Gobierno de Santa Fe
Ministerio de Gobierno y Reforma del Estado
Secretaría de Tecnologías para la Gestión

*Política de Seguridad*

# Uso y Gestión de Contraseñas

# Índice de contenido

# 1 - Objetivo

El propósito de este documento es establecer los requerimientos de seguridad estándar para la creación de contraseñas seguras, la protección de las mismas y la frecuencia de cambios.

# 2 - Ámbito de Aplicación

Esta política alcanza a todo el personal estable, temporario y contratado del Gobierno de Santa Fe que tenga responsabilidad sobre una cuenta con privilegios de acceso a servicios informáticos, cualquiera sea su función o cargo jerárquico.

También se detallan los controles y medidas de protección que el personal de informática y especialmente los desarrolladores tendrán la responsabilidad de implementar y desarrollar.

# 3 - Política General

- Todas las contraseñas de cuentas genéricas con privilegios administrativos en servidores, bases de datos, aplicativos, etc. deben ser cambiadas con una periodicidad no mayor a doce (12) meses. Ej.: root, administrator, enable, NT admin, mysql, cuentas de administrador en aplicaciones web, etc.
- Todas las contraseñas de cuentas personales deben ser cambiadas con una periodicidad no mayor a seis (6) meses. Todas las contraseñas deben obedecer el estándar de calidad enunciado más abajo en la presente política.
- Las contraseñas nunca deben enviadas por medios de comunicación electrónicos (correo, mensajes de texto, etc.). En caso de necesidad extrema, se permite el envío siempre y cuando se utilice algún mecanismo criptográfico adecuado para proteger la confidencialidad de las mismas.
- A los efectos de manejar muchas contraseñas, se recomienda la utilización de gestores de contraseñas (Ej: Keepass, Password Safe, etc) los cuales poseen mecanismos criptográficos adecuados para garantizar la confidencialidad de las mismas. Las contraseñas NUNCA deben ser escritas en papel u otras superficies.

# 4 - Estándar de Calidad

Todos los usuarios alcanzados por la presente política deberían estar advertidos de cómo crear una contraseña fuerte. No obstante, la fortaleza de la misma se forzará por sistema (ver punto 7).

Se considera que una contraseña fuerte si cumple, al menos, con los siguientes requisitos:

**Extensión**

- La longitud debe ser igual o superior a ocho (8) caracteres.

**Complejidad**

- Utiliza en conjunto al menos dos clases de caracteres distintas. Son clases de caracteres distintas cuando se utilizan números, letras (mayúsculas y minúsculas) y símbolos (#, $,&, etc).
- No se corresponde con palabras de diccionarios (independientemente del idioma o jerga) ni al derecho ni al revés, ni precedida o seguida por números o letras.
- No se relaciona con información fácilmente deducible del dueño de la cuenta (Ej: nombre, dirección, fechas de nacimiento, datos de familiares o mascotas, aliases, nicks, etc.) .
- No se relaciona con términos comunes utilizados en la operatoria diaria. (Ej: nombre de la organización, productos, nombres de computadoras o aplicativos, comandos, hardware o software, etc.).
    - No posee patrones comunes que se puedan tipear fácilmente en los teclados.

(Ej: 123qwe, 1q2w3e, aaabbb, qwerty, 123321, etc.)

- No se corresponde con ejemplos de contraseñas utilizados en documentos públicos.

## 5 - Protección de las Contraseñas

Los usuarios no deben nunca ceder o divulgar una contraseña personal a terceros, aún si se trata un superior o de personal de informática que se encuentre diagnosticando o resolviendo algún problema. En caso de que alguien le solicite su contraseña personal, refiéralo al presente documento y comunique el incidente al personal informático local.

Si sospecha, o confirma, que alguien más conoce o está utilizando su contraseña personal, debe cambiarla de manera inmediata y reportar el incidente al personal informático local.

El personal de informática nunca debe solicitar la contraseña a un usuario. En caso de necesidad para diagnosticar o resolver algún problema, debe avisar previamente al usuario y solicitar el cambio de contraseña al personal de Soporte. En este caso, se debe forzar un cambio una vez finalizado el trabajo para que el usuario vuelva a poner una contraseña de su exclusivo conocimiento.

