POLITICA DE CUENTAS DE USUARIO Y CLAVES DE ACCESO

DIRECCION DEL SERVICIO DE SALUD

VIÑA DEL MAR - QUILLOTA

NOTA DE CONFIDENCIALIDAD

LA INFORMACIÓN CONTENIDA EN EL PRESENTE DOCUMENTO, ES DE PROPIEDAD Y USO EXCLUSIVO DEL SERVICIO DE SALUD VIÑA DEL MAR – QUILLOTA, PARA LOS FINES QUE DETERMINE, Y SOLO LOS FUNCIONARIOS DE ESTA INSTITUCIÓN EXPRESAMENTE AUTORIZADOS PODRÁN CONOCER Y UTILIZAR SU CONTENIDO DE ACUERDO A SU FINALIDAD.

Firmas de los responsables.

ELABORADO POR	**REVISADO POR**	**APROBADO POR**
_____	_____	_____
Representante del Comité de Seguridad	Encargado de Seguridad	Director(a) del Servicio

INDICE

CONTROL DE VERSIONES

REVISIONES DEL DOCUMENTO DE POLITICA				
Nº Revisión	**Fecha Aprobación**	**Motivo de la revisión**	**Páginas Modificadas**	**Autor**
0(Cero)		Elaboración inicial	Todas	JVL
1				
2				
3				

1.- DECLARACIÓN INSTITUCIONAL

Los activos de información del Servicio de Salud no deben quedar disponibles a personas o entidades externas, salvo en situaciones y formas expresamente establecidas según normas y controles que garanticen su protección.

El Servicio de Salud define que el acceso a la información de los sistemas informáticos estará salvaguardado solamente a usuarios identificados y autentificados en los sistemas de información.

El Servicio de Salud ha desarrollado una estrategia de outsourcing de los sistemas de información que forman la columna vertebral de los procesos administrativos y clínicos, de esta forma, todos los usuarios de sistemas de información son administrados en las plataformas de cada proveedor de aplicaciones. Esta política pretende normar la administración de esas cuentas de usuario.

El uso inapropiado de los usuarios de sistemas y de las contraseñas, puede llevar a sanciones administrativas y judiciales.

2.- OBJETIVOS DE LA POLITICA DE CUENTAS DE USUARIO Y CLAVES DE ACCESO

El método específico de autenticación para cada sistema deberá ser proporcional con el nivel de sensibilidad del sistema para tener acceso (es decir, mientras más sensibles sean los sistemas se deberá utilizar métodos de autenticación más fuerte). Varios métodos de autenticación (por ejemplo, uso de la contraseña) puede ser necesaria para la sensibilidad de alta -confidencialidad o de alto riesgo.

3.- ÁMBITO DE APLICACIÓN DE LA POLÍTICA DE CUENTAS DE USUARIO Y CLAVES DE ACCESO

El alcance de la política de cuentas de usuario y claves de acceso abarca a todos los usuarios de sistemas de información y computadores personales del Servicio de Salud Viña del Mar – Quillota, así como también a los proveedores de sistemas de información, para que implementen estas medidas en sus sistemas.

4.- ROLES Y RESPONSABILIDADES

Director/a del Servicio de Salud Viña del Mar-Quillota

- Sancionar las propuestas realizadas por el comité de seguridad, respecto a las políticas de cuentas de usuario y claves de acceso, además deberá

- Asegurar que estas políticas sean incluidas en los contratos de outsoursing con los proveedores.

Comité de Seguridad

- Elaborar y aprobar la presente política de claves de acceso.
- Supervisar la implementación de la presente política.
- Proponer estrategias y soluciones específicas para la implementación de los controles necesarios para implantar la presente política.
- Monitorear los incidentes de seguridad y proponer estrategias para dar solución a las situaciones de riesgo detectadas en esta política.
- Monitorear el avance general en la implementación de la presente política.
- Divulgar la política de seguridad al interior de la institución.
- Implementar las medidas de seguridad definidas en la presente política.
- Mantener esta política de seguridad y sus procedimientos actualizados, con el fin de asegurar su vigencia y nivel de eficacia y su correcta aplicación.

Sub departamento de Informática

Velar por el cumplimiento de la presente política, en la elaboración de contratos con terceros y en la aplicación a los usuarios del Servicio de Salud

Usuarios del Servicio de Salud

Cumplir a cabalidad las políticas de cuentas de usuario y claves de acceso del Servicio de Salud.

