GOBIERNO REGIONAL DE LOS LAGOS

Acción de Futuro

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

CÓDIGO	**SSI-A.13.02.01**	**CLASIFICACIÓN INFORMACIÓN**		**Reservada**
			X	**Uso Interno**
				Pública
VERSIÓN	1.0	**FECHA DE LA VERSIÓN**	28-07-2019	
RESPONSABLE	Encargado de Seguridad de la Información			

Historial de modificaciones

Creación/Modificaciones del Documento

Versión	Fecha	Autor	Debido a	Páginas	Firma
1.0	28-07-2019	Oscar Oyarzo Pérez, Profesional Unidad de Informática	Creación de la primera versión de la política	Todas	

Revisiones

Versión	Fecha	Autor	Observación	Páginas	Firma
1.0	28-07-2019	Eduardo Madrid Osorio, Encargado Unidad de Informática	Sin observaciones	Todas	

Visto Bueno

Versión	Fecha	Encargado	Firma
1.0	27-11-2019	Oscar Oyarzo Pérez, Encargado de Seguridad de la Información	
1.0	27-11-2019	Alejandro Montaña Ampuero, Administrador Regional del Gobierno Regional de Los Lagos	GOBIERNO REGIONAL ADMINISTRADOR REGIONAL DE LOS LAGOS

Distribuciones

Versión	Fecha	Encargado	Observaciones
1.0	06-11-2019	Nicanor Bahamonde Loustau Profesional Unidad de Informática	Enviado por correo electrónico e instruida la publicación en intranet a la Unidad de Informática

INDICE

1 ASPECTOS GENERALES.

Los computadores, servidores y la red del Gobierno Regional de Los Lagos, son tecnologías que permiten de forma eficiente el acceso, transferencia y distribución de información tanto dentro como fuera de la organización. Como estas tecnologías nos permiten acceder, copiar y compartir información con otros usuarios de la red, los usuarios deben estar conscientes de sus derechos y de los demás, tales como la privacidad o protección de la propiedad intelectual, la integridad del sistema y de los recursos físicos, así como respetar las leyes y regulaciones vigentes.

Esta política aporta una serie de recomendaciones y líneas de actuación para formalizar el uso correcto de los sistemas de información y comunicación y la aplicación de buenas prácticas.

1.1 Resumen del Documento.

Los usuarios del Gobierno Regional de Los Lagos que utilizan la infraestructura TIC (Tecnologías de la Información y Comunicación), deberán respetar la integridad de los recursos basados en los sistemas de información, evitar actividades destinadas a obtener accesos no autorizados o suplantación de identidad, no acaparar en exceso los recursos compartidos con otros usuarios y respetar las políticas de licencias de software. Esta política se deberá aplicar a la red, los equipos conectados a ella y a toda la información contenida en los equipos, además este documento explica qué se considera un uso adecuado de la red y sistemas con relación a los derechos de otros y menciona las responsabilidades que supone el uso de estos recursos y de las consecuencias de su abuso y transferencias no autorizadas.

1.2 Objetivo de la Política.

Definir un marco procedimental que permita asegurar una infraestructura informática que facilite la realización de las misiones básicas del Servicio, como son la comunicación y tareas administrativas, y a su vez, asegurar la existencia de procedimientos y controles formales para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación, tanto dentro de la Institución, como a entidades externas.

1.3 Alcance o Ámbito de la aplicación interno.

Este procedimiento es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), y personal a honorarios. Es importante consignar, que se aplicará también a cualquier otra entidad externa que utilice los recursos informáticos o preste servicios al Gobierno Regional de Los Lagos.

1.4 Recursos a los que se refiere esta política

Son todos aquellos sistemas de información, sean éstos individuales o compartidos, y estén o no conectados a nuestra red. Se aplicará a todos los equipos (estaciones de trabajo, notebooks, servidores, access point (wifi), impresoras, etc.) e infraestructura de comunicaciones que sean propiedad o estén administrados por la Unidad de Informática del Servicio. Esto incluye terminales, computadores personales, estaciones de trabajo, servidores y periféricos asociados, así como el software, independiente de que se use para gestión administrativa, económica, investigación u otros. De forma específica, se podrán redactar procedimientos y recomendaciones de buen uso de servicios e infraestructuras, como por ejemplo:

- Servicios informáticos (correo electrónico, Web, multimedia, sistemas, etc.)
- Buen uso de la infraestructura de redes y del acceso a Internet.

- Acceso a servidores con datos de carácter personal.
- Incidencias de seguridad.
- Detección de virus y malware.

1.5 Aspectos legales

Se aplicará las Leyes y normativas chilenas, en relación con protección de datos personales, propiedad intelectual y uso de herramientas Informáticas, así como las que puedan ir surgiendo en el futuro al respecto. Por ello, el Gobierno Regional, podrá ser requerido por los órganos administrativos pertinentes para que proporcione los registros electrónicos o cualquier otra información relativa al uso de los sistemas de información.

Esta política se sitúa dentro del marco legal jurídico definido por las Leyes y decretos siguientes:

- Ley 19.223 que regula: "Tipifica figuras penales relativas a la informática".
- Artículo 1: El que maliciosamente destruya o inutilice su sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena del presidio menor en su grado medio a máximo, Si como consecuencia de estas conductas se afectasen los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.
- Artículo 2: El que, con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en el sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.
- Artículo 3: El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.
- Artículo 4: El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quién incurre en estas conductas en el responsable del sistema de información, la pena aumentará en su grado.

Asimismo, forma parte Integrante de este documento la normativa vigente en el país referido a las Tecnologías de la Información.

- Norma Chilena de Seguridad NCh 2777 hace referencia a los controles de la seguridad informática.
- Ley 19.223: Tipifica delitos informáticos.
- Ley 17.336: Sobre propiedad intelectual.
- Ley 19.628: Sobre la protección de la vida privada o protección de datos de carácter personal.
- Ley 19.812: sobre protección de la vida privada.
- Ley 19.799: Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma.
- Ley 18.168: General de Telecomunicaciones.
- Ley 19.927: Ley contra la Pedofilia.
- DS 77/2004: Aprueba Norma Técnica sobre Eficiencia de La Comunicaciones Electrónicas entre Órganos de la Administración del Estado y entre éstos y los ciudadanos.
- DS 81 /2004: Establece las características mínimas obligatorias de interoperabilidad que deben cumplir los documentos electrónicos en su generación, envío, recepción procesamiento y almacenamiento.
- DS 83/2004: Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad del Documento Electrónico.
- DS 93: Aprueba Norma Técnica para minimizar la recepción de mensajes electrónicos no deseados en las casillas electrónicas de los Órganos de la Administración del Estado y de sus funcionarios y funcionarias.
- DS 100/2006: Fija características mínimas obligatorias que deben cumplir los sitios WEB de los Órganos de la Administración del Estado.
- Ley 19.880: Bases y Procedimientos Administrativos, se refiere a acceso a información personal y privacidad.

• Decreto 26/2001: Reglamento sobre el Secreto o Reserva de los Actos y Documentos de la Administración del Estado.
• DS N°14, de febrero de 2014. Modifica Decreto N° 181, de 2002, que aprueba Reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.
• Número 1, 2 de Marzo 2015 Aprueba norma técnica sobre sistemas y sitios web de los órganos de la administración del estado
• Norma NCH 27001:2013.
• Guía Metodológica del Sistema de Seguridad de la Información.

1.6 Periodicidad de evaluación y revisión de la política.

Esta política, tendrá como plazo máximo de evaluación, revisión, actualización e integración de nuevas normativas, a lo menos cada 3 años o cuando existan cambios significativos que afecten su continuidad.

1.7 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, y la publicación en la intranet institucional una vez totalmente tramitada.

2 ROLES Y RESPONSABILIDADES

2.1 Roles Institucionales

2.1.1 Comité de Seguridad

El Comité de Seguridad de la Información del Gobierno Regional, en adelante CSI, que estará conformado por el Encargado de Seguridad quien será su Presidente, y por las personas que desempeñan los roles que a continuación se indican:

- Encargado de Seguridad de la Información (Presidente)
- Jefe Unidad de Informática (Secretario Ejecutivo)
- Jefa Depto. Recursos Humanos;
- Jefa Depto. de Finanzas y Presupuesto;
- Jefe Unidad de Auditoría;
- Jefa Depto. Jurídico;
- Encargada de Riesgos;
- Presidente (a) Comité Paritario;
- Jefe Unidad de Adquisiciones;
- Encargada Unidad de Archivos

El Comité de Seguridad de la Información tendrá un Secretario Ejecutivo, quien llevará un registro de actas de las reuniones periódicas del Comité con su respectivo control de asistencia. El Encargado de Seguridad velará por el mantenimiento actualizado de estos registros.

En los casos en que el Secretario Ejecutivo titular no asistiere a una reunión del Comité lo deberá hacer el suplente, quien efectuará el registro del acta correspondiente con su respectivo control de asistencia de la reunión y posteriormente entregará estos antecedentes al Secretario Ejecutivo titular o en su defecto al Encargado de Seguridad de la Información.

Por cada titular de alguno de los roles que se señalan en el artículo precedente se designará un suplente que lo reemplazará en sus funciones con derecho a voz y voto

para aquellos casos en que el titular se encuentre impedido de participar en alguna reunión del Comité de Seguridad de la Información.

Los suplentes podrán asistir a las reuniones conjuntamente con su respectivo titular pero en este caso, sólo tendrán derecho a voz.

El quórum mínimo de funcionamiento del Comité de Seguridad será de seis de sus integrantes. Sus acuerdos se adoptarán por mayoría de votos, En caso de empate dirimirá el Encargado de Seguridad.

En todo lo demás el Comité de Seguridad acordará su forma de funcionamiento y normas que estime necesarias.

Los funcionarios y funcionarias del Servicio, serán responsables en las tareas propias de su cargo de aplicar las políticas y normas sobre seguridad de la información y de procurar posibilidades mejora en ellas.

El Comité de Seguridad, cuando lo estime necesario, podrá invitar a terceros a sus sesiones, con sólo derecho a voz Además podrá solicitar información a los funcionarios y funcionarias indicados en el punto anterior y que no pertenezcan al Comité.

2.1.2 Responsables del Sistema de Seguridad

Defínanse los responsables del sistema de seguridad de la Información (SSI) y sus roles claves, funciones y atribuciones de la siguiente forma:

Responsabilidad en la Administración de seguridad	**Roles claves**	**Funciones y atribuciones**
Jefe Superior del Servicio	Liderar el proceso	1. Aprobar políticas y validar el proceso de gestión de Seguridad de la Información. 2. Aprobar las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucional, que se generen como resultado de los reportes o propuestas del Comité de Seguridad, así como los recursos necesarios para su ejecución.
Encargado de Seguridad (Presidente CSI)	Presidir y Coordinar las actividades de gestión de seguridad	1. Coordinar actividades para el comité establecido para temas de seguridad de la información. 2. Alinear la debida respuesta y priorización al tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales y sus objetivos de negocio. 3. Monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos. 4. Mantener coordinación con otras unidades del Servicio para apoyar los objetivos de Seguridad. 5. Informar al jefe del Servicio, 6. Dirimir en caso de empate, en los acuerdos.

Comité de Seguridad de información	Gestionar la Política de Seguridad	1. Supervisar la implementación, Procedimientos y estándares que se desprenden de las políticas de seguridad de la información. 2. Proponer estrategias y soluciones específicas para la implantación de los controles necesarios para implementar las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas. 3. Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones. 4. Coordinarse con los Comités de Calidad y de Riesgos de la institución, para mantener alineamiento y estrategias comunes de gestión. 5. Reportar a la dirección, respecto a opciones de mejora en el sistema de gestión de seguridad de la información, así como de los incidentes relevantes y su solución.
Secretario Ejecutivo del CSI (Jefe de la Unidad de Informática)	Coordinación de actividades de gestión segundad Implementación Política de Seguridad Información.	1. Será el responsable del seguimiento y control del PMG Seguridad de la Información. 2. Llevar el registro de actas de las reuniones periódicas del Comité, con su respectivo control de asistencia. 3. Velará por el mantenimiento actualizado de estos registros. 4. Subrogar al presidente del Comité de seguridad en ausencia, con todas sus facultades. 5. Citar a reuniones del Comité y preparar la Tabla de Reuniones. 6. Comunicar a los Funcionarios los acuerdos que tome el Comité de Seguridad de la Información.
Auditoria Interna	Monitoreo y seguimiento	1.- Monitorear el avance de cada una de las etapas de la implementación del Proceso de Gestión de Seguridad de la Información, reportando periódicamente al Jefe Superior del Servicio. 2.- Revisar independientemente la implementación de políticas y controles, a través de mecanismos de control, seguimiento y evaluación.

2.2 Responsable Administrativo del Equipamiento a su Cargo

Responsable de los equipos informáticos que haya instalado en el Servicio y estén a su cargo. Este acto se registra al momento de firmar el acta de recepción del equipamiento entregado. Esto debe ser incorporado dentro del contrato establecido, indicando claramente los roles y responsabilidades que debe cumplir sobre seguridad de la información de los distintos funcionarios y funcionarias que posee el servicio.

2.3 Administrador del Sistema

Responsable de la gestión y administración de los sistemas a su cargo y de supervisar el cumplimiento de la política de uso de los mismos. Será generalmente, el informático a cargo del sistema bajo su responsabilidad.

2.4 Responsable Administrativo de los recursos informáticos del Servicio

Esta responsabilidad recae en el Encargado de la Unidad de Informática.

2.5 Usuarios

Toda aquella persona que utilice los recursos informáticos del Gobierno Regional de Los Lagos sea planta, contrata y honorarios.

2.6 Servicio externos

Responsable externo que realiza trabajos dentro de las distintas oficinas para los cuales han sido contratados, por lo que se deben incorporar dentro de los contratos con terceros las responsabilidades que ellos deben tener.

3 DEFINICIONES

3.1 Activo de la Información

Es todo aquello que una organización considera importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos de usuarios, contraseñas, números de cuentas, etc. Seria critico que intrusos pudieran acceder a una entidad que maneja información confidencial, afectando así la confidencialidad, la disponibilidad y la integridad de dicha información por eso algunas de tantas entidades adoptan un plan de seguridad para los activos de información y así evitar que los datos se fuguen, se modifiquen o se pierdan, sin conocer su destino.

En general es toda la información que la entidad posee dentro de un activo informático tales como servidores, switch, documentación, equipos de comunicaciones, equipos de procesamiento, etc. Es importante destacar la política define los lineamientos necesarios para mantener la seguridad de los activos de información que maneja el servicio.

3.2 Seguridad de los Activos de Información

Es proteger, resguardar y asegurar la disponibilidad, privacidad, confidencialidad e integridad de los activos de información y tecnologías para su procesamiento a efecto de garantizar la continuidad operacional de la institución.

3.3 Medios Físicos

El medio físico es el encargado de transmitir señales electromagnéticas que son interpretadas por el protocolo de enlace de datos como bits. En principio, cualquier medio físico podría ser utilizado, a condición que asegure la transmisión de toda la información sin interferencias. De hecho, las líneas telefónicas, las de televisión por cable y las de energía eléctrica pueden ser utilizadas con ese fin. Sin embargo, en redes locales se utilizan cableados dedicados lo que mejora las velocidades de transmisión. Otra posibilidad es la transmisión a través del aire, en forma de señales de radio, microondas, WIFI, Bluetooth, etc.

3.4 Comercio Electrónico

El comercio electrónico, también conocido como e-commerce (electronic commerce en inglés), consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas. Originalmente el término se aplicaba a la realización de transacciones mediante medios electrónicos tales como el Intercambio electrónico de datos, sin embargo, con el advenimiento de la Internet y la www comenzó a referirse principalmente a la venta de bienes y servicios a través de Internet, usando como forma de pago medios electrónicos, tales como las tarjetas de crédito.

3.5 Conexión segura

Una conexión segura es un intercambio cifrado de información entre el sitio Web que está visitando e Internet Explorer. El cifrado se ofrece mediante un documento proporcionado por el sitio Web que se denomina certificado. Cuando se envía información al sitio Web, se cifra en su equipo y se descifra en el sitio Web. En circunstancias normales, no es posible leer ni alterar la información mientras se envía, pero es posible que alguien encuentre una forma de descifrar esta información.

Aunque la conexión entre el equipo y el sitio Web esté cifrada, esto no garantiza que el sitio Web sea de confianza. Su privacidad aún puede ser puesta en peligro por la forma en la que el sitio Web usa o distribuye la información.

3.6 Transacción o transferencias en Línea

Si bien no existe una garantía de seguridad en Internet, puede minimizar los problemas de seguridad y privacidad en línea usando sitios Web que conoce y en los que confía. El explorador no puede determinar si el propietario de un sitio Web es de confianza. Por lo cual, intente usar sitios que ya haya utilizado previamente o sitios recomendados por el servicio. También debería activar el Filtro de suplantación de identidad (phishing) del explorador para identificar sitios Web fraudulentos. El antivirus usado actualmente por el servicio cuenta con esta funcionalidad.

3.7 Trabajo remoto

Actualmente es frecuente escuchar el término trabajo o conexión remota, donde los usuarios trabajan en lugares diferentes a la oficina, mediante la utilización de las nuevas tecnologías de la comunicación. Esto significa una mayor importancia de la informática y las telecomunicaciones, elevando los mecanismos de seguridad y el mayor cumplimiento de las políticas de seguridad establecidas en cuanto al control de acceso.

3.8 Seguridad perimetral.

Para este caso el Gobierno Regional cuenta con un firewall de hardware el cual monitorea el tráfico y los sitios visitados o que se han querido visitar por parte de los usuarios. Este firewall de hardware cuenta con un sistema de antivirus y antispam.

3.9 Seguridad física de acceso a las dependencias informáticas.

Actualmente se cuenta con una puerta de acceso a las oficinas de la Unidad de Informática y otro acceso independiente que restringe el acceso a la sala de Servidores/Comunicaciones del Gobierno Regional de Los Lagos.

3.10 Seguridad de acceso a Data Center.

El Gobierno Regional de Los Lagos tiene alojados sus Servidores tanto en un Datacenter ubicado en la Unidad Operativa de Control de Tránsito (UOCT), como en el

Datacenter de la empresa Telefónica del Sur (TELSUR-GTD). Los accesos son restringidos solo a los funcionarios de la Unidad de Informática y técnicos de servicios externos pero acompañados por un funcionario de la Unidad de Informática.

Igualmente, se cuenta con una sala de Servidores/Comunicaciones, cuyo acceso es al interior de la Unidad de Informática, que aloja los switch, patch panel, y los servicios de seguridad (respaldo y cámaras de vigilancia).

3.11 Seguridad de Servicio Informáticos.

Los sistemas críticos se encuentran en los servidores del Gobierno Regional. Éstos cuentan con fuentes de poder redundantes y con arreglo de discos en modalidad raid. Y a fin de eliminar la dependencia del hardware casi todos los sistemas funcionan en modalidad de virtualización.

3.12 Seguridad de Clima a Data Center

Ambos datacenter cuentan con equipos de aire acondicionado, estos permiten mantener una temperatura adecuada tanto para los servidores y los equipos de comunicaciones que prestan los servicios.

3.13 Seguridad respecto a la energía eléctrica

Ambos datacenter cuentan con grandes equipos UPS, lo que permite una autonomía en caso de cortes de energía.

3.14 Seguridad a nivel de usuario

Todos los funcionarios y funcionarias del Gobierno Regional de Los Lagos que requieran, podrán tener acceso a los servicios informáticos. Todos los usuarios de la red del Servicio deberán ser autentificados para el acceso a los sistemas institucionales y a los recursos de la red.

A nivel de PC se provee de un antivirus licenciado y que es actualizado contra el sitio corporativo del proveedor una vez al día y chequeo automático de todos los archivos que se manejan en los equipos.

3.15 Seguridad para la navegación a Internet

Todos los funcionarios y funcionarias tienen la posibilidad de utilizar los servicios de Internet, sin embargo, el servicio se entrega con algunas restricciones a páginas que son consideradas como peligrosas para la estabilidad de los servicios informáticos en general, a través de perfiles de usuario administrados por la Unidad de Informática.

Se restringe el acceso a servicios tipo P2P, chat, radios online o TV. Estos bloqueos son para proteger el buen uso del ancho de banda, además de evitar posibles contagios de virus al interior de nuestra red y transferencia de información no autorizada, especialmente a sitios de descarga y subida de información.

4 POLITICA Y PROCEDIMIENTO

4.1 Uso adecuado del equipamiento computacional

El propósito es esbozar un uso aceptable del equipamiento computacional del Gobierno Regional de Los Lagos. Estas reglas se aplican para proteger a los funcionarios y a la Institución en sí, de uso inapropiados que exponen a la Institución a riesgos como ataques de virus, comprometer sistemas y servicios de red y asuntos legales, entre otros.

4.1.1 Uso general y propiedad

1. Mientras la administración de redes del Gobierno Regional de Los Lagos desee proveer un nivel razonable de privacidad, los empleados deben tener en cuenta que los datos creados con los sistemas del servicio, siguen siendo propiedad del servicio. Debido a la necesidad de proteger la red del servicio, la Unidad de Informática no puede garantizar la confidencialidad de la información almacenada en cualquier dispositivo de red perteneciente al Gobierno Regional de Los Lagos.
2. Los empleados son responsables de establecer un buen juicio a la hora de manejar datos personales. Cada departamento o unidad es responsible de la creación de directrices sobre el uso personal de los sistemas relacionados con internet, intranet y extranet. De no existir estas políticas, los empleados deberán guiarse por la política de seguridad de la información, y si existiese alguna duda, deberán consultar a su jefe directo o al Jefe de la Unidad de Informática.
3. La Unidad de Informática recomienda que cualquier información que el empleado considere sensible o vulnerable sea encriptada.
4. Para fines de seguridad y mantenimiento de la red, personas autorizadas por el Gobierno Regional de Los Lagos pueden monitorizar equipamiento, sistemas y tráfico en la red en cualquier momento, todo explicitado en la Política de Seguridad de la Información.
5. El Gobierno Regional de Los Lagos se reserva el derecho para auditar redes y sistemas de forma periódica para asegurar el cumplimiento de esta política.

4.1.2 Seguridad e información privilegiada

1. Las interfaces de usuario para la información contenida en los sistemas relacionados con internet, intranet y extranet, debieran ser clasificados como confidenciales o no confidenciales por cada uno de los jefes de división, departamentos y unidades. Ejemplos de información confidencial incluyen, pero no están limitados a: características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen social, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
2. Mantener contraseñas seguras y no compartir cuentas. Los usuarios autorizados son los responsables de la seguridad de sus contraseñas y cuentas. Contraseñas a nivel de sistema deben ser cambiadas semestralmente, y contraseñas a nivel de usuario anualmente.
3. Todos los computadores personales, computadores portátiles o estaciones de trabajo deben estar protegidos con un protector de pantalla con activación automática de 10 minutos o menos.
4. Usar la encriptación de información de acuerdo con la política de encriptación.
5. Debido a que la información contenida en computadores portátiles es especialmente vulnerable, se debe poner especial atención. Los computadores portátiles deben ser protegidos de acuerdo a la política de seguridad de portátiles.
6. Publicaciones de los empleados en grupos de noticias o similares con una cuenta de correo electrónico del Gobierno Regional de Los Lagos debe contener una exención de responsabilidad afirmando que las opiniones expresadas son estrictamente responsabilidad de quien las emite, y no representan necesariamente el pensar del servicio, a menos que se esté publicando a nombre del servicio algo claramente relacionado con las funciones de la institución.

7. Todos los dispositivos utilizados por algún empleado y que esté alojado en la red del Gobierno Regional de Los Lagos, ya sea propiedad del mismo servicio o del empleado, debe continuamente estar corriendo un programa de escaneo de virus con una base de datos actualizada.
8. Los empleados deben tener extrema precaución cuando abran un archivo adjunto recibido de un recipiente desconocido, el cual puede contener virus, bombas de correo electrónico o códigos troyanos.

4.1.3 Uso inaceptable

Las siguientes actividades están, en general, prohibidas. Los empleados pueden quedar exentos de estas restricciones durante el curso de sus legítimas labores (e.g. los administradores de sistemas pueden verse en la necesidad de desactivar el acceso a la red de una máquina si ésta está interrumpiendo los servicios de producción).

Bajo ninguna circunstancia un empleado está autorizado a participar de una actividad utilizando recursos pertenecientes al Gobierno Regional de Los Lagos. La actividad listada a continuación no corresponde a un listado completo, pero intentan proporcionar un marco para las actividades que entran en la categoría de uso inaceptable.

a) Actividades de sistemas y red

Las siguientes actividades están estrictamente prohibidas, sin excepciones:

1. Violaciones de los derechos de cualquier persona, empresa protegida por derechos de autor, secretos comerciales, patentes u otra propiedad intelectual, leyes o regulaciones similares, incluyendo pero no limitando a: la instalación o distribución de productos "pirateados" o de otros productos de software que no se cuenta con la licencia correspondiente para el uso del Gobierno Regional de Los Lagos.
2. La copia no autorizada de material con *copyright,* incluyendo pero no limitado a: digitalización y distribución de fotografías de revistas, libros o fuentes de derechos de autor, la música con derechos de autor, y la instalación de software sin contar con la licencia correspondiente, está estrictamente prohibido.
3. La venta y exportación de software, información técnica y tecnología de encriptación, en violación a las leyes de control internacional o nacional de exportación, es ilegal. El manejo apropiado debe ser consultado antes de la exportación de cualquier material que este en cuestión.
4. Introducción de programas maliciosos dentro de la red y/o servidor (por ejemplo, virus, gusanos, troyanos, bombas de correo, etc.).
5. Revelar la contraseña de sus cuentas a los demás o permitir el uso de su cuenta a otros. Esto incluye a miembros de su familia y otros cuando se está trabajando en su casa.
6. El uso de un activo de información del Gobierno Regional de Los Lagos para la adquisición o transmisión de material que viole las leyes de acoso sexual o de ambiente de trabajo intimidatorio u hostil.
7. Hacer ofertas fraudulentas de productos, elementos o servicios procedentes de cualquier cuenta del Gobierno Regional de Los Lagos.
8. Hacer declaraciones sobre autorizaciones, explícita o implícitamente, a menos que sea parte de sus labores designadas.
9. Realizar infracciones de seguridad o interrupciones en la comunicación de la red. Las infracciones de seguridad incluyen, pero no se limita a: acceder a los datos de empleados o entrar en un servidor o cuenta de un empleado sin expresa autorización para ello, a menos que estas tareas estén dentro del alcance de los deberes regulares. Para propósitos de esta sección, "interrupción" incluye, pero no se limita a, capturar tráfico en la red, saturar la

red, suplantación de paquetes en la red, denegación de servicio, y falsificar la información de enrutamiento con fines maliciosos.

10. El escaneo de puertos o escaneo de seguridad está expresamente prohibido, salvo bajo autorización previa del Jefe de la Unidad de Informática.
11. Ejecutar cualquier forma de monitorizado de la red que intercepte datos no destinados a la estación de trabajo de un empleado, a menos que esta actividad forme parte del trabajo normal del empleado.
12. Eludir la seguridad o autenticación de un usuario en cualquier computador, red o cuenta.
13. Interferir o negar el servicio a cualquier usuario que no pertenezca al computador del empleado (por ejemplo, ataque de denegación de servicio).
14. El uso de cualquier programa, *script,* comando, o el envío de mensajes de cualquier tipo, con la intención de interferir o deshabilitar una sesión de usuario, a través de cualquier medio, de forma local o vía la internet, intranet o extranet.
15. Proporcionar una lista de empleados del Gobierno Regional de Los Lagos a terceros.

b) Actividades de comunicación y correo electrónico

1. Envío de mensajes de correo electrónico no solicitados, incluyendo el envío de "correo basura" u otro material publicitario a las personas que no han solicitado específicamente dicho material (SPAM).
2. Cualquier forma de acoso a través de correo electrónico, teléfono o públicamente, ya sea a través del lenguaje, frecuencia o tamaño de los mensajes.
3. El uso no autorizado o falsificación de la información del encabezado del correo electrónico.
4. Solicitar direcciones de correo electrónico para otra cuenta de correo que no sea la institucional, con la intención de acosar o recibir y coleccionar respuestas.
5. Crear o reenviar cadenas de correo electrónico, efectuar operaciones fraudulentas como el esquema Ponzi u otros esquemas tipo pirámide.
6. Uso de correos electrónicos no solicitados originados dentro de las redes del Gobierno Regional de Los Lagos a partir de otros proveedores de servicios de internet, intranet o extranet en nombre de (o para hacer publicidad) cualquier servicio hospedado en la institución o conectados a través de la red de la misma.
7. La publicación de mensajes no relacionados con la organización o similares, a un gran número de grupos de noticias de la "red de usuarios".

4.2 Detección y prevención efectiva de virus computacionales

El propósito es establecer requerimientos que deben ser cumplidos por todos los computadores conectados a la red del Gobierno Regional de Los Lagos, para así asegurar la prevención y detección efectiva de virus, así como de malware, que se pueden transmitir a través de los equipos de comunicaciones, portátiles, etc.

Para ello todos los equipos computacionales del Gobierno Regional deben cumplir con los estándares definidos, además del apoyo de software antivirus instalado y programado para ser ejecutado en intervalos regulares. Además, el software antivirus y los patrones de virus deben mantenerse actualizados. Los computadores infectados con un virus deberán ser removidos de la red, hasta que se verifique que están limpios de cualquier virus. Los administradores de la Unidad de Informática son los responsables de crear procedimientos que aseguren que el software antivirus se ejecuta en intervalos regulares, y que los computadores estén libres de virus. Cualquier actividad con la intención de crear o distribuir programas maliciosos dentro

de las redes del Gobierno Regional (entiéndase, virus, gusanos, troyanos, etc) quedan prohibidos, en acuerdo con lo descrito en procedimiento de uso adecuado del equipamiento computacional.

Excepciones: Máquinas con sistema operativo distinto a los basados en productos Microsoft quedan excluidas actualmente.

4.3 Seguridad de computadores portátiles

1. Los Laptop sacados fuera de las instalaciones del Gobierno Regional de Los Lagos están sujetos a riesgos de seguridad especiales: Pueden ser perdidos, robados, o estar expuestos a accesos no autorizados o manipulación por personas que no corresponden. Los laptops que son llevados al extranjero también están en riesgo, por ejemplo, podrían ser confiscados por la policía o por oficiales de aduana.

2. Los laptops que se pierdan significará no sólo la pérdida de la disponibilidad del equipo, sino que también puede conducir a la divulgación de información confidencial. Esta pérdida de confidencialidad, y potencial integridad, es considerada, a menudo, más seria que la pérdida de activos fijos.

3. Cuando grandes cantidades de datos son mantenidos en un solo laptop (o cualquier otro medio de almacenamiento), la evaluación de riesgos debe considerar el impacto de perder toda la información. Se asume que los archivos borrados persisten en el disco duro del portátil.

4. Accesos no autorizados y manipulación de información en un laptop, particularmente si existen repetidas oportunidades para realizarlo.

5. Los Jefes de División son responsables de la gobernabilidad de la información de actividades realizadas por sus departamentos, y esto incluye la confidencialidad, integridad y disponibilidad de la información por parte del Gobierno Regional de Los Lagos.

4.4 Derechos de propiedad intelectual

El Gobierno Regional de Los Lagos promueve la preocupación por los derechos de autor. Este apartado busca promover la concientización de las implicancias comerciales, legales y de seguridad asociadas al intercambio, descargas, comercio electrónico, que se producen en una transferencia de información.

Todos los usuarios de los recursos del Gobierno Regional de Los Lagos deben cumplir con la utilización de instrumentos (software, hardware, material en general) de forma legal. La distribución, replicación, o instalación no autorizada de material protegido por derecho de autor está prohibida. Los usuarios que descarguen software que no esté cubierto por alguna licencia existente puede ser considerado responsable de cualquier reclamo legal, litigio que pueda producirse por el uso ilegal de un software.

4.5 Uso de correo electrónico

Su propósito como parte de esta política es asegurar el uso correcto del sistema de correos electrónicos del Gobierno Regional de Los Lagos e informar a los usuarios acerca de lo que el Gobierno Regional de Los Lagos considera como un uso aceptable, o inaceptable, acerca del sistema de correos electrónicos. El Gobierno Regional de Los

Lagos se reserva el derecho de corregir esta política a su discreción. En caso de correcciones, los usuarios serán informados apropiadamente.

4.5.1 Riesgos legales

Los correos electrónicos son una herramienta de comunicación Institucional, y los usuarios están obligados a utilizar esta herramienta de una forma responsable, efectiva y legal. Aunque por naturaleza, los correos electrónicos parecen ser menos formales que otros medios de comunicación escrita, aplican las mismas leyes. Por lo tanto, es importante que los usuarios estén al tanto de los riesgos legales de los correos electrónicos.

- Si se envía correos electrónicos con cualquier comentario difamatorio, calumnioso, ofensivo, racista u obsceno, la persona y el Gobierno Regional de Los Lagos pueden ser considerados responsables.
- Si la persona reenvía información confidencial, ella y el Gobierno Regional de Los Lagos pueden ser considerados responsables.
- Si la persona reenvía o copia mensajes sin el debido permiso, ella y el Gobierno Regional de Los Lagos pueden ser considerados responsables por infracción a los derechos de autor.
- Si la persona envía un archivo adjunto que contiene virus o malware, ella y el Gobierno Regional de Los Lagos pueden ser considerados responsables.

Siguiendo las directrices de esta política, el usuario de correos electrónicos puede minimizar los riesgos legales involucrados en la utilización de correos electrónicos. Si cualquier usuario no tiene en cuenta las reglas descritas en esta política, el usuario será completamente responsable, y el Gobierno Regional de Los Lagos se desvinculará del usuario en la medida de lo jurídicamente posible.

4.5.2 Requerimientos legales

Las siguientes reglas son requeridas por ley, y deben ser seguidas de forma estricta:

- Está estrictamente prohibido enviar o reenviar correos electrónicos que contengan comentarios difamatorios, calumniosos, ofensivos, racistas u obscenos.
- Si un usuario recibe un correo electrónico de esta naturaleza, deberá notificarlo al supervisor.
- No se debe reenviar un mensaje sin obtener el permiso de quien lo envió por primera vez.
- No se debe enviar correos electrónicos no solicitados.
- No se debe falsificar, o intentar falsificar mensajes de correo electrónico.
- No se debe enviar mensajes de correo electrónico utilizando la cuenta de correo de otra persona.
- No se debe copiar un mensaje o archivo adjunto perteneciente a otro usuario, sin el permiso del original.
- No disfrazar o intentar disfrazar la identidad al momento de enviar un correo electrónico.

4.5.3 Uso personal

El sistema de correo electrónico del Gobierno Regional de Los Lagos está destinado sólo a su uso corporativo, por lo tanto, no está permitido el uso personal de esta casilla. Entiéndase por esto: Envío de mensajes personales, registro en foros externos, entre otras actividades.

