PS-NC-003

POLITICA IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Sistema de Gestión de Seguridad de la Información – Nivel Central

Versión Oficial Actual v03 – Octubre del 2019

	Responsable	Fecha	Firma
Elaborado	Rodrigo Vidal / Encargado PMG SSI	Octubre 2019	
Revisado	José Villa / Área Seguridad de la Información (Representante Comité de Seguridad)	Octubre 2019	
Aprobado	Gabriel Reveco / Encargado Ciberseguridad (Presidente Comité de Seguridad de la Información)	Octubre 2019	

MINISTERIO DE SALUD COMITÉ SEGURIDAD DE LA INFORMACIÓN

MINISTERIO DE SALUD ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Contenido

1 PROPOSITO

El Ministerio de Salud (en adelante MINSAL) considera que todos los sistemas computacionales que permitan acceder a la información que éste administra, deben contar con un sistema de identificación y autenticación de usuarios que permita garantizar que sólo personal debidamente autorizado tiene acceso a la información, considerando además sólo el acceso a través de claves seguras.

Esta política define los estándares y controles que deben cumplirse para el acceso a los recursos y sistemas computacionales del MINSAL en el nivel central, considerando la identificación y autenticación de usuarios que acceden a las plataformas institucionales.

2 ALCANCE O AMBITO DE APLICACIÓN

Esta política aplica a todos los recursos computacionales de MINSAL en el nivel central para los que es necesario controlar el acceso. Define el uso de nombres de usuario y contraseñas, así como sus solicitudes y administración.

Es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para la Subsecretaría de Salud Pública y la Subsecretaría de Redes Asistenciales.

En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de esta política corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Alcance de Dominios y Controles de Seguridad de la Información (Nch-ISO 27001:2013)		
Nombre del Dominio	ID Control ISO 27001	Nombre del Control
Control de acceso	A.09.02.01	Registro y cancelación de registro de usuario
	A.09.03.01	Uso de información de autenticación secreta
	A.09.04.03	Sistema de gestión de contraseñas

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- Marco Normativo
  - NCh-ISO27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
  - El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.

- Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
- Leyes relacionadas

- **Documentos Relacionados**
  - Política protección de los datos y privacidad de la información personal.
  - Procedimiento gestión de derechos de acceso y protección de activos.
  - Procedimiento gestión de incidentes de seguridad de la información.

4 ROLES Y RESPONSABILIDADES

- **Operaciones TIC**
  - Establecer mecanismos de información para permitir a los usuarios supervisar la actividad normal de su cuenta, así como alertarlos oportunamente sobre actividades inusuales.
  - Proponer controles y resguardo de claves de acceso.
  - Velar por el cumplimiento de las políticas, estándares y procedimientos establecidos para los controles de identificación y autenticación.

- **Operaciones TIC (Desarrollo de Sistemas / Soporte) / Áreas de Negocio que cuenten con equipos de Desarrollo de Sistemas.**
  - Gestionar los accesos de usuarios a las aplicaciones, resguardar las contraseñas de administración. Velar por que el desarrollo de las aplicaciones se realice en concordancia con los requisitos descritos en esta política.
  - Mantener un registro actualizado de las reasignaciones. Autorizar la asignación de usuarios y contraseñas para personal externo a la institución, cuando corresponda.
  - Aprobar controles y resguardo de claves de acceso con privilegios.

- **Administrador de Sistemas**
  - Gestionar y ser responsable de los accesos de usuarios a las aplicaciones en las que tienen derechos de administración, resguardar las contraseñas de administración.

- **Encargado de Seguridad de la Información / Encargado de Ciberseguridad**
  - Gestionar la resolución de incidencias en el manejo de las cuentas de usuarios.

- **Jefes de División, Departamento o Subdepartamento**
  - Solicitar formalmente a la División TIC, cada vez que sea necesario, realizar algún cambio en el perfil de privilegios de acceso para una cuenta de usuario de su dependencia.

- Informar a la División TIC y RRHH cualquier cambio de funciones o alejamiento de las personas que tiene a su cargo.

- **Departamento de Gestión de Personas**
  - Actuar en forma coordinada con la División TIC, para notificar de las altas, bajas y traslados de miembros del personal MINSAL.

- **Funcionarios de MINSAL**
  - Cada miembro del personal MINSAL debe tener asignada una cuenta de usuario segura (con su correspondiente usuario y contraseña), para acceder a los recursos y activos de información de la red informática institucional, y asumirá la responsabilidad de la correcta utilización de esta credencial, teniendo presente que los datos de su cuenta de usuario son personales e individuales[1].

