



Gobierno de Chile



GOBIERNO REGIONAL DE LOS LAGOS  
*Acción de Futuro*



# GOBIERNO REGIONAL DE LOS LAGOS


*Acción de Futuro*

## SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

### PROCEDIMIENTO "SISTEMA DE GESTIÓN DE CONTRASEÑAS"


<b>CÓDIGO</b>	<b>SSI-A.09.04.03</b>	<b>CLASIFICACIÓN INFORMACIÓN</b>	<b>Reservada</b>
			<b>X</b> <b>Uso Interno</b>
			<b>Pública</b>
<b>VERSIÓN</b>	1.0	<b>FECHA DE LA VERSIÓN</b>	28-07-2017
<b>RESPONSABLE</b>	Encargado de Seguridad de la Información		




Código : SSI-A.09.04.03	PROCEDIMIENTO SISTEMA GESTIÓN DE CONTRASEÑAS	 <b>GOBIERNO REGIONAL DE LOS LAGOS</b> <i>Acción del Futuro</i>
Versión: 1.0		
Fecha : 28-07-2017		
Página : 2 de 8		

## Historial de modificaciones

### Creación/Modificaciones del Documento

Versión	Fecha de modificación	Autor	Motivo	Páginas modificadas	Firma
1.0	28-07-2017	Oscar Oyarzo Pérez, Jefe Unidad de Informática	Creación de la primera versión del procedimiento	Todas	

### Revisiones


Versión	Fecha	Autor	Observación	Páginas	Firma
1.0	28-07-2017	Oscar Oyarzo Pérez, Jefe Unidad de Informática	Sin observaciones	Todas	

### Visto Bueno

Versión	Fecha	Encargado	Firma
1.0	23-10-2017	Fabiola Yáñez Rojas, Jefa Depto. Jurídico	


### Distribuciones

Versión	Fecha	Encargado	Observaciones
1.0	25-10-2017	Daniel Olhabe Espinosa, Encargado de Seguridad de la Información	Enviado por correo electrónico e instruida la publicación en intranet a la Unidad de Informática

Código : SSI-A.09.04.03	PROCEDIMIENTO SISTEMA GESTIÓN DE CONTRASEÑAS	
Versión: 1.0		
Fecha : 28-07-2017		
Página : 3 de 8		

## Contenido

1. Objetivo .....	4
2. Alcance o ámbito de aplicación interno .....	4
3. Roles y Responsabilidades .....	4
3.1. Jefa Departamento de Recursos Humanos: .....	4
3.2. Jefe/Encargado y Profesional de la Unidad de Informática: .....	4
3.3. Encargado de Seguridad de la Información: .....	4
3.4. Funcionarios y funcionarias:.....	4
4. Procedimiento .....	4
4.1. Política General .....	4
4.2. Pauta General de construcción de claves .....	5
4.3. Estándar de protección de claves.....	6
4.4. Acceso remoto a redes de la Institución.....	6
4.5. Diagrama de proceso de cambio contraseña Active Directory (Modo de operación).....	7
4.6. Registros de Control del procedimiento.....	8
5. Validez y gestión de documentos .....	8

Código : SSI-A.09.04.03	PROCEDIMIENTO SISTEMA GESTIÓN DE CONTRASEÑAS	
Versión: 1.0		
Fecha : 28-07-2017		
Página : 4 de 8		

## 1. Objetivo

Establecer un estándar para la creación de claves adecuadas, la protección de estas claves y la frecuencia de cambio, donde todos los funcionarios y funcionarias deben definir y utilizar sus propias contraseñas y cuidar su correcto uso dentro del Gobierno Regional de Los Lagos.

## 2. Alcance o ámbito de aplicación interno.

Este procedimiento es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia) y personal a honorarios, que presten servicios para el Gobierno Regional de Los Lagos.

## 3. Roles y Responsabilidades

### 3.1. Jefa Departamento de Recursos Humanos:

- Solicitar los accesos de los sistemas de información a la Unidad de Informática.

### 3.2. Jefe/Encargado y Profesional de la Unidad de Informática:

- Crear los accesos básicos a los nuevos funcionarios y funcionarias.
- Entregar a los nuevos funcionarios o funcionarias sus cuentas y contraseñas de sistemas.
- Definir una nueva contraseña cuando el usuario lo solicite.

### 3.3. Encargado de Seguridad de la Información:

- Asegurar que la gestión y creación de las contraseñas se definan bajo norma establecida.


### 3.4. Funcionarios y funcionarias:

- Todos funcionarios y funcionarias son responsables de manejar sus contraseñas y mantenerlas en estricta reserva.

