Gobierno de Chile

GOBIERNO REGIONAL DE LOS LAGOS
Acción de Futuro

CERTIFICO QUE LA PRESENTE FOTOCOPIA ES FIEL DEL ORIGINAL QUE SE ENCUENTRA ARCHIVADO EN LA OFICINA DE PARTES DEL GOBIERNO REGIONAL DE LOS LAGOS, y consta de 13 Páginas. 24 NOV 2017 V°B° Idoc.
PUERTO MONTT,

FORMALIZA, DIFUNDE Y PUBLICA LA POLITICA DE CONTROL DE ACCESO DEL GOBIERNO REGIONAL DE LOS LAGOS.

RESOLUCION EXENTA Nº 3720 /

PUERTO MONTT, 22 NOV 2017

VISTOS:

a) Que se requiere formalizar la Política de Control de Acceso del Gobierno Regional de Los Lagos, en función de lo indicado en el punto 3.4.1 del documento que define la "Estrategia de trabajo red SSI 2017", publicado en la página web "http://ssi.digital.gob.cl/documentos".

b) Las facultades que me otorga la Ley 19.175, Orgánica Constitucional sobre Gobierno y Administración Regional.

c) Resolución N°1600/2008 de la Contraloría General de la República, que fija normas sobre exención del trámite de Toma de Razón.

R E S U E L V O:

1. **FORMALIZAR** la **POLITICA DE CONTROL DE ACCESO** del Gobierno Regional de Los Lagos, con el objeto de definir los perfiles y privilegios de los diferentes sistemas informáticos del Gobierno Regional de Los Lagos, y establecer la relevancia de controlar la asignación y uso de privilegios; y cuyo texto es el siguiente:

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

"POLITICA DE CONTROL DE ACCESO"

CÓDIGO	**SSI-A.09.01.01**	**CLASIFICACIÓN INFORMACIÓN**		**Reservada**
			X	**Uso Interno**
				Pública
VERSIÓN	1.0	**FECHA DE LA VERSIÓN**	15-11-2017	
RESPONSABLE	Encargado (a) de Seguridad de la Información			

Gobierno de Chile

GOBIERNO REGIONAL DE LOS LAGOS
Acción de Futuro

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	20-11-2017	Fabiola Yáñez Rojas, Jefa Depto. Jurídico	

Distribuciones

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

Gobierno de Chile

GOBIERNO REGIONAL DE LOS LAGOS
Acceso de Futuro

Contenido

1. Objetivo

Documentar y Formalizar una política de control de acceso, basada en las características del negocio y de seguridad de la información. La presente política describe los perfiles y privilegios de los diferentes sistemas informáticos del Gobierno Regional de Los Lagos, y establece la necesidad de contar con controles de seguridad de la información con el objeto de controlar la asignación y uso de privilegios.

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, para la oportuna creación, modificación y eliminación de todas las cuentas de usuario asociadas al personal y, asimismo, establecer los procedimientos para el adecuado registro y respaldo 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 de División, Departamento o Unidad:** Solicita formalmente a la Unidad de informática, 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:** Autoriza la asignación de privilegios de las 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:** Debe 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 y oficina asignada.

- **Funcionarios:** cada funcionario del personal del Gobierno Regional de Los Lagos, debe tener asignada una cuenta de usuario (con su correspondiente 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 intransferibles. La contraseña 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, y/o cada tres meses, teniendo especial cuidado en cumplir con los estándares definidos en el procedimiento "Sistema de Gestión de contraseñas", control A.09.04.03.

4. Definiciones.

Para los propósitos de esta Política, se entenderá por:

- **Acceso a la información:** El acceso que tiene toda persona para buscar, pedir, recibir y difundir información que se encuentre en poder del Gobierno Regional de Los Lagos.

- **Derechos de accesos:** Conjunto de permisos o atributos dados a un usuario, quien de acuerdo con sus funciones y/o tareas encomendadas, pueda acceder a un determinado recurso.

- **Restringir el acceso:** Delimitar el acceso de los usuarios a determinados recursos.

- **Sanción:** Puede ser definida como una consecuencia administrativa, civil, jurídica o penal por el incumplimiento de la actual política de seguridad de la información u otra norma.