5 MATERIAS QUE ABORDA.

- Registro y cancelación de registro de usuario.
- Uso de información de autenticación secreta.
- Sistema de gestión de contraseñas.

6 DIRECTRICES DE LA POLÍTICA

6.1 Cumplimiento de la legislación

Las medidas de control de acceso a la información definidas deben cumplir y ser consistentes con lo dispuesto por las normas y requerimientos legales definidos en el documento “Normativa del Sistema de Gestión de Seguridad de la Información”.

6.2 Definiciones asociadas a la Seguridad de las Telecomunicaciones

Programas de utilidad (también conocidos como rutinas de servicios):
Un programa de utilidad es una aplicación de software que permite la resolución de problemas y diagnóstico de fallas. Un programa de utilidad puede escanear un sistema u otro programa para encontrar errores. Las utilidades adicionales incluyen programas de copia para seguridad de datos, software para comprimir archivos y herramientas para desinstalar otros programas.

Un programa de utilidad está diseñado para analizar, configurar, optimizar y mantener un equipo, incluyendo el hardware, sistema operativo, software de aplicaciones y almacenamiento de datos.

[1] las responsabilidades en el tratamiento de los datos y sanciones al incumplimiento de las políticas de seguridad se encuentran definidas en la Política General de Seguridad de la Información y la Política protección de los datos y privacidad de la información personal

Ejemplos de programas de utilidad son:

- Anti-virus
- Restaurador del sistema operativo
- Defragmentador del disco duro
- Particionador del disco duro
- Programas de respaldo
- Limpiadores del registro
- Administrador de archives
- Testeadores de memoria
- Protectores de pantalla

6.3 Registro y cancelación de registro de usuarios

Todo acceso de usuario a los recursos de red o sistemas de información de MINSAL debe ser solicitado y autorizado por la Jefatura correspondiente al Departamento TIC, estos accesos deben contar con un mecanismo que identifique al usuario (cuenta de usuario) y lo autentifique (clave de acceso).

Este mecanismo de autentificación (claves de acceso, dispositivo u otro) debe ser asignado individualmente, quedando prohibido el uso de un nombre de usuario ajeno o facilitar el usuario y su contraseña personal a un tercero.

Toda vez que un funcionario o colaborador que cuente con una cuenta de usuarios abandone la organización, el Departamento de Gestión de Personas deberá notificar al Departamento TIC cuando se deba deshabilitar o eliminar su cuenta de usuario.

La Jefatura a cargo de la dependencia será responsable de notificar por escrito al Departamento TIC sobre el ingreso, salida o traslado de un usuario a su cargo. Esto con el fin de que se creen, inhabiliten, modifiquen o eliminen privilegios de acceso a las diferentes plataformas, dominios y dispositivos correspondientes.

La administración de los accesos de las cuentas de usuarios se llevará de acuerdo con lo establecido en el procedimiento de gestión de derechos de acceso.

6.4 Administración de la información de autenticación secreta de los usuarios (usuario y contraseña)

La administración de los accesos de las cuentas de usuarios se llevará de acuerdo con lo establecido en el procedimiento de gestión de derechos de acceso.

6.5 Uso de la información de autenticación secreta

Todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para las Subsecretarías de Salud Pública y Redes Asistenciales tienen la obligación de cumplir con las siguientes directrices:

Mantener la información de autenticación secreta como confidencial, asegurándose de que no se divulgue a ninguna otra parte, incluidas las personas con autoridad

Evitar mantener un registro (es decir, en papel, archivo de software o en un dispositivo de mano) de la información de autenticación secreta, a menos que esto se pueda almacenar de manera segura y de que el método de almacenamiento haya sido aprobado como lo es una bóveda de contraseñas;

Cambiar la información de autenticación secreta cuando exista alguna indicación que pudiera haber sido vulnerada o conocida por terceros.

No se debe compartir la información de autenticación secreta de usuario de una persona.

No se debe utilizar la misma información de autenticación secreta para fines distintos a los relacionados con las actividades de Minsal (por ejemplo: cuentas personales de redes sociales, bancos, casas comerciales, etc.)

Utilizar contraseñas con una longitud mínima suficiente que tengan las siguientes características:

6.5.1 Características de Contraseñas

- Las contraseñas temporales deben ser proporcionadas a los usuarios de una manera segura, no se deben utilizar mensajes de correo electrónico de terceros o no protegidos (sin texto).

- Las contraseñas de acceso creadas por el usuario deben ser difíciles de adivinar por terceros y ser sólo de su conocimiento personal, quedando prohibido su divulgación, así como mantener anotada su clave de acceso en lugar visible.

