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 "SEGREGACIÓN DE FUNCIONES"

CÓDIGO	**SSI-A.06.01.02**	**CLASIFICACIÓN INFORMACIÓN**		**Reservada**
			X	**Uso Interno**
				Pública
VERSIÓN	1.0	**FECHA DE LA VERSIÓN**	28-07-2017	
RESPONSABLE	Encargado de Seguridad de la Información			

Historial de modificaciones

Creación/Modificaciones del Documento

Versión	Fecha de creación / modificación	Autor	Motivo	Páginas creadas / 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

Contenido

1. Objetivo

Entregar las directrices para la correcta gestión de los usuarios, asignación y revisión de privilegios, y el uso de contraseñas.

2. Alcance o ámbito de aplicación interno.

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

3. Roles y Responsabilidades.

a) **Encargado de Seguridad de la Información:** auditar los perfiles de usuarios según la frecuencia establecida en el punto 4.2. del presente procedimiento.

b) **Unidad de Informática:** implementar los requerimientos establecidos en el presente procedimiento, gestionar los perfiles de usuarios, asegurar que este procedimiento quede debidamente operativo en todos los sistemas de uso corporativo.

4. Procedimiento

4.1. Documentos de Referencia.

Código	Descripción
SSI-A.05.01.01	Política de Seguridad de la Información.
SSI-FR-001	Solicitud de cambios a la política de seguridad de la Información.
SSI-A.09.02.03	Procedimiento gestión de derechos de acceso privilegiado
SSI-A.08.01.04	Procedimiento devolución de activos.

4.2. Segregación de Usuarios

Los usuarios deben ser segregados mediante roles y/o perfiles de usuario que den cuenta de su respectiva descripción de cargo y que contengan los accesos necesarios para el desarrollo de sus funciones.

Estos perfiles serán gestionados por la Unidad de Informática mediante la controladora de dominio utilizada por la institución (la gestión de permisos incluye administración del equipo, acceso a sistemas, acceso a sitios web, etc.) y en lo relativo al usos de los sistemas informáticos por la Unidad de Administración y Operaciones.

Para efectos de articular lo señalado en el párrafo precedente se usará un control de acceso mediante una identificación de usuario y una contraseña, donde sea posible, se podrá usar en su reemplazo algún patrón biométrico (por ejemplo, la huella dactilar del usuario).

El Encargado de Seguridad de la Información debe validar los perfiles de usuario y auditarlos al menos 2 veces al año.

4.3. Gestión de privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema es uno de los factores preponderantes en la falla de los mismos, toda vez que se accede de forma no autorizada o bajo la ilegalidad.

Para evitar irrupciones no deseadas, el funcionario encargado de la administración de la red debe gestionar los privilegios de acuerdo a lo que a continuación se establece:

- Se identificarán los privilegios asociados a cada sistema disponible, por ejemplo, sistema operativo, base de datos, aplicaciones Web, aplicaciones internas, sistemas informáticos, etc.

- Se asignarán privilegios a los funcionarios sobre la base de la necesidad de uso y por evento, por ejemplo, el requerimiento mínimo para su rol funcional.

- Se otorgarán privilegios de acceso extraordinarios, previa autorización y justificación del jefe directo y/o jefe de división según corresponda.

- Se establecerá un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.

La creación de usuarios y gestión de derechos de acceso se realizará de acuerdo a lo descrito en los procedimientos gestión de derechos de acceso privilegiado (A.09.02.03) y devolución de activos (A.08.01.04).

4.4. Directrices para la gestión de usuarios

Utilizar identificación de usuarios (ID) únicos, para permitir así vincularlos y ser responsables de sus acciones; sólo se deben permitir el uso de ID grupales en casos excepcionales y cuando sea operacionalmente necesario. En este caso se deberá obtener una autorización especial de parte del Encargado de Seguridad de la Información.

El Administrador de los Sistemas será el responsable de mantener un registro formal de todas las personas autorizadas y de los permisos asignados en cada una de ellas en cada uno de los sistemas Institucionales, eliminando, modificando o bloqueando inmediatamente los derechos de acceso en el caso de que, previo aviso por escrito de la jefatura directa, algunos de los usuarios hayan cambiado de función, puesto o

trabajo o haya dejado de pertenecer a la organización. En este último caso se necesitará una comunicación oficial de parte de la jefatura respectiva de acuerdo a lo descrito en el procedimiento de Gestión de Derechos de Acceso y Devolución de Activos.

Para los privilegios de acceso asociados a los elementos del sistema (por ejemplo, sistema de operación, sistema de gestión de base de datos y cada aplicación) se debe mantener un registro, identificando los usuarios que poseen estos privilegios.

4.5. Registros de control del procedimiento.

a) Correo electrónico de validación y creación de cuentas de usuario.
b) Pantallazos de la controladora de dominio utilizada para la segregación de funciones.

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.

Aprobado Por
Daniel Olhabe Espinosa **Encargado de Seguridad de la Información**
24 de Octubre de 2017