5.- MARCO GENERAL PARA LAS POLÍTICAS DE CUENTAS DE USUARIO Y CLAVES DE ACCESO

5.0 Funciones de los referentes y administradores de sistemas

Administradores de Sistemas (funciones relacionadas con cuentas de usuarios)

- Administración de cuentas de usuarios y sus perfiles de accesibilidad (crear, eliminar usuarios, modificar perfiles)
- Atención usuarios (cambios u olvido de contraseñas).
- Aplicar las políticas para el uso del sistema informático y de red.
- Aplicación de las políticas de seguridad para los usuarios.
- Documentación del sistema y las cuentas de usuario

Referentes de Sistemas

- Interlocutor válido para las relaciones externas a los sistemas; con los organismos institucionales, empresas externas, servicios de mesa de ayuda.
- Formular y mantener permanentemente actualizados los Documentos de gestión, como: Reglamentos, Procedimientos, Directivas y otras normas relacionadas con su especialidad, en coordinación con las diferentes Unidades Orgánicas.
- Recomendar y coordinar acciones que conllevan a optimizar la perfomance de los sistemas en base a requerimientos realizados por los usuarios finales.
- Supervisar cambio de versiones en los sistemas informáticos.
- Convocar y coordinar reuniones de trabajo relacionadas con los distintos interlocutores del sistema.
- Detectar, gestionar e informar las necesidades de los usuarios finales del sistema.

5.1.- Procedimientos y directrices para los proveedores de servicios a incluir en las bases técnicas de licitación y contratos:

- Cada sistema debe incorporar la autenticación de usuario y la identificación para garantizar que el acceso no se concederá a personas no autorizadas. Los usuarios no tendrán el acceso a los recursos de información del Servicio de Salud Viña del Mar - Quillota sin identificarse y autenticarse en ellos.
- Las contraseñas podrán ser cambiadas por el propio usuario.
- El referente del Servicio de Salud solicitará formalmente la asignación de identificadores o contraseñas las que serán entregadas al jefe directo del usuario.
- Una contraseña generada deberá ser entregada personalmente al usuario final., esta no podrá ser enviada por correo electrónico.
- Las contraseñas o identificadores deberán tener una longitud mínima de ocho caracteres.
- Las cuentas de usuario deben cumplir con las siguientes directrices:

  a) Permitir sólo un usuario por cada cuenta.
  b) Nunca se debe activar/habilitar una cuenta de invitado. A menos que sea absolutamente necesario, aprobado por el referente del Servicio. Todas las cuentas deben estar asociadas a un responsable.
  c) Para las labores específicas que requieran cuentas de acceso transitorio, se deberán desactivar inmediatamente después del término de su utilización.
  d) Las cuentas no utilizadas, informadas por los supervisores deben ser desactivadas. Para esto se deberá generar un proceso de monitoreo, que se ejecute al menos una vez al mes, donde se informará su resultado a todos los supervisores de la red.

- Las cuentas de administrador deben cumplir con las siguientes directrices:

  a) Los nombres de las cuentas de administración deben ser cambiadas con una frecuencia que no dificulte la administración de los sistemas.
  b) El uso de la cuenta de administrador principal para cada uno del sistema debe delimitarse a un grupo limitado de usuarios.
  c) Todas las cuentas con privilegios de administrador deben tener contraseñas fuertes u otros métodos alternativos de autenticación confiables.
  d) Otros métodos de autenticación distintos de contraseñas (por ejemplo, sistemas biométricos, tarjetas inteligentes, tokens, otros), deben ser aprobados por El Subdepartamento de TI del Servicio de Salud Viña del Mar-Quillota.

- La información de las contraseñas que se almacenan en los servidores deben ser encriptados.
- Para evitar ataques de fuerza bruta, los sistemas deberán contar con una función de bloqueo de intrusos que debe ser implementada en cada sistema, suspendiendo temporalmente la cuenta después de tres intentos de inicio de sesión no válido. La reactivación de las cuentas bloqueadas deberá realizarse de forma manual por un administrador de sistema del Servicio de Salud.
- Los proveedores deberán llevar un registro de las autorizaciones, modificaciones y revocaciones de los accesos a los recursos y sistemas de información.
- Los proveedores no podrán incorporar las claves de acceso en el código fuente de los sistemas.
- Deberán existir procedimientos permanentes de monitoreo a ataques a las cuentas de usuarios.
- EL comité de Seguridad de la Información debe identificar los sistemas críticos o sensibles y definir controles de acceso adecuados a su nivel de criticidad.
- Deberán existir medidas de seguridad de acceso para aquellos equipos ubicados en zonas de riesgo elevado (atención a público, por ejemplo), tales como:

  a) Bloqueo de pantalla después de un periodo de tiempo sin operación.
  b) Bloqueo automático del sistema de información en caso de abandono.
  c) No se desbloquea de forma automática pasado un tiempo de bloqueo.

5.2.- Procedimientos y directrices para los usuarios del Servicio de Salud:

- Las contraseñas no deberán ser fáciles de ser reconocidas por terceros; deben contener letras, mayúsculas, dígitos, y caracteres de puntuación; no estarán basados en cosas obvias o de fácil deducción a partir de datos relacionados con el usuario, por ejemplo, nombres, números telefónicos, cédula de identidad, fecha de nacimiento; estén libres de caracteres idénticos consecutivos o grupos completamente numéricos o alfabéticos; tampoco deben ser nombres comunes.