- Los sistemas de información deben validar la robustez de las contraseñas de los usuarios.

- Las contraseñas de acceso de los usuarios deben contar con un archivo histórico, debidamente encriptado, con el objetivo de no permitir reutilizar una clave de acceso utilizada recientemente.

- Las contraseñas nunca deberían ser almacenadas de una forma desprotegida (ej. Contraseñas almacenadas en el navegador, post-it, cuadernos, etc.).

- Toda contraseña predeterminada por el vendedor debe ser cambiada después de la instalación de los sistemas o software.

- Las contraseñas deben ser únicas para cada funcionario y deben cumplir, a lo menos, con los siguientes requisitos:

  - ✓ Debe contener 8 caracteres como mínimo.
  - ✓ No debe contener: los nombres o apellidos del funcionario, el user name o nombre de usuario, el nombre de la institución o unidad funcional.
  - ✓ No debe contener palabras completas.
  - ✓ Contener al menos un carácter de las siguientes categorías:

Categoría	Ejemplo
Letras mayúsculas	A, B, C
Letras minúsculas	a, b, c
Números	0, 1, 2, 3, 4, 5, 6, 7, 8, 9

Ejemplo de contraseña: A23J77c31

6.5.2 Cambio de las contraseñas

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

- Los usuarios deben cambiar su contraseña de acceso en forma periódica, con la frecuencia establecida por el Departamento TIC (Soporte TIC).

- Las contraseñas no deben ser reutilizadas en el tiempo ni en distintos sistemas. Los usuarios no deben construir contraseñas que sean idénticas o similares a las últimas ya utilizadas.

- Cualquier archivo de contraseñas históricas debe mantenerse siempre encriptado, en aquellas plataformas donde sea factible.

6.5.3 Almacenamiento de Contraseñas

- No se deben incorporar contraseñas en el código fuente de las aplicaciones.

- No se deben mantener listados de contraseñas en archivos de texto plano. Los archivos con listas de usuario/contraseñas deben mantenerse encriptados en todo momento.

- Las contraseñas de cuentas de administración deben ser resguardadas por el responsable del aplicativo y/o el Departamento TIC.

- Las contraseñas de los usuarios deben contar con un archivo histórico, debidamente encriptado, con el objeto de no permitir reutilizar una clave de acceso

próxima utilizada. La cantidad de contraseñas históricas a almacenar se encuentra definida en el estándar del Departamento TIC (Soporte TIC).

6.5.4 Contraseñas en Dispositivos de Red

- Todos los dispositivos de red (routers, firewalls, switches) deben tener contraseñas únicas u otro mecanismo de control de acceso.

- Si un dispositivo no posee contraseña de acceso, se debe impedir su administración remota, permitiendo la intervención sólo al personal autorizado y en forma directa (conexión local).

6.5.5 Contraseña por Omisión

- Toda contraseña por omisión provista por el fabricante de cualquier sistema debe ser reemplazada.

6.5.6 Recordatorios de Contraseñas

- Queda absolutamente prohibido anotar las contraseñas de acceso en lugares públicos.

- Cualquier contraseña encontrada en estos medios será informada y podrá ser motivo de sanción disciplinaria de acuerdo con lo establecido en el Estatuto Administrativo y la Política General de Seguridad de la Información.

6.5.7 Asignación de Contraseñas Expiradas y Reasignación de Contraseñas

- Cuando el usuario olvide u extravíe su contraseña, deberá solicitarla al Departamento TIC (Soporte TIC), e identificarse como propietario de la cuenta para que se le proporcione una nueva, o la utilización de cualquier otro medio de verificación que permita identificación positiva.

- Toda reasignación de contraseñas será registrada en la bitácora del sistema y deberá notificarse al usuario de la cuenta, a su casilla de correo registrada al crear la cuenta asociada. Esto permite detectar suplantación de identidad.

- El Departamento TIC (Soporte TIC) debe disponer de herramientas que eviten posibles tácticas de suplantación de identidad de usuarios u otros artilugios para obtener información a la cual no tiene acceso normalmente[2].

[2] Se denomina Ingeniería Social en el campo de la Seguridad Informática.

6.6 Procedimientos de inicio de sesión seguro

El acceso a los sistemas o aplicaciones debe ser controlado mediante el uso de IDs únicos y contraseñas robustas. Cuando se requiera un nivel alto de autenticación y verificación de identidad, se podrán utilizar métodos alternativos a las contraseñas, como medios criptográficos, tarjetas inteligentes, tokens, o medios biométricos.