- **Sistema informático:** Es un sistema que permite almacenar y procesar información, es el conjunto de partes interrelacionadas: hardware, software y personal informático, capaces de realizar procesamiento de información y/o transferencia de información.

- **Usuario:** persona que utiliza un sistema informático y que obtiene un servicio, por ejemplo, correo electrónico proporcionado o administrado por el Gobierno Regional de Los Lagos, ya sea que lo utilice en virtud de un empleo, de una función o de cualquier prestación de servicio, sin importar la naturaleza jurídica de ésta o del estatuto que lo rija.

- **Documento electrónico:** toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

- **Documento público:** aquellos documentos que no son reservados y cuyo conocimiento no está circunscrito.

- **Documento reservado:** aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano que sean remitidos.

- **Documento electrónico institucional:** Documento electrónico creado, enviado, comunicado o recibido, por los usuarios del Gobierno Regional de Los Lagos, en el ejercicio de las funciones propias de la institución.

- **Unidad de Informática:** Unidad de Informática del Gobierno Regional de Los Lagos.

Seguridad del documento electrónico.

La seguridad del documento electrónico se logra garantizando los siguientes atributos esenciales del documento:

- **Activos de información:** Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y/o

recuperación de información de valor para la Institución cualquiera sea el formato que la contenga y los equipos y sistemas que la soporten.

- **Riesgo:** Es la contingencia de un daño a un activo de información. A su vez, contingencia significa que el daño puede materializarse en cualquier momento o no suceder nunca.

- **Amenaza:** Causa potencial de un incidente no-deseado por el cual puede resultar dañado un sistema u organización. A modo de ejemplo. Terremotos, inundaciones, Sabotajes, Amenazas de bombas, negligencias humanas, cortes eléctricos, fallas en sala de servidores, entre otras.

- **Gestión del riesgo:** Proceso definido para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto al alcance de los objetivos de la organización.

- **Evaluación del riesgo:** Comparar los niveles de riesgo encontrados contra los criterios de riesgo preestablecidos (si es que han sido establecidos por la dirección) considerando el balance entre los beneficios potenciales y resultados adversos. Ordenar y priorizar mediante un ranking los riesgos analizados.

- **Seguridad de la Información:** Proceso encargado de asegurar que los recursos de un sistema de información sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea factible para las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la Integridad, Confidencialidad y Disponibilidad del sistema.

- **Proceso:** Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.

- **Incidente de Seguridad:** Se define incidente como cualquier evento o situación que comprometa de manera importante la disponibilidad, integridad y confidencialidad de la información.

- **Confidencialidad:** Es la propiedad de un documento o mensaje, que autoriza únicamente a algunas personas para acceder a él.

- **Integridad:** Se entiende por la corrección y plenitud de los datos o de la información manejada.

- **Disponibilidad:** es la certeza de contar con acceso a la información y a los activos asociados cuando sea requerido.

- **Medios de procesamiento de información:** Son los dispositivos internos y/o externos que tenga la capacidad de procesar información, almacenarla y que se encuentren disponibles para ser manipulados por el usuario. Algunos ejemplos de medios de procesamiento de información son:

  - ✓ Servidores de aplicaciones: de correo, de impresión, aplicaciones web.
  - ✓ Servidores de Almacenamientos.
  - ✓ Computadores personales.
  - ✓ Discos duros externos.
  - ✓ Pendrives.
  - ✓ Teléfonos móviles.

- **Operaciones informáticas:** Todas las actividades que estén relacionadas con un sistema informático y/o procesamiento de la información.

- **Terceras partes:** Persona u organismo reconocido como independiente de las partes implicadas en lo que se refiere a la materia en cuestión.

- **Estación de Trabajo:** En una red de computadores, una estación de trabajo es un computador que facilita a los usuarios el acceso a los servidores y periféricos de la red.

- **Programa malicioso:** Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

- **Virus:** Se usa para designar un programa que, al ejecutarse, se propaga infectando otros softwares ejecutables dentro de la misma computadora.

- **Malware:** El término malware es muy utilizado para referirse a una variedad de software hostil, intrusivo o molesto. El término malware incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware y otros softwares maliciosos e indeseables.

- **SPAM:** Se llama spam al correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo, habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor). La acción de enviar dichos mensajes se denomina spamming.