- Las contraseñas deben tener al menos las siguientes características:

  a) Un periodo de vigencia (máximo de 90 días), los sistemas deberán obligar al usuario a cambiar periódicamente su contraseña.
  b) No deben estar en blanco
  d) No se deben aceptar “enter” como un carácter.
  e) No se pueden repetir al menos las 4 últimas contraseñas
  f) La contraseña debe tener un largo variable de 5 a 10 caracteres

- Los usuarios a quienes se haya asignado privilegios especiales deberán cambiar sus contraseñas con una frecuencia no superior a 1 mes.
- Los usuarios no deberán mantener la misma contraseña para los distintos sistemas usados en el servicio.
- Los identificadores de usuario no deben ser compartidos.
- Deberán notificar inmediatamente a un supervisor, jefe directo o al Subdepartamento de TI si se sospecha que una contraseña ha sido comprometida por un usuario no autorizado.
- Es absoluta responsabilidad del usuario al terminar su jornada laboral o no estar frente a su computador, cerrar su sesión de usuario.
- El usuario debe configurar su computador para el uso de protector de pantalla y que este solicite contraseña para iniciar sesión nuevamente.
- Los usuarios no deben permitir que los sistemas recuerden las contraseñas. Tampoco deberán incluir el identificador en cualquier proceso de inicio de sesión automatizado.
- Los directivos y encargados deberán asegurar que su personal cumpla con todas las directrices que figuran en esta política, además deberán notificar sin demora al Subdepartamento de TI, la Información de las cuentas que deben ser desactivadas, y reportar cualquier sospecha o violaciones de las contraseñas.

5.3.- Procedimientos y directrices prohibidos para los usuarios del Servicio de Salud:

- Facilitar la contraseña de acceso personal, a un tercero.
- El uso de una contraseña fácil de predecir.
- Mantener listados de claves de acceso en archivos almacenados en su computador sin encriptar.
- Anotar las contraseñas en lugares visibles.

5.4.- Almacenamiento de Contraseñas

- No se debe 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 Usuarios/Contraseñas deben mantenerse encriptados en todo momento.

5.5.- Contraseñas en dispositivos de Red

- Todos los dispositivos de red (routers, firewall, switch) deben tener contraseñas 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).

5.6.- Vulnerabilidades detectadas en algunos de los puntos anteriores

- 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 del Servicio de Salud Viña del Mar – Quillota deberán informar a sus superiores y al Subdepartamento de TI, cualquier evento anómalo o vulnerabilidad que detecten durante la operación de los sistemas.
- La completa eliminación de vulnerabilidades en este ámbito deberá ser una actividad prioritaria dentro de las funciones del Subdepartamento de TI.

6.- APLICACIÓN DE LAS POLITICAS DE CUENTAS DE USUARIO Y CLAVES DE ACCESO

La infracción a las obligaciones establecidas en esta norma, podrá constituir una violación al principio de probidad administrativa, y será sancionada en conformidad a lo dispuesto en la Ley Nº 18.834, sobre Estatuto Administrativo. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.

El Subdepartamento de TI no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de seguridad.

7.- MONITOREO

El Subdepartamento de TI del Servicio de Salud Viña del Mar – Quillota controlará la aplicación de estas políticas de cuentas de usuario y claves de acceso.

8.- GLOSARIO DE TERMINOS

- **Autentificación:** es el acto de establecimiento o confirmación de algo (o alguien) como auténtico. La autenticación de un objeto puede significar (pensar) la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad.

- **Ataques de fuerza bruta:** Un **Ataque de fuerza bruta** dentro del campo de la criptografía es una técnica que permite probar todas las combinaciones posibles hasta encontrar la palabra o texto legible que fue cifrado para obtener el criptograma (contraseña).

- **Contraseñas fuertes:** Estas contraseñas son largas y usan combinaciones de letras mayúsculas y minúsculas, de números y de símbolos. No pueden hallarse fácilmente en listas de contraseñas y son suficientemente largas para provocar que una búsqueda burda resulte impráctica en la mayor parte de los casos

- **Sistemas biométricos:** Son métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o rasgos físicos intrínsecos.

- **Tarjetas inteligentes:** Son tarjetas del tamaño de una tarjeta de credito convencional, que contienen un pequeño microprocesador, que es capaz de hacer diferentes cálculos, guardar información y manejar programas, que están protegidos a traves de mecanismos avanzados de seguridad.

- **Tokens:** Es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

- **Outsoursing:** Es el proceso económico en el cual una empresa mueve o destina los recursos orientados a cumplir ciertas tareas hacia una empresa externa por medio de un contrato. Esto se da especialmente en el caso de la subcontratación de empresas especializadas.

- **Switchs**: Dispositivo digital lógico de interconexión de redes de computadoras

- **Routers**: Dispositivo que proporciona conectividad a nivel de red

- **Firewall:** Dispositivo diseñado para bloquear el acceso no autorizado