No utilizar nunca la opción de «Recordar Contraseña» que ofrecen los navegadores, clientes de correo, servicios de mensajería o aplicativos en general. En caso de hacerlo, su contraseña será almacenada en un formato fácilmente recuperable dentro de su PC, con el riesgo potencial de divulgación que ello significa.

Los usuarios deberán tomar los recaudos necesarios si debe ingresar la contraseña en presencia de uno o más personas a su alrededor.

## 6 - Responsabilidad del Usuario

Todos los registros de auditoría generados por los servidores, aplicativos y servicios informáticos en general almacenan la cuenta del usuario, **siendo su propietario el único responsable de las acciones ejecutadas.**

## 7 - Estándar obligatorio para el desarrollo de aplicaciones

Todo aplicativo que provea acceso a información sensible debe tener implementado un mecanismo de identificación y autenticación de usuarios. En caso de que la autenticación sea utilizando contraseñas, el aplicativo de implementar los mecanismos de control y protección establecidos en el presente documento.

Todo aplicativo debe ofrecer al usuario la posibilidad de cambiar en cualquier momento la contraseña de su cuenta personal a través de una interfaz amigable y sencilla.

Para aplicativos que provean acceso a información confidencial se recomienda el uso de mecanismos más confiables de identificación y autenticación de usuarios. Ejemplos de este tipo de mecanismos son: la tecnología PKI (utilizada para firma digital) y las contraseñas de uso único por medio de tokens.

A continuación se detallan los ítems obligatorios que deben aplicarse en el desarrollo de aplicaciones o servicios informáticos:

- **Fortaleza de Contraseñas:** se deberá forzar la aplicación del estándar de calidad enunciado en el punto cuatro (4).
- **Notificación al Usuario:** el aplicativo o servicio informático debe contar con un mecanismo de notificaciones al usuario (claro y efectivo) acerca de la proximidad de caducidad de su contraseña. Se notificará por primera vez a los treinta (30) días antes. Si la contraseña aun no fué cambiada, se notifica una vez mas quince (15) días antes del vencimiento.
- **Bloqueo de Usuarios:** Si transcurridos quince (15) días después del forzado de cambio la clave no ha sido modificada, se debe bloquear la cuenta correspondiente, notificar al

usuario y debiendo el mismo utilizar un mecanismo definido de recuperación o requerir la participación de personal de informática para rehabilitar la misma.

- **Transmisión de contraseñas:** Todo aplicativo o servicio informático que utilice contraseñas para la autenticación de usuarios, debe implementar mecanismos criptográficos adecuados para proteger el envío de las mismas durante el procedimiento de autenticación. Ejemplos comunes de estos mecanismos son: SSL o TLS, SSH, SFTP, Kerberos (Active Directory), NT/LM Hashes, etc. Se deben reemplazar todos los servicios informáticos que utilicen envíos de contraseñas en formato plano por servicios equivalentes que ofrezcan las medidas de protección arriba enunciadas. Ej: POP3 por POP3S, IMAP por IMAPS, FTP por SFTP o SCP, etc.
- **Histórico de Contraseñas:** Todo aplicativo o servicio informático debe mantener un archivo histórico cifrado de las contraseñas utilizadas por cada usuario, con el fin de prevenir que los mismos vuelvan a utilizarlas. Dicho archivo debe contener por lo menos las veinte (20) últimas contraseñas seleccionadas por cada usuario.

# 8 - Cumplimiento

Cualquier empleado o tercero contratado que viole la presente política de seguridad, será sujeto al proceso disciplinario correspondiente, siendo posible la suspensión y/o finalización de un contrato o una relación laboral.

# Anexo A - Control de Documentación

| | | | |
|---|---|---|---|
| Título | Uso y Gestión de Contraseñas | | |
| Código de Documento | STG-PS-1 | | |
| Elaborado por | Ramiro Caire | Fecha Elaboración | 05/04/2013 |
| Revisado por | Martín Degrati | Fecha Revisión | 16/07/2013 |
| Aprobado por | Martín Degrati | Fecha Publicación | 27/08/2013 |
| Nombre de Archivo | STG-PS-1-Contraseñas | | |

| Versión | Revisor | Fecha Publicación | Resumen de Cambios |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |