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 "GESTION DE DERECHOS DE ACCESO PRIVILEGIADOS"

CÓDIGO	**SSI-A.09.02.03**	**CLASIFICACIÓN INFORMACIÓN**		**Reservada**
			X	**Uso Interno**
				Pública
VERSIÓN	1.0	**FECHA DE LA VERSIÓN**	15-11-2017	
RESPONSABLE	Encargado (S) de Seguridad de la Información			

Historial de modificaciones

Creación/Modificaciones del Documento

Versión	Fecha de modificación	Autor	Motivo	Páginas modificadas	Firma
1.0	15-11-2017	Nicanor Bahamonde Loustau, Profesional unidad de Informática	Creación de la primera versión del procedimiento	Todas	

Revisiones

Versión	Fecha	Autor	Observación	Páginas	Firma
1.0	15-11-2017	Oscar Oyarzo Pérez, Jefe Unidad de Informática	Sin observaciones	Todas	

Visto Bueno

Versión	Fecha	Encargado	Firma
1.0	29-11-2017	Fabiola Yáñez Rojas, Jefa Depto. Jurídico	

Distribuciones

Versión	Fecha	Encargado	Observaciones
1.0	Diciembre 2017	Carmen Mella Fagalde, Encargada (S) de Seguridad de la Información	Enviado por correo electrónico e instruida la publicación en intranet a la Unidad de Informática

Contenido

1. Objetivo

Restringir el acceso a los sistemas y servicios, únicamente a usuarios autorizados, controlando la asignación y uso de privilegios, con el objeto de evitar el ingreso sin autorización.

2. Alcance o ámbito de aplicación interno.

El alcance es para todos los funcionarios del Gobierno Regional de Los Lagos, cualquiera sea su calidad contractual ya que la política general de seguridad de la información define los criterios esenciales, normativos y acciones a seguir en temas relacionados con seguridad de la información de todo medio de computación y equipo de comunicación móvil.

3. Roles y Responsabilidades

- **Unidad de Informática:** actuar de forma coordinada con el Departamento de Recursos Humanos (RRHH), para la oportuna creación, modificación y eliminación de cuentas de usuario asociadas al personal y, asimismo, velar por el adecuado registro de la información asociada a dichas cuentas; establecer mecanismos de información para permitir a los usuarios supervisar la actividad normal de su cuenta, así como alertarlos oportunamente sobre actividades inusuales.

- **Jefe (a) de Departamento o Unidad:** Solicitar formalmente a la unidad de Recursos Humanos (RRHH), cada vez que sea necesario, realizar algún cambio en el perfil de privilegios de acceso para una cuenta de usuario de su dependencia; revisar y confirmar periódicamente los derechos de acceso; se debe llevar a cabo la comparación periódica entre los recursos y los registros de las cuentas para reducir el riesgo de errores, fraudes, alteración no autorizada o accidental.

- **Encargado (a) de Seguridad de la Información:** Autorizar la asignación de privilegios de administración a cuentas que no pertenecen al grupo administradores; autorizar la asignación de código-usuario y contraseñas para personal externo a la institución, cuando corresponda.

- **Departamento de Recursos Humanos (RRHH):** actuar en forma coordinada con la unidad de Informática, para notificar de las altas, bajas y traslados de miembros del personal, de modo tal que se puedan mantener actualizadas las correspondientes cuentas de usuario. Este departamento debe ser la fuente oficial que certifique los datos de identidad de todo el personal de la institución, así como la información relativa a su área de trabajo, cargo, oficina y anexo telefónico asignado.

- **Funcionarios (as):** cada miembro del personal, cualquiera sea su calidad jurídica, podrá tener asignada una cuenta de usuario (con su correspondiente nombre de usuario y contraseña), para acceder a los recursos y activos de

información de la red informática institucional, y asumirá la responsabilidad de la correcta utilización de esta credencial, teniendo presente que los datos de su cuenta de usuario son personales e individuales.

La creación de contraseñas, así como su modificación y/o recuperación se regirá por lo definido en el procedimiento "Sistema de Gestión de Contraseñas".

4. Definiciones.

1. **Privilegio**: nivel de acceso otorgado a un usuario.

2. **Perfil**: Conjunto de privilegios que se le asignan a un usuario de un servicio informático.

3. **Perfil Administrador**: Entrega privilegios para el control total de un sistema específico y para la asignación de privilegios de usuario.

4. **Perfil Usuario**: Entrega privilegios para la interacción y el uso restringido con un sistema, con acceso a las propiedades generales del mismo y para el desarrollo de las labores encomendadas al usuario de este perfil

5. Procedimiento

1. Cada Jefe de departamento o unidad vinculado con el Gobierno Regional de Los Lagos, deberá definir y entregar, al departamento de Recursos Humanos (RRHH), un registro de los funcionarios, indicando los sistemas a los cuales debe acceder y los privilegios asignados (Perfil Administrador o Perfil usuario).

2. Cada jefatura de departamento o unidad, antes de solicitar privilegios, deberá verificar con el departamento de RRHH, el vínculo contractual del funcionario con la institución.

3. El Departamento de Recursos humanos, será el encargado de solicitar, a la unidad de informática, la activación de perfiles, en función de lo requerido por cada jefe de departamento o unidad.

4. La situación contractual de cada funcionario debe ser indicada en el registro de solicitud de privilegios que será entregada a la unidad de informática. Además de lo anterior, para el caso de usuarios "nuevos", el Departamento de RRHH deberá remitir una ficha de ingreso a la unidad de informática.

5. El otorgamiento de privilegios se realizará una vez que se haya completado el proceso anterior.

6. Un funcionario solo tendrá acceso a los sistemas que requiere para su trabajo y que han sido previamente solicitados por su jefatura directa (Departamento o Unidad).

7. Los privilegios serán eliminados ante desvinculaciones o cambios de funciones, situación que deberá ser informada por el Departamento de RRHH a la unidad de informática.

5.1. Acceso a Privilegios.

Los usuarios de los servicios y sistemas de información, deberán ser funcionarios del Gobierno Regional de Los Lagos, o bien usuarios externos autorizados por el/la Encargado/a de Seguridad de la Información Institucional para su acceso.

Todo usuario de los servicios y sistemas de información, deberán ser informados al Encargado/a de Seguridad de la información Institucional.

Bajo ninguna circunstancia el usuario deberá dar acceso a información (divulgar su clave personal e intransferible) a personas no autorizadas.

5.2. Cancelación de Privilegios.

Debe distinguirse entre cancelación de privilegios y bloqueo de privilegios:

Cancelación de privilegios: Es definitivo y se efectúa al desvincularse el funcionario de la institución.

En el caso que el usuario deje de laborar en la institución, el jefe de la Unidad o Departamento donde se desempeña deberá dar aviso al departamento de Recursos Humanos, quien deberá notificar a la unidad de informática de la baja, para la cancelación de cuentas y atributos (correo electrónico, Internet e Intranet y/o acceso a sistemas institucionales), a efecto de que sus contraseñas, privilegios y su cuenta individual sean canceladas, a su vez será la unidad de informática la responsable de notificar al Encargado/a de Seguridad de la información.

El Bloqueo de privilegios: Es de carácter transitorio y se usa en los casos que el funcionario haga uso de Licencias Médicas-Vacaciones-Prenatal, o cuando se cambia de función y debe modificarse el perfil con más o menos y privilegios o atributos o tenga una sanción.

En el caso que el usuario se encuentre en alguna de estas circunstancias, el jefe de la Unidad o Departamento donde se desempeña deberá dar aviso al departamento de Recursos Humanos, quien deberá notificar a la unidad de informática, para el bloqueo transitorio de cuentas y atributos (correo electrónico, Internet e Intranet y/o acceso a sistemas institucionales), a efecto de que sus contraseñas, privilegios y su cuenta individual sean bloqueadas, a su vez será la unidad de informática la responsable de notificar al Encargado/a de Seguridad de la información.

5.3. Incumplimiento, Uso Indebido y Denuncias

- Al detectar un uso indebido, se debe notificar inmediatamente al Encargado (a) de Seguridad de la Información y cuando corresponda, se deberán seguir los procedimientos locales de denuncia.

- Si por cualquier motivo no se puede notificar al Encargado (a) de Seguridad de la Información, se puede presentar la denuncia de incumplimiento a cualquier miembro del Comité de Seguridad de la Información.

- Las denuncias podrán ser de manera anónima. Esto se encuentra regulado en el Art. 90 B del DFL N°29 de 2004 del Ministerio de Hacienda, el que señala que las denuncias deben ser por escrito y firmadas por el denunciante. En ella podrá solicitarse que sean secretos los datos del denunciante.

- Si un jefe, supervisor o empleado presenta una denuncia falsa sobre un incumplimiento o un comportamiento cuestionable con la intención de perjudicar a otra persona. el denunciante será susceptible de una medida disciplinaria, conforme a la legislación vigente según proceda.

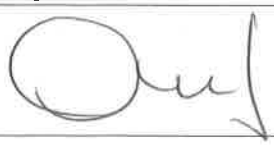
5.4. Registros de Control del procedimiento.

a) Formulario de ingreso de Funcionarios (as) enviado a la Unidad de Informática por parte del Departamento de Recursos Humanos.
b) Registro de funcionarios indicando los sistemas a los cuales puede acceder y los privilegios asignados.
c) Pantallazos de Active Directory.

6. Validez y gestión de documentos

Este documento es válido desde la fecha de su aprobación por parte del encargado (a) de seguridad de la Información.

El responsable de este documento es el Encargado (a) 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.

Aprobado Por

Carmen Mella Fagalde **Encargada (S) de Seguridad de la Información**
30 de Noviembre de 2017