4.5.4 Información confidencial

Evitar el envío de información confidencial por correo electrónico. Si se envía, deberá asegurar la información incluyéndola en algún tipo de archivo adjunto y protegiendo con una contraseña. Después, enviar al receptor la ya mencionada contraseña, pero por otro medio de comunicación.

4.5.5 Monitorizado del sistema

No se debe esperar que exista privacidad en cualquier correo electrónico que se almacene, envíe o reciba en los sistemas computacionales de la organización. Los correos electrónicos pueden ser monitorizado sin notificación si el Gobierno Regional de Los Lagos lo considera necesario. Si existe evidencia de que alguien no está siguiendo las directrices expuestas en este conjunto de políticas, el Gobierno Regional de Los Lagos se reserva el derecho de tomar cualquier acción disciplinaria, incluyendo el despido y/o acciones legales.

4.5.6 Cuentas de correo electrónico

Todas las cuentas de correo electrónico mantenidas dentro de los sistemas del Gobierno Regional de Los Lagos son propiedad del Gobierno Regional de Los Lagos. Las contraseñas no serán entregadas a otras personas, y deberán ser cambiadas cada un mes. Las cuentas de correo electrónico no utilizadas por 60 días podrán ser desactivadas.

4.6 Uso de encriptación

El propósito de este procedimiento es proporcionar una guía que limite el uso de la encriptación a algoritmos que hayan sido revisados públicamente, y se ha comprobado que trabajan de forma eficiente, de manera de usar técnicas criptográficas adecuadas para proteger la confidencialidad, la integridad y la autenticidad de la información.

El proceso de cifrado y encriptación del Gobierno Regional de Los Lagos tomará como referencia los módulos criptográficos aprobados por el NIST (National Institute of Standards and Technology, U.S.A.). Cifrados comunes incluyen AES de 256 bits, Triple DES y RSA. Las longitudes de las claves criptográficas simétricas deben ser de al menos 128 bits. Las claves criptográficas asimétricas deberán tener un largo que asegure el mejor rendimiento. El tamaño de las claves del Gobierno Regional de Los Lagos será revisado anualmente como parte de una revisión de seguridad anual, y se actualizará, en la medida en que la tecnología lo permita. La utilización de algoritmos de encriptación propietarios no está permitida para ningún propósito, a menos que sea revisado por expertos calificados, externos al proveedor y aprobado por la Unidad de Informática.

4.6.1 Aplicación

Cualquier empleado que sea encontrado violando este procedimiento como parte de la política general puede ser sometido a medidas disciplinarias, incluyendo la terminación de su contrato.

4.6.2 Uso adecuado de contraseñas

Las contraseñas son un aspecto importante en lo que respecta a seguridad computacional. Una contraseña pobremente escogida puede significar accesos no autorizados y/o aprovechamiento de los recursos del Gobierno Regional de Los

Lagos. Todos los usuarios, incluyendo contratistas y proveedores con acceso a los sistemas del Gobierno Regional de Los Lagos, son responsables de seguir los pasos que se detallan más abajo, para seleccionar y proteger sus contraseñas:

- Todas las contraseñas a nivel de sistema (Por ejemplo: root, administrador de windows, administrador de cuentas y aplicaciones, etc) deben ser cambiadas, a lo menos, trimestralmente.
- Todas las contraseñas a nivel de usuario (mail, web, acceso al computador) deben ser cambiadas, al menos, cada seis meses.
- Las cuentas de usuario que tienen privilegios a nivel de sistema a través de grupos de trabajo, o programas tipo "sudo", deben tener una contraseña única, distinta a las otras cuentas que pueda mantener el usuario.
- Todas las contraseñas a nivel de usuario, o de sistema, deben seguir las directrices descritas donde corresponde.

4.6.3 Directrices generales para la construcción de contraseñas.

Todos los usuarios del Gobierno Regional de Los Lagos deben estar en conocimiento de cómo seleccionar contraseñas seguras. Contraseñas seguras tienen las siguientes características:

- Contienen al menos tres de las siguientes cinco clases de caracteres:
  - ✓ Caracteres en minúscula.
  - ✓ Caracteres en mayúscula.
  - ✓ Números.
  - ✓ Signos de puntuación.
  - ✓ Caracteres especiales (Por ejemplo: 1@#"-$%&/0=A[]{} etc).
  - ✓ Contienen al menos 15 caracteres alfanuméricos.

- Las contraseñas débiles tienen las siguientes características:
  - ✓ La contraseña contiene menos de 15 caracteres.
  - ✓ La contraseña es una palabra encontrada en el diccionario (Español, inglés, etc).
  - ✓ La contraseña es una palabra comúnmente utilizada,

4.6.4 Estándares de protección de contraseñas.

- Siempre utilizar diferentes contraseñas para las cuentas del Gobierno Regional de Los Lagos y las cuentas que no tienen que ver con esta organización (beneficios, cuenta de correo privada, etc.).
- Siempre utilizar distintas contraseñas para distintos accesos al sistema del Gobierno Regional. Por ejemplo, seleccionar una contraseña para la cuenta de correo electrónico, y otra distinta para la autenticación local en el computador de escritorio.
- No compartir las contraseñas del Gobierno Regional de Los Lagos con nadie, incluyendo asistentes administrativos o secretarias. Todas las contraseñas deben ser tratadas como información sensible y confidencial del Gobierno Regional de Los Lagos.
- Las contraseñas nunca deben ser escritas o almacenadas en línea sin encriptación.
- No se debe revelar la contraseña dentro de un email, chat, o algún otro medio electrónico de comunicación.
- No se debe hablar acerca de contraseñas en frente de otras personas.
- No se debe dar pistas acerca de la forma de una contraseña (Por ejemplo, nombre familiar).
- No se debe revelar la contraseña en cuestionarios o formularios de seguridad.
- Siempre negarse a utilizar el "Recordar contraseña" de las aplicaciones (por ejemplo, Gmail, Firefox, Edge, Internet Explorer, etc.).

