

Boletín Informativo TIC SSM



**Servicio de
Salud
Magallanes**

Región de
Magallanes

Ministerio de
Salud

Tecnologías de la Información y
Comunicación
Servicio de Salud Magallanes
Ministerio de Salud

Seguridad de la Información

Política de Cuentas de Usuarios

Tecnologías de la Información y
Comunicación
Servicio de Salud Magallanes
Ministerio de Salud





A continuación se dan a conocer algunos importantes para comprender el manejo de cuentas de usuario y como realizar gestión de ellas sin caer en errores y haciendo uso de todos los canales de comunicación correspondientes.

Las instrucciones sobre la gestión de cuentas están escritas en las Políticas de seguridad y para realizar cambios en dichas cuentas se debe comunicar con el "Comité de Seguridad de la Información" y "Gestor de Red"

¿Que Roles y Responsabilidades cumplen el comité de Seguridad de la información y el Gestor de red con respecto a las cuentas de usuario?

El **comité de seguridad de información**, revisara que el almacenamiento de las claves de las cuentas de usuario se realice de manera correcta y segura.

El **Gestor de Red**, se hará cargo de diferentes puntos entre ellos encontramos:

- Materializar los requerimientos de administración de usuario, aplicándolos al ámbito de acción que se le fue asignado.
- Validación de solicitudes de cambio de privilegios a un usuario.
- Autorizar la asignación de privilegios de administración y de las cuentas para usuarios externos.

Reglas de la Política de Seguridad:

Dentro de la política de seguridad existen cierto tipos de reglas que el usuario debe conocer, para hacer un correcto uso de su cuenta y entender cuales son sus derechos como funcionario a la hora de poseer una cuenta, para esto se debe entender que existen dos niveles de cuenta y ambos niveles hacen referencia a los accesos de red, sistemas aplicativos, sistemas operativos y dispositivos.

- Nivel Estándar: se otorgan niveles de acceso y privilegios a las distintas aplicaciones de las que hace uso la institución.
- Nivel Administrador: Se define el acceso para el personal calificado y que cumplen las funciones de soporte y administración de sistemas y dispositivos componentes de la red.

Todos los usuarios deben seguir las siguientes normas generales:

- Las claves son únicas e intransferibles.
- Todo usuario es responsable de las actividades que se realicen con su cuenta, pudiendo recibir sanciones disciplinarias.



Soy funcionario nuevo y no poseo cuenta de usuario.

Cualquier solicitud de cambio de privilegios o una cuenta nueva debe ser realizada por el jefe directo del funcionario que se incorpora al equipo de trabajo.

Soy usuario externo y no poseo cuenta de usuario.

La única forma de que un usuario externo posea cuenta de usuario es que el contacto administrativo definido según el contrato con la empresa prestadora de servicios, solicite dicha cuenta con los requerimientos y motivos justificados

Auditorias de cuentas:

Las cuentas se deben monitorear periódicamente y auditar que las cuentas existentes son las debidamente autorizadas, ademas de que poseen los privilegios correspondientes, de esta forma asegurar las cuentas de administración como uso del personal capacitado.