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 "INICIO DE SESION SEGURO"

CÓDIGO	**SSI-A.09.04.02**	**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	Oscar Oyarzo Pérez, Jefe 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 4
2. Alcance o ámbito de aplicación interno. 4
3. Roles y Responsabilidades 4
4. Definiciones 5
5. Procedimiento 5
   - 5.3.1. Usuario/contraseña 7
   - 5.3.2. Certificados: 8
   - 5.3.3. Asignación de Permisos, Perfiles y Roles 9
   - 5.3.4. Incumplimiento, uso indebido y denuncias 9
6. Registros de Control del procedimiento 10
7. Validez y gestión de documentos 10

1. Objetivo

Evitar el acceso sin autorización a los sistemas y aplicaciones, asegurando un procedimiento de inicio de sesión seguro, que permita restringir el acceso a la información y a las funciones del sistema, de acuerdo con la política de control de acceso.

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, además de establecer mecanismos de información para permitir a los usuarios supervisar la actividad normal de su cuenta, así como alertarlos oportunamente sobre actividades inusuales.

- **Jefe de Departamento o Unidad:** Solicitar formalmente al Departamento 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 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 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:** cada miembro del personal, debe tener asignada una cuenta de usuario (con su correspondiente código-usuario y contraseña), para acceder a su "sesión del computador" y por ende 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 con personales e individuales.

La contraseña para acceder a una "sesión" debe ser cambiada cada vez que un usuario crea que su contraseña la conocen otras personas, cuando la haya olvidado y requiera una contraseña nueva o cuando el sistema se lo requiera.

4. Definiciones

- **Privilegio**: nivel de acceso otorgado a un usuario
- **Perfil**: Conjunto de privilegios que se le asignan a un usuario de un servicio informático.
- **Perfil Administrador**: Entrega privilegios para el control total de un sistema específico y para la asignación de privilegios de usuario.
- **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
- **Usuarios internos**: serán todas aquellas personas que sean funcionados del Gobierno Regional de Los Lagos.
- **Usuarios externos**: serán aquellos que estén adscritos o pertenezcan a un tercero que no sean del Gobierno Regional de Los Lagos y que estén autorizados a conectarse a los sistemas de información de su propiedad.
- **Usuarios genéricos**: Como excepción a las normas generales descritas, y de manera autorizada por el Responsable designado podrán definirse y utilizarse usuarios genéricos.

5. Procedimiento

5.1. Reglas Generales:

Los Sistemas de información del Gobierno Regional de Los Lagos, deben disponer de los mecanismos necesarios que permitan la validación de todos los usuarios en el momento de su conexión. Por lo tanto, no se permitirá la existencia de sistemas de información que no puedan identificar y autentificar al usuario mediante un proceso lógico. Por consiguiente, se deberán garantizar las siguientes reglas:

a) Cada usuario, dispondrá de un identificador único que pueda ser reconocido por los sistemas de información de la Organización.

b) A cada identificador de usuario le corresponderá una y sólo una persona física, y sólo esta persona, estará autorizada a utilizarlo.

c) Todas aquellas operaciones realizadas por un usuario, serán siempre imputadas al identificador utilizado que se hubiere identificado ante el sistema de información, independientemente de la persona física que lo haya realizado.

El procedimiento de generación de identificadores u otro de usuario para los sistemas de información del Gobierno Regional de Los Lagos, deberá, al menos, cumplir los siguientes requisitos mínimos:

a) El código generado para este requisito deberá proveer de una identificación inequívoca, como por ejemplo el RUN.

b) El procedimiento de generación, garantizará la imposibilidad de reasignar o reutilizar identificadores de usuario previamente utilizados.

c) El procedimiento de generación garantizará la no duplicidad de los mismos.

d) El procedimiento, garantizará que se cumpla con las reglas de identificación y nomenclatura, así como demás estándares aplicables.

e) Se deberá establecer una nomenclatura de usuarios para el personal externo a la Organización, con el fin de identificar fácilmente si un usuario es o no empleado del Gobierno Regional de Los Lagos.

f) Será responsabilidad de los administradores, la implementación y gestión del mismo.

Este procedimiento, con ayuda de la función de administración de usuarios, deberá exigir, para generar un alta válida de usuario, como mínimo el cumplimiento y registro de los siguientes datos:

a) Nombre y apellidos del usuario.
b) RUN del usuario.
c) Tipo de usuario (interno, externo, genérico).
d) Identificador asignado.
e) Fecha de alta.
f) Detalle de los permisos concedidos.

Siempre que sea técnicamente posible, se deberá automatizar el procedimiento de bloqueo de identificadores de usuario, en los casos que se refieren a continuación, y según la clasificación de los sistemas o el perfil de las cuentas afectadas. Dichos procedimientos de bloqueo, se podrían ejecutar en los siguientes casos:

a) Por caducidad de los identificadores.
b) Por la inactividad de los identificadores.
c) Por intento de acceso fallido, utilizando dicho identificador en más de cinco intentos fallidos.
d) Por baja temporal.
e) Por baja definitiva o desvinculación (lo cual implicará la eliminación del identificador).