Si se sospecha que una cuenta o contraseña se encuentra comprometida, reportar el incidente a la Unidad de Informática.

4.6.5 Estándares de desarrollo de aplicaciones.

Los desarrolladores de aplicaciones deben asegurar sus programas, con las siguientes precauciones de seguridad:

- Las aplicaciones deben soportar autenticación de usuarios individuales, no grupales.
- Las aplicaciones no deben almacenar contraseñas en texto plano, o en alguna forma fácilmente reversible.
- Las aplicaciones deben proveer algún tipo de administrador de roles y funciones, de tal manera que un usuario pueda tomar las funciones de otro, sin necesidad de saber su contraseña.
- Las aplicaciones deben soportar autenticación vía LDAP (sólo si aplica).

4.6.6 Utilización de contraseñas y frases para usuarios de acceso remoto.

El acceso remoto a las redes del Gobierno Regional de Los Lagos será controlado utilizando una autenticación vía contraseña, o un sistema de claves pública/privada utilizando una frase secreta y segura.

4.7 Información sensible

La protección de la información electrónica sensible pretende ayudar a los funcionarios a determinar qué información puede ser revelada, así como la sensibilidad relativa de la información que no debe ser revelada fuera del Gobierno Regional de Los Lagos sin la debida autorización.

Las informaciones cubiertas en estas directrices incluyen, pero no se limita a, la información que se almacena o comparte a través de cualquier medio. Esto incluye: la información electrónica, la información en papel, y la información compartida por vía oral o visual (por ejemplo, conferencias telefónicas y de vídeo).

Todos los empleados deben familiarizarse con el manejo y etiquetado de información que siguen a continuación. Cabe señalar que las definiciones de nivel de sensibilidad se han creado como guía y así hacer hincapié en las medidas de sentido común que se puede tomar para proteger la información confidencial.

4.7.1 Clasificación

Toda la información del servicio deberá ser clasificada en dos principales categorías:

- Pública.
- Confidencial.

La información pública es aquella que ha sido declarada para público conocimiento de cualquiera sin necesidad de autorización, y que puede ser distribuida libremente sin perjudicar a la Institución.

La información confidencial contiene toda la otra información. Es un continuo, en el que se entiende que alguna información es más sensible que otro tipo de información, y deben ser protegidos de una manera más segura. Se incluye la información que debe ser protegida muy de cerca, como los sumarios o bases de concursos en su desarrollo, y otra información esencial cuya divulgación en el proceso de desarrollo pudiere causar algún perjuicio para la institución o la honra de una persona. También se incluye información que es menos crítica, tales como

directorios telefónicos, información personal, entre otras, que no requiere de un estricto grado de protección.

Un subconjunto de la información confidencial es la "confidencialidad de terceras partes". Se trata de información confidencial perteneciente o relativa a una empresa u otro organismo público que se ha entregado al Gobierno Regional de Los Lagos con los acuerdos de confidencialidad y otros contratos.

Al personal se les anima a utilizar su criterio de sentido común en la obtención de información confidencial en la medida adecuada. Si un funcionario no está seguro de la sensibilidad de la información, debe contactar a su jefe directo.

4.7.2 Mínima sensibilidad

Información general de la organización, alguna información técnica y personal. Algunas directrices para la calificación de la información en papel o formato electrónico se detallan a continuación:

La calificación es a discreción del propietario o custodio de la información. Si la calificación es deseada, la palabra "confidencial" puede ser escrita sobre un lugar conspicuo o en la información en cuestión. Otros etiquetados que pueden ser utilizados son "propiedad del Gobierno Regional de Los Lagos", o etiquetados a discreción de las diferentes unidades y departamentos.

- Acceso: empleados, contratistas, personas que requieran información.
- Distribución dentro del servicio: correo interno, correo electrónico y métodos de transmisión de archivos electrónicos.
- Distribución fuera del servicio: correo certificado, correo electrónico y métodos de transmisión de archivos electrónicos.
- Distribución electrónica: Sin restricciones.
- Almacenamiento: Ocultar de la vista de personas no autorizadas, borrar pizarras, no dejar a la vista sobre la mesa. Las máquinas debiesen ser administradas siempre pensando en la seguridad. Proteger de pérdidas; información electrónica debería tener controles para un acceso individual donde fuere posible y apropiado.

4.7.3 Mayor sensibilidad

- Acceso: empleados y no empleados con acuerdos firmados de no divulgación.
- Distribución dentro del servicio: correo interno, correo electrónico y métodos de transmisión de archivos electrónicos.
- Distribución fuera del servicio: correo certificado.
- Distribución electrónica: Sin restricciones para receptores autorizados dentro del Gobierno Regional de Los Lagos, pero debería ser encriptado para su envío a receptores externos.
- Almacenamiento: Controles de acceso individual son altamente recomendados para información electrónica.

4.7.4 Máxima sensibilidad

- Acceso: sólo personal autorizado (interno o externo) y con acuerdos de no divulgación firmados.
- Distribución dentro del servicio: Entrega directa, requiere firma; sobres estampados confidenciales; métodos de transmisión de datos electrónicos aprobados.
- Distribución fuera del servicio: correo certificado; entrega directa, requiere firma.
- Distribución electrónica: Sin restricciones para receptores autorizados dentro del Gobierno Regional de Los Lagos, pero altamente recomendado que toda la información sea fuertemente encriptada.

- Almacenamiento: Controles de acceso individual son altamente recomendados para información electrónica. Seguridad física es generalmente usada, y la información debe ser almacenada en computadores físicamente seguros.

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 la Unidad de Informática, que debe verificar, y si es necesario actualizar el documento, por lo menos una vez cada tres años.

Aprobado Por Comité de Seguridad de la Información

GOBIERNO REGIONAL - ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN - Región de Los Lagos

GOBIERNO REGIONAL - COMITÉ DE SEGURIDAD DE LA INFORMACIÓN - Región de Los Lagos

Oscar Alejandro Oyarzo Pérez
Encargado de Seguridad de la Información

27 de noviembre de 2019