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

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

5. Procedimiento

La Unidad de Informática establece como Política de Control de Acceso el controlar el acceso a la información, a las instalaciones de procesamiento de la información (Datacenter) y a los procesos de provisión, los cuales deberán ser controlados sobre la base de los requisitos y seguridad.

Para ello, a través de la Administración de Bases de Datos, Soporte y Seguridad permitirá administrar el ciclo de vida de los usuarios, desde la creación de las cuentas, otorgar roles y permisos necesarios hasta su eliminación.

5.1. Control de Acceso

5.1.1. Reglas para el control de acceso

Las reglas para el control de acceso, estará documentado a través de los diferentes procedimientos de control de acceso a los recursos tecnológicos.

5.1.2. Gestión de identidades

Se deberá asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información.

5.1.3 Responsabilidad de los usuarios

Todos los funcionarios que tengan un usuario en la plataforma tecnológica, deberán conocer y cumplir con su uso de esta Política específica, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado de los usuarios, así como políticas de protección de usuario desatendido, escritorio y pantalla limpia.

5.1.4 Control de Acceso a la Red

Las conexiones no seguras a los servicios de red pueden afectar a toda la institución, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos, esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de los mismos.

Las reglas de acceso a la red a través de los puertos, estarán basadas en la premisa "todo está restringido, a menos que este expresamente permitido"

5.2. Servicios de RED

5.2.1 Política de utilización de los servicios de red

Se desarrollarán procedimientos para la activación y desactivación de derechos de usuarios de acceso a las redes.

5.2.2 Autenticación de usuarios para conexiones externas

La Unidad de Informática contempla como servicios de conexiones externas SSL, para funcionarios que requieran conexión remota a la red de datos institucional.

5.2.3 Identificación de equipos en la Red

La Unidad de Informática controlará e identificará los equipos conectados a su red, mediante el uso de asignación de IP estáticas.

5.2.4 Separación de redes

La Unidad de Informática utilizará dispositivos de seguridad tales como firewalls, para controlar el acceso a la red.

El control se realizará en equipos de enrutamiento mediante la configuración de lista de control de acceso y configuraciones de VLANs en los equipos de comunicaciones layer.

5.2.5 Control de conexión de las redes

Dentro de la red de datos institucional se restringirá el acceso a:

- Mensajería instantánea.
- La telefonía a través de internet.
- Correo electrónico comercial no autorizado.
- Descarga de archivos de sitio peer to peer (punto a punto).
- Conexiones a sitios de streaming no autorizado.
- Acceso a sitios de pornografía.
- Servicios de escritorio remoto a través de internet.
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma.

5.2.6 Control de enrutamiento de red

La Unidad Informática, proveerá a través de sus ISP's (Proveedor de Servicio de Internet) el servicio de internet institucional, el cual será administrado por el proceso de direccionamiento tecnológico y será el único servicio de internet autorizado.

5.3. Control de Acceso al Sistema Operativo

5.3.1 Registro de inicio seguro

El acceso a los sistemas operativos estará protegido. Mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:

- No mostrar información del sistema. hasta que el proceso de inicio se haya completado.
- No suministrar mensajes de ayuda, durante el proceso de autenticación.
- Validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada.

5.3.2 Gestión de contraseñas

La asignación de contraseñas se deberá controlar a través de un proceso formal de gestión. Las recomendaciones son:

- No escribirlas en papeles de fácil acceso, ni en archivos sin cifrar.
- No habilitar la opción "recordar clave en este equipo", que ofrecen los programas.
- No enviarla por correo electrónico.
- Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.
- Las contraseñas se deben mantener confidenciales en todo momento.
- No compartir las contraseñas, con otros usuarios.
- Cambia tu contraseña si piensas que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Selecciona contraseñas que no sean fáciles de adivinar.
- Nunca grabes tu contraseña en una tecla de función o en un comando de caracteres predefinido.
- Cambia tus contraseñas regularmente.
- No utilizar la opción de almacenar contraseñas en Internet.
- No utilizar contraseña con números telefónicos, nombre de familia etc.
- No utilizar contraseña con variables (soporte1, soporte2, soporte3 etc.)

5.3.3 Uso de utilitarios del sistema

El uso de software utilitario del sistema, estará restringido a usuarios administradores.