5.2. Autorización

a) Para que exista un correcto control, el acceso a los recursos (ficheros, aplicaciones, bases de datos, sistema operativo, configuración, etc.) debe ser autorizado por los propietarios de los recursos.

b) Las solicitudes de autorización, deben ser ejecutadas por los administradores de dichos recursos siguiendo las normativas impuestas por cada Responsable y que estas cuenten con la validación de la alta administración.

c) Como regla general, los usuarios únicamente tendrán acceso a los recursos necesarios para el ejercicio de sus funciones. Cualquier otro requerimiento al respecto se tramitará siguiente el circuito de excepciones.

d) Independientemente del tipo de acceso, interno o externo, dicho acceso debe ser autorizado previamente siempre por el propietario/responsable del recurso.

e) En ningún caso asignarán privilegios y accesos a usuarios sin una solicitud previamente autorizada.

f) Se deberán resguardar todas las solicitudes autorizadas, y se pondrán a disposición en caso de auditorías internas o externas, así como para el control interno.

g) En el caso de que se autorice el acceso a recursos por un tiempo determinado, los administradores deberán cuidar que éste se cumpla, eliminando los privilegios en el tiempo establecido.

5.3. Autenticación

5.3.1. Usuario/contraseña

Se deberá adoptar una política adecuada de contraseñas para validación o autenticación de usuarios, es el primer y más importante control para evitar los accesos no autorizados, o utilización indebida de los usuarios de los sistemas de información del Gobierno Regional de Los Lagos.

Se deberá cumplir, mediante el establecimiento de medidas automatizadas, las siguientes reglas de aplicación en la generación y utilización de contraseñas:

a) Las contraseñas deberán tener una longitud mínima de 8 caracteres alfanuméricos (alfabéticos, numéricos y especiales, como por ejemplo %&$/0"1) y la longitud dependerá de la importancia de la información protegida.

b) Mediante el registro y conservación de un histórico de contraseñas por usuario, el sistema informático impedirá la utilización, al menos, de las últimas 4 contraseñas.

c) El usuario podrá realizar el cambio de su contraseña siempre que lo considere necesario.

d) Ante un cambio de contraseña, el sistema informático solicitará la última contraseña con objeto de validar la misma.

e) Las contraseñas caducarán de forma automática cada cierta cantidad de días como máximo, y cumplido dicho plazo, el sistema obligará al usuario a cambiar su contraseña. La periodicidad marcada depende del nivel de información protegida, lo habitual es 30-60 días.

f) Un usuario quedará bloqueado al cabo de 5 intentos de accesos fallidos. Esta medida protege al sistema frente a ataques de fuerza bruta o muchos intentos fallidos. El número de intentos suele estar entre 5-8.

g) El sistema, al cabo de 5 minutos de inactividad, realizará el bloqueo del terminal de usuario activando el Protector de Pantalla, exigiendo nuevamente la validación de la contraseña.

h) Al cabo de 30 días corridos como máximo de inactividad del identificador del usuario, éste quedará automáticamente bloqueado. Esta medida protege al sistema de usuarios que ya no deben tener acceso por haber causado baja.

i) Además, usuarios en pre y post natal no quedarían afectados por estas medidas

Mayor detalle del correcto uso, gestión y creación de contraseñas, se puede encontrar el documento que define el procedimiento "Sistema de Gestión de Contraseñas", correspondiente al control A.09.04.03

5.3.2. Certificados:

a) Existe la posibilidad de que los clientes se identifiquen en el servidor mediante la presentación de un certificado. Los certificados de cliente normalmente contienen información como su nombre, empresa, departamento, dirección de correo, ciudad, país, etc., lo que permite establecer mecanismos de autenticación y control de acceso más complejos, utilizando uno de estos atributos o en un conjunto de ellos.

b) La forma de uso es fácil e intuitiva, ya que el usuario simplemente instala el certificado en su sistema y posteriormente, cuando se conecte al servidor, sólo tiene que presentarlo para que se produzca la autenticación. Los certificados

pueden almacenarse localmente en el disco duro del ordenador del usuario o en una tarjeta inteligente. En ambos casos, se encontrarán protegidos por una contraseña, para evitar el acceso fraudulento a los mismos.

c) Los certificados de usuarios, emitidos por una Autoridad de Certificación, pueden emplearse para uso internos, pudiendo emplear para ello una Autoridad de Certificación propia.-. Los sistemas operativos Microsoft Windows Server y Linux incluyen servicios de certificación que permiten a las empresas emitir sus propios certificados.

5.3.3. Asignación de Permisos, Perfiles y Roles

a) Los usuarios que acceden a los sistemas de información de la Organización pertenecerán a un tipo de usuario determinado de acuerdo al rol o funciones que tenga en el Gobierno Regional de Los Lagos.

b) Usuarios internos: serán todas aquellas personas que sean funcionados del Gobierno Regional de Los Lagos.

c) Usuarios externos: serán aquellos que estén adscritos o pertenezcan a un tercero que no sean del Gobierno Regional de Los Lagos y que estén autorizados a conectarse a los sistemas de información de su propiedad.

d) Usuarios genéricos: Corno excepción a las normas generales descritas, y de manera autorizada por el Responsable designado podrán definirse y utilizarse usuarios genéricos.

5.3.4. 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.

- No se permitirá ningún tipo de represalia contra ningún jefe, supervisor o empleado que, de buena fe, pida consejo al respecto o denuncie el incumplimiento de esta Política. Lo cual se encuentra regulado en el Art. 90 A del DFL N°29 de 2004 del Ministerio de Hacienda.

- 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 al Art. 62 N°9 del DFL 1.

- El Encargado (a) de Seguridad de la Información debe ser informado inmediatamente en caso que se reciba cualquier comunicado (por teléfono, correo postal o correo electrónico) de parte de una autoridad de protección de datos u otro ente regulador.

6. Registros de Control del procedimiento.

a) Pantallazos de Active Directory del acceso de distintos tipos de usuarios.
b) Registro de funcionarios indicando los sistemas a los cuales puede acceder y los privilegios asignados.

7. 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 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