POLÍTICA DE **GESTIÓN DE CONTRASEÑAS**

Las contraseñas son un aspecto fundamental de la seguridad de la información. Una contraseña mal elegida o protegida puede resultar en un agujero de seguridad para toda QUASAR. Por ello, todos los usuarios de QUASAR son responsables de velar por la seguridad de las contraseñas.

Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de QUASAR.

Todas las contraseñas de cuentas que den acceso a recursos y servicios de QUASAR, deberán seguir las siguientes directrices generales:

- Todas las contraseñas de sistema (root, administradores, cuentas de administración de aplicaciones, cuentas de email, etc…) deben ser cambiados al menos una vez cada 6 meses.
- Se deben cambiar las claves en el primer ingreso al sistema.
- Cada vez que se cambien estas, deben ser distintas por lo menos de las últimas tres anteriores.
- Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas.
- En la medida de lo posible, las contraseñas serán generadas automáticamente con las características recomendadas en esta política y se les comunicará a los usuarios su contraseña siempre en estado “expirado” para obligar al usuario a cambiarla en el primer uso que hagan de la cuenta o servicio.
- Las contraseñas por defecto asociadas a los sistemas o aplicaciones nuevas deberán ser cambiadas antes de poner estos sistemas en producción. También se desactivarán aquellas cuentas “por defecto” que no sean imprescindibles.
- Todas las contraseñas de sistema y de usuario de recursos y servicios deben respetar las recomendaciones descritas en la presente política.
- Las claves no deben ser almacenadas en un sistema de registro automatizado (por ej., macros o explorador).
- No se deben utilizar las mismas claves personales para fines privados y para fines comerciales.

Algunos servicios en los que sea crítico el mantener la seguridad de la contraseña podrán determinar medidas adicionales de protección de la misma.

SELECCIÓN Y CUSTODIA DE CONTRASEÑAS

- **Recomendaciones generales para la selección de contraseñas**

Las contraseñas son usadas con múltiples propósitos en QUASAR, como pueden ser, las contraseñas de cuentas de usuario intranet, servicios Web, cuentas de correo electrónico, protectores de pantalla en los recursos de los usuarios, administración de dispositivos remotos, etc…

La seguridad de este tipo de autentificación se basa en dos premisas:

- La contraseña personal sólo la conoce el usuario.
- La contraseña es lo suficientemente "fuerte" para no ser descifrada.

La contraseña, para ser considerada "fuerte" (segura), debe poseer las siguientes características:

- Debe tener al menos 8 caracteres.
- Utiliza caracteres de tres de los cuatro grupos siguientes, y SIEMPRE UNO DE ELLOS DEBERÁ SER UN SÍMBOLO:
    1. Letras minúsculas.
    2. Letras mayúsculas.
    3. Números (por ejemplo, 1, 2, 3).
    4. Símbolos (por ejemplo, ¡, @, Ñ, =\`{}[]:";'<>?,./) -, etc.).

- No utilizar contraseñas que se puedan adivinar fácilmente, como pueden ser:
    1. Una cadena de caracteres derivada del nombre de la cuenta del usuario.
    2. Una cadena de caracteres formada por la repetición de caracteres.
    3. Una palabra contenida en un diccionario (de lengua española o extranjera).
    4. Una palabra de diccionario seguida o precedida de un carácter (p.ej. "palabra1" o "Xpalabra" o "palabra!".
    5. Un nombre de pila: Nombres de familiares, amigos, mascotas, ciudades, etc.
    6. Fechas de cumpleaños u otra información personal tales como dirección o número de teléfono.
    7. Conjuntos de letras o números que sigan un patrón sencillo, tales como aaabbb, qwerty, abcdef, 123321, etc.
    8. Una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma, como tampoco ninguna de estas palabras escritas hacia atrás.

Las contraseñas no deben ser almacenadas por escrito nunca. Intente crear contraseñas que pueda recordar fácilmente. Una forma de recordarlo con facilidad es crear una contraseña basada en una frase fácilmente recordable.