El inicio de sesión de los sistemas o aplicaciones debe divulgar el mínimo de información acerca del sistema o aplicación, para evitar proporcionar asistencia innecesaria a un usuario no autorizado. Algunas medidas de protección que pueden ser consideradas para el inicio de sesión seguro son:

- No proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que pudieran servir de ayuda a un usuario no autorizado
- Validar la información de inicio de sesión sólo al completar todos los datos de entrada. Si surge una condición de error, el sistema no debería indicar qué parte de los datos son correctos o incorrectos.
- Proteger contra intentos de inicio de sesión forzados.
- No mostrar la contraseña que se ingresa.
- No transmitir contraseñas en texto sin cifrar a través de una red.
- Terminar las sesiones activas después de un período de inactividad, en especial en ubicaciones de alto riesgo, como áreas públicas o externas fuera de la administración de seguridad o en dispositivos móviles.
- Restringir los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo y reducir la ventana de oportunidad de acceso no autorizado.

6.7 Uso de programas de utilidad privilegiados

El uso de programas de utilidad que pueden ser capaces de anular el sistema y los controles de aplicación se deben restringir al personal del Departamento TIC, Administradores de Sistemas y aquellos funcionarios que por la naturaleza de sus funciones requieran acceso, en esto casos se deberá solicitar autorización al Encargado de Seguridad / Encargado de Ciberseguridad. Para estos efectos sólo tendrán permisos de administrador en los equipos, los funcionarios antes mencionados.

Cuando se habilite equipamiento para usuarios se deben revisar los siguientes puntos:

- Segregación de programas de utilidad de software de aplicaciones;
- Autorización para programas de utilidad ad hoc.
- Eliminación o deshabilitación de todos los programas de utilidad innecesarios.
- No dejar los programas de utilidad disponibles a los usuarios que tienen acceso a las aplicaciones de los sistemas donde se requiere la segregación de deberes.

6.8 Intentos fallidos

El número de intentos erróneos de acceso a una cuenta debe estar limitado según se indique en el estándar definido por el Departamento TIC (Soporte TIC).

De cumplirse el número de intentos fallidos establecido, la cuenta debe quedar bloqueada, siendo los únicos autorizados para su desbloqueo el Departamento TIC (Soporte TIC). Todo desbloqueo deber ser solicitado a Soporte TIC, por el jefe directo o el propietario de la cuenta.

Toda reasignación de contraseña debe ser solicitada por el jefe directo del usuario titular de la cuenta.

En caso de usuarios externos sólo podrá ser reactivado el acceso por consentimiento del contacto establecido al momento de crear la cuenta del usuario.

6.9 Acceso a Información Sensible

En el caso del control de acceso a información, se deben utilizar contraseñas robustas (o seguras, (ver punto 6.5.1 de esta política).

La contraseña nunca debe ser compartida o relevada; hacer esto responsabiliza al usuario que prestó la contraseña de acceso y a todas las acciones que se realicen de la misma.

6.10 Vulnerabilidades detectadas

Frente a la evidencia de un compromiso del sistema por uso indebido de cuentas con privilegios, todas las contraseñas de cuentas con privilegios del sistema deberán ser reemplazadas.

Los usuarios o administradores de MINSAL deberán informar cualquier evento anómalo o vulnerabilidad que detecten durante la operación de los sistemas a sus superiores, al Departamento, Encargado de Seguridad de la Información y Encargado de Ciberseguridad, según lo descrito en el Procedimiento de Gestión de Incidentes de Seguridad de la Información.

7 MECANISMO DE DIFUSIÓN.

La comunicación de la presente política 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 intranet de Minsal http://isalud.minsal.cl/
- Correo informativo.

8 PERÍODO DE REVISIÓN.

La revisión del contenido de esta Política se efectuará a lo menos cada dos años por el Comité de Seguridad de la Información, o atendiendo necesidades de cambios para garantizar su idoneidad, adecuación y efectividad.

9 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

Frente a casos de especiales, el Comité de Seguridad de la Información evaluará y podrá establecer condiciones puntuales de excepción en el cumplimiento de las presentes directrices, siempre que no infrinja la legislación vigente. Toda excepción debe ser documentada y generar un proceso de revisión de la política, que determine si se deben agregar directrices en lo particular.

10 HISTORIAL Y CONTROL DE VERSIONES

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio
01	Agosto 2014	Todas	Creación del Documento
02	Octubre 2016	Actualización de la normativa de referencia	Se modifican los puntos1 al 4 y puntos 5.1 al 5.7. Se incluye el punto 7 y 8.
03	Octubre 2019	Todas	Cambio de formato de documento. Se actualizan las referencias normativas. Se actualizan todos los puntos de la política.