## 4. Procedimiento

### 4.1. Política General

- Se utilizará el servicio de la controladora de dominio utilizada y del Gobierno Regional de Los Lagos para la administración del sistema de contraseñas.
- Las claves de sistemas de todo nivel (ej., root, habilitaciones, administración de máquinas, cuentas de administración de aplicaciones, etc.) deben ser cambiadas al menos 1 vez por trimestre.
- Las claves de producción de todo nivel deben ser parte de la base de datos de administración global.

Código : SSI-A.09.04.03	PROCEDIMIENTO SISTEMA GESTIÓN DE CONTRASEÑAS	
Versión: 1.0		
Fecha : 28-07-2017		
Página : 5 de 8		

- Las claves de usuario (ej., email, web, escritorio, etc.) deben ser cambiadas cada seis meses como mínimo, el intervalo recomendado es cada cuatro meses.
- Las cuentas de usuario que implican ciertos niveles de privilegios sobre los sistemas administrativos-financieros deben tener una clave única manejada sólo por tal usuario.
- Las claves No deben ser enviadas por email ni por otro tipo de formulario electrónico.

#### 4.2. Pauta General de construcción de claves

Las claves son usadas para varios propósitos en el Gobierno Regional de Los Lagos. Algunos de los usos más comunes incluyen: cuentas de usuarios, cuentas de web, cuentas de correo, protectores de pantalla, claves de correo de voz, e ingreso para rutas locales. Para los sistemas que requieren ingreso por una sola vez (Claves dinámicas que requieren existir sólo para un uso), se debe ser extremadamente cuidadoso al emitirlas para lograr claves adecuadas y seguras.


Claves pobres y débiles tienen las siguientes características:

- Contienen menos de 8 caracteres.
- Es una palabra que está o es basada en alguna del diccionario
- La clave es común y se basa en:
  - Nombre de la familia, mascota, amigos, colega, sobrenombre, etc.
  - Términos y nombres computacionales, comandos, sitios, compañías, hardware, software.
  - Las palabras "goreloslagos", "password", "gore" o algún derivado.
  - El cumpleaños o algún otro tipo de información personal, como nombre, dirección, teléfono.
  - Palabras o patrones como aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Cualquiera de las anteriores escrita al revés.
  - Cualquiera de las anterior sucedida o precedida por algún dígito (e.g., gore1, 1gore)

Una clave fuerte tiene las siguientes características:

- Contiene mayúsculas y minúsculas (ej., a-z, A-Z)
- Tiene tantos dígitos y signos de puntuación como letras ej., 0-9, !@#\$%^&\*()\_+|~-=\`{ } [ ] : " ; ' < > ? , . / )
- Tiene por lo menos 8 caracteres.
- No es una palabra en ningún idioma, dialecto ni jerga, etc.
- No está basada en información personal ni de la familia, etc.
- Las claves no deben ser escritas en papel ni almacenadas en línea. Hay que intentar crear claves fáciles de recordar.

NOTA: Nunca usar los ejemplos dados como claves.

Código : SSI-A.09.04.03	PROCEDIMIENTO SISTEMA GESTIÓN DE CONTRASEÑAS	
Versión: 1.0		
Fecha : 28-07-2017		
Página : 6 de 8		

### 4.3. Estándar de protección de claves

No usar la misma clave para las cuentas del Gobierno Regional de Los Lagos y para otras cuentas que no tengan relación con la Institución (ej. cuenta personal de correo, clave de compras, clubes, etc.). Cuando sea posible, no use la misma clave si necesita varios tipos de acceso. Por ejemplo, use una clave diferente para sistemas de ingeniería, y otra para sistemas IT, también use claves diferentes para los sistemas Windows que las que usa en sistemas Linux.

Nunca comparta sus claves con nadie, incluyendo a asistentes administrativos y secretarías. Las claves deben ser tratadas como sensibles e información confidencial del Gobierno Regional de Los Lagos.

Esta es una lista de prohibiciones:

- No revele su clave por teléfono a nadie
- No revele su clave por correo electrónico
- No le revele su clave al jefe
- No hable de su clave en frente de otras personas
- No revele datos sobre la forma o estructura de sus claves
- No revele su clave a quien se lo pregunte ni en formularios de seguridad
- No comparta claves con miembros de la familia
- No revele su clave a colegas cuando salga de vacaciones

Si alguien le pide su clave referencia este documento o envíelo a hablar con algún encargado de seguridad informática.

