.

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

El Ministerio, a través de la jefatura de la Unidad de Tecnologías de la Información, deberá tener el control total de los accesos al código fuente de cada programa y/o aplicaciones con las que cuenta el servicio.

Si existieran usuarios que por necesidad de sus tareas debieran acceder al código fuente, deberá solicitar autorización mediante su jefatura directa. La jefatura de la Unidad de Tecnologías de la Información deberá evaluar si es necesario otorgar el permiso que corresponda, entregando dicho permiso por tiempo limitado y estrictamente controlado, retirando los accesos en cuanto se haya realizado la función para la que fue solicitada.

Está estrictamente prohibido el uso de repositorios externos gratuitos para almacenamiento de código fuente o control de versiones de aplicaciones o portales de la institución.

m) Controles A.09.04.03 A.10.01.02 Gestión de contraseñas y claves

La asignación de clave deberá ser realizada para cada persona, no se permitirá el uso de claves compartidas, salvo que sea con autorización directa de la jefatura.

Una vez asignada la clave de acceso, el usuario tendrá la obligación de cambiarla por una clave personal.

Si el usuario olvida, bloquea o extravía su clave de acceso, deberá comunicarse con el Área de Soporte para la solución del evento.

Las claves de acceso no deberán estar escritas en ningún medio impreso en lugar visible.

La clave de acceso a los equipos tendrá una duración de 3 meses. Al finalizar este periodo, los usuarios deberán recibir una advertencia que indique que se debe cambiar la contraseña.

Las claves no deben ser almacenadas en programas o sistema que puedan ser leídos, en equipos que no cuente con un control de acceso adecuado o en lugares donde el personal no autorizado tenga acceso.

La contraseña deberá contar con un mínimo de 10 caracteres, los cuales deberán ser alfanuméricos y considerar al menos 1 caracter especial.

No se permitirá la utilización de claves similares a las usadas previamente hasta 3 periodos.

Si se detecta que un usuario está haciendo uso de la clave de acceso de otro, deberá avisar a su jefatura directa y ser comunicada a la Unidad de Tecnologías de la Información.".

2º.- DÉJASE SIN EFECTO la Resolución Exenta Nº 313, de 30 de abril de 2021, de esta Secretaría de Estado, que aprueba la Política de Acceso a la Información del 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/STG/JRV/VVH
DISTRIBUCIÓN:
1. MINSEGPRES (Gabinete Subsecretaria)
2. MINSEGPRES (Unidad de Fiscalía Interna)
3. MINSEGPRES (División de Administración General:
   - Unidad de Tecnologías de la Información)
4. MINSEGPRES (Oficina de Partes)