5.3.4 Inactividad del sistema

Después de tiempo de inactividad del sistema, se considerará tiempo muerto y se bloqueará la sesión, sin cerrar las sesiones de aplicación o de red.

Los usuarios procederán a bloquear sus sesiones, cuando deban abandonar temporalmente su puesto de trabajo. Las estaciones de trabajo deberán quedar apagadas al finalizar la jornada laboral o cuando una ausencia temporal supere dos (2) horas.

5.3.5 Limitación de tiempo de conexión

Por la tarea de la Unidad de Informática, no se limitará el tiempo de conexión, ni se establecerán restricciones en la jornada laboral.

5.3.6 Control de acceso a la información

El control de acceso a la información a través de una aplicación, se realizará a través de roles que administren los privilegios de los usuarios dentro del sistema de información.

El control de acceso a información física o digital, se realizará teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información.

5.4. Computación Móvil

Teniendo en cuenta las ventajas de la computación móvil, así mismo el nivel de exposición a amenazas que pongan en riesgo la seguridad de la información institucional, a continuación se establecen directrices que permitirán regular el uso de la computación móvil.

5.4.1 Computación y comunicaciones móviles

Se entiende como dispositivos de cómputo y comunicación móviles, todos aquellos que permitan tener acceso y almacenar información institucional, en lugares diferentes a las instalaciones institucionales.

El uso de equipos de cómputo y dispositivos de almacenamiento móviles, está restringido únicamente a los provistos por la institución y deberán contemplar las siguientes directrices:

- Uso de usuario y contraseña para acceso al mismo.
- Cifrado de la información.
- Uso de software antivirus provisto por la Unidad Informática.
- Restricción de privilegios administrativos para los usuarios.
- Uso de software licenciado y provisto por la Unidad Informática.
- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.
- No llamar la atención, acerca de portar equipos móviles.
- No identificar el dispositivo con distintivos de la Institución.
- No colocar datos de contacto técnico en el dispositivo
- Informar de inmediato al Área de Soporte sobre la pérdida o hurto del dispositivo, quien procederá al bloqueo del usuario.

6. Incumplimiento, uso indebido y denuncias

a) Al detectar un uso indebido de la presente Política, se debe notificar inmediatamente al Encargado (a) de Seguridad de la Información institucional y cuando corresponda, se deberán seguir los procedimientos establecidos para su denuncia.

b) 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.

c) 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.

d) 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 anterior se encuentra regulado en el Art, 90 A del DFL N°29 de 2004 del Ministerio de Hacienda.

e) 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.

f) 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.

7. Periodicidad de evaluación y revisión de la política.

Esta política, tendrá un plazo máximo de 3 años para cualquier evaluación, revisión, actualización e integración de nuevas normativas, o cuando existan cambios significativos que afecten su continuidad.

8. Mecanismos de difusión de la política.

La difusión de esta política será realizada a través de los siguientes mecanismos:

1) Correo electrónico institucional dirigido a todos los funcionarios o funcionarias de la institución, con el documento de la política adjunto.

2) Publicación a través de las distintas plataformas web de la institución una vez totalmente tramitada.

Gobierno de Chile

GOBIERNO REGIONAL DE LOS LAGOS
Acción de Futuro

2. **DIFUNDIR** el documento de la **POLITICA DE CONTROL DE ACCESO** del Gobierno Regional de Los Lagos, a todos los funcionarios del Gobierno Regional de Los Lagos, a través del correo electrónico institucional de cada uno de éstos.

3. **PUBLICAR** el documento de la **POLITICA DE CONTROL DE ACCESO** del Gobierno Regional de Los Lagos, en la página web institucional http://transparencia.goreloslagos.cl/web/.

ÁNOTESE, COMUNÍQUESE Y ARCHÍVESE,

INTENDENTE REGIONAL
REGIÓN DE LOS LAGOS

LEONARDO DE LA PRIDA SANHUEZA
INTENDENTE
REGION DE LOS LAGOS

CMF/FYR/OOP/dlh.

Distribución:

- Funcionarios Planta, Contrata y Honorarios del GORE Los Lagos.
- Arch. Encargado de Seguridad de la Información, GORE Los Lagos.
- Arch. Unidad de Informática, GORE Los Lagos.
- Arch. Oficina de Partes, GORE Los Lagos.