GOBIERNO REGIONAL DE LOS LAGOS

Acción de Futuro

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

PROCEDIMIENTO "CONTROL Y RESTRICCIÓN DE INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERACIONALES"

CÓDIGO	**SSI-A.12.05.01** **SSI-A.12.06.02**	**CLASIFICACIÓN INFORMACIÓN**		**Reservada**
			X	**Uso Interno**
				Pública
VERSIÓN	1.0	**FECHA DE LA VERSIÓN**	02-09-2019	
RESPONSABLE	Encargado de la Unidad de Informática.			

Historial de modificaciones

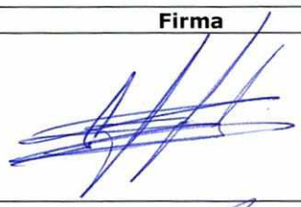
Creación/Modificaciones del Documento

Versión	Fecha de modificación	Autor	Motivo	Páginas modificadas	Firma
1.0	02-09-2019	Eduardo Madrid Osorio, Encargado Unidad de Informática	Creación de la primera versión del procedimiento	Todas	

Revisiones

Versión	Fecha	Autor	Observación	Páginas	Firma
1.0	02-09-2019	Javier Soto Mancilla, Apoyo Profesional Finanzas	Sin observaciones	Todas	

Visto Bueno

Versión	Fecha	Encargado	Firma
1.0	13-09-2019	Oscar Alejandro Oyarzo Pérez, Encargado de Seguridad de la Información	
1.0	13-09-2019	Alejandro Montaña Ampuero, Administrador Regional del Gobierno Regional de Los Lagos	

Distribuciones

Versión	Fecha	Encargado	Observaciones
1.0	06-12-2019	Nicanor Bahamonde Loustau Profesional Unidad de Informática	Enviar por correo electrónico y gestionar la publicación en la Página Web Institucional del Gobierno Regional de Los Lagos.

Contenido

1. Objetivo

Normar y establecer mecanismos de control y restricción en cuando a la instalación de softwares en sistemas operacionales.

De acuerdo al control establecido en la norma chilena ISO 27001:2013

- 12.05.01 Instalación de Software en sistemas operacionales.
- 12.06.02 Restricciones en la instalación de software.

2. Alcance o ámbito de aplicación interno

El presente procedimiento es aplicable a todos los usuarios, ya sean funcionarios(as) planta, contrata, reemplazos y suplencia, prestadores de servicio a honorarios y terceros (proveedores, compra de servicios, etc.) del Gobierno Regional de Los Lagos.

La Política General, Políticas Específicas y sus Procedimientos de la Seguridad de los Activos de la información definen los criterios esenciales, normativos y acciones a seguir en temas relacionados con la seguridad de los Activos de la Información del Gobierno Regional de Los Lagos.

El ámbito de Aplicación y protección de este procedimiento abarca los productos estratégicos: Instrumentos de Planificación y Ordenamiento Territorial; Instrumento de inversión y gasto público en la Región de Atacama e Inversión Pública en la Región de Los Lagos.

3. Roles y Responsabilidades.

Para asegurar la correcta implementación, verificación y control del Procedimiento de Control y Restricción de Instalación de Software, se definen los siguientes roles y responsabilidades

ROLES	RESPONSABILIDADES
Encargado de Seguridad de la Información	• Velar por el cumplimiento del Procedimiento de Control y Restricción de Instalación de Software. • Realizar controles constantes sobre el cumplimiento del Procedimiento de Control y Restricción de Instalación de Software. • Difundir el Procedimiento de Control y Restricción de Instalación de Software a todos los funcionarios del Gobierno Regional de Los Lagos.
Encargado de la Unidad de Informática	• Realizar la Actualización del Procedimiento de Control y Restricción de Instalación de Software cuando se requiera. • Revisión de Solicitudes referentes al Procedimiento de Control y Restricción de Instalación de Software. • Autorización de Solicitudes referentes al Procedimiento de Control y Restricción de Instalación de Software. • Delegación de Solicitudes referentes al Procedimiento de Control y Restricción de Instalación de Software. • La correcta implementación y aplicación del Procedimiento de Control y Restricción de

	Instalación de Software. • Realizar pruebas de funcionalidad sobre sincronización de relojes entre clientes del dominio. • Realizar pruebas de funcionalidad sobre instalación de software en clientes del dominio.
Usuarios Finales	• Conocer el Procedimiento de Control y Restricción de Instalación de software en sistemas operacionales.

4. Procedimiento

a) El Encargado de la Unidad de Informática configura el servidor de dominio con Active Directory para que los usuarios que hagan uso del servicio de dominio tengan limitada su capacidad de instalación de software en el computador que usan para el servicio.

b) El Encargado de la Unidad de Informática configura el servidor de dominio con Active Directory para que limite la capacidad de instalación de software en los computadores del servicio que usan los usuarios.

e) Una vez configurada la política de grupo en el servidor Active Directory, el Responsable de Administración de Sistemas realiza pruebas para verificar la efectividad de la configuración.
Si la configuración es satisfactoria informa al Encargado de Seguridad de la Información, en caso contrario realiza nuevamente las configuraciones.

d) Fin del procedimiento.

4.1. Documentos de referencia

En la siguiente tabla, se presentan los documentos que se han utilizado como referencia, para la formulación del presente manual de procedimientos.

Código	Descripción
SSI-A.05.01.01	Política de Seguridad de la Información
SSI-A.09.01.02	Procedimiento de Accesos a las Redes y a los Servicios de la Red.
NCh-ISO 27001	Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información.
NCh-ISO 27002	Tecnologías de la información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información.

4.2. Diagrama de proceso

Sin diagrama.

4.3. Registros de control del procedimiento.

a) Pantallazo: Active Directory configurado con el Servidor de Dominio.
b) Correo Electrónico, que remite la Unidad de Informática al encargado de Seguridad de la Información, informando la configuración satisfactoria del Active Directory.
c) Pantallazo acceso denegado al Panel de Control del equipo del usuario.

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
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**
13 de Septiembre de 2019