No use las características de recordatorio de claves que traen las aplicaciones. Nuevamente, no escriba sus claves en papel y no las almacene en ninguna parte de su oficina. No almacene claves en un archivo en ningún computador (incluidos dispositivos móviles) sin encriptación.

Cambie la clave por lo menos una vez cada 6 meses (excepto las claves de sistemas, que deben ser cambiadas cada 3 meses). La recomendación general es períodos de 4 meses.

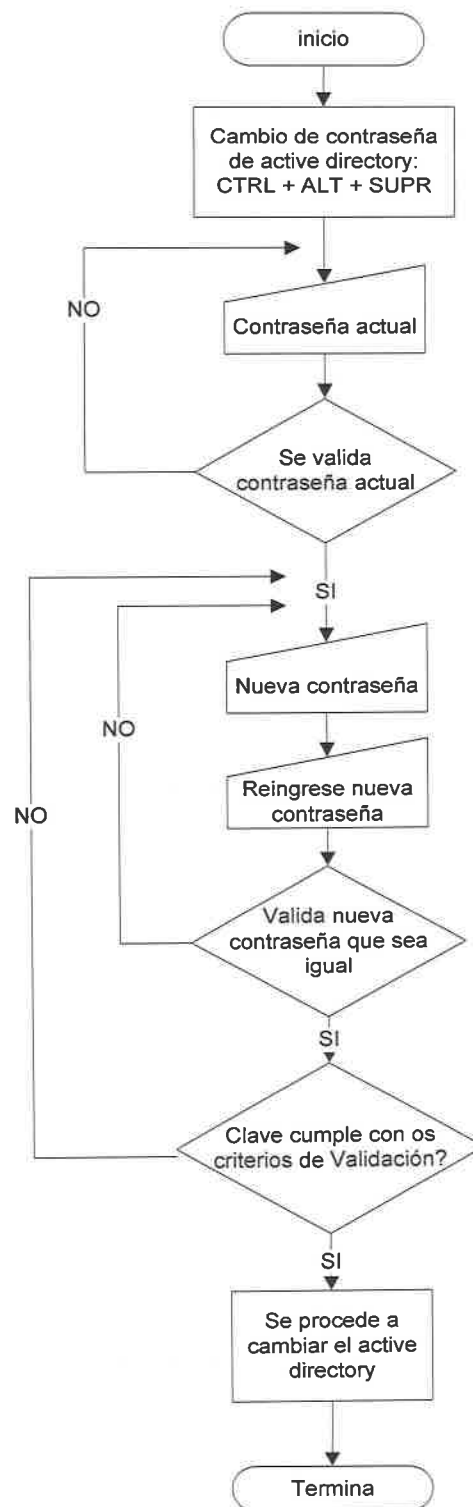
Si alguna cuenta o clave es sospechosa de estar comprometida, reportar el incidente a la Unidad de Informática o cambie todas las claves.


Las claves comprometidas o conocidas pueden ser cambiadas periódicamente por la Unidad de Informática. Si alguna clave es comprometida durante este proceso, el usuario debe requerir su cambio.

### 4.4. Acceso remoto a redes de la Institución

El acceso a las redes del Gobierno Regional de Los Lagos en forma remota debe ser controlado usando acceso mediante red privada virtual (VPN) y luego acceso al servidor o servicio específico, todo administrado y asignado por la Unidad de Informática.

#### 4.5. Diagrama de proceso de cambio contraseña Active Directory (Modo de operación)



Código : SSI-A.09.04.03	PROCEDIMIENTO SISTEMA GESTIÓN DE CONTRASEÑAS	 <b>GOBIERNO REGIONAL DE LOS LAGOS</b> <small>Acción por el Futuro</small>
Versión: 1.0		
Fecha : 28-07-2017		
Página : 8 de 8		

#### 4.6. Registros de Control del procedimiento.

- a) Formulario de ingreso de Funcionarios (as) enviado a la Unidad de Informática por parte del Departamento de Recursos Humanos.
- b) Correo electrónico de validación y creación de cuentas de usuario.
- c) Pantallazos de la controladora de dominio utilizada para la creación de cuentas de usuario.

#### 5. Validez y gestión de documentos

Este documento es válido desde la fecha de su aprobación.

El responsable de este documento es el Encargado de Seguridad de la Información que debe verificar, y si es necesario actualizar, el documento por lo menos una vez cada tres años o cuando el procedimiento lo necesite.

<b>Aprobado Por</b>

<b>Daniel Olhabe Espinosa</b> <b>Encargado de Seguridad de la Información</b>
<b>24 de Octubre de 2017</b>