- **Recomendaciones para la protección de la contraseña**

No utilice la misma contraseña.

Se recomienda cambiar la contraseña en el primer momento de acceder a la cuenta, para que la nueva contraseña sea distinta a la que va en la solicitud.

No comparta las cuentas y contraseñas con nadie, incluyendo administrativos, secretarias, etc… Todas las contraseñas deben ser tratadas como información sensible y confidencial.

A continuación se presenta una lista de cosas que NO se deben hacer:

- No revele su contraseña por teléfono a NADIE, incluso aunque le hablen en nombre del servicio de informática o de un superior suyo en QUASAR.
- Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.); las claves deben ser cambiadas si existen indicios de que puedan estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad).
- Nunca escriba la contraseña en papel y lo guarde. Tampoco almacene contraseñas en ficheros de ordenador sin cifrar o proveerlo de algún mecanismo de seguridad.
- No revele su contraseña a sus superiores, ni a sus colaboradores.
- No hable sobre una contraseña delante de otras personas.
- No revele su contraseña en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo.
- No comparta la contraseña con familiares.
- No revele la contraseña a sus compañeros cuando se marche de vacaciones.
- No utilice la característica de “Recordar Contraseña” existente en algunas aplicaciones (Outlook, Netscape, Internet Explorer).
- No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por el responsable del sistema.

- **Recomendaciones sobre contraseñas de servicios y servidores**

Estas últimas recomendaciones van dirigidas a aquéllos que administran o son responsables de algún servidor o servicio que sea accesible a distintos usuarios (externos o internos):

- Tener unos criterios para la creación y asignación de contraseñas lo más similares posibles a los requisitos obligatorios expuestos en esta Política.
- Los servidores y dispositivos se deben configurar con cuentas separadas para los que tienen privilegios de administración y los que no.
- Los usuarios se deberían autenticar con cuentas que no tuvieran más privilegios que los necesarios para hacer uso del servicio.
- El acceso a los privilegios correspondientes (para administrar la máquina) debe hacerse mediante mecanismos de “escalado de privilegios”; en este caso además quedará traza de qué usuario ha accedido a estos privilegios especiales.
- Sólo se tendrán los privilegios especiales el tiempo que sea estrictamente necesario.
- Se deberá dar de baja a aquellos usuarios que dejen de pertenecer al colectivo al que va destinado el servicio.

GESTIÓN DE LA CLAVE DEL USUARIO

Cuando se asignan y utilizan claves de usuarios, se deben seguir las siguientes reglas:

- Al firmar la Declaración de aceptación de los documentos del Sistema, los usuarios también aceptan la obligación de mantener sus claves en forma confidencial, como se establece en este documento.
- Cada usuario puede utilizar solamente su propio nombre de usuario asignado de forma exclusiva.
- Cada usuario debe tener la posibilidad de escoger su propia clave, en los casos que corresponda.
- Las claves utilizadas para el primer acceso al sistema deben ser exclusivas y seguras, según lo establecido precedentemente.
- El Responsable de IT facilitará la clave de primer acceso al empleado que lo solicite. Las claves de primer acceso deben ser comunicadas al usuario de forma segura, y se debe verificar previamente la identidad del usuario.
- El usuario debe confirmar la recepción de la clave.
- El usuario debe modificar la clave de primer acceso cuando ingrese al sistema por primera vez.
- Se requiere al usuario que escoja contraseñas seguras.
- Los usuarios deberán cambiar sus claves cada seis meses.
- La contraseña no debe ser visible en la pantalla durante el inicio de sesión.
- Si un usuario ingresa una clave incorrecta un número máximo de veces consecutivas, el sistema debe bloquear la cuenta de usuario en cuestión, cuando proceda.
- Las claves creadas por el fabricante del software o hardware deben ser cambiadas durante la instalación inicial.
- Los archivos que contienen claves deben ser guardados en forma separada de los datos del sistema de la aplicación.

En Las Rozas de Madrid, 18 de septiembre de 2025

Juan Martitegui González
Administrador Único de Quasar Science